Documentation Data Infrastructure Insights

Data Infrastructure Insights

NetApp
August 20, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/data-infrastructure-insights/index.html on August 20, 2025. Always check docs.netapp.com for the latest.

Sommaire

Documentation Data Infrastructure Insights . . . 1
Avantages de la fonctionnalité Data Infrastructure . . . 1
Mise en route . . . 1
Nouveautés de Data Infrastructure Insights . . . 2
Juin 2025 . . . 2
VM Analyzer : visibilité et dépannage holistiques des machines virtuelles vers le stockage . . . 2
Systèmes d'exploitation pris en charge . . . 2
Mai 2025 . . . 3
Les nouvelles pages de destination vous permettent de rester dans la circulation . . . 3
Amélioration de la sécurité des workloads . . . 3
Exportation asynchrone .CSV . . . 5
Avril 2025 . . . 5
Widgets en ligne d'anomaly alimentés par ML pour une résolution proactive des problèmes . . . 5
Optimisez les coûts VMware avec la prise en charge du stockage VSAN . . . 6
Des détails d'alerte à portée de main . . . 7
Exportation asynchrone pour l'analyse de la sécurité des charges de travail . . . 7
Notifications du Data Collector regroupées en règles . . . 7
Mars 2025 . . . 8
Navigation contextuelle améliorée pour une gestion efficace de l'infrastructure . . . 8
Conserver l'historique des ressources supprimées . . . 8
Mise à niveau par bouton-poussoir de l'opérateur Kubernetes . . . 9
Tester la connectivité pour les collecteurs de données Storage Workload Security . . . 10
Systèmes d'exploitation pris en charge . . . 10
Février 2025 . . . 11
Suivi de l'utilisation de l'API DII : améliorer la sécurité et l'efficacité . . . 11
API de sécurité des charges de travail pour limiter les utilisateurs . . . 12
Janvier 2025 . . . 12
Gérez les risques de manière proactive grâce au regroupement des événements . . . 12
Contrôle d'accès au tableau de bord . . . 13
Décembre 2024 . . . 14
Présentation de SAN Analyzer : meilleure visibilité pour les charges de travail en mode bloc . . . 14
Optimisez les coûts des ordinateurs virtuels grâce à la mise hors service intelligente de l'hôte et à la récupération des ordinateurs virtuels . . . 15
Découvrez les informations de journalisation avec la prise en charge des graphiques de temps et des widgets de tableau . . . 16
Novembre 2024 . . . 17
Nouvelle API d'alertes de sécurité des workloads . . . 17
Analysez les modifications de configuration dans votre environnement . . . 17
Prise en charge de KubeVirt : surveillez les workloads des machines virtuelles s'exécutant dans votre cluster Kubernetes . . . 17
Octobre 2024 . . . 18
Déverrouiller de nouvelles informations avec des expressions personnalisées dans les moniteurs . . . 18
Réduisez les interruptions d'alerte pendant la période de maintenance . . . 18

Rationalisez la gestion des alertes grâce aux nouvelles règles de notification des alertes . . . 19
Analyse des journaux dans les tableaux de bord . . . 20
Meilleure observabilité VMware avec les événements VMware . . . 20
Mises à jour du Data Collector : . . . 21
Septembre 2024 . . . 21
Présentation de Data Infrastructure Insights, anciennement Cloud Insights . . . 21
Août 2024 . . . 21
Afficher les données spécifiques à votre plage horaire . . . 21
Analyse du taux de changement (%) . . . 21
Exporter les résultats de la requête de journal au format .CSV . . . 22
Résolution des alertes par heure . . . 22
Juillet 2024 . . . 23
Fonctionnalités basées sur l'IA : détection des anomalies . . . 23
Amélioration de la sécurité des workloads . . . 23
Navigation facilitée dans le tableau de bord . . . 23
Juin 2024 . . . 24
Systèmes d'exploitation pris en charge . . . 24
Mai 2024 . . . 24
Résolvez automatiquement les alertes en fonction de l'heure . . . 24
Avril 2024 . . . 25
Prise en charge d'iSCSI pour Kubernetes . . . 25
Systèmes d'exploitation pris en charge . . . 26
Mars 2024 . . . 26
Détails de l'agent de sécurité de la charge de travail . . . 26
Tracez plus rapidement davantage de données . . . 26
Février 2024 . . . 27
Facilité d'utilisation améliorée . . . 27
Voir toutes les modifications apportées à votre espace de noms . . . 28
Journaux associés pour les alertes . . . 29
Collecter les données du commutateur ONTAP . . . 29
API Data Collector de Workload Security . . . 29
Janvier 2024 . . . 30
Essayez des fonctionnalités Cloud Insights que vous n'avez pas encore utilisées . . . 30
Mes workloads sont-ils sains ? . . . 30
Mises à jour du Data Collector . . . 30
Algorithme amélioré de détection DES ransomwares par ML . . . 30
Fonctionnalités obsolètes . . . 31
Décembre 2023 . . . 31
Analyse des changements en un coup d'œil . . . 31
Tableau de bord des performances des workloads Kubernetes . . . 32
Détails de la requête sur un écran . . . 33
Mises à jour du Data Collector : . . . 34
Novembre 2023 . . . 34
Sécurité de la charge de travail : interrompre/reprendre un collecteur . . . 34
Informations sur la prise en charge du nœud de stockage . . . 35

Mapper les balises VMware aux annotations Cloud Insights . . . 35
Améliorations de la fiabilité du collecteur CLI Brocade pour le micrologiciel FOS 9.1.1c et supérieur . . . 35
Octobre 2023 . . . 35
Sécurité améliorée des workloads . . . 35
Essais de module . . . 36
Restreindre l'accès aux domaines spécifiés . . . 36
Mises à jour du Data Collector . . . 36
Septembre 2023 . . . 37
Trouvez facilement ce que vous voulez dans les journaux . . . 37
Panneau de détails du journal « flottant » . . . 38
Réduire le menu . . . 39
Améliorations du Data Collector . . . 40
Août 2023 . . . 40
Collecte des journaux Isilon/PowerScale et des données d'analyse avancées . . . 41
Amélioration de la cartographie des charges de travail . . . 41
Ajustement de l'utilisation des unités gérées Kubernetes . . . 41
Modifications du collecteur/de l'acquisition : . . . 42
Menus améliorés . . . 42
Juillet 2023 . . . 44
Afficher les modifications récentes . . . 44
Améliorations pour l'opérateur . . . 44
Insight : récupération du stockage à froid . . . 45
Signature de l'image de l'opérateur . . . 45
Agrégation, mise en forme conditionnelle, etc. Pour les requêtes . . . 45
API pour l'audit . . . 46
Data Collector : économie de Trident . . . 47
Juin 2023 . . . 47
Découvrez votre utilisation . . . 47
La surveillance et le mappage du réseau Kubernetes sont disponibles pour tous . . . 47
Modifications du collecteur/de l'acquisition : . . . 47
Nouveaux tableaux de bord ONTAP Essentials . . . 48
Moniteurs système supplémentaires . . . 48
Mai 2023 . . . 48
Amélioration de l'installation des opérateurs de surveillance Kubernetes . . . 48
Virtualisation du stockage . . . 48
Nouveaux paramètres Webhook . . . 49
Reporting sur les données Kubernetes . . . 49
Moniteurs système ONTAP par défaut activés pour les nouveaux clients . . . 49
Avril 2023 . . . 49
Contrôle des performances et mappage Kubernetes . . . 49
Tableau de bord de sécurité ONTAP Essentials . . . 50
Récupération du stockage à froid ONTAP . . . 51
La notification d'abonnement contrôle également les messages de bannière . . . 52
Le reporting a une nouvelle apparence . . . 52
Moniteurs en pause par défaut . . . 52

Vous recherchez l’onglet mesure API ? 52
Mars 2023 53
Cloud Connection pour ONTAP 9.9+ est obsolète 53
Janvier 2023 53
Nouveaux moniteurs de journaux 53
Exportation .CSV pour tous les widgets de la table du tableau de bord 53
Décembre 2022 53
Découvrez les fonctionnalités de protection par ransomware et d’autres fonctionnalités de sécurité de Cloud Insights lors de l’essai 53
Les workloads Kubernetes ont leur propre page d’accueil 53
Vérifiez vos checksums 54
Amélioration des alertes de journaux 54
11 nouveaux moniteurs ONTAP par défaut couvrant SnapMirror pour la continuité de l’activité 55
Novembre 2022 55
Plus de 40 nouveaux moniteurs de sécurité, de collecte de données et de Cloud volumes ONTAP ! 55
Octobre 2022 55
Détection plus précise et plus efficace des attaques par ransomware avec l’intégration autonome de ONTAP en cas de protection 56
Septembre 2022 56
Moniteurs disponibles en édition de base 56
Tableaux de bord ONTAP Power and StorageGRID 56
Visibilité des seuils d’un seul coup d’œil dans les tableaux 56
Moniteur de sécurité 57
Discutez où vous voulez 57
Informations plus visibles 57
Nouveaux collecteurs de données 57
Autres mises à jour du Data Collector 57
Systèmes d’exploitation pris en charge 57
Août 2022 58
Le nouveau look de Cloud Insights ! 58
Vous ne savez pas par où commencer ? Découvrez ONTAP Essentials ! 58
Les familles de données de stockage sont fusionnées 59
Quelle est la puissance de mon stockage ? 60
Fonctions avec un dégradé de l’aperçu 61
Comment ma collecte de données est-elle en bonne santé ? 61
Tokens de l’API de renouvellement automatique 61
Basic Edition vous donne plus qu’avant 62
Vous souhaitez en savoir plus dès maintenant ? 62
Systèmes d’exploitation pris en charge 62
Juin 2022 62
La saturation du cluster Kubernetes et d’autres détails 62
Quel est l’âge de votre cluster Kubernetes ? 63
Prévision du délai avant utilisation de la capacité 63
Qu’est-ce qui a changé dans mon environnement ? 64
Systèmes d’exploitation pris en charge 64

Agent Telegraf mis à jour . . . 64
Aperçu des fonctions . . . 65
Mai 2022 . . . 65
Discutez en direct avec le support NetApp . . . 65
Opérateur Kubernetes . . . 65
Gestion des utilisateurs et des invitations à l'aide d'une API . . . 66
Alertes de collecte de données . . . 66
Alertes sur les modifications du stockage ONTAP . . . 66
Aperçu des fonctions . . . 66
Avril 2022 . . . 67
Faites-nous part de vos commentaires ! . . . 67
Editeur de tableau de bord mis à jour . . . 67
Amélioration de la surveillance de votre infrastructure Kubernetes . . . 68
Aperçu des fonctions . . . 68
Nouveau Data Collector . . . 69
Autres mises à jour du Data Collector . . . 69
Mars 2022 . . . 69
Connexion cloud pour ONTAP 9.9+ . . . 69
Nouveau FSX pour moniteurs ONTAP NetApp . . . 69
Nouvelles fonctionnalités de Cloud Secure disponibles à tous . . . 70
Agent Telegraf mis à jour . . . 70
Mises à jour du Data Collector . . . 70
Février 2022 . . . 70
Cloud Insights corrige les vulnérabilités Apache Log4j . . . 70
Page de détails de l'espace de noms Kubernetes . . . 71
Décembre 2021 . . . 71
Intégration plus étroite pour les systèmes ONTAP . . . 72
Interrogation des journaux . . . 72
Notifications au niveau du Data Collector. . . . 72
Une plus grande flexibilité des rôles Cloud Secure . . . 72
Systèmes d'exploitation pris en charge . . . 73
Mises à jour du Data Collector . . . 73
Novembre 2021 . . . 73
Tableaux de bord adaptatifs . . . 73
Accéder à la base de données de rapports via l'API . . . 74
Tableaux POD sur la page d'accueil de VM . . . 74
Mises à jour du Data Collector . . . 74
D'autres systèmes d'exploitation sont pris en charge . . . 75
Octobre 2021 . . . 75
Filtres sur les pages de l'Explorateur K8S . . . 75
Données K8s pour la création de rapports . . . 75
Le thème sombre est arrivé . . . 76
Prise en charge du Data Collector . . . 76
Septembre 2021 . . . 76
Les règles de performance sont désormais des moniteurs . . . 76

Suggestions complètes, caractères génériques et expressions dans moniteurs . . . 77
Agent Telegraf mis à jour . . . 77
Prise en charge du Data Collector . . . 77
Août 2021 . . . 78
Nouvelle interface utilisateur de la page d'audit . . . 78
Gestion améliorée des rôles utilisateur . . . 78
Juin 2021 . . . 78
Suggestions, caractères génériques et expressions dans filtres . . . 78
API disponibles par édition . . . 79
Visibilité sur les volumes persistants et pod pour Kubernetes . . . 79
Liens entre un nœud Kubernetes et une machine virtuelle . . . 79
Moniteurs d'alertes remplacement des règles de performance . . . 80
Cloud Secure prend en charge NFS . . . 81
Suppression du snapshot Cloud Secure . . . 81
Vitesse de collecte des données Cloud Secure . . . 81
Mai 2021 . . . 81
Agent Telegraf mis à jour . . . 81
Ajouter des actions correctives à une alerte . . . 82
API Cloud Insights pour toutes les éditions . . . 82
Avril 2021 . . . 82
Gestion simplifiée des moniteurs . . . 83
Options d'alerte améliorées à l'aide de Webpatères . . . 83
Identification améliorée des périphériques . . . 83
Vous en avez demandé plus ! . . . 84
Plusieurs abonnements dans un environnement Cloud Insights . . . 84
Choisissez votre voie . . . 84
Intégration Cloud Secure plus simple . . . 84
Février 2021 . . . 85
Agent Telegraf mis à jour . . . 85
Analyseur de coût du cloud . . . 85
Recherche d'objets ayant des valeurs nulles à l'aide de filtres . . . 86
Prise en charge multi-région . . . 86
Janvier 2021 . . . 86
Mesures ONTAP supplémentaires renommées . . . 86
Nouveau Kubernetes Explorer . . . 88
Décembre 2020 . . . 89
Installation Kubernetes simplifiée . . . 89
Novembre 2020 . . . 89
Tableaux de bord supplémentaires . . . 89
Colonne Renommer dans les widgets du tableau . . . 89
Octobre 2020 . . . 90
Extension par défaut des données d'intégration . . . 90
Assistance technique Edition de base . . . 90
API publique Cloud Secure . . . 90
Septembre 2020 . . . 90

Page de requête avec données d'intégration . . . 90
Formatage de l'affichage de l'unité dans le widget de tableau . . . 91
Page de détails de l'unité d'acquisition . . . 91
Dépendance vis-à-vis de Cloud Secure Docker supprimée . . . 91
Génération de rapports des rôles utilisateur . . . 91
Nouvelle catégorie d'API pour l'acquisition de données . . . 92
Août 2020 . . . 92
Surveillance et alertes . . . 92
Juillet 2020 . . . 93
Cloud Secure *prendre une action instantané* . . . 93
Mises à jour des mesures/compteurs . . . 94
Détection des attaques potentielles au Cloud Secure . . . 95
Abonnez-vous à Premium Edition via AWS . . . 96
Widget Table amélioré . . . 96
Filtrage de metrics . . . 97
Données de compteur avancées ONTAP . . . 98
Tableaux de bord avancés . . . 100
En savoir plus . . . 100
Menu stratégies et violations . . . 100
Agent Telegraf mis à jour . . . 100
Juin 2020 . . . 101
Rapport d'erreurs du Data Collector simplifié . . . 101
Améliorations des widgets . . . 101
Mai 2020 . . . 102
Génération de rapports des rôles utilisateur . . . 102
Mises à jour Cloud Secure . . . 103
Regroupement du tableau de bord . . . 103
Épinglage du tableau de bord . . . 104
Mode TV et actualisation automatique . . . 104
Avril 2020 . . . 105
Nouveaux choix de plage de temps du tableau de bord . . . 105
Mises à jour Cloud Secure . . . 105
Heure par défaut du tableau de bord . . . 105
Optimisation des temps d'agrégation . . . 105
Format automatique de l'unité d'affichage . . . 105
Importer des annotations à l'aide de l'API . . . 106
Sélecteur de widget simplifié . . . 106
Février 2020 . . . 107
API avec édition Premium . . . 107
Interrogation initiale après ajout D'Un Data Collector . . . 107
Duplication simplifiée des widgets . . . 108
Authentification unique (SSO) . . . 108
Janvier 2020 . . . 108
Documentation swagger pour l'API REST . . . 109
Barre de progression Tutoriels de fonctionnalités . . . 109

Modifications de l’unité d’acquisition . . . 109
Agrégation de temps optimisée dans les widgets . . . 109
Processus simplifié « mise en route avec Cloud Insights » . . . 109
Décembre 2019 . . . 110
L’entité métier peut être utilisée dans les filtres . . . 110
Informations détaillées disponibles pour les widgets à valeur unique et jauge, ainsi que pour tous les widgets ajoutés par « tous » . . . 110
Période d’essai prolongée . . . 110
Calcul de l’unité gérée . . . 110
Novembre 2019 . . . 110
Octobre 2019 . . . 111
Création de rapports . . . 111
Améliorations apportées à Active IQ . . . 111
Septembre 2019 . . . 111
Nouveaux widgets Gauge . . . 111
Formatage conditionnel des couleurs pour le widget valeur unique . . . 112
Inviter des utilisateurs pendant l’intégration . . . 112
Amélioration de la page de détails du Data Collector . . . 112
Août 2019 . . . 113
Tous vs. Collecteurs de données disponibles . . . 113
Intégration d’ActiveIQ . . . 113
Juillet 2019 . . . 113
Améliorations tableau de bord . . . 113
Rétrograder à l’édition de base . . . 113
Collecte des mesures Kube-State . . . 113
Juin 2019 . . . 114
Éditions Cloud Insights . . . 114
Nouveau collecteur de données d’infrastructure : NetApp HCI . . . 114
Mai 2019 . . . 114
Nouveau collecteur de données de service : Kapacitor . . . 114
Intégration aux services via Telegraf . . . 114
Actifs Storage Virtual machine . . . 114
Exigences du système de l’unité d’acquisition réduites . . . 114
Autres plateformes prises en charge . . . 115
Avril 2019 . . . 115
Filtrer les machines virtuelles par balises . . . 115
Mars 2019 . . . 115
Notifications par e-mail pour les événements liés à un abonnement . . . 115
Tableaux de bord supplémentaires . . . 115
Février 2019 . . . 116
Collecte depuis les comptes enfants AWS . . . 116
Dénomination du Data Collector . . . 116
Unité d’acquisition pour Windows . . . 116
Janvier 2019 . . . 116
Le champ « propriétaire » est plus lisible . . . 116

Répartition de l'unité gérée sur la page d'abonnement . . . 116
Décembre 2018 . . . 116
Amélioration du temps de chargement de l'interface utilisateur . . . 116
Edition groupée de collecteurs de données . . . 116
Des pages d'assistance et d'abonnement sont disponibles pendant l'intégration . . . 117
Novembre 2018 . . . 117
Abonnez-vous via les équipes commerciales NetApp ou AWS Marketplace . . . 117
Liens hypertexte d'annotations de texte . . . 117
Présentation de l'intégration . . . 117
Importer des tableaux de bord à partir de la Galerie . . . 117
Duplication des tableaux de bord . . . 117
Menu des produits Cloud Central . . . 117
Intégration de données exploitables de l'infrastructure de données . . . 118
Création de votre compte NetApp BlueXP . . . 118
Que se passe-t-il si je dispose déjà d'un identifiant de connexion NetApp BlueXP ? . . . 118
Commencez l'essai gratuit de Data Infrastructure Insights . . . 118
Connectez-vous et allez . . . 119
Déconnexion . . . 119
Délai d'inactivité . . . 119
Sécurité . . . 121
Sécurité des informations exploitables de l'infrastructure de données . . . 121
Présentation de la sécurité . . . 121
Information et région . . . 123
Quelles sont les informations stockées par Data Infrastructure Insights ? . . . 123
Où mes informations sont-elles stockées ? . . . 124
Plus d'informations . . . 125
Outil SecurityAdmin . . . 125
Mise à niveau et installation . . . 126
Gestion de la sécurité sur l'unité d'acquisition . . . 126
Avant de commencer . . . 126
Utilisation de l'outil SecurityAdmin . . . 126
Spécification d'un utilisateur pour exécuter l'outil . . . 128
Mise à jour ou suppression du proxy . . . 129
Récupération de clé externe . . . 131
Cryptage d'un mot de passe à utiliser dans l'API . . . 131
Mise en route . . . 135
Tutoriels de fonctionnalités . . . 135
Liste de contrôle et didacticiels vidéo . . . 135
Collecte des données . . . 136
Début de la collecte des données . . . 136
Exigences relatives à l'unité d'acquisition . . . 139
Configuration des unités d'acquisition . . . 141
Configuration d'un agent pour collecter des données (Windows/Linux) . . . 148
Configuration des collecteurs de données . . . 161
Détermination de l'état d'acquisition du collecteur de données . . . 161

Gestion des collecteurs de données configurés . . . 162
Recherche d'un collecteur de données défectueux . . . 164
Importation à partir de la galerie de tableaux de bord . . . 164
Comptes utilisateur et rôles . . . 165
Niveaux d'autorisation . . . 165
Créer des comptes en invitant des utilisateurs . . . 168
Modification du rôle d'un utilisateur existant . . . 170
Suppression d'utilisateurs . . . 171
Authentification unique (SSO) et fédération des identités . . . 171
Restriction de l'accès par domaine . . . 174
Liste Data Collector de Data Infrastructure Insights . . . 176
Abonnement à Data Infrastructure Insights . . . 180
Version d'essai . . . 180
Essai via AWS Marketplace . . . 181
Que se passe-t-il si mon essai a expiré ? . . . 181
Que se passe-t-il si mon **abonnement** a expiré ? . . . 181
Évaluation du module . . . 181
Estimateur . . . 182
Options d'abonnement . . . 183
Mesure de l'observabilité . . . 183
Mesure de la sécurité des charges de travail . . . 184
Comment s'inscrire ? . . . 184
Abonnez-vous via NetApp Sales Direct . . . 184
Vous pouvez vous inscrire via AWS Marketplace . . . 185
Afficher l'état de votre abonnement . . . 185
Affichez votre gestion de l'utilisation . . . 186
Que se passe-t-il si je dépasse mon utilisation souscrite ? . . . 187
Inscrivez-vous directement et ignorez l'essai . . . 187
Ajout d'un ID de droit . . . 187
Observabilité . . . 189
Création de tableaux de bord . . . 189
Présentation des tableaux de bord . . . 189
Fonctionnalités du tableau de bord . . . 193
Exemple de tableaux de bord . . . 226
Meilleures pratiques pour les tableaux de bord et les widgets . . . 232
Utilisation des requêtes . . . 235
Ressources utilisées dans les requêtes . . . 235
Création de requêtes . . . 237
Affichage des requêtes . . . 244
Exportation des résultats de la requête dans un fichier .CSV . . . 244
Modification ou suppression d'une requête . . . 246
Attribution ou suppression de plusieurs applications à des ressources ou à des applications multiples 247
Copie des valeurs de table . . . 248
Explorateur de journaux . . . 248
Identification des périphériques inactifs . . . 254

Visibilité . . . 255
Visibilité . . . 255
Perspectives : partage de ressources sous stress . . . 255
Indications : espaces de noms Kubernetes manque d'espace . . . 258
Informations : récupération du stockage à froid ONTAP . . . 259
Surveille et alerte . . . 262
Alertes avec les moniteurs . . . 262
Affichage et gestion des alertes à partir des moniteurs . . . 272
Configuration des notifications par e-mail . . . 275
Moniteurs de détection d'anomalies . . . 278
Moniteurs système . . . 282
Configuration des notifications par e-mail . . . 365
Notifications de Webhook . . . 368
Utilisation des annotations . . . 382
Définition des annotations . . . 382
Utilisation d'annotations . . . 385
Création de règles d'annotation . . . 387
Importation d'annotations . . . 389
Utilisation des applications . . . 391
Suivi de l'utilisation des ressources par application . . . 391
Création d'applications . . . 392
Résolution automatique des périphériques . . . 393
Présentation de la résolution automatique des périphériques . . . 393
Règles de résolution du périphérique . . . 396
Résolution de périphérique Fibre Channel . . . 398
Résolution du périphérique IP . . . 401
Configuration des options dans l'onglet Préférences . . . 403
Exemples d'expression régulière . . . 404
Informations sur la page de ressources . . . 410
Présentation de la page de ressources . . . 410
Filtrage des objets dans le contexte . . . 417
Virtualisation du stockage . . . 418
Conseils et astuces pour rechercher des ressources et des alertes . . . 420
Analyse des données . . . 422
Présentation de SAN Analyzer . . . 422
Présentation de VM Analyzer . . . 425
Surveiller la santé de l'infrastructure . . . 427
Création de rapports . . . 429
Présentation des rapports sur les informations d'infrastructure de données . . . 429
Rôles utilisateur du reporting Data Infrastructure Insights . . . 430
Les rapports prédéfinis sont faciles à réaliser . . . 432
Tableau de bord de Storage Manager . . . 436
Création d'un rapport (exemple) . . . 439
Gestion des rapports . . . 442
Création de rapports personnalisés . . . 445

Accéder à la base de données de rapports via l'API . . . 453
Conservation des données historiques pour les rapports . . . 457
Diagrammes de schéma de reporting des informations d'infrastructure de données . . . 458
Schémas d'informations d'infrastructure de données pour le reporting . . . 510
Kubernetes . . . 512
Présentation du cluster Kubernetes . . . 512
Raffinage du filtre . . . 512
Avant d'installer ou de mettre à niveau l'opérateur de surveillance NetApp Kubernetes . . . 513
Points importants à noter avant de commencer . . . 514
Installation et configuration de l'opérateur de contrôle Kubernetes . . . 517
Avant d'installer l'opérateur de surveillance Kubernetes . . . 517
Installation de l'opérateur de surveillance Kubernetes . . . 518
Composants de surveillance Kubernetes . . . 520
Mise à niveau vers le dernier opérateur de surveillance Kubernetes . . . 521
Arrêt et démarrage de l'opérateur de surveillance Kubernetes . . . 522
Désinstallation . . . 522
À propos des indicateurs Kube-State . . . 523
Configuration/personnalisation de l'opérateur . . . 524
Remarque sur les secrets . . . 527
Vérification des signatures d'images de l'opérateur de surveillance Kubernetes . . . 528
Dépannage . . . 529
Options de configuration de l'opérateur de surveillance Kubernetes . . . 537
Exemple de fichier AgentConfiguration . . . 541
Page des détails du cluster Kubernetes . . . 550
L'espace de noms, les nœuds et le Pod . . . 551
Ressources partagées et saturation . . . 551
Espaces de noms . . . 551
Charges de travail . . . 552
Le groupe d'instruments « roue » . . . 552
Une note sur les jauges . . . 555
Surveillance et mappage des performances du réseau Kubernetes . . . 555
Conditions préalables . . . 556
Moniteurs . . . 557
La carte . . . 557
Détails de la charge de travail et alertes . . . 559
Recherche et filtrage . . . 559
Étiquettes de charge de travail . . . 560
Plongez au cœur de l'aventure . . . 561
Analyse des changements Kubernetes . . . 563
Filtrage . . . 564
Statut rapide . . . 565
Panneau de détails . . . 566
ONTAP Essentials . . . 568
Présentation . . . 568
Protection des données . . . 569

Sécurité . . . 570
Alertes . . . 574
Infrastructures . . . 575
Mise en réseau . . . 576
Charges de travail . . . 576
Administration et autres tâches . . . 578
API Data Infrastructure Insights . . . 578
Conditions requises pour l'accès aux API . . . 578
Documentation API (swagger) . . . 578
Jetons d'accès à l'API . . . 579
Type API . . . 580
Traversée des stocks . . . 581
Se développe . . . 581
Données de performance . . . 583
Mesures de performances de l'objet . . . 585
Données d'historique des performances . . . 585
Objets avec attributs de capacité . . . 586
Utilisation de la fonction Rechercher pour rechercher des objets . . . 587
Désactivation ou révocation d'un token API . . . 587
Rotation des tokens d'accès API expirés . . . 588
Contrôle de votre environnement . . . 589
Audit . . . 589
Conseiller digital Active IQ . . . 592
Sécurité des workloads . . . 595
À propos de la sécurité des charges de travail du stockage . . . 595
Visibilité . . . 595
La protection . . . 595
La conformité . . . 595
Mise en route . . . 595
Mise en route de la sécurité des charges de travail . . . 595
Exigences de l'agent de sécurité de la charge de travail . . . 596
Installation de l'agent de sécurité de charge de travail . . . 600
Suppression d'un agent de sécurité de charge de travail . . . 607
Configuration d'un collecteur d'annuaire d'utilisateurs Active Directory (AD) . . . 608
Configuration d'un collecteur de serveur d'annuaire LDAP . . . 614
Configuration du SVM Data Collector de ONTAP . . . 619
Dépannage du Data Collector SVM ONTAP . . . 629
Configuration de Cloud Volumes ONTAP et d'Amazon FSX pour NetApp ONTAP Collector . . . 637
Gestion des utilisateurs . . . 639
Vérificateur de taux d'événements SVM (Guide de dimensionnement des agents) . . . 640
Alertes . . . 644
Alerte . . . 644
Options de filtre . . . 645
La page Détails de l'alerte . . . 646
Prendre une action instantané . . . 647

Notifications d’alerte . . . 648
Stratégie de conservation . . . 648
Dépannage . . . 649
Médecine légale . . . 649
Analyse - toute l’activité . . . 649
Vue d’ensemble de l’utilisateur judiciaire . . . 660
Stratégies de réponse automatisées . . . 661
Stratégies de types de fichiers autorisées . . . 663
Intégration avec la protection ONTAP autonome contre les ransomwares . . . 664
Prérequis . . . 665
Autorisations utilisateur requises . . . 665
Alerte exemple . . . 665
Limites . . . 667
Dépannage . . . 667
Intégration avec l’accès ONTAP refusée . . . 667
Prérequis . . . 667
Autorisations utilisateur requises . . . 668
Événements d’accès refusé . . . 668
Blocage de l’accès utilisateur . . . 669
Conditions préalables au blocage de l’accès utilisateur . . . 669
Comment activer la fonction ? . . . 670
Comment configurer le blocage automatique des accès utilisateur ? . . . 670
Comment savoir s’il y a des utilisateurs bloqués dans le système ? . . . 670
Limitez et gérez l’accès des utilisateurs manuellement . . . 670
Historique des limitations d’accès utilisateur . . . 671
Comment désactiver cette fonction ? . . . 671
Restaurez manuellement les adresses IP pour NFS . . . 671
Restaurez manuellement les utilisateurs pour SMB . . . 672
Dépannage . . . 673
Sécurité des charges de travail : simulation d’une attaque . . . 674
À noter avant de commencer . . . 674
Lignes directrices : . . . 675
Étapes : . . . 675
Générez les fichiers d’exemple par programmation : . . . 676
Reprendre le collectionneur . . . 677
Générez les fichiers d’exemple par programmation : . . . 677
Générer une alerte dans Workload Security . . . 678
Déclenchement de l’alerte plusieurs fois . . . 679
Configuration des notifications par e-mail pour les alertes, les avertissements et l’état de santé du collecteur d’agents/de sources de données . . . 679
Alertes et avertissements d’attaque potentielle . . . 679
Surveillance de l’état de santé des agents et des Data Collector . . . 679
Réception de notifications de mise à niveau d’agent et de Data Collector . . . 680
Dépannage . . . 680
Notifications de Webhook . . . 680

Notifications de sécurité des workloads à l'aide de webhooks . . . 680
Exemple de Webhook de sécurité des charges de travail pour la discorde . . . 686
Exemple de Webhook pour PagerDuty . . . 689
Exemple de Webhook pour Slack pour Workload Security . . . 694
Exemple de Webhook de sécurité des charges de travail pour les équipes Microsoft . . . 698
API de sécurité du workload . . . 701
Documentation API (swagger) . . . 702
Jetons d'accès à l'API . . . 702
Script pour extraire les données via l'API . . . 703
Dépannage du Data Collector SVM ONTAP . . . 703
Dépannage . . . 712
Résolution des problèmes liés à l'analyse générale de l'infrastructure de données . . . 712
Problèmes de connexion . . . 712
Autres questions . . . 713
Ressources . . . 713
Dépannage des problèmes d'unité d'acquisition sous Linux . . . 714
Considérations sur Proxies et pare-feu . . . 716
Ressources . . . 717
Dépannage des problèmes d'unité d'acquisition sous Windows . . . 717
Considérations sur Proxies et pare-feu . . . 719
Ressources . . . 720
Recherche d'un collecteur de données défectueux . . . 720
Matrice de prise en charge du Data Collector Data Infrastructure Insights . . . 722
HP Enterprise 3PAR / Alletra 9000 / stockage Primera StoreServ . . . 722
Amazon AWS EC2 . . . 739
Amazon AWS S3 . . . 745
Microsoft Azure NetApp Files . . . 749
Commutateurs Fibre Channel Brocade . . . 758
Brocade Network Advisor HTTP . . . 769
Brocade FOS REST . . . 773
Commutateurs de structure Cisco MDS & Nexus . . . 783
Cohesity . . . 791
EMC Celerra (SSH) . . . 798
EMC CLARiiON (NaviCLI) . . . 807
EMC Data Domain (SSH) . . . 820
EMC ECS . . . 829
Dell EMC Isilon et PowerScale Rest . . . 838
Dell EMC Isilon / PowerScale (CLI) . . . 857
EMC PowerStore REST . . . 873
EMC RecoverPoint (HTTP) . . . 889
EMC ScaleIO et POWERFLEX REST . . . 892
CLI EMC Symmetrix . . . 898
REST Dell Unisphere . . . 916
EMC VNX (SSH) . . . 933
EMC VNXe & Unity Unisphere (interface de ligne de commande) . . . 952

EMC VPLEX . . . 966
EMC XtremIO (HTTP) . . . 975
NetApp E-Series . . . 989
Pure Storage FlashBlade REST . . . 1002
Google Cloud Compute . . . 1013
HDS HCP (HTTPS) . . . 1018
HiCommand Device Manager . . . 1023
Hitachi Ops Center . . . 1037
HDS HNAS (INTERFACE DE LIGNE DE COMMANDE) . . . 1053
HPE Nimble / Alletra 6000 Storage . . . 1062
Huawei OceanStor (REST/HTTPS) . . . 1075
IBM Cleversafe . . . 1094
IBM DS 8K (DSCLI) . . . 1099
IBM PowerVM (SSH) . . . 1110
IBM SVC (CLI) . . . 1113
IBM XIV ET A9000 (XIVCLI) . . . 1128
Infinidat Box (HTTP) . . . 1137
Ressources de calcul Microsoft Azure . . . 1146
Microsoft Hyper-V . . . 1152
Mode NetApp 7 . . . 1162
NetApp E-Series REST . . . 1186
Amazon FSX pour NetApp ONTAP . . . 1195
NetApp clustered Data ONTAP versions 8.1 et supérieures . . . 1218
ASA . . . 1257
NetApp ONTAP REST . . . 1271
NetApp SolidFire 8.1+ . . . 1292
NetApp StorageGRID (HTTPS) . . . 1309
Nutanix Storage (REST) . . . 1319
Oracle ZFS (HTTPS) . . . 1333
Pure Storage FlashArray (HTTP) . . . 1347
Red Hat RHV (REST) . . . 1359
Stockage Rubrik . . . 1365
VASTE stock de données . . . 1375
Centre virtuel NetApp HCI . . . 1386
VMware Cloud sur AWS . . . 1397
VMware vSphere (services Web) . . . 1404
Référence et support . . . 1419
Demande d’aide . . . 1419
Activation des droits de support . . . 1419
Obtention d’informations de support . . . 1422
Matrice de prise en charge du Data Collector Data Infrastructure Insights . . . 1424
Data Collector Reference - Infrastructure . . . 1424
Référence spécifique au fournisseur . . . 1424
Configuration du collecteur de données Amazon EC2 . . . 1424
Amazon FSX pour le collecteur de données NetApp ONTAP . . . 1428

Configuration du collecteur de données de calcul Azure . . . 1430
Broadcom . . . 1432
Collecteur de données des commutateurs Cisco MDS Fabric . . . 1440
Le collecteur de données SmartFiles de Cohesity . . . 1443
Dell . . . 1444
Dell EMC . . . 1444
Collecteur de données ETERNUS de Fujitsu . . . 1471
Collecteur de données NetApp Google Compute . . . 1472
Collecteur de données Google Cloud NetApp Volumes . . . 1474
HP Enterprise . . . 1475
Hitachi Data Systems . . . 1483
Collecteur de données Infinidat Box d'Infinidat . . . 1491
Collecteur de données Huawei OceanStor . . . 1493
IBM . . . 1494
Collecteur de données Lenovo . . . 1503
Microsoft . . . 1504
NetApp . . . 1507
Collecteur de données Nutanix NX . . . 1536
Collecteur de données Oracle ZFS Storage Appliance . . . 1538
Collecteur de données FlashArray de Pure Storage . . . 1540
Collecteur de données Red Hat Virtualization . . . 1541
Data Collector Rubrik CDM . . . 1542
Configuration du collecteur de données VMware vSphere . . . 1544
Data Collector Reference - Services . . . 1547
Collecte des données de nœud . . . 1547
Data Collector ActiveMQ . . . 1550
Collecteur de données Apache . . . 1552
Collecteur de données consul . . . 1555
Collecteur de données Couchbase . . . 1556
Collecteur de données CouchDB . . . 1558
Collecteur de données Docker . . . 1560
Collecteur de données Elasticsearch . . . 1568
Collecteur de données Flink . . . 1570
Collecteur de données Hadoop . . . 1577
Collecteur de données HAProxy . . . 1582
Collecteur de données JVM . . . 1588
Collecteur de données Kafka . . . 1593
Collecteur de données Kibana . . . 1596
Installation et configuration de l'opérateur de contrôle Kubernetes . . . 1598
Collecteur de données Memcached . . . 1617
Collecteur de données MongoDB . . . 1620
Collecteur de données MySQL . . . 1622
Collecteur de données netstat . . . 1627
Collecteur de données Nginx . . . 1628
Collecteur de données PostgreSQL . . . 1631

Collecteur de données Puppet Agent . . . 1633
Redis Data Collector . . . 1635
Référence de l’icône d’objet . . . 1637
Icônes d’infrastructure : . . . 1637
Icônes Kubernetes : . . . 1637
Contrôle des performances du réseau Kubernetes et icônes de carte : . . . 1638
Mentions légales . . . 1639
Droits d’auteur . . . 1639
Marques déposées . . . 1639
Brevets . . . 1639
Politique de confidentialité . . . 1639

Documentation Data Infrastructure Insights

NetApp Data Infrastructure Insights (anciennement Cloud Insights) est un outil de surveillance de l'infrastructure cloud qui permet de bénéficier d'une grande visibilité sur l'ensemble de votre infrastructure. Avec Data Infrastructure Insights, vous pouvez surveiller et optimiser toutes les ressources et résoudre les problèmes, y compris dans les clouds publics et dans vos data centers privés.

Avantages de la fonctionnalité Data Infrastructure

Les informations sur l'infrastructure de données fournissent une surveillance multicloud hybride, ce qui assure l'observabilité intégrale de l'infrastructure et des workloads.

- Collecteurs de données pour infrastructure et workloads hétérogènes, y compris Kubernetes
- Ouvrez le collecteur Telegraf et les API ouvertes pour faciliter l'intégration
- Alertes et notifications complètes
- Machine learning pour des informations exploitables
- Optimisez l'utilisation des ressources
- Tableaux de bord intégrés ou personnalisables avec filtres avancés pour réduire le bruit d'affichage afin de répondre aux questions
- Découvrez l'état de santé des opérations de stockage ONTAP
- Protégez vos ressources les plus précieuses : les données contre les attaques par ransomware ou les destructions de données

---

Mise en route

- Comment **"lancez-vous"**utiliser une infrastructure de données exploitables ?
- Je suis inscrit. Que dois-je faire ? "Acquisition des données" "Configuration des utilisateurs"
- Génial ! Et la suite ? "Préparation des ressources : annotation" "Recherche des ressources que vous voulez : interrogation" "Voir les données que vous voulez : tableaux de bord" "Surveillance et alertes" "Sécurisation des données"
- C'est super ! Je suis prêt à **"abonnez-vous"**.

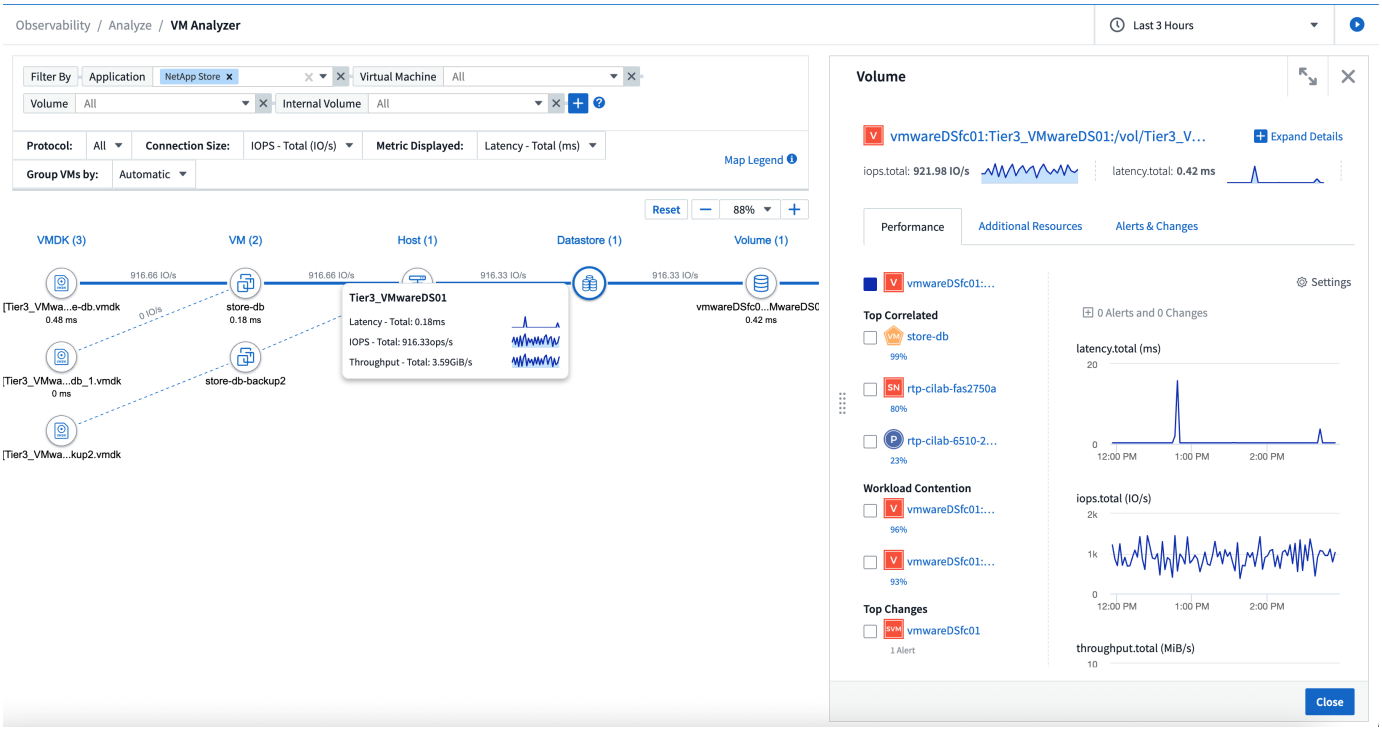
Nouveautés de Data Infrastructure Insights

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

Juin 2025

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

La fonctionnalité **VM Analyzer** de DII offre une vue complète et complète de vos environnements virtualisés. VM Analyzer simplifie le dépannage en cartographiant l'intégralité du chemin, des machines virtuelles au stockage, permettant ainsi 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, au filtrage et à des indicateurs de performance détaillés, les administrateurs peuvent facilement identifier les goulots d'étranglement, analyser les déséquilibres de trafic et optimiser les performances globales du stockage.



Systèmes d'exploitation pris en charge

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"-ci :

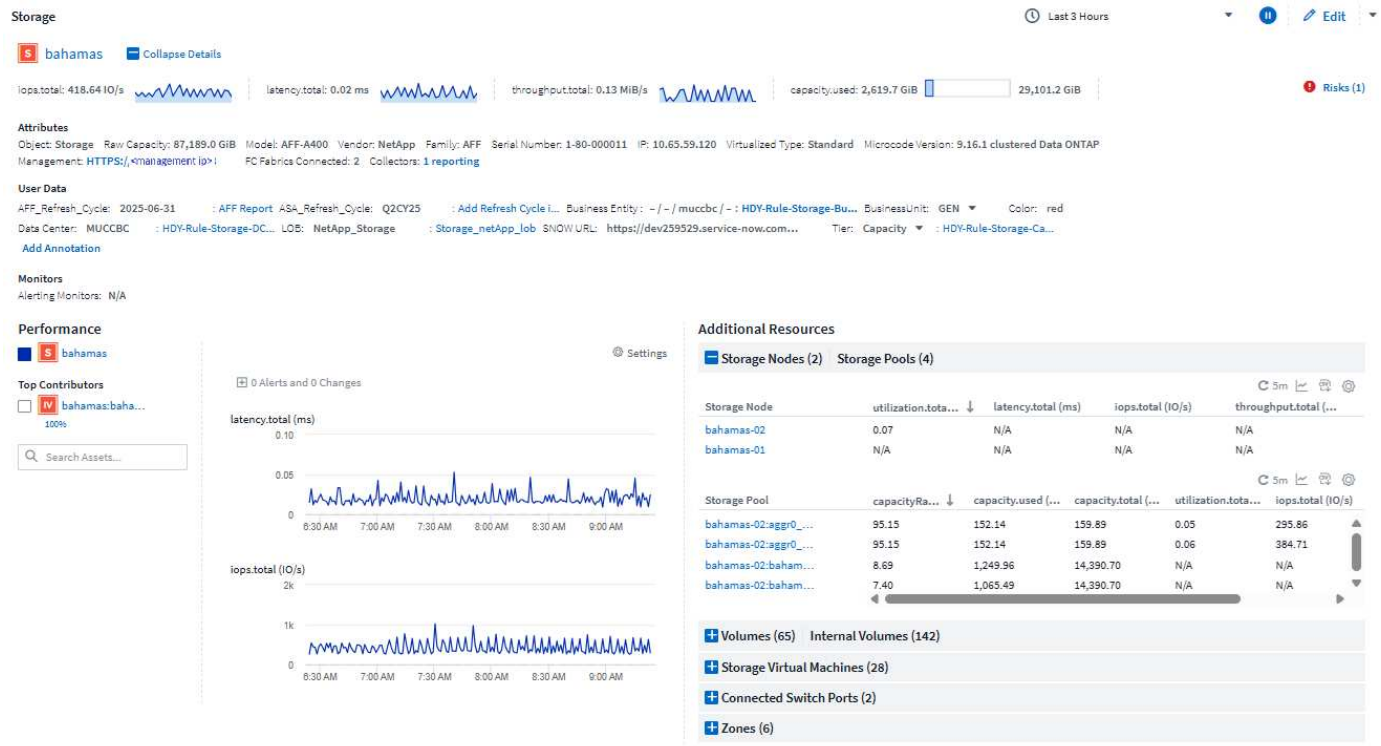
- Debian (64 bits) 12
- Oracle Enterprise Linux (64 bits) 9.6
- Red Hat (64 bits) 9.6

Mai 2025

Les nouvelles pages de destination vous permettent de rester dans la circulation

Les pages d'accueil repensées représentent tout ce dont vous avez besoin, à savoir des données récapitulatives, des graphiques de performances, des corrélations, des alertes et des changements, et des ressources clés, dans une seule vue.

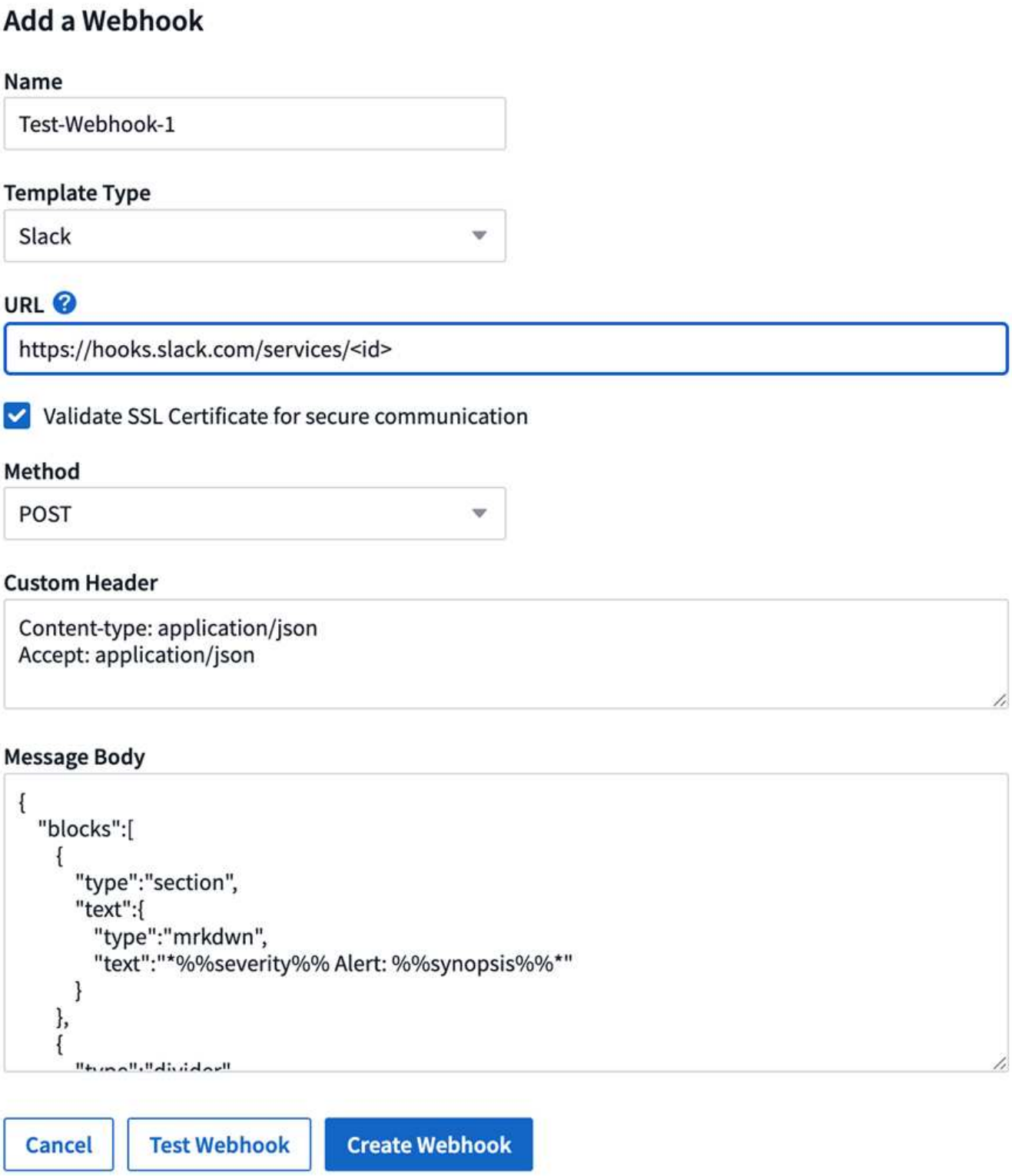
Désormais, vous pouvez résoudre les problèmes plus rapidement et rester en mouvement, sans passer d'un onglet à l'autre ni perdre le contexte.



Amélioration de la sécurité des workloads

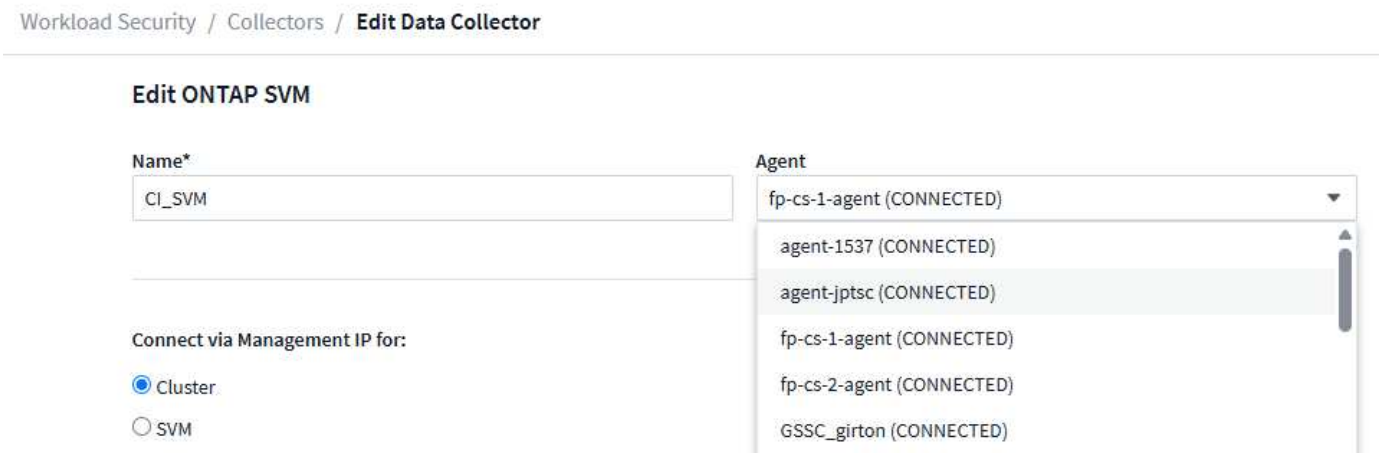
Webhooks maintenant disponibles pour les alertes Workload Security

Workload Security prend désormais en charge les notifications Webhook prêtes à l'emploi pour 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 toute autre application SIEM ou tierce. Acheminez les alertes critiques directement dans vos workflows de sécurité existants, afin que votre équipe puisse enquêter et répondre plus rapidement.



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

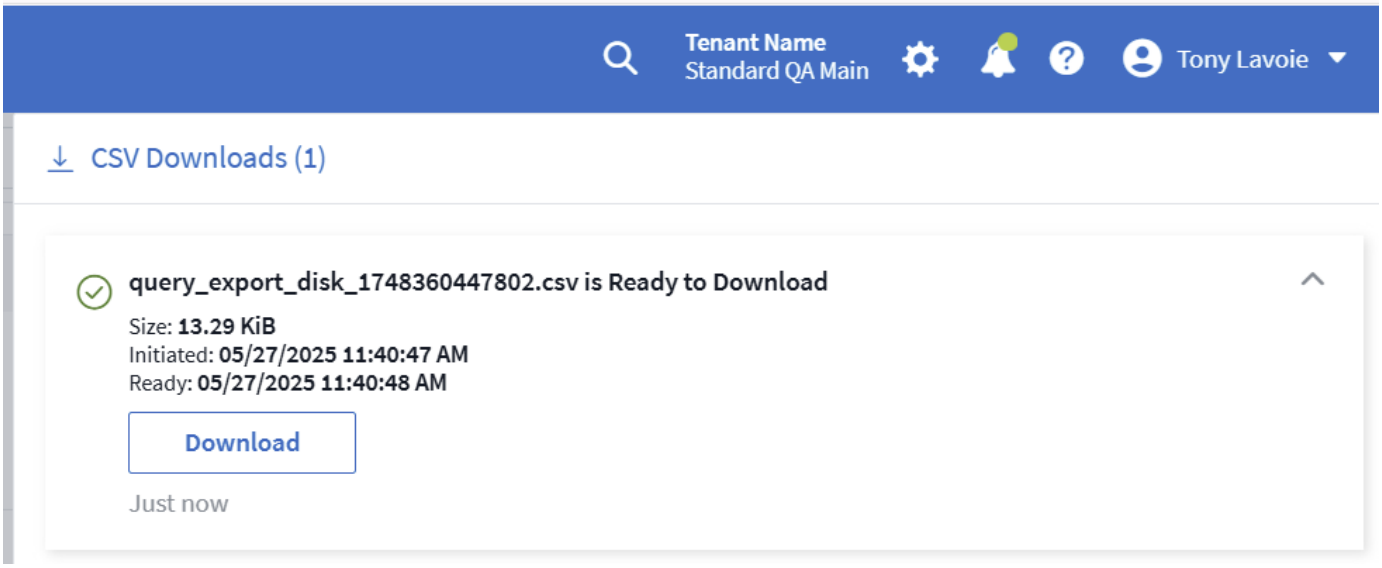
Vous pouvez facilement migrer un collecteur Workload Security d'un agent à un autre, ce qui permet un équilibrage de charge efficace des collecteurs entre les agents. La migration est aussi simple que la modification du collecteur et la sélection de l'agent de destination dans la liste.



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.



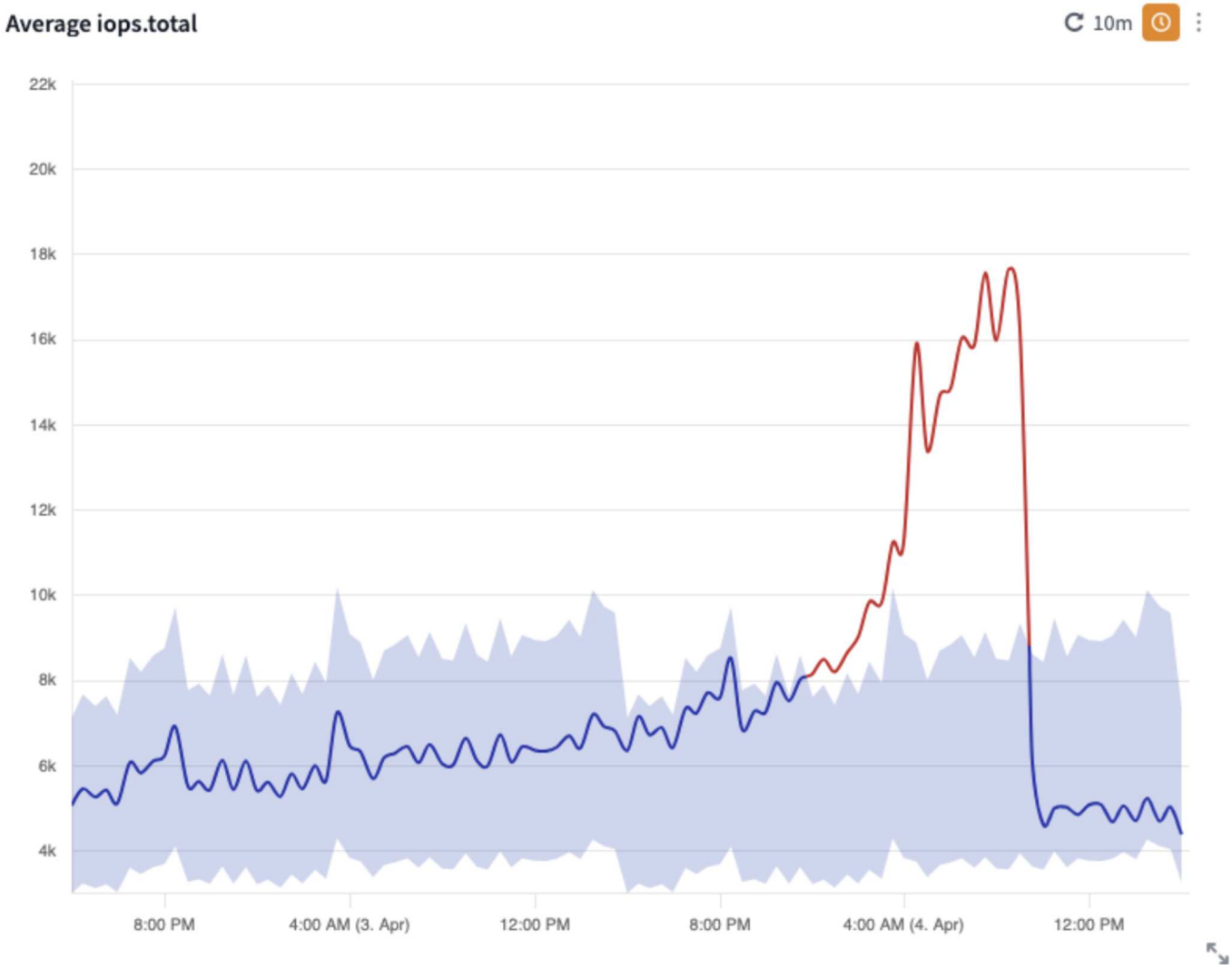
Avril 2025

Widgets en ligne d'anomaly alimentés par ML pour une résolution proactive des problèmes

Pour résoudre les problèmes de performances avec les widgets de graphique de ligne ou de spline, vous pouvez désormais afficher les limites de comportement prévues avec les mesures réelles, ce qui vous permet de distinguer les tendances métriques normales et anormales.

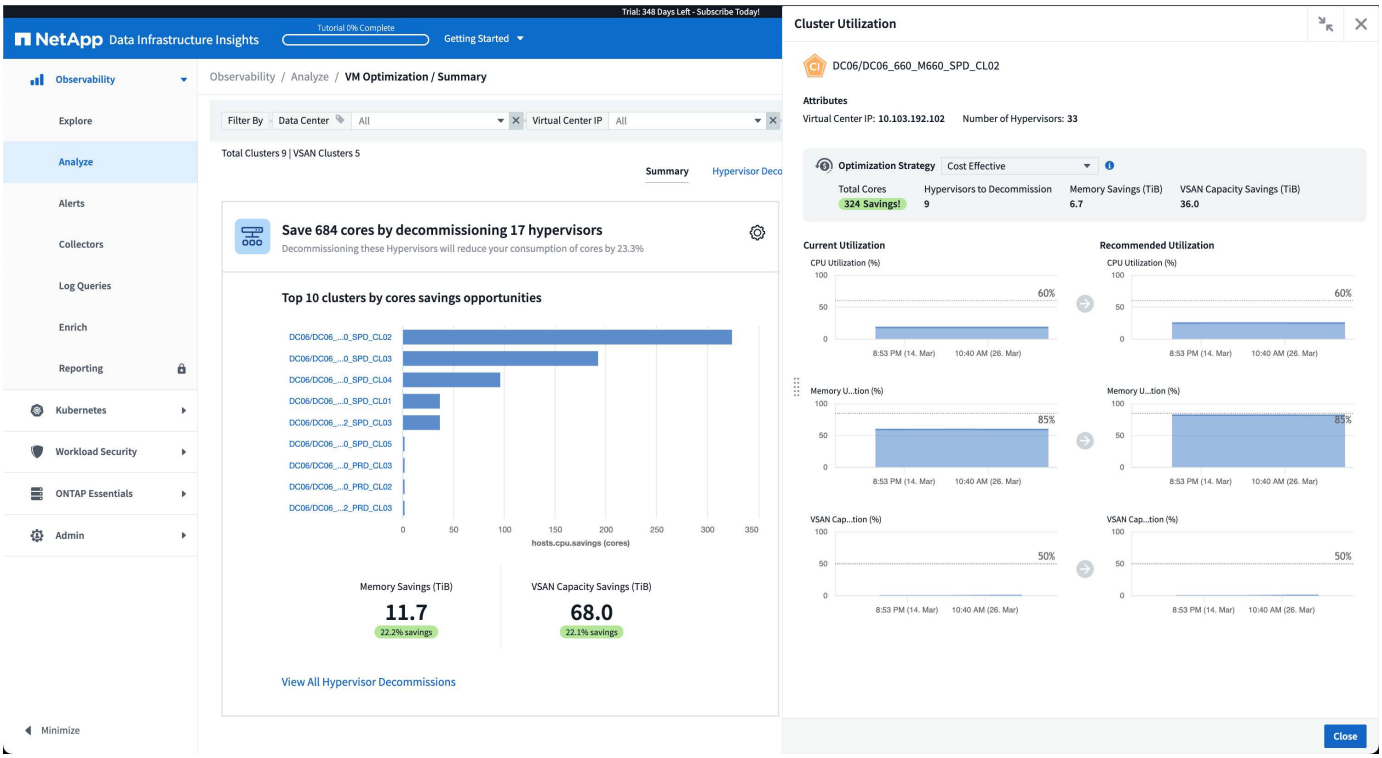
Le machine learning DII avec analyse saisonnière des données établit des seuils intelligents basés sur des modèles historiques. Lorsque les mesures diffèrent des plages prévues, le système les met en évidence

comme des anomalies, ce qui permet d'identifier rapidement les problèmes, de réduire le temps moyen de résolution et de résoudre les problèmes avant qu'ils n'affectent les opérations.



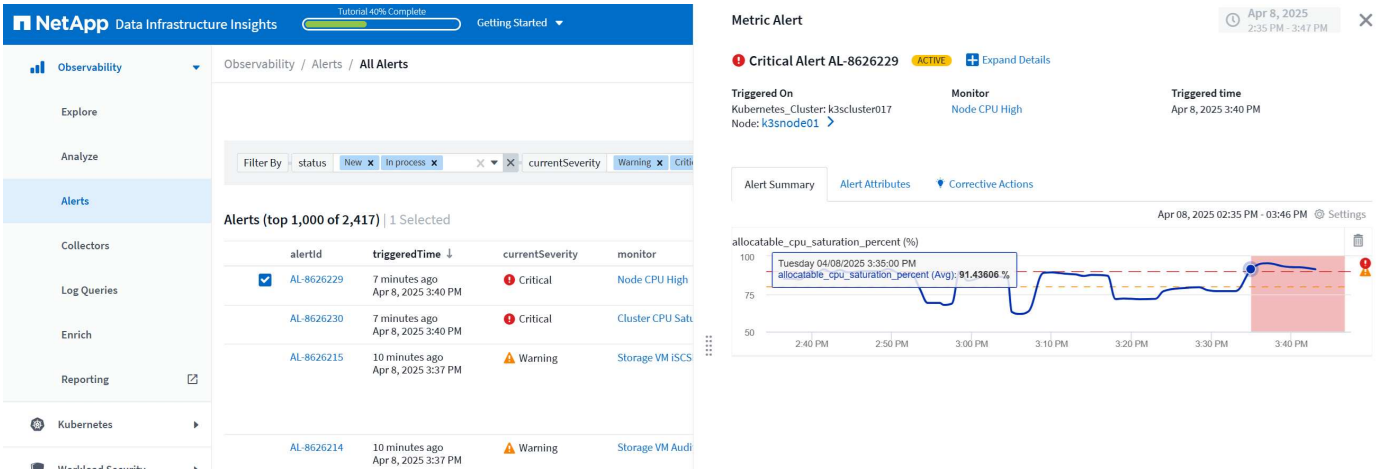
Optimisez les coûts VMware avec la prise en charge du stockage VSAN

Notre fonctionnalité d'optimisation des machines virtuelles 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 récupérer des recommandations et ainsi réduire encore les coûts de licence.



Des détails d’alerte à portée de main

Les enquêtes sur les alertes sont plus simples que jamais grâce au nouveau panneau coulissant. Sélectionnez une alerte pour afficher les détails de cette alerte, et passez facilement d’une alerte à l’autre sans perdre votre place lors de l’analyse des problèmes.



Exportation asynchrone pour l’analyse de la sécurité des charges de travail

L’exportation des données d’analyse peut prendre de quelques secondes à plusieurs heures, selon la quantité de données à exporter. La sécurité des charges de travail exporte ces données de manière asynchrone, ce qui vous permet de continuer à travailler pendant la compilation du fichier .CSV.

Notifications du Data Collector regroupées en règles

Si vous avez configuré des notifications sur des collecteurs de données, à partir d’avril 15, ces notifications seront traitées dans les règles de notification, avec une seule règle pour les collecteurs qui ont des

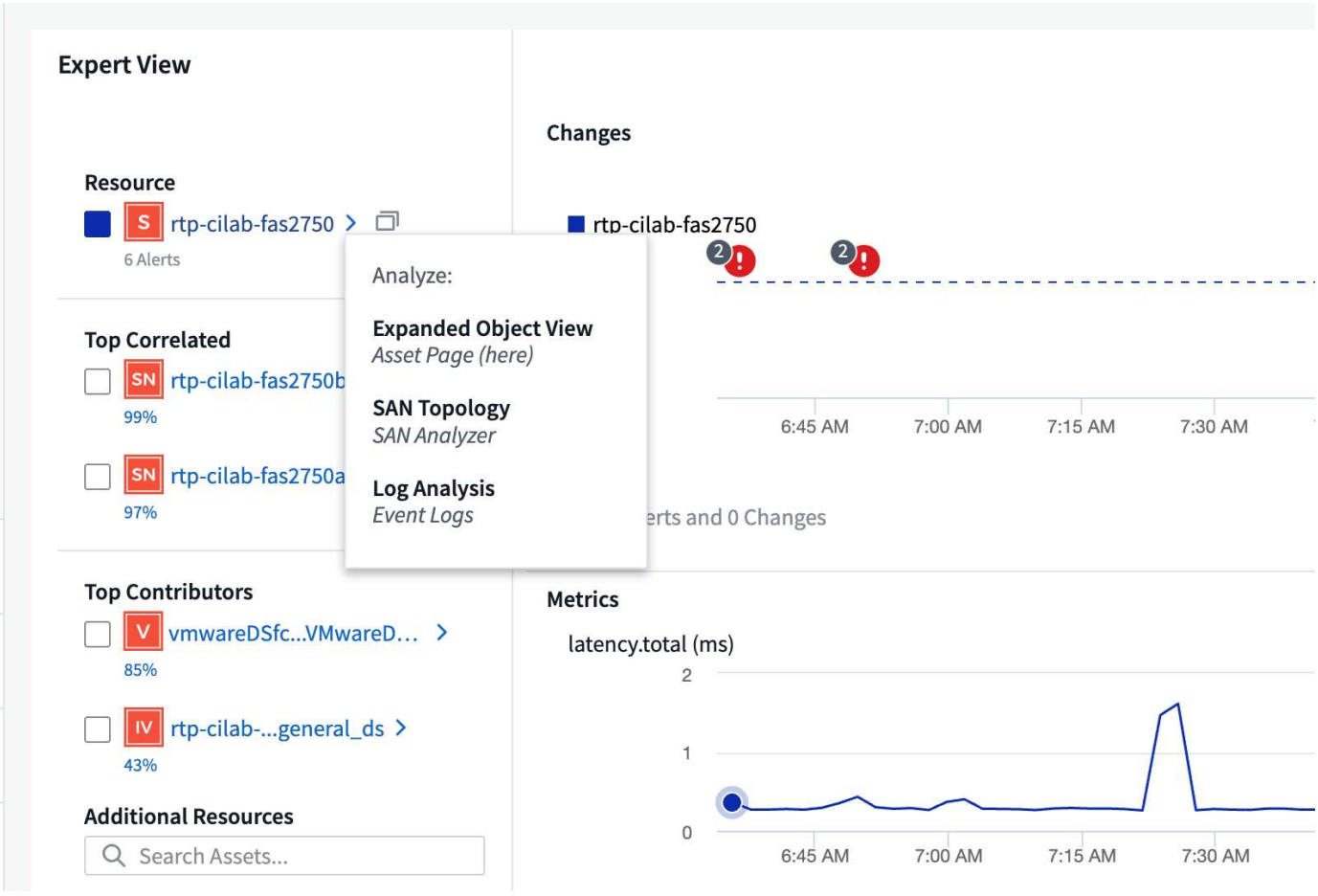
destinataires identiques. Les collecteurs avec différents destinataires auront des règles distinctes. Les notifications de collecteur existantes sont migrées vers des règles de notification.

Mars 2025

Navigation contextuelle améliorée pour une gestion efficace de l'infrastructure

Gagnez du temps en tirant parti des informations exploitables de l'infrastructure de données pour atteindre l'excellence opérationnelle. Nous ajoutons maintenant des liens de menu contextuel qui vous permettent de passer directement de n'importe quel objet à la page d'accueil de la ressource pour obtenir des informations sur les performances des périphériques, à SAN Analyzer pour la visualisation de la topologie réseau, à des journaux pour la sensibilisation au fonctionnement ou à change Analyzer pour la gestion de la configuration.

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



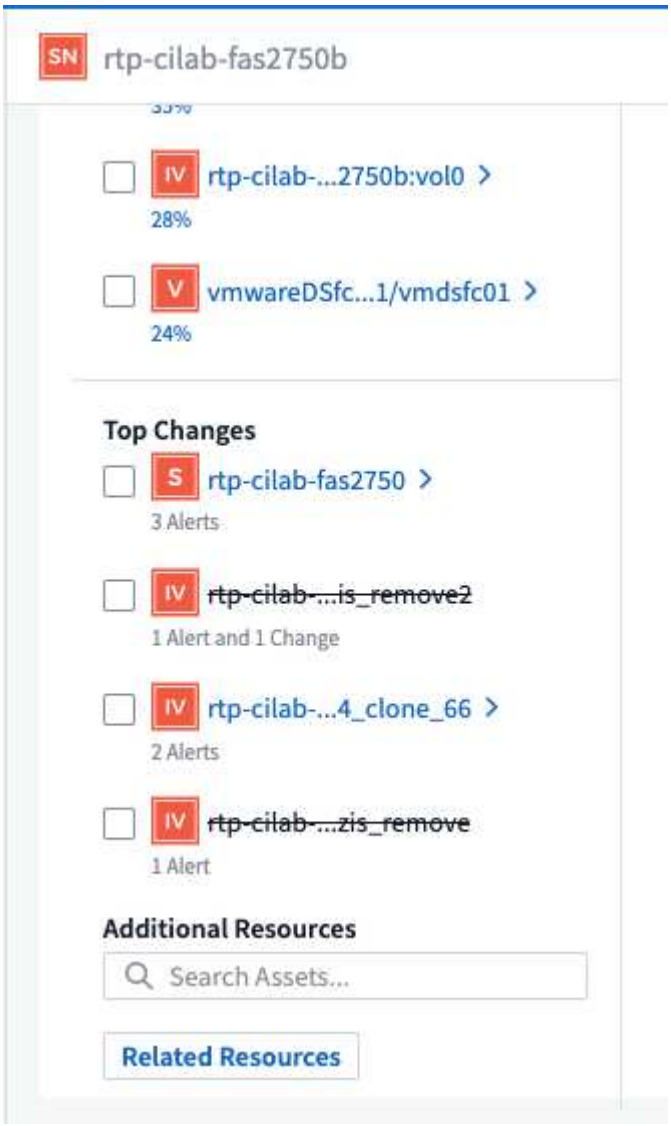
Conserver l'historique des ressources supprimées

Notre fonctionnalité avancée d'infrastructure change préserve désormais l'historique des ressources supprimées, telles que les qtrees et les volumes qui ont été déplacés et qui ne sont plus disponibles.

Vous avez oublié quelque chose dans votre puzzle de dépannage ? Plus que jamais ! Vous verrez tout, y

compris les objets supprimés marqués d'une frappe, ce qui vous donne un contexte complet, même après la suppression des ressources, pour vous assurer de ne jamais manquer les éléments critiques des modifications ou alertes passées sur le chemin de bout en bout.

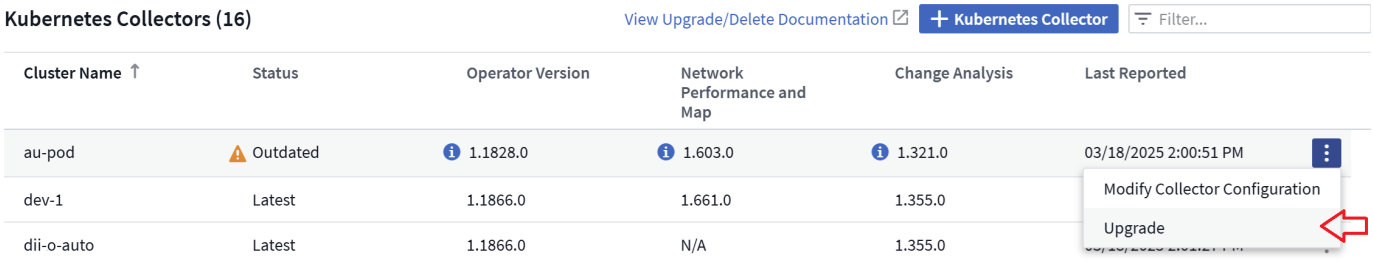
Le résultat ? Des délais de résolution plus rapides et des décisions d'infrastructure plus fiables, même lorsque les ressources en question n'existent plus.



Mise à niveau par bouton-poussoir de l'opérateur Kubernetes

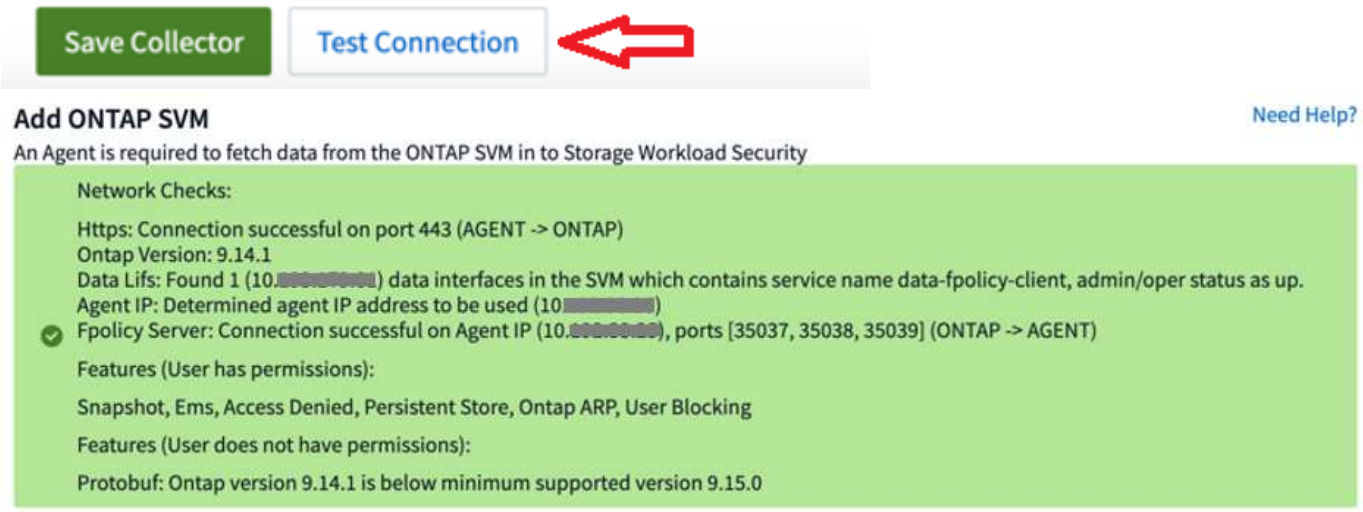
Vous voulez être sûr de disposer du dernier opérateur Kubernetes ? Mettez à niveau l'opérateur à la demande à partir du menu du cluster DII Kubernetes Collectors. Il vous suffit de sélectionner mettre à niveau dans le menu pour que l'opérateur vérifie les signatures d'image, capture un instantané de votre installation actuelle et effectue la mise à niveau.

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



Tester la connectivité pour les collecteurs de données Storage Workload Security

La fonctionnalité de test de connectivité a pour but d'aider les utilisateurs finaux à identifier les causes spécifiques de défaillances lors de la configuration de 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.



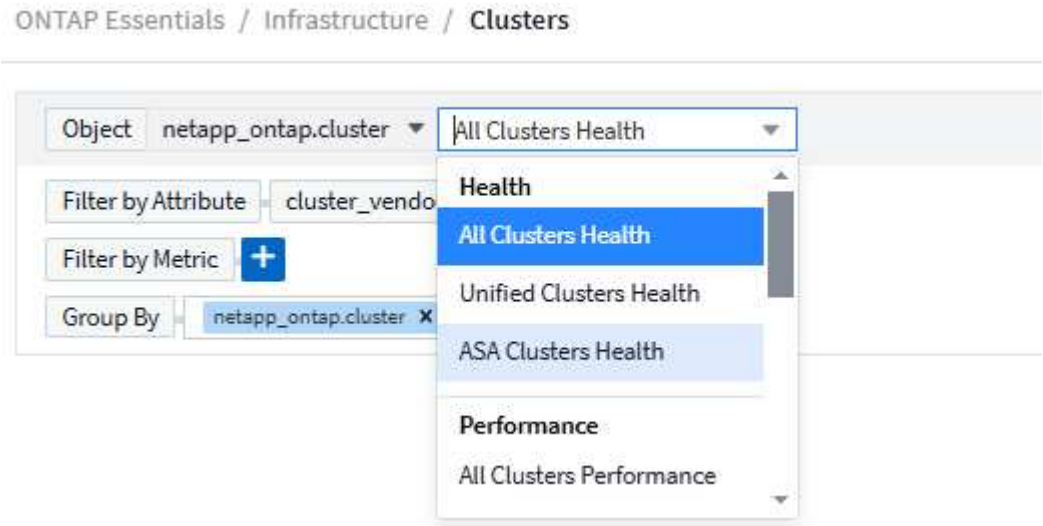
Systèmes d'exploitation pris en charge

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"-ci :

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

Février 2025

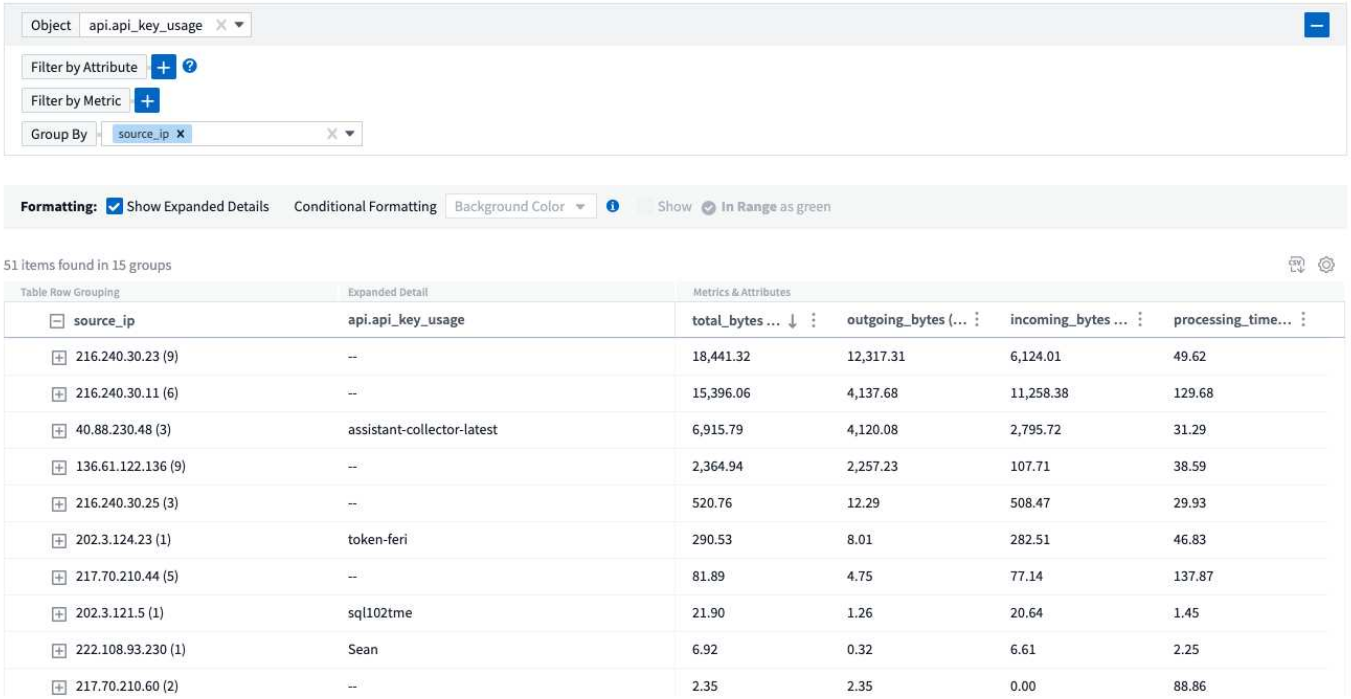
ONTAP Essentials inclut désormais une fonctionnalité de gestion prête à l'emploi pour la dernière génération d'"ASA"appareils. Cela inclut SAN Analyzer pour les topologies VM-LUN des charges de travail exécutées sur ONTAP, désormais également disponible avec la prise en charge de NetApp dans le cadre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



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

Renforcez votre stratégie de sécurité et rationalisez la gestion des ressources avec un meilleur suivi de l'utilisation de l'API REST, disponible pour les utilisateurs Admin. Le suivi de l'utilisation de l'API vous permet de voir quels tokens API sont utilisés, à partir de quelles adresses IP et le volume de trafic qu'ils génèrent. En reliant les jetons à des adresses IP et des niveaux d'utilisation spécifiques, vous obtenez de puissantes informations sur l'accès au système et les tendances d'utilisation, ce qui vous donne le contrôle dont vous avez besoin pour maintenir un environnement sûr et efficace et assurer le bon fonctionnement des opérations.

Pour afficher l'utilisation de l'API, accédez à **observabilité > Admin > API Access** et sélectionnez *View API usage*. Notez que cette API est disponible uniquement pour les API d'observabilité DII ; elle ne s'applique pas à Workload Security.



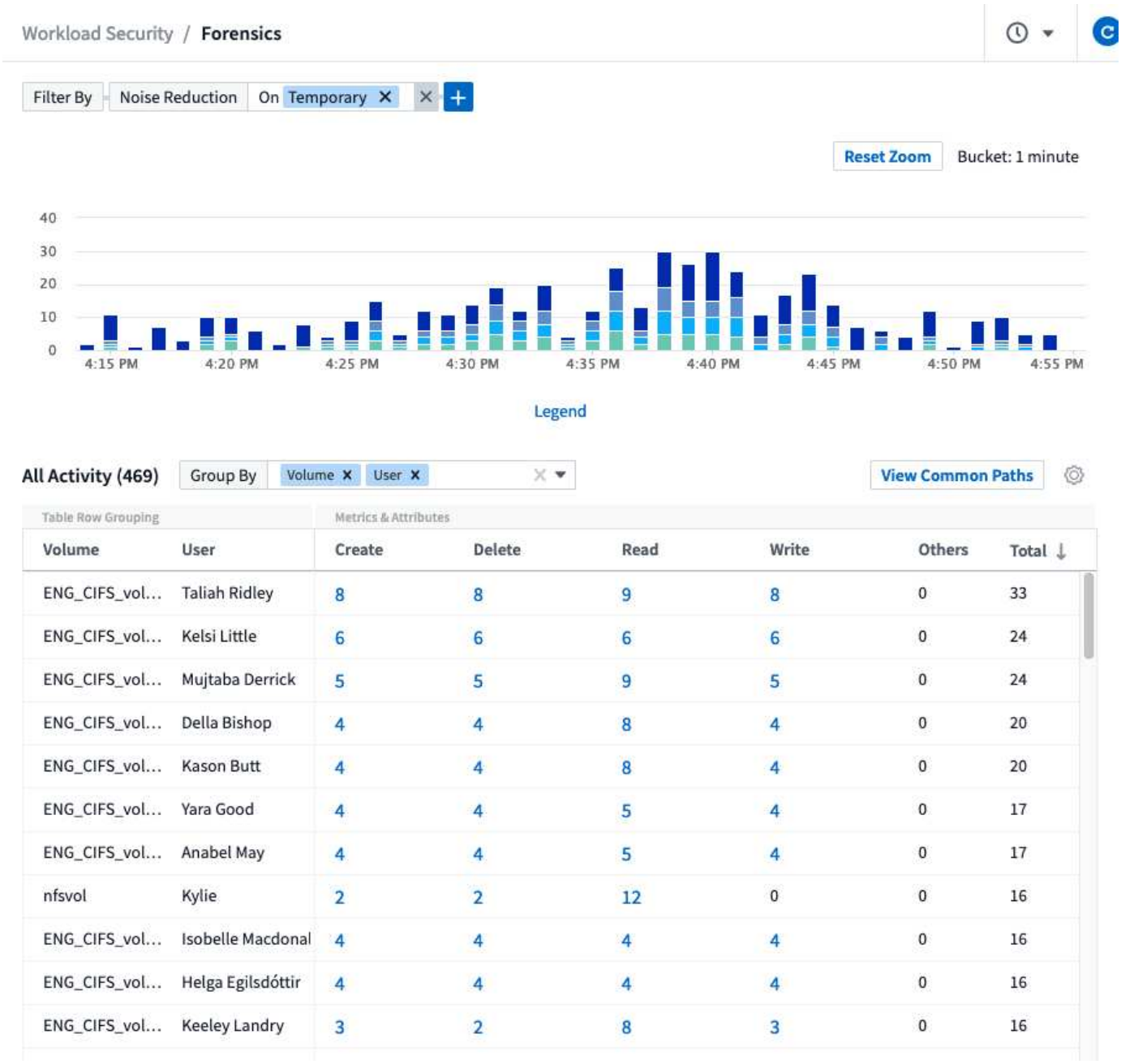
API de sécurité des charges de travail pour limiter les utilisateurs

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

Janvier 2025

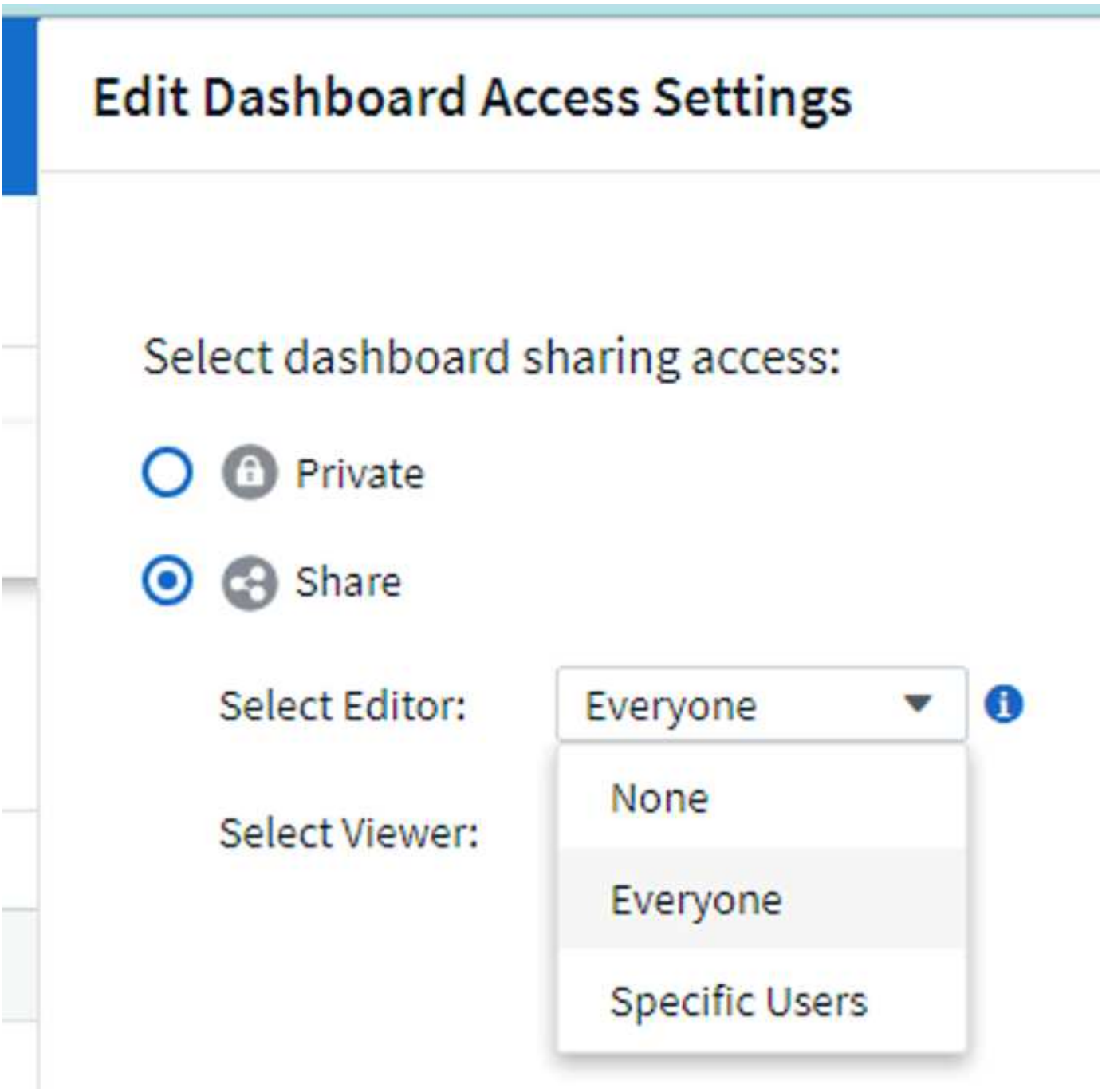
Gérez les risques de manière proactive grâce au regroupement des événements

Découvrez notre dernière fonctionnalité conçue pour améliorer vos capacités de sécurité et de gestion des ressources ! Grâce à la fonctionnalité avancée de groupe par groupe et à la prise en charge hiérarchique de plusieurs groupes par groupe, vous pouvez désormais identifier facilement les utilisateurs ayant accédé à des dossiers spécifiques, déterminer les utilisateurs et partages les plus actifs et gérer les risques de manière proactive en suivant les adresses IP des clients actifs. Optimisez votre stockage et votre utilisation de la bande passante en localisant les fichiers et dossiers les plus utilisés et en améliorant le contrôle de l'accès au système en identifiant les utilisateurs.



Contrôle d’accès au tableau de bord

Data Infrastructure Insights vous permet désormais de mieux contrôler l’accès aux tableaux de bord que vous créez. Vous pouvez choisir qui modifier vos graphiques. Vous contrôlez l’exposition aux informations potentiellement sensibles. Vous travaillez encore 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.

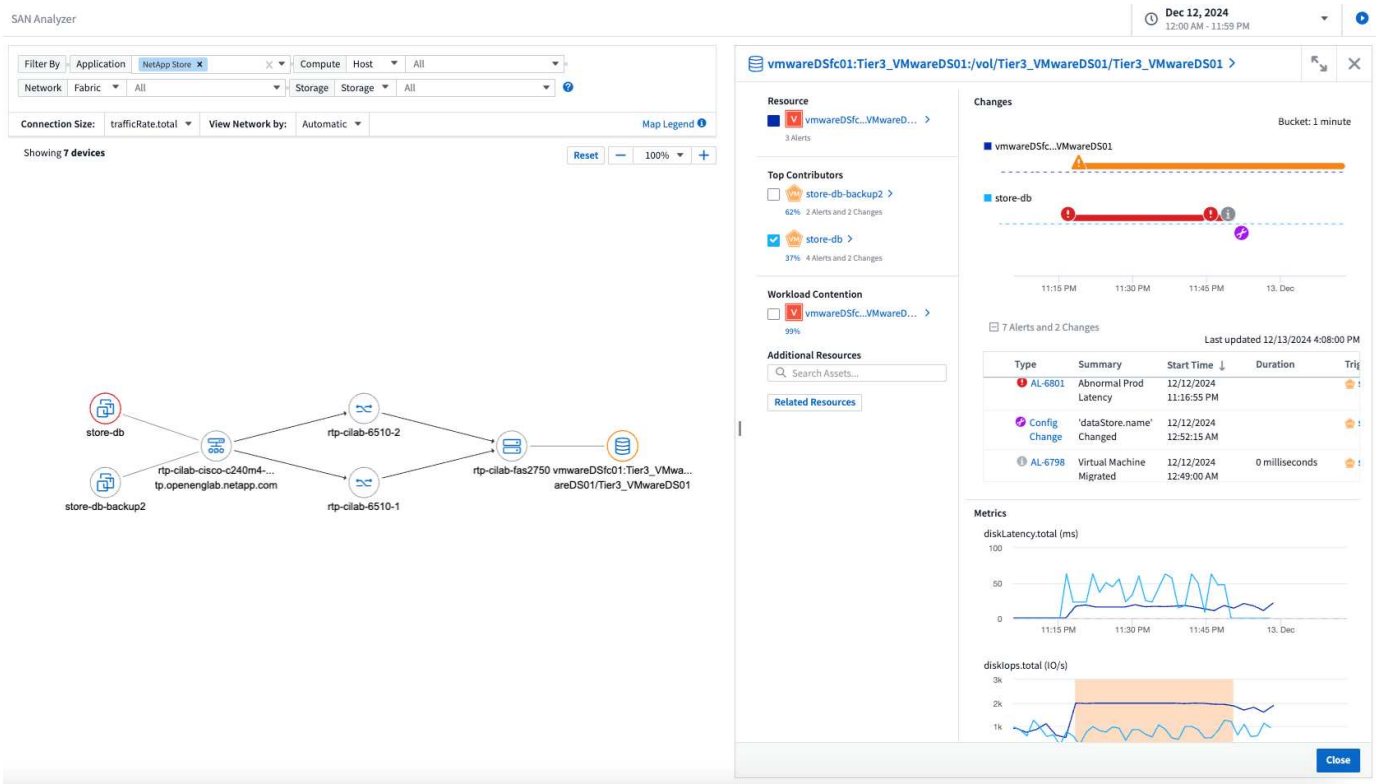


Décembre 2024

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

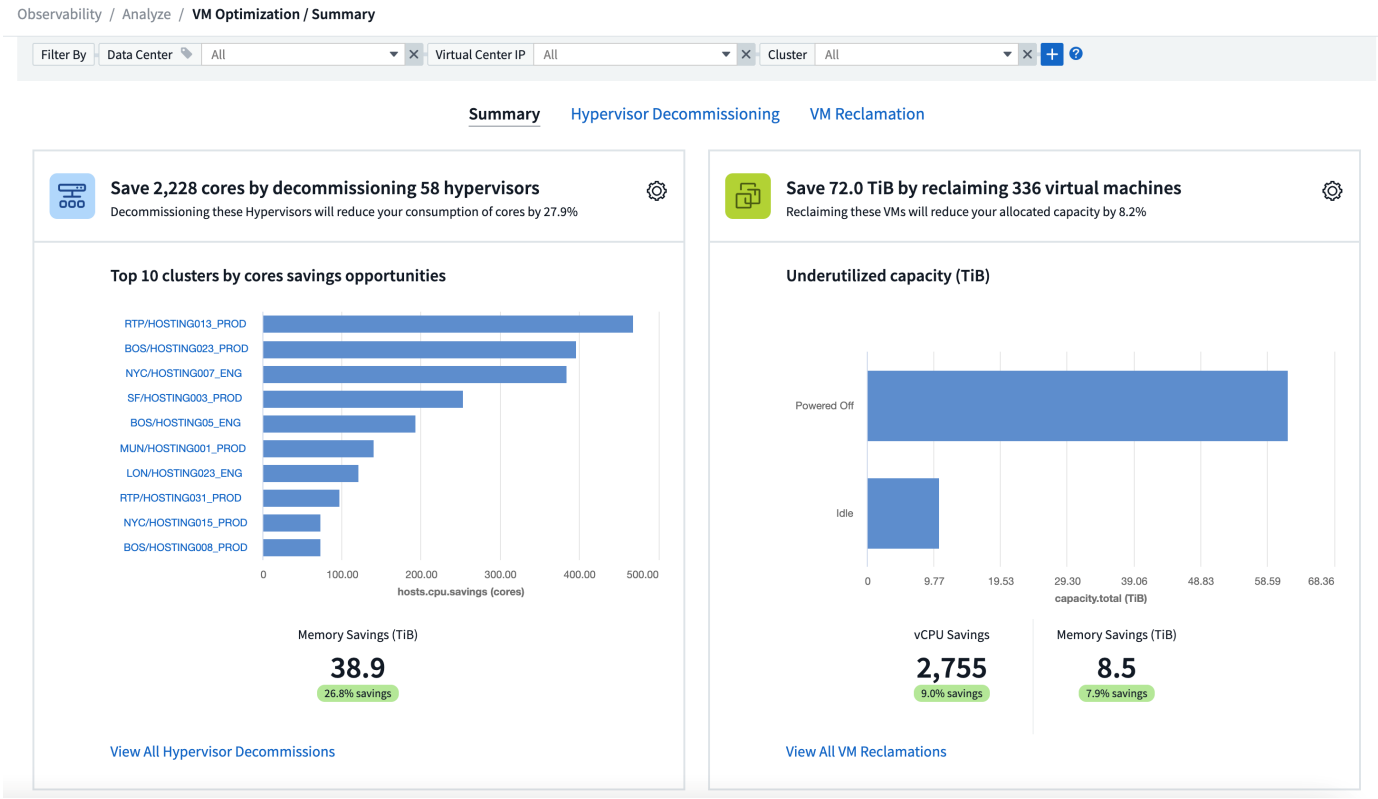
LE SAN joue un rôle crucial dans la gestion des charges de travail stratégiques, mais sa complexité peut entraîner des pannes importantes et des perturbations pour les clients. Grâce à **SAN Analyzer** de DII, la gestion du SAN devient plus simple et plus efficace. Cet outil puissant offre une visibilité de bout en bout, en mappant les dépendances entre les ordinateurs virtuels/l'hôte et le réseau vers les LUN et le stockage. Grâce à une carte topologique interactive, SAN Analyzer vous permet de repérer les problèmes, de comprendre les modifications et d'améliorer la compréhension du flux de données. Rationalisez la gestion SAN dans des

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



Optimisez les coûts des ordinateurs virtuels grâce à la mise hors service intelligente de l'hôte et à la récupération des ordinateurs virtuels

Data Infrastructure Insights vous aide à gérer les coûts d'infrastructure et de licences en analysant l'historique du comportement de l'environnement et en établissant des prévisions à court et à long terme, et en générant des recommandations détaillées pour la désaffectation et la récupération des serveurs virtuels hors tension et inactifs. Ces recommandations vous aident à assurer la stabilité des performances, à libérer de la capacité inutilisée et à réduire l'allocation de mémoire et de processeur.



Découvrez les informations de journalisation avec la prise en charge des graphiques de temps et des widgets de tableau

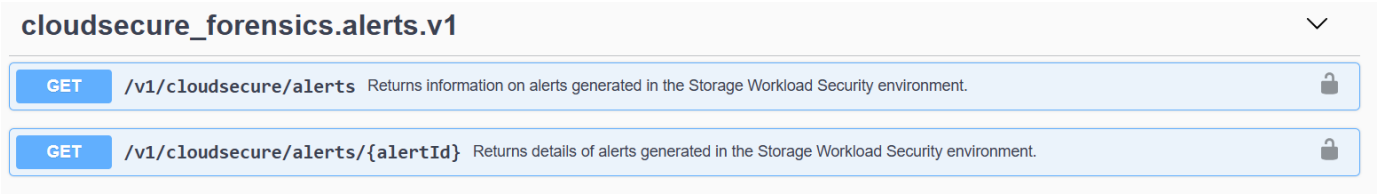
Vous pouvez désormais utiliser les graphiques de temps (barre, ligne, zone) pour identifier les tendances et les modèles des données de journal, tels que les erreurs récurrentes ou les pics d'activité, ce qui vous permet d'obtenir des informations précieuses sur le comportement du système au fil du temps. De plus, grâce aux tableaux, vous pouvez désormais inclure les messages de journal directement dans le tableau de bord, offrant ainsi une vue plus complète des détails du journal.



Novembre 2024

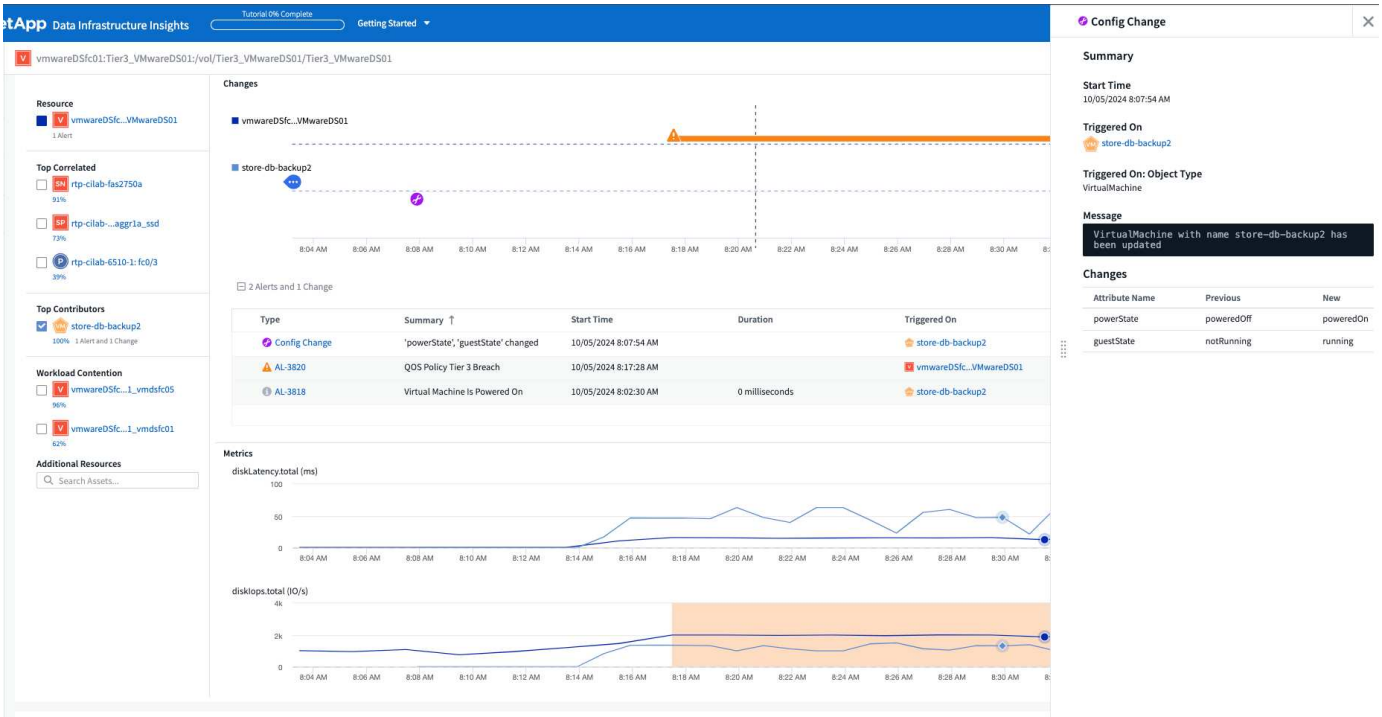
Nouvelle API d'alertes de sécurité des workloads

Récupérez les détails des alertes d'analyse avec le nouveau Workload Security "**Cloudsecure_Forensics.Alerts** API".



Analysez les modifications de configuration dans votre environnement

Les modifications de configuration sont l'une des causes les plus courantes de problèmes dans l'INFORMATIQUE moderne. Les nouvelles fonctionnalités de Data Infrastructure Insights (DII) "analyse des modifications"vous permettent de comprendre clairement les changements à l'origine des problèmes dans votre environnement. Accélérez le temps de résolution des problèmes en affichant toutes les modifications apportées aux périphériques et aux composants de l'infrastructure qui ont pu être à l'origine d'un problème. De plus, lorsque vous ou votre équipe effectuez des modifications planifiées, vous pouvez les valider rapidement et vous assurer qu'il n'y a aucun effet inattendu avant que les niveaux de service ne soient affectés.



Prise en charge de KubeVirt : surveillez les workloads des machines virtuelles s'exécutant 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 metrics, les événements, les modifications de configuration et le trafic réseau des machines virtuelles et des workloads de conteneurs dans vos clusters Kubernetes.

Octobre 2024

Déverrouiller de nouvelles informations avec des expressions personnalisées dans les moniteurs

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

- Ratio : IOPS/To pour détecter si les limites de niveau de services 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 ressources avec le point de marge optimal pour identifier les ressources qui ne fonctionnent pas à pleine capacité.



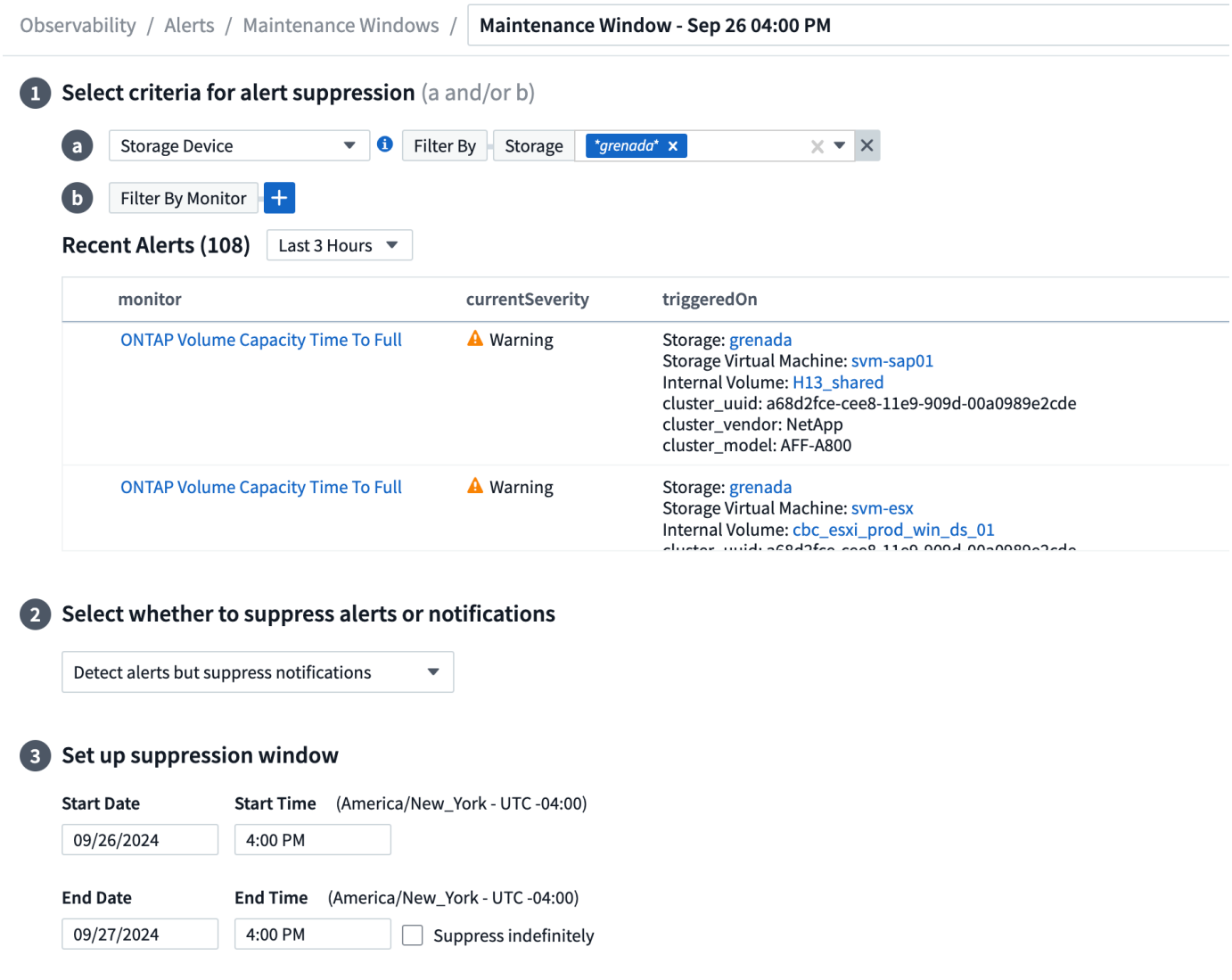


Réduisez les interruptions d'alerte pendant la période de maintenance

Les fenêtres de maintenance vous permettent de supprimer les notifications d'alerte pendant les périodes de maintenance planifiées, ce qui vous permet d'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 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 au cours d'une période de mise à niveau planifiée.

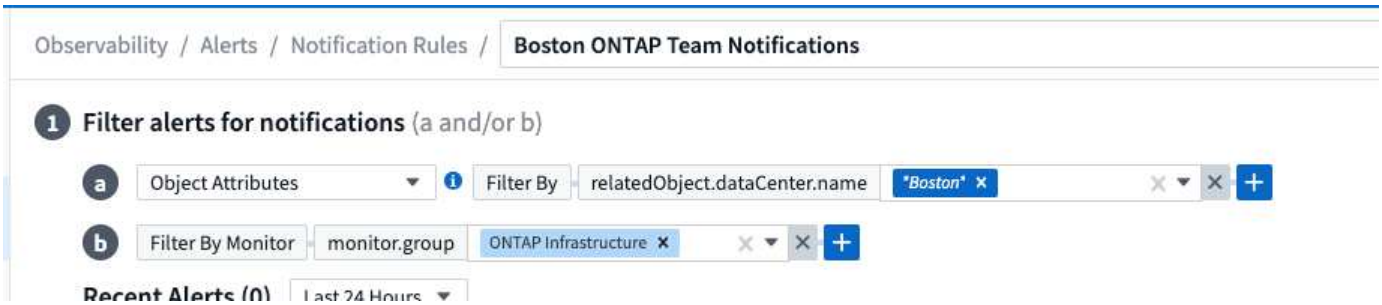
Notez que seules les notifications d'alerte sont supprimées (e-mail, webhook) ; les alertes elles-mêmes sont toujours affichées sur la page observabilité > alertes > toutes les alertes.



Rationalisez la gestion des alertes grâce aux nouvelles règles de notification des alertes

Les règles de notification des alertes simplifient la gestion des notifications entre les moniteurs et les équipes.

Contrôlez la transmission des alertes via les canaux de votre entreprise, en veillant à ce que les bonnes informations parviennent à l'équipe appropriée. Inutile de gérer des moniteurs distincts pour différentes équipes ; il n'est pas nécessaire d'acheminer les alertes en fonction d'attributs d'objet associés (nom du stockage, data Center, nom de l'application) ou d'attributs de surveillance (groupe, gravité).



Analyse des journaux dans les tableaux de bord

Vous pouvez désormais inclure des événements de journalisation dans vos tableaux de bord pour visualiser les données d'événement et avoir une compréhension plus complète et contextuelle de votre environnement. Examiner les journaux et afficher les mesures associées sans quitter le tableau de bord.



Meilleure observabilité VMware avec les événements VMware

Gérez et dépannez votre environnement VMware de manière proactive avec des événements en temps réel. Les événements VMware fournissent des informations sur les migrations des ordinateurs virtuels, l'allocation des ressources et l'état de l'hôte. Désormais disponible pour les requêtes, les tableaux de bord et les moniteurs. Requiert VMware version 8 ou supérieure. Il vous suffit de sélectionner 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 Data Collector :

- **Pure FlashBlade** : ce collecteur rassemble 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

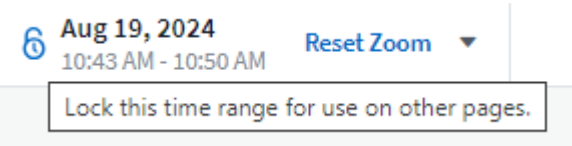
Le mardi 24 septembre 2024, NetApp a officiellement changé le nom de Cloud Insights pour **Data Infrastructure Insights** (DII). Cela a été annoncé lors de la conférence des utilisateurs Insight par Haiyan Song dans sa présentation principale et dans un communiqué de presse produit de la conférence Insight.

Le service DII reste le même ; il n'y a pas de modification ou de modification des fonctions. Il s'agit d'une modification de nom qui permet d'aligner le nom du service sur ses fonctionnalités pour l'ensemble de l'infrastructure IT.

Août 2024

Afficher les données spécifiques à votre plage horaire

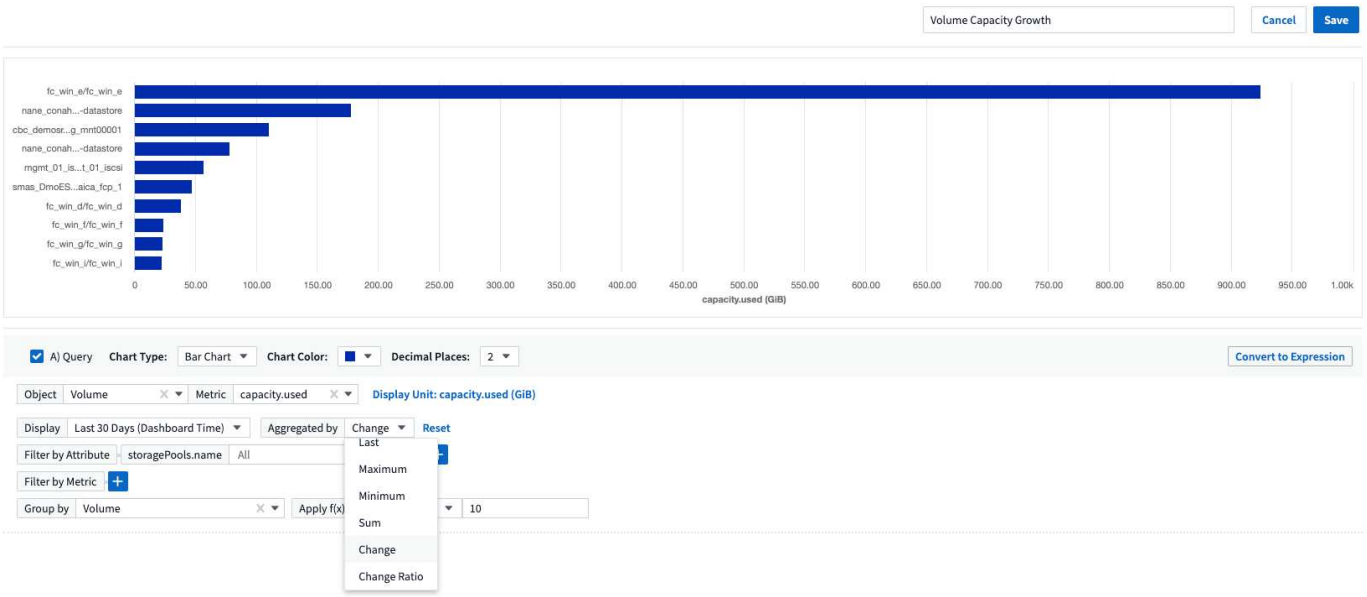
Vous êtes en train d'examiner une alerte ? Vous avez effectué un zoom avant sur une carte ? Ces actions modifient la plage horaire de ces pages. Vous pouvez maintenant verrouiller cette plage de temps, naviguer vers d'autres pages Cloud Insights et afficher des données spécifiques à cette plage de temps verrouillée. Les recherches et le dépannage sont désormais beaucoup plus faciles !



Analyse du taux de changement (%)

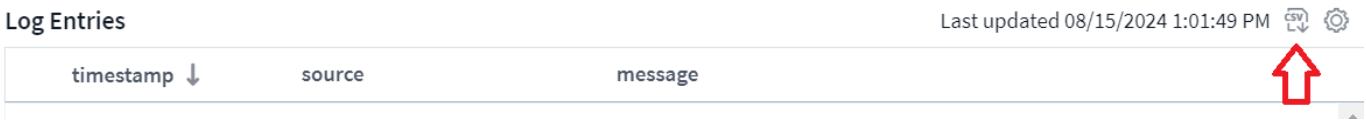
Les agrégations de temps de rapport de changement vous aident à identifier les changements et tendances significatifs des valeurs métriques au fil du temps. Ces informations sont essentielles pour comprendre ce qui a changé, par exemple une augmentation considérable de la capacité pour une période donnée ou une modification des performances d'un seul port.

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



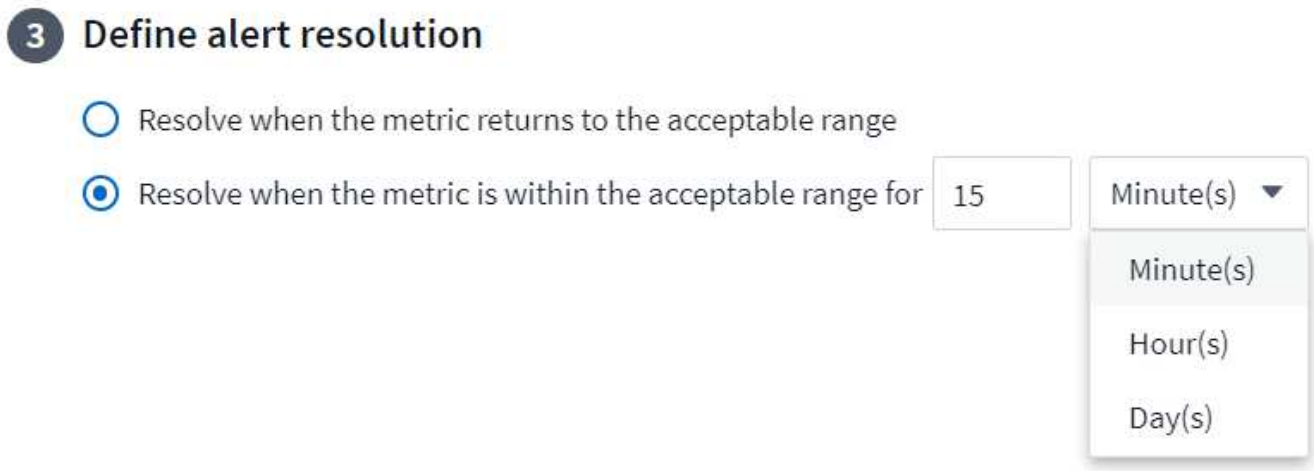
Exporter les résultats de la requête de journal au format .CSV

Lors de l'affichage des résultats des requêtes 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 le reporting des données et facilite l'intégration transparente avec d'autres outils Data Processing.



Résolution des alertes par heure

Cloud Insights vous permet désormais de résoudre une alerte lorsque la mesure surveillée reste dans la plage acceptable pendant une durée spécifiée. Cela vous permet de vous concentrer sur les problèmes réels et de réduire le bruit associé aux mesures en franchissant de manière répétée des seuils définis en consolidant plusieurs alertes en une seule.



Juillet 2024

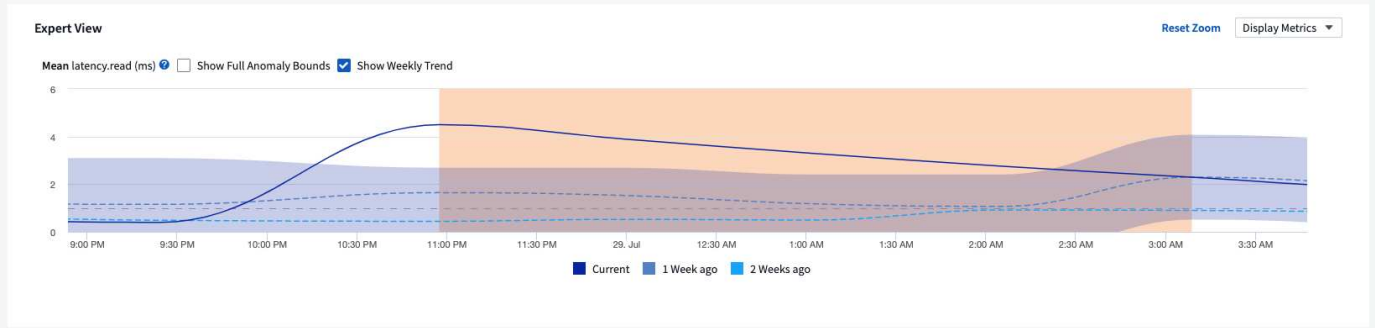
Fonctionnalités basées sur l'IA : détection des anomalies

Cloud Insights utilise le machine learning 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 plus tôt.

Un data Center 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 pour chaque jour et heure.

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

"Moniteurs de détection d'anomalies"Alerte lorsque des anomalies de ce type se produisent sur les metrics d'objet de votre choix.



Amélioration de la sécurité des workloads

Prise en charge NFS 4.1

Le Data Collector SVM prend désormais en charge les versions NFS jusqu'à **NFS 4.1** avec ONTAP 9.15.1 ou version ultérieure.

Nouvelle API d'activité Forensics

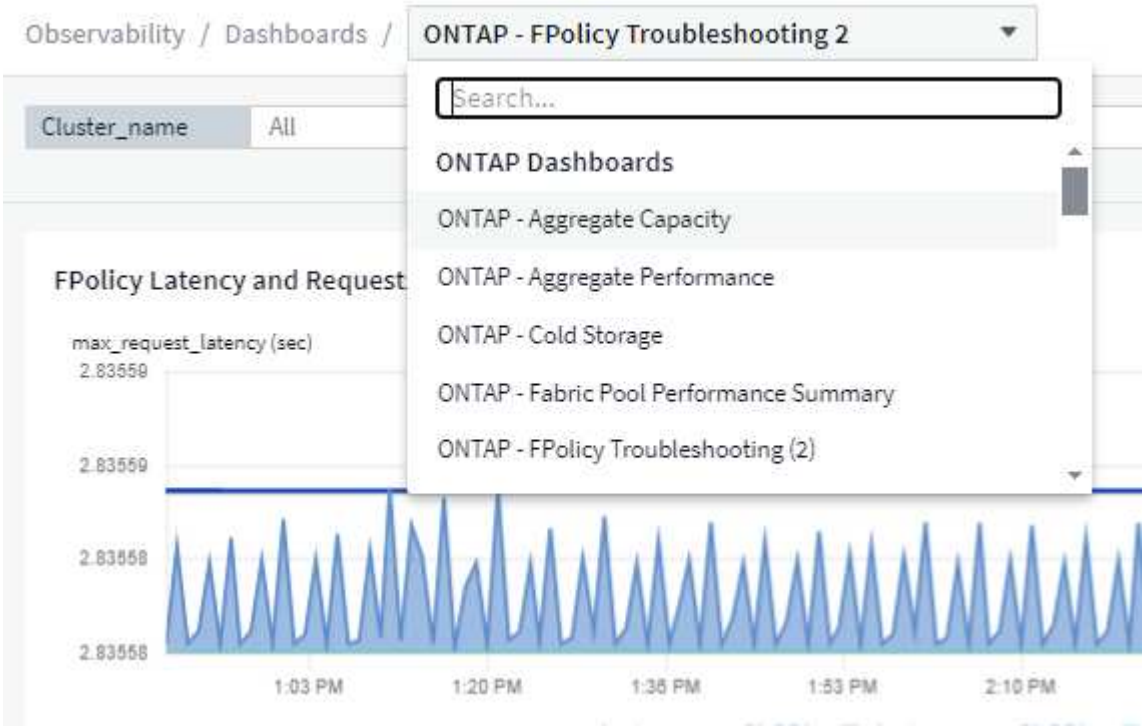
L'activité Forensics "API" a une nouvelle version. Lorsque vous appelez l'API pour Forensics Activity, utilisez l'API **cloudsecure_Forensics.Activities.*v2***.

Notez que si vous effectuez plusieurs appels vers cette API, pour de meilleurs résultats, assurez-vous que les appels se produisent séquentiellement, au lieu de en parallèle. Plusieurs appels parallèles peuvent entraîner la temporisation de l'API.

Navigation facilitée dans le tableau de bord

Il s'agit de rationaliser vos workflows opérationnels et de faciliter la collaboration entre les équipes.

Le regroupement de vos tableaux de bord vous permet d'obtenir plus facilement la visibilité dont vous avez besoin. 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 sur vos runbooks opérationnels pour améliorer votre expérience.



Juin 2024

Systèmes d'exploitation pris en charge

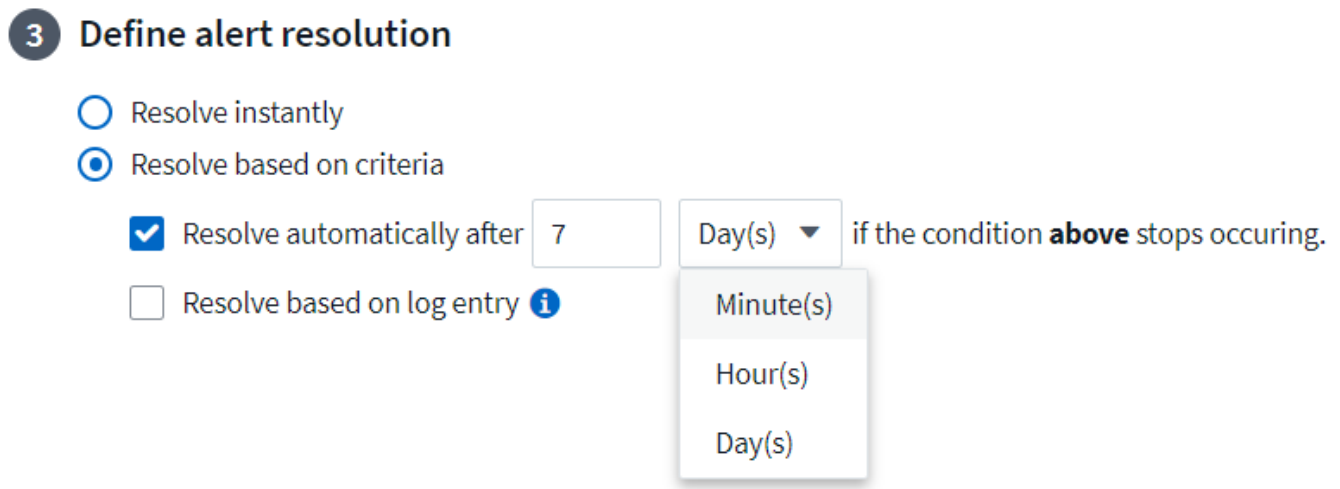
Les systèmes d'exploitation suivants sont pris en charge avec les unités d'acquisition Cloud Insights, en plus de ceux"déjà pris en charge"-ci :

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

Mai 2024

Résolvez automatiquement les alertes en fonction de l'heure

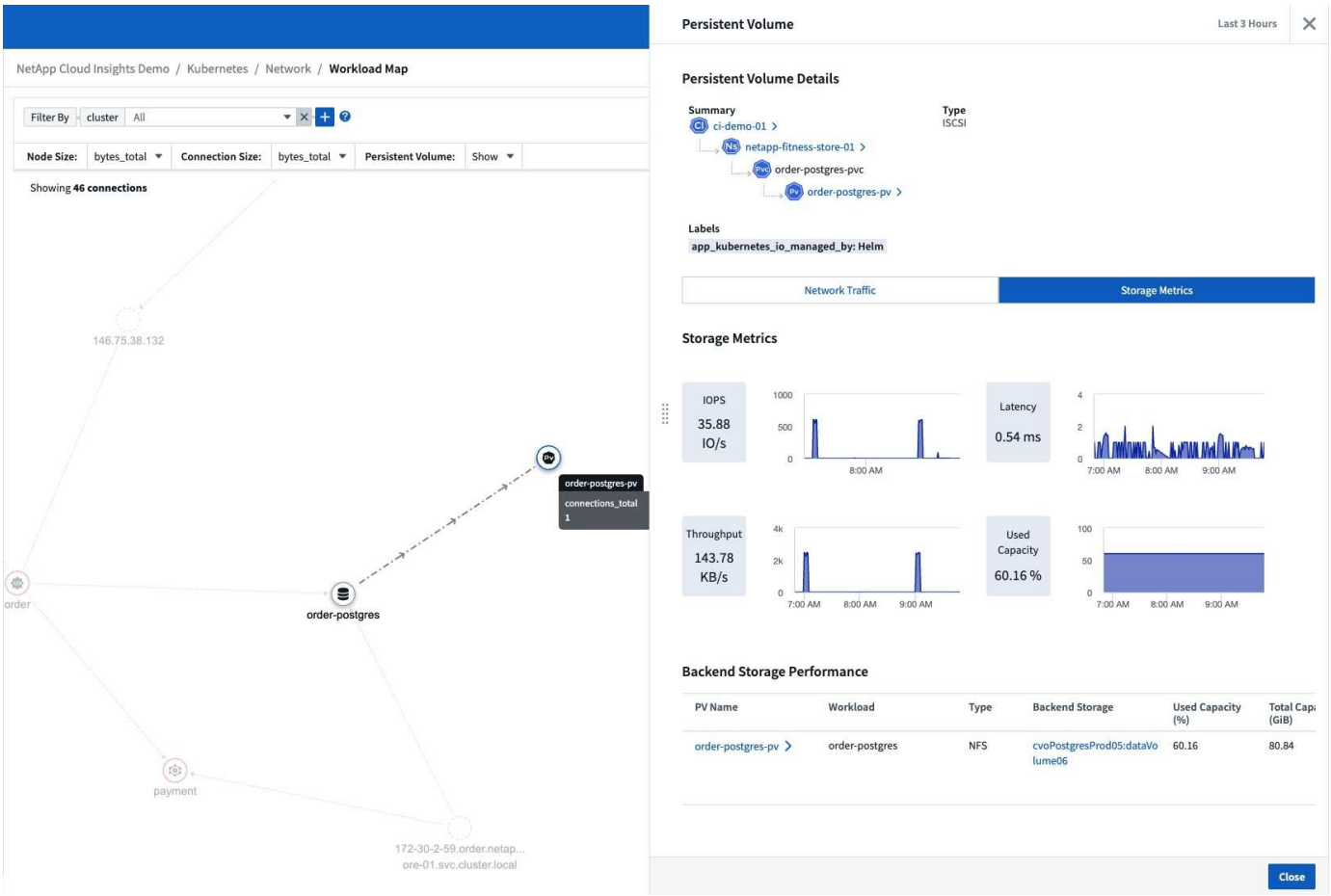
Les alertes de journal peuvent désormais être résolues en fonction de l'heure. Si la condition d'alerte cesse de se produire, Cloud Insights peut résoudre l'alerte automatiquement après un délai spécifié. Vous pouvez choisir de résoudre l'alerte en minutes, heures ou jours.



Avril 2024

Prise en charge d'iSCSI pour Kubernetes

Cloud Insights prend désormais en charge la cartographie du stockage iSCSI associé à Kubernetes, ce qui accélère le dépannage à l'aide de la carte réseau Kubernetes et permet de fournir des rapports de facturation interne ou de justification via le reporting.



Systèmes d’exploitation pris en charge

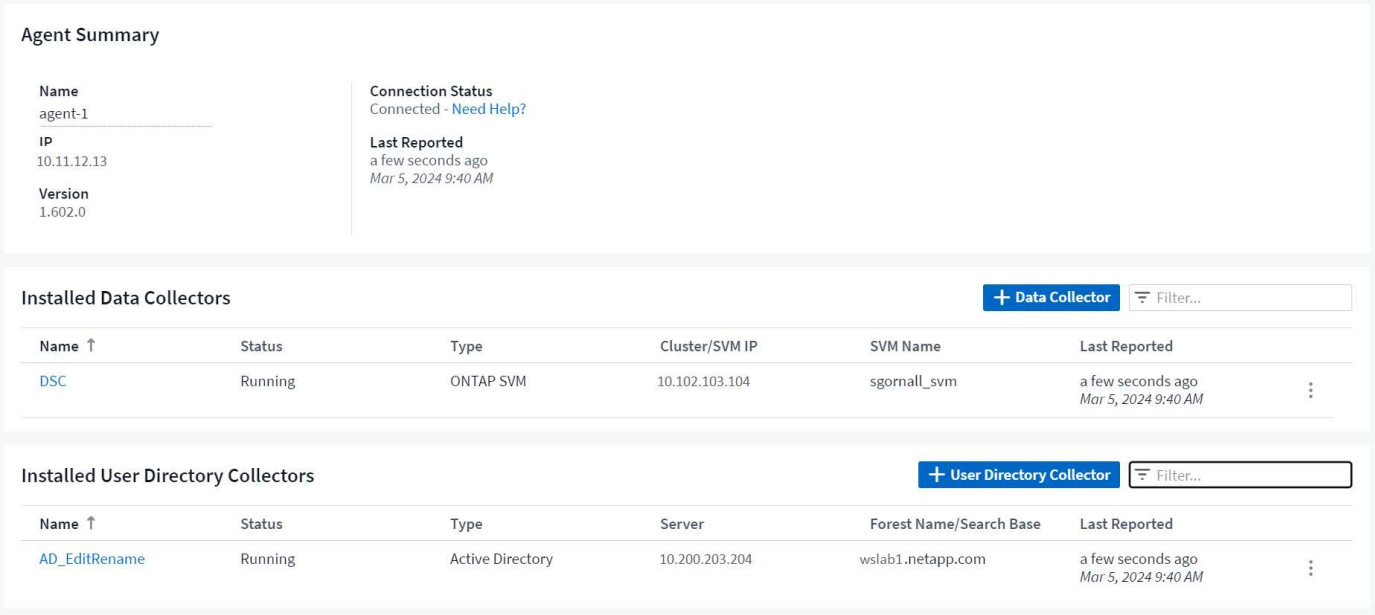
Les systèmes d’exploitation suivants sont pris en charge avec les unités d’acquisition Cloud Insights, en plus de ceux"déjà pris en charge"-ci :

- 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

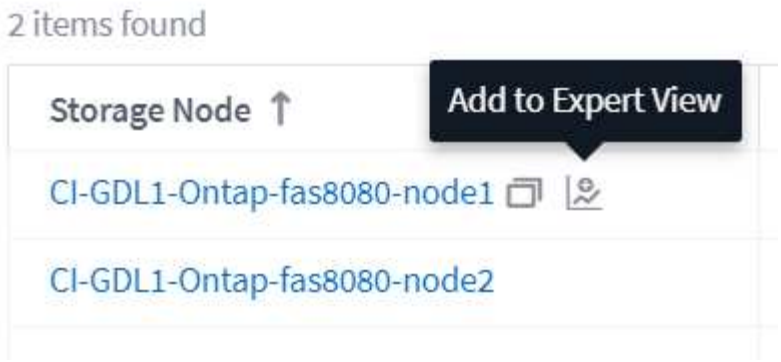
Détails de l’agent de sécurité de la charge de travail

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

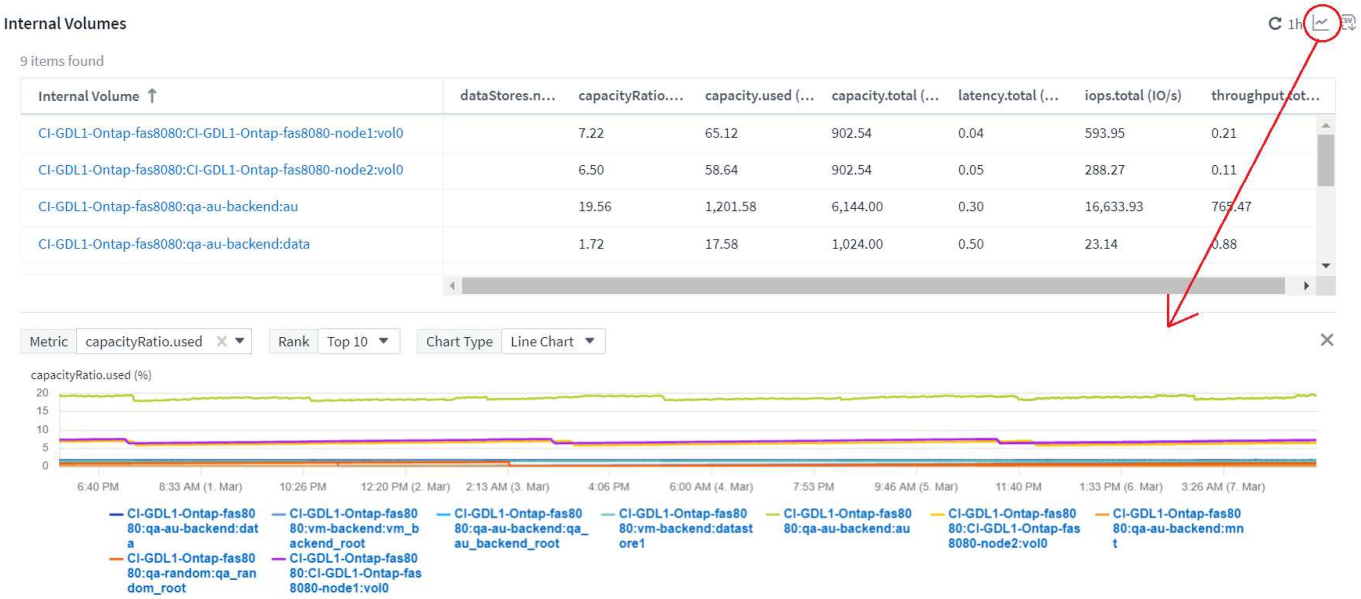


Tracez plus rapidement davantage de données

Lors de l’analyse de données sur la page d’accueil d’une ressource, l’ajout de données supplémentaires aux graphiques de la vue Expert est un jeu d’enfant. Pour chaque table de la page d’accueil, si un type d’objet contient des données pertinentes, placez le pointeur de la souris sur cet objet pour afficher l’icône « Ajouter à la vue experte ». La sélection de cette icône ajoute cet objet aux Ressources supplémentaires et l’affiche dans les graphiques de la vue Expert.



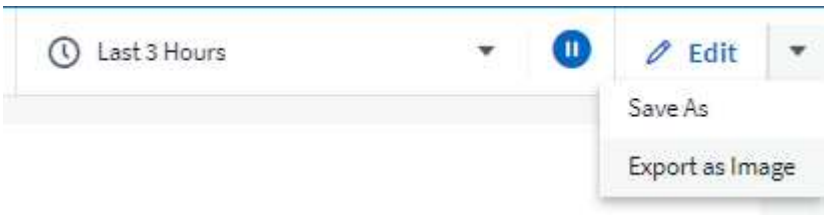
Ou peut-être voulez-vous voir les données d'une table de page d'accueil dans son propre graphique. Il vous suffit de sélectionner l'icône *Afficher le diagramme* pour ouvrir le graphique sous le tableau :



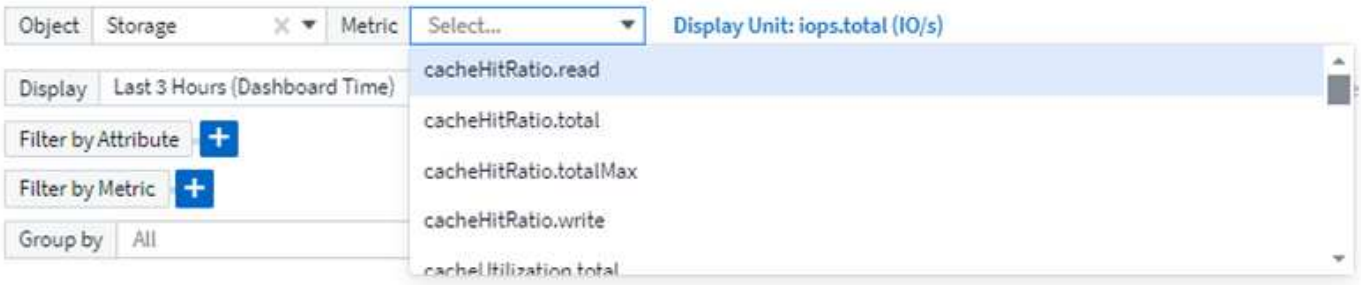
Février 2024

Facilité d'utilisation améliorée

Enregistrez un **instantané** de votre tableau de bord actuel en sélectionnant *Exporter en tant qu'image* dans le menu déroulant situé dans le coin droit. Cloud Insights crée un fichier .PNG des États de widget actuels.



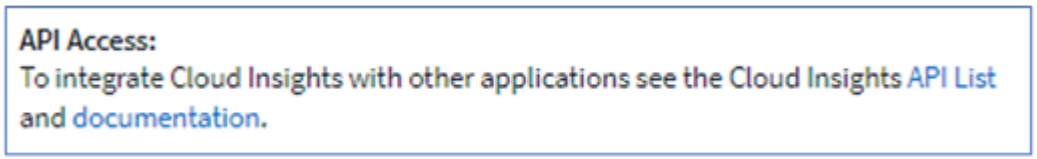
La sélection d'objet et de métrique est plus facile que jamais pour Widgets, moniteurs, etc. Choisissez le type d'objet souhaité, puis sélectionnez une mesure pertinente pour cet objet dans la liste déroulante séparée.



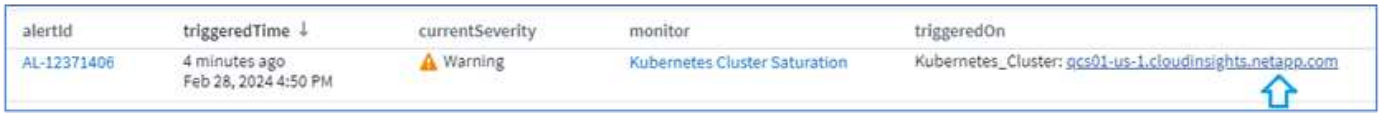
Exporter les listes Data Collector et acquisition Unit au format .CSV en sélectionnant l'icône en haut de ces pages.



Nous avons **ré-organisé la page aide > support** afin de trouver plus facilement ce que vous cherchez, et comme vous l'avez demandé, nous avons ajouté des liens directs sur cette page vers **API swagger** et la documentation utilisateur.

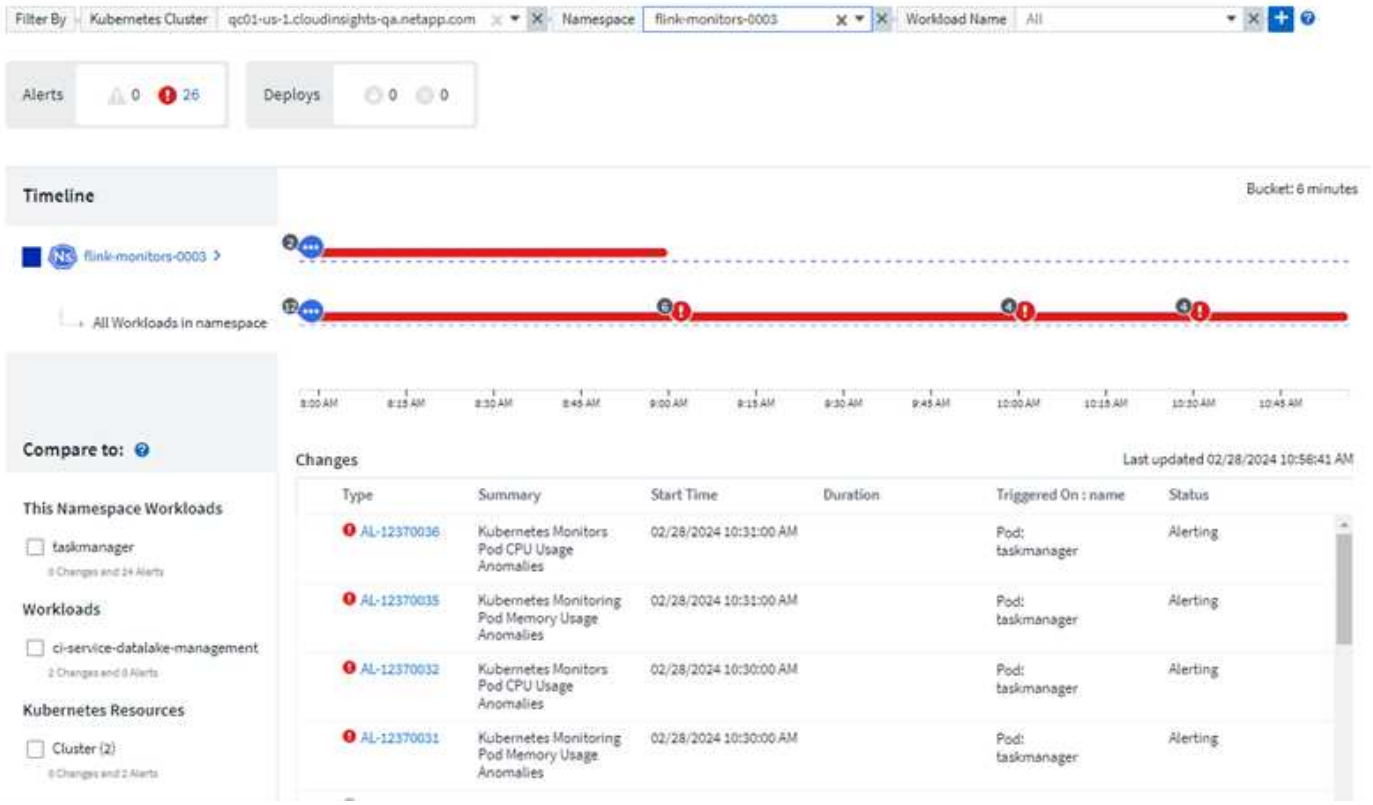


Links dans la colonne « trigeredOn » de la page de liste alertes, vous accédez à la page de destination appropriée, si une page de destination est disponible pour cet objet.



Voir toutes les modifications apportées à votre espace de noms

L'analyse des changements Kubernetes vous permet désormais d'afficher une chronologie des modifications lors de la sélection du cluster et de l'espace de noms. Auparavant, la charge de travail doit également avoir été sélectionnée. Lors du filtrage sur le cluster et l'espace de noms, la chronologie des modifications de tous les workloads dans cet espace de noms s'affiche sur une ligne.



Journaux associés pour les 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 en savoir plus.



Collecter les données du commutateur ONTAP

Cloud Insights peut collecter des données à partir des commutateurs back-end du système ONTAP ; il vous suffit d'activer la collecte dans la section *Configuration avancée* du collecteur de données et de vous assurer que le système ONTAP est configuré pour fournir "informations sur le commutateur" et dispose de l'ensemble approprié"autorisations".

API Data Collector de Workload Security

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 *Workload Security* pour en savoir plus.

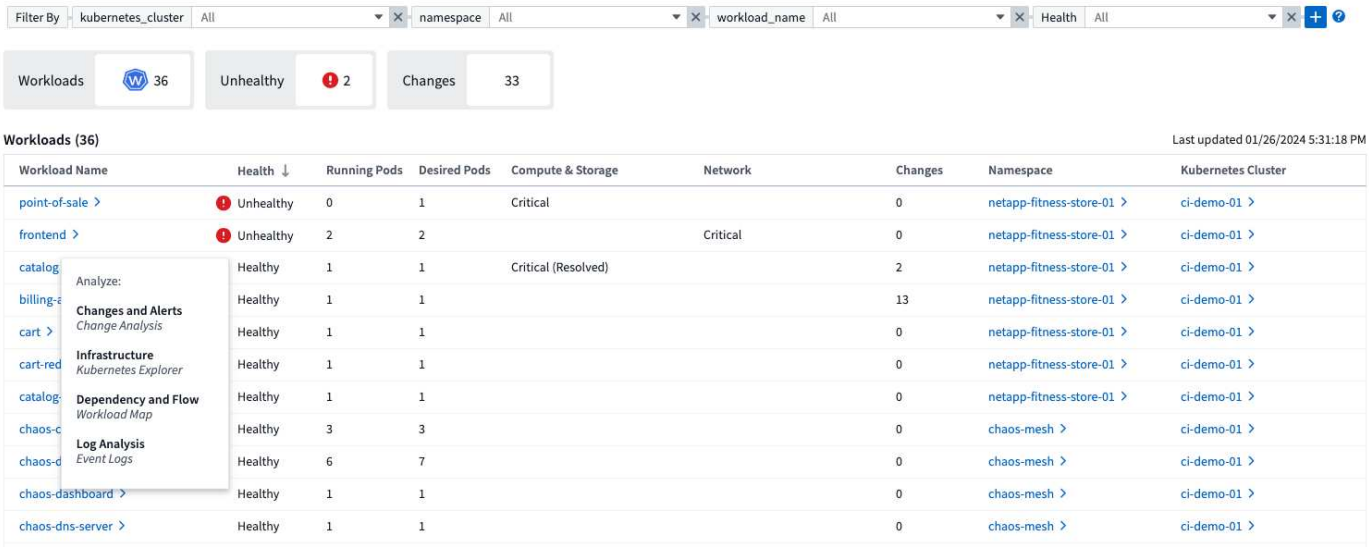
Janvier 2024

Essayez des fonctionnalités Cloud Insights que vous n'avez pas encore utilisées

En plus de votre essai initial de Cloud Insights, vous pouvez également profiter de "Évaluations du module". Par exemple, si vous êtes abonné à Cloud Insights et que vous avez surveillé le stockage et les machines virtuelles, lorsque vous ajoutez Kubernetes à votre environnement, vous essai automatique de 30 jours de l'observabilité Kubernetes. L'utilisation d'unités gérées d'observabilité Kubernetes ne compte pas sur vos droits souscrits avant la fin de la période d'essai.

Mes workloads sont-ils sains ?

L'état des workloads est disponible en un coup d'œil sur la page **Kubernetes > Explore > workloads**. Vous pouvez ainsi identifier rapidement les workloads qui fonctionnent correctement et ceux qui ont besoin d'aide. Identifiez facilement si le problème d'intégrité est lié à des modifications de l'infrastructure, du réseau ou de la configuration, puis explorez la source des problèmes pour en analyser la cause.



Mises à jour du Data Collector

Identification Data Domain

Le collecteur Data Domain a été amélioré afin de mieux identifier les systèmes haute disponibilité pour la durabilité lors des événements de basculement. Cette modification entraînera une réidentification **unique** des appliances Data Domain dans les systèmes haute disponibilité, ce qui entraînera la suppression des annotations sur ces ressources (car ces baies seront réidentifiées). Vous devrez rattacher des annotations à vos objets Data Domain.

Algorithme amélioré de détection DES ransomwares par ML

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

« Saisonnalité » des comportements : le comportement du week-end peut suivre des modèles différents par rapport au jour de la semaine ou au comportement du matin par rapport à l'après-midi. Les algorithmes de sécurité des workloads tiennent compte de cette saisonnalité.

Fonctionnalités obsolètes

Les fonctionnalités sont parfois obsolètes à mesure que les fonctions évoluent. Voici quelques-unes des fonctionnalités qui ont été obsolètes dans Cloud Insights :

L'API de workload Secure REST cloudSecure_Forensics.Activities.v1 est obsolète

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

OBTENIR pour cette API a précédemment renvoyé ce qui suit :

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

Cette API renvoie maintenant :

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

Pour plus d'informations, consultez la documentation de swagger à l'adresse suivante : « Admin > API Access > API Documentation > Workload Security ».

Décembre 2023

Analyse des changements en un coup d'œil

Kubernetes "Analyse des changements"vous offre une vue complète des modifications récentes de 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 mettre en corrélation avec l'état et les performances des services, de l'infrastructure et des clusters K8s.

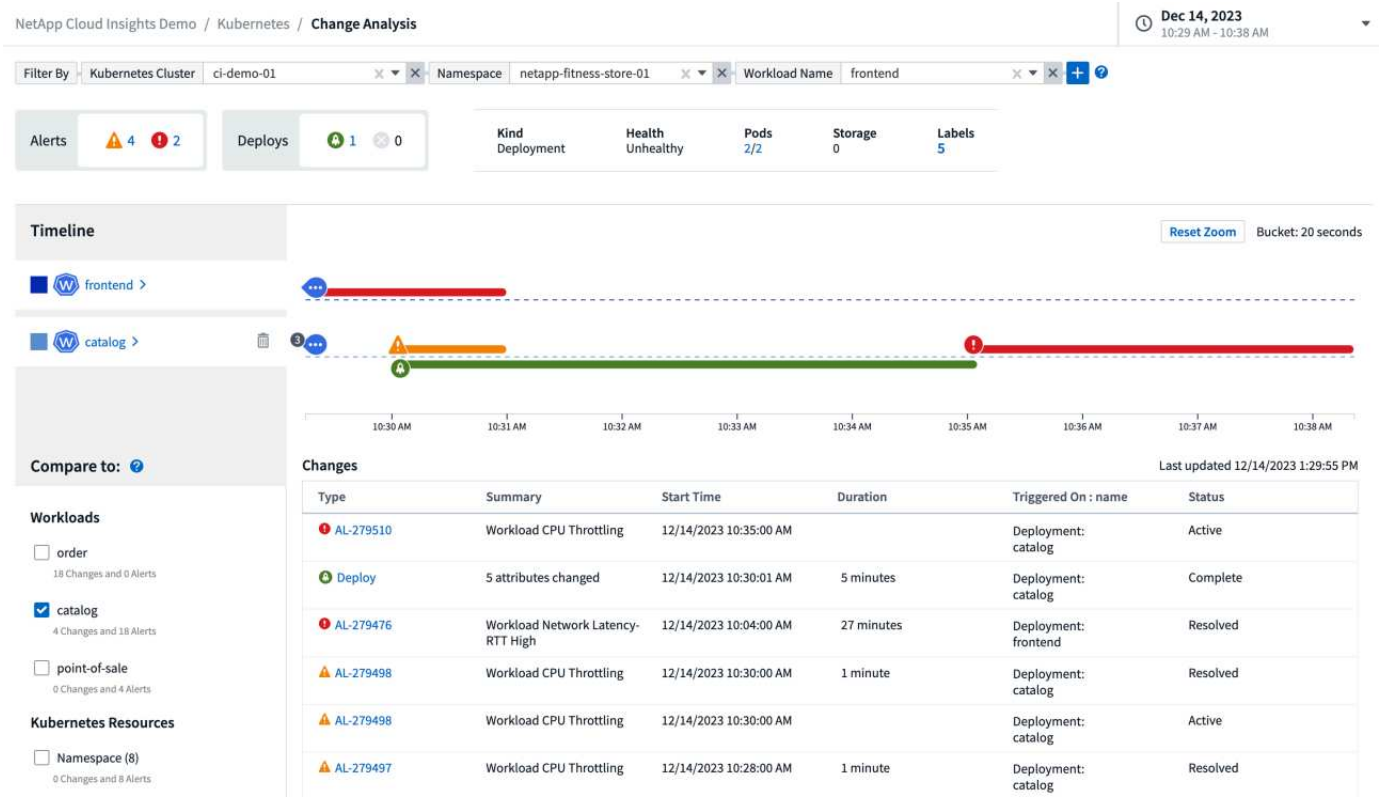
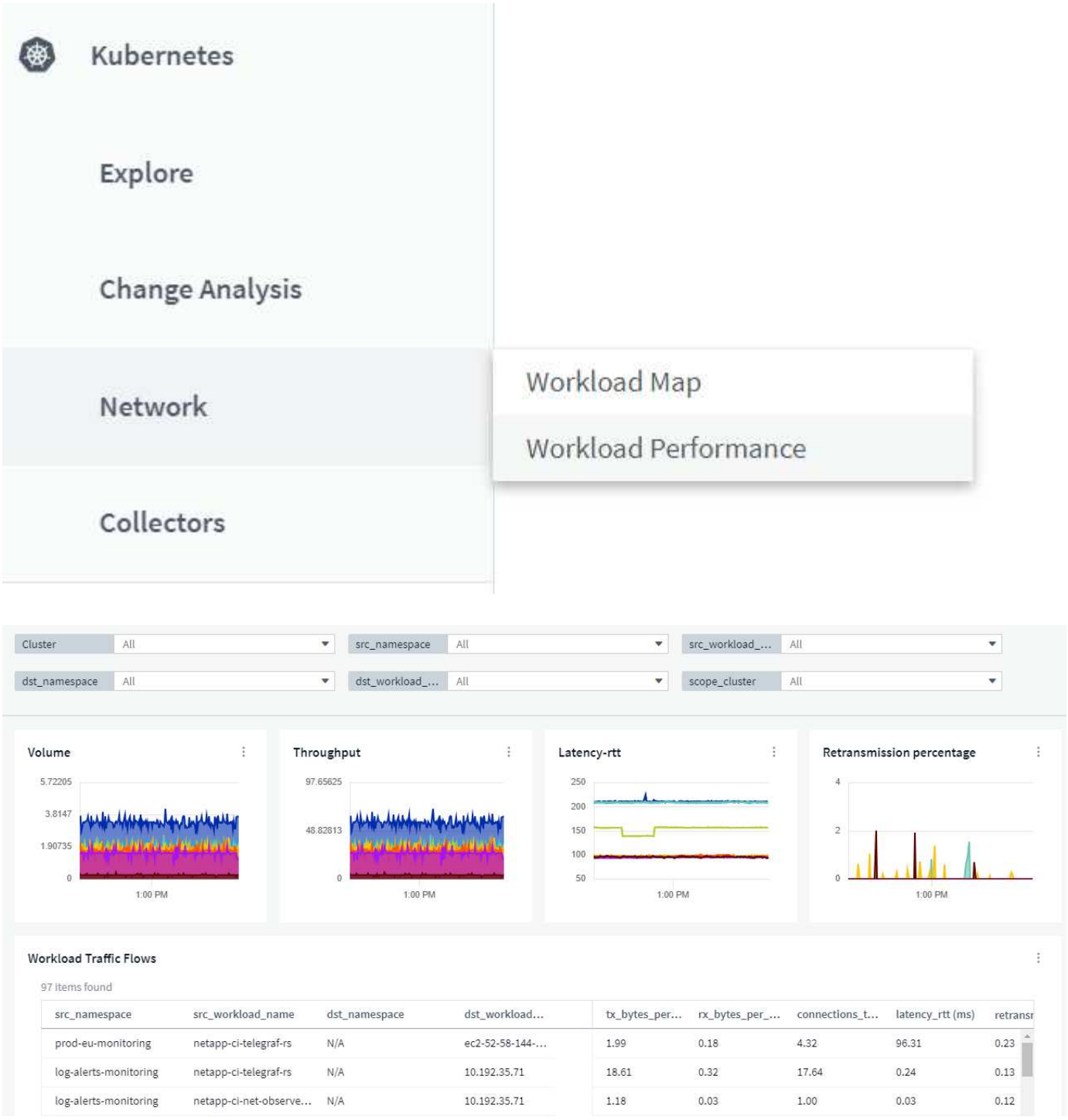


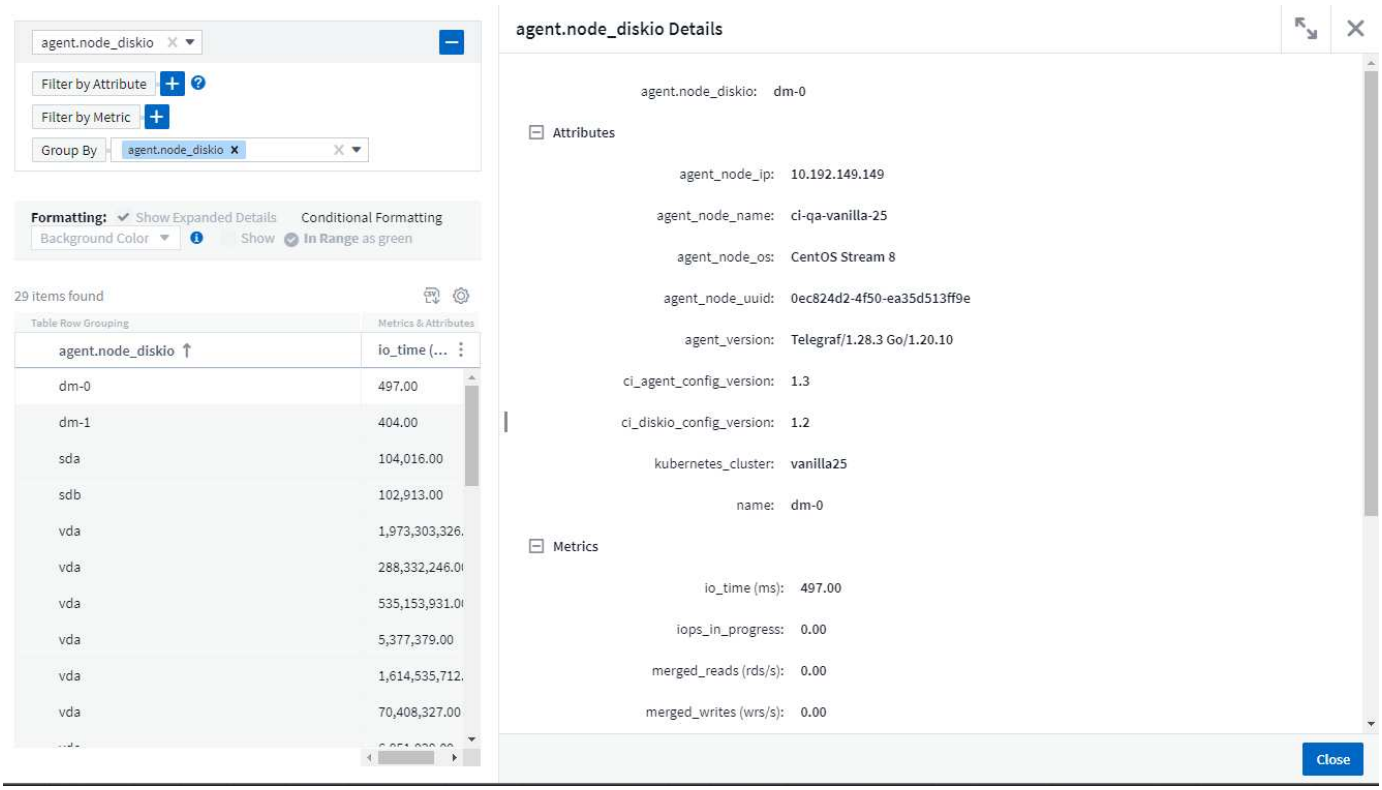
Tableau de bord des performances des workloads Kubernetes

Les performances des workloads sont disponibles en un coup d'œil dans le tableau de bord complet des performances des workloads Kubernetes. Affichez rapidement des graphiques des tendances Volume, débit, latence et retransmission, ainsi qu'un tableau du trafic des charges de travail pour chaque espace de noms de votre environnement. Les filtres facilitent la mise au point sur les zones d'intérêt.



Détails de la requête sur un écran

Dans une requête, la sélection d'une ligne ouvre un panneau latéral affichant les détails d'attribut, d'annotation et de mesure pour la ligne sélectionnée, fournissant des informations utiles sans avoir à explorer la page d'accueil de l'objet. Les liens de la rangée ou du panneau latéral facilitent la navigation.



Mises à jour du Data Collector :

- **Brocade FOS REST**: Ce collecteur est déplacé hors de "Prévisualisation" et est maintenant 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 que des fonctionnalités d'API REST avec la version 9.0.
  - Si vous disposez d'une structure composée de plusieurs actifs FOS de 8.2 versions supérieures, ainsi que de moins de 8.2, le collecteur de REPOS FOS Cloud Insights ne pourra pas détecter ces anciens actifs. Vous pouvez modifier le collecteur de REPOS FOS et créer une liste séparée par des virgules de l'adresse IPv4 de ces périphériques pour exclusion de ce collecteur.
- **SELinux**: Cloud Insights inclut des améliorations à l'installation initiale de l'unité d'acquisition Linux pour assurer la robustesse du fonctionnement dans les environnements Linux avec l'application SELinux activée. Ces améliorations n'ont qu'un impact sur les déploiements *New* au ; si vous rencontrez des problèmes SELinux liés aux mises à niveau au, contactez le support NetApp pour résoudre votre configuration SELinux.

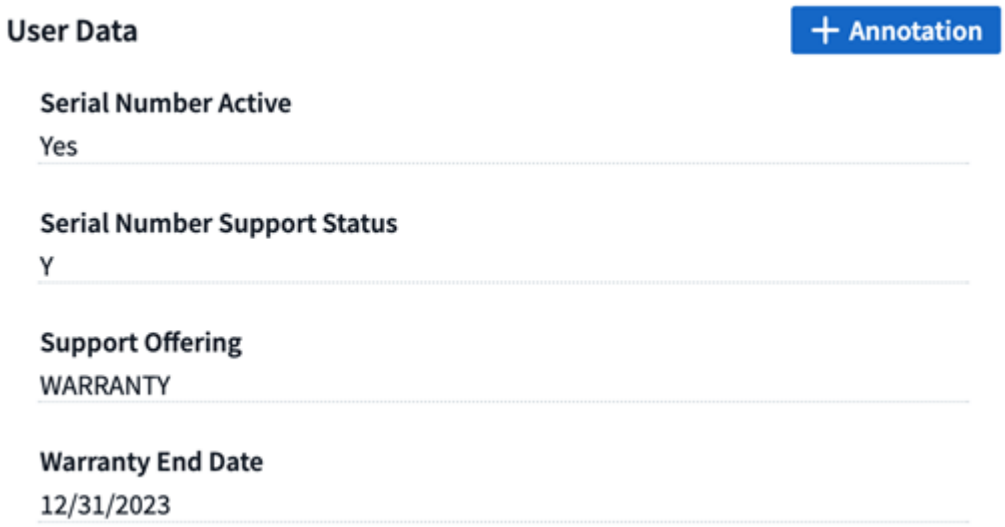
Novembre 2023

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

Dans Workload Security, vous pouvez mettre en pause un Data Collector si le collecteur est à l'état *running*. Ouvrez le menu « trois points » du collecteur et sélectionnez PAUSE. Lorsque le collecteur est en pause, aucune donnée n'est collectée à partir de ONTAP et aucune donnée n'est envoyée du collecteur vers ONTAP. Sélectionnez reprendre pour recommencer la collecte.

Informations sur la prise en charge du nœud de stockage

Sur la page d'accueil d'un nœud de stockage, la section *données utilisateur* fournit des informations d'un coup d'œil sur votre offre de support, votre statut actuel, votre statut du support et la date de fin de garantie. Notez que Cloud Insights ne publie actuellement que ces informations pour les terminaux NetApp. Notez également que ces champs de support sont des annotations, de sorte qu'ils peuvent être utilisés dans les requêtes et les tableaux de bord.



Mapper les balises VMware aux annotations Cloud Insights

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

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

Sur certains commutateurs Brocade Fibre Channel exécutant le micrologiciel 9.1.1c, le résultat de certaines commandes de l'interface de ligne de commande peut être précédé du texte de la bannière de connexion « motd » ou des avertissements pour que les utilisateurs modifient les mots de passe par défaut. Le collecteur CLI Brocade a été amélioré pour ignorer ces deux types de texte étranger.

Avant cette amélioration, seuls les commutateurs FOS 9.1.1c sans structure virtuelle étaient susceptibles d'être détectés avec ce type de collecteur.

Octobre 2023

Sécurité améliorée des workloads

La sécurité des charges de travail a été améliorée grâce aux éléments suivants :

- **Accès refusé** : la sécurité de la charge de travail s'intègre à ONTAP pour recevoir "Événements « accès refusé »" et fournir une couche supplémentaire d'analyse et de réponses automatiques.
- **Autorisé types de fichiers** : si une attaque par ransomware est détectée pour une extension de fichier

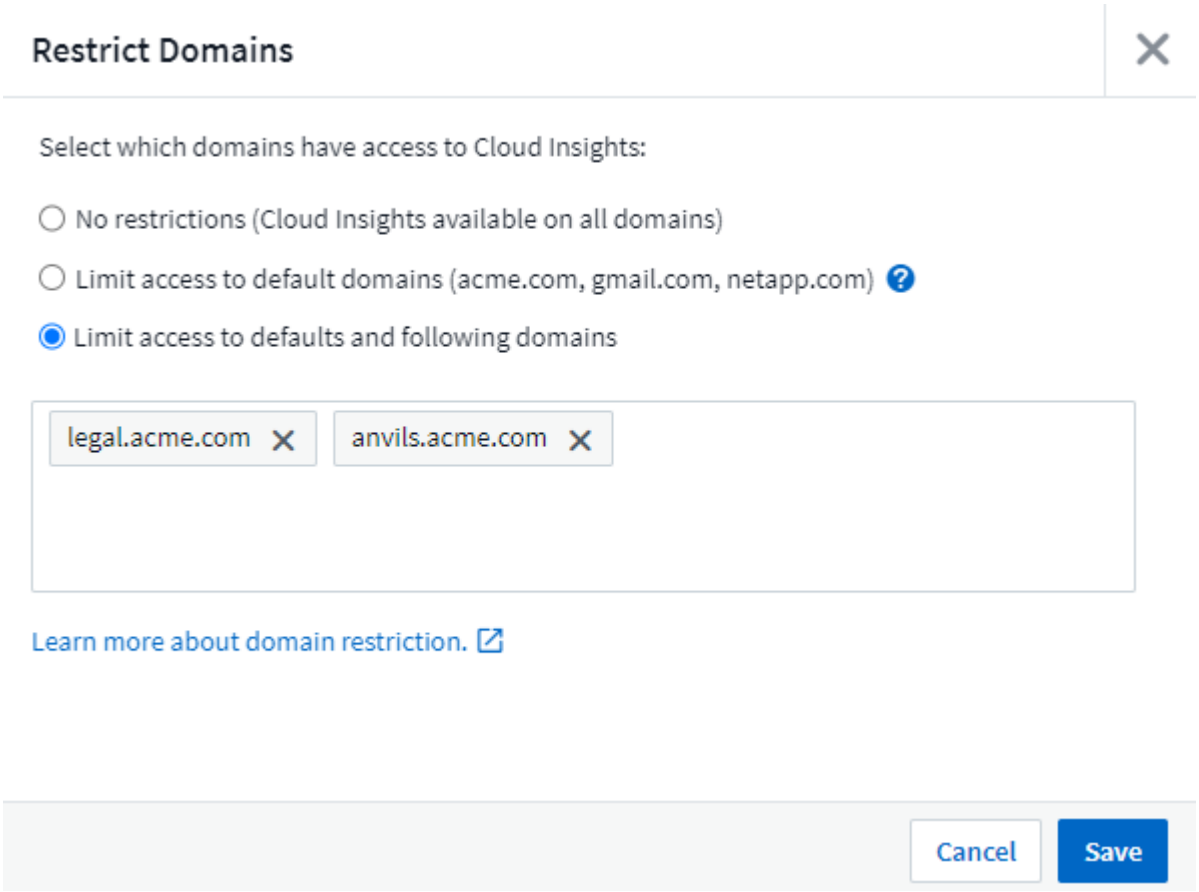
connue, cette extension de fichier peut être ajoutée à une "types de fichiers autorisés" liste pour empêcher des alertes inutiles.

Essais de module

En plus de votre essai initial de Cloud Insights, vous pouvez également profiter de "Évaluations du module". Par exemple, si vous êtes déjà abonné à l'observabilité de l'infrastructure, mais que vous ajoutez Kubernetes à votre environnement, vous exécuterez automatiquement un essai de 30 jours de l'observabilité Kubernetes. Vous ne serez facturé que pour l'utilisation de votre unité gérée d'observabilité Kubernetes à la fin de la période d'évaluation.

Restreindre l'accès aux domaines spécifiés

Les administrateurs et les propriétaires de compte ont désormais la possibilité d'"Limitez l'accès Cloud Insights"envoyer des adresses électroniques aux domaines qu'ils spécifient. Accédez à **Admin > gestion des utilisateurs** et sélectionnez le bouton *restreindre les domaines*.



Mises à jour du Data Collector

Les modifications suivantes du Data Collector/de l'unité d'acquisition sont en place :

- **Isilon / PowerScale REST** : plusieurs 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 permettent aux utilisateurs de créer des tableaux de bord et des moniteurs pour la consommation de la capacité *node_pool* ; les utilisateurs avec des clusters Isilon construits à partir de modèles de nœuds différents disposent de plusieurs pools de nœuds. Il est donc utile de comprendre la consommation de votre disque dur/SSD/capacité totale au niveau d'un pool de nœuds 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 HTTP basique (nom d'utilisateur et mot de passe) classique et l'approche de compte de service de Rubrik, qui nécessite un nom d'utilisateur + un secret + un ID d'organisation.

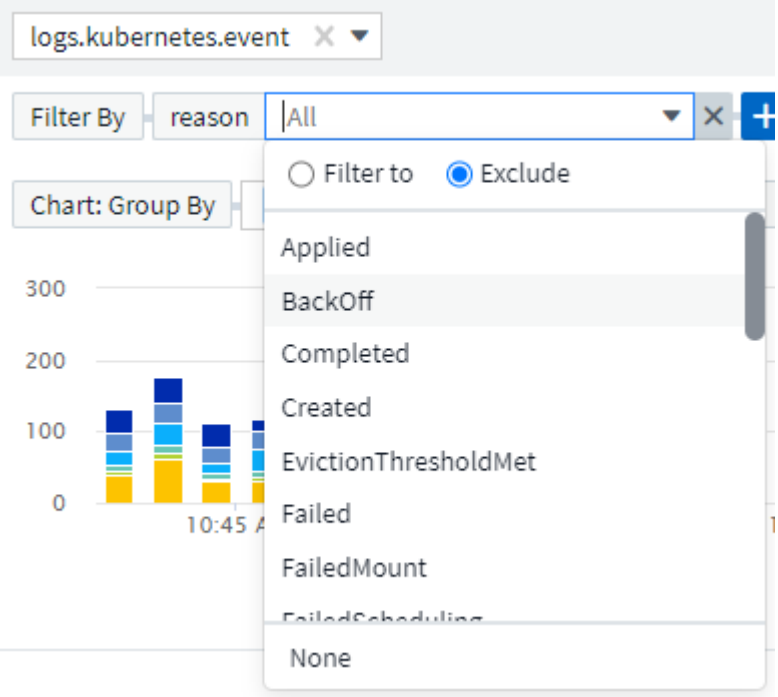
Septembre 2023

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 faciliter l'exploration des journaux et les rendre plus informatives.

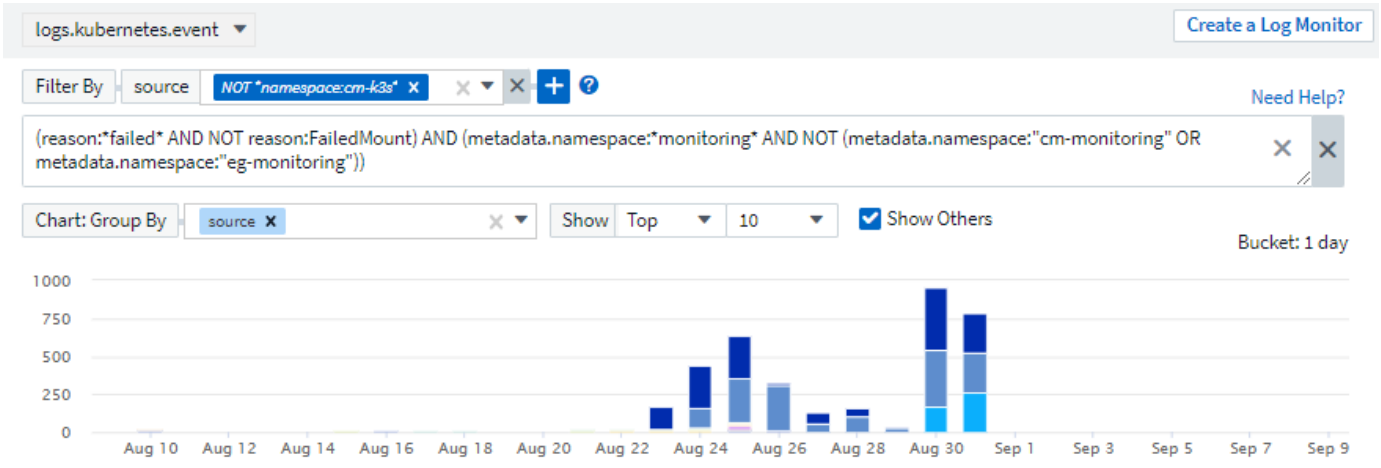
Inclure/exclure

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



Requête avancée

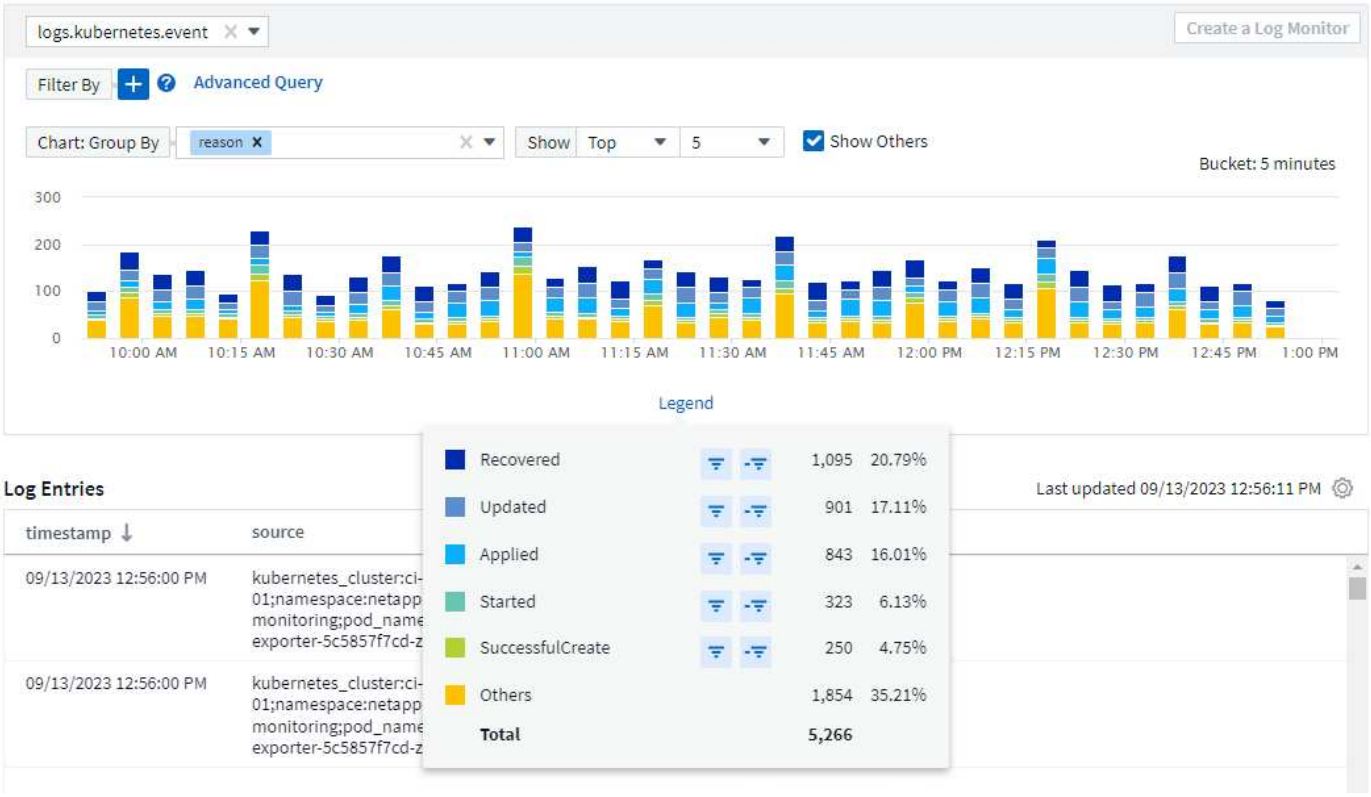
Advanced Querying vous donne la possibilité de créer des filtres "forme libre", combinant ou excluant des valeurs en utilisant ET, PAS, OU, des caractères génériques, etc



Les options « Filtrer par » et « requête avancée » sont « ET « td » ensemble pour former une seule requête. Les résultats sont affichés dans la liste de résultats et dans le graphique.

Regroupement dans le graphique

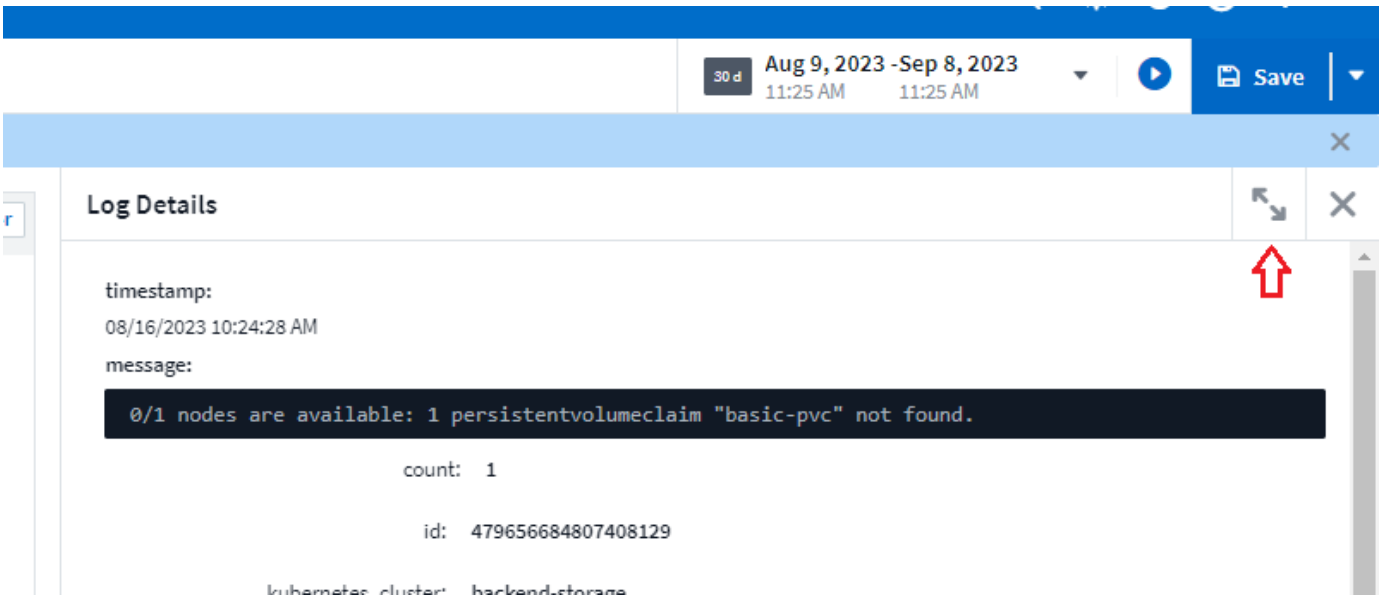
Lorsque vous sélectionnez un attribut de journal dans **Grouper par**, la liste et le graphique affichent les résultats du filtre actuel. Dans le graphique, colonnes regroupées en couleurs. Passez le curseur sur une colonne du graphique pour afficher des détails sur les entrées spécifiques, similaires 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 »

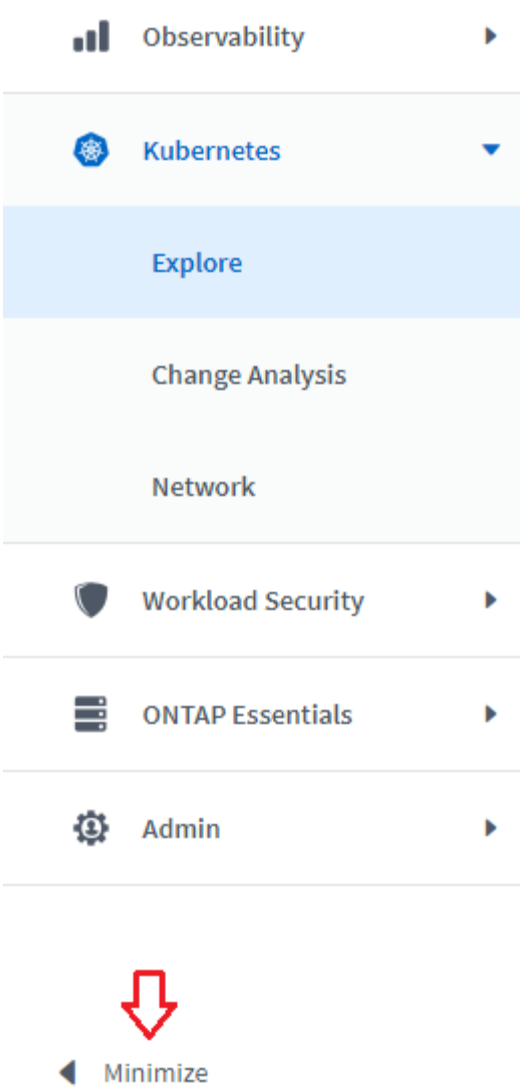
Lors de l'exploration des journaux à l'aide de la requête de journal, la sélection d'une entrée dans la liste ouvre un panneau de détails pour cette entrée. Vous pouvez maintenant choisir d'afficher ce panneau coulissant «

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



Réduire le menu

Vous pouvez réduire le menu de navigation Cloud Insights de gauche en sélectionnant le bouton « réduire » sous le menu. Lorsque le menu est réduit, passez le curseur sur une icône pour voir la section qui s'ouvre ; sélectionnez l'icône pour ouvrir le menu et accéder directement à cette section.



Améliorations du Data Collector

Cloud Insights a facilité l'affichage et la recherche des informations du collecteur de données :

- **Le traitement des listes de collecteurs de données** est plus efficace, ce qui signifie que le temps nécessaire pour afficher et naviguer dans ces listes est considérablement réduit. Si vous avez un grand environnement avec de nombreux collecteurs de données, vous verrez une amélioration significative en listant vos collecteurs de données.
- La **Data Collector support Matrix** est passée d'un fichier .PDF à une page .HTML, plus rapide à naviguer et plus facile à entretenir. Découvrez la nouvelle matrice 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 REST Isilon et REST PowerScale contiennent les améliorations suivantes :

- Les événements du journal Isilon sont disponibles pour les requêtes et les alertes
- Les attributs Isilon Advanced Analytic 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

Ils sont activés par défaut pour les utilisateurs des collecteurs REST Isilon et/ou REST PowerScale. NetApp encourage vivement 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.

Amélioration de la cartographie des charges de travail

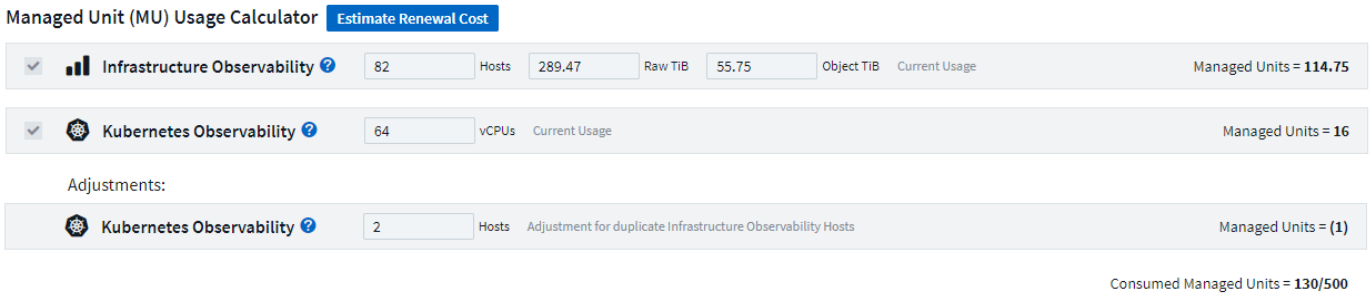
La carte des charges de travail est plus utilisable et moins bruyante. Elle regroupe tous les services externes similaires en un seul nœud s'ils communiquent avec les mêmes charges de travail, ce qui réduit la complexité du graphique et facilite la compréhension de l'interconnexion des services.

La sélection d'un nœud groupé affiche un tableau détaillé avec les mesures du trafic réseau pour chaque service externe correspondant à ce nœud.

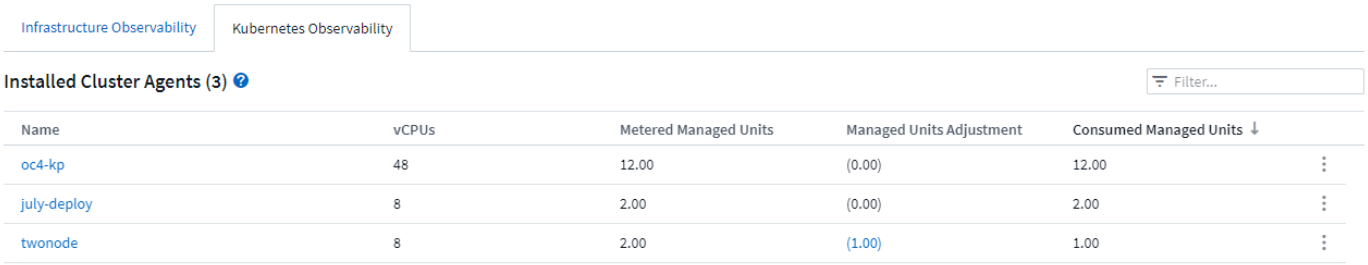
Ajustement de l'utilisation des unités gérées Kubernetes

Si une ressource de calcul est comptabilisée dans l'environnement de cluster Kubernetes par l'opérateur de surveillance NetApp Kubernetes et un collecteur de données d'infrastructure sous-jacente (par exemple, VMware), l'utilisation de ces ressources sera ajustée pour assurer le comptage le plus efficace des unités gérées. Vous pouvez afficher les ajustements des UM Kubernetes sur la page Admin > abonnement, dans les onglets Résumé et utilisation.

Onglet Résumé :



Onglet utilisation :



Modifications du collecteur/de l'acquisition :

Les modifications suivantes du Data Collector/de l'unité d'acquisition sont en place :

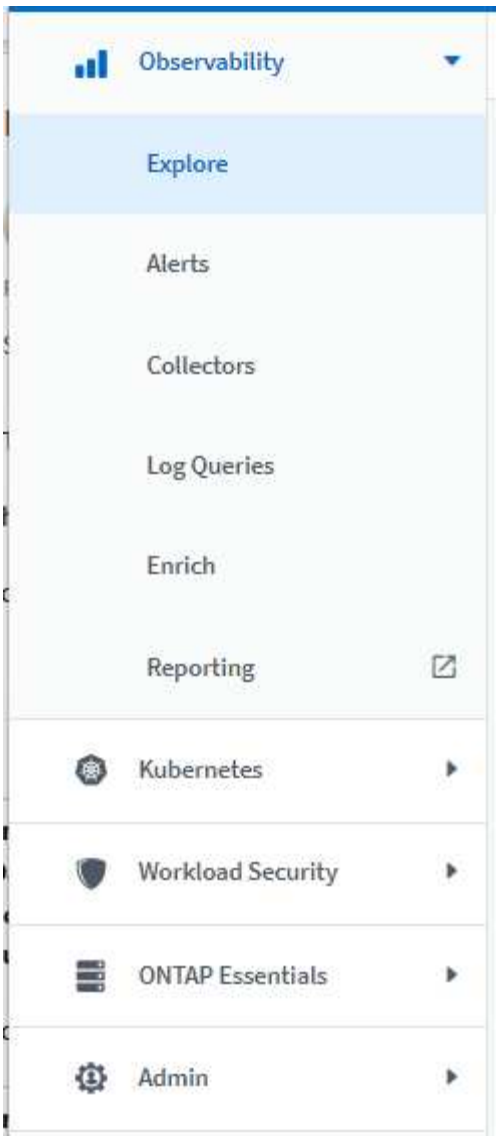
- Les unités d'acquisition prennent désormais en charge RHEL 8.7.

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. Les nouveaux éléments de premier plan, tels que *Kubernetes*, accélèrent l'accès à ce dont le client a besoin, et la console d'administration consolidée prend en charge le rôle de propriétaire du locataire.

Voici quelques exemples supplémentaires de ces modifications :

- Le menu *observabilité* de premier niveau présente la découverte de données, les alertes et les requêtes de journal
- La fonctionnalité d'accès aux API pour l'observabilité et la sécurité des workloads se trouve dans un seul menu
- De même pour les fonctionnalités d'observabilité et de notification de sécurité des workloads, désormais disponibles dans un seul menu



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

Observabilité :

- Explore (tableaux de bord, requêtes relatives aux indicateurs, 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)
- Création de rapports

Kubernetes :

- Exploration de cluster et carte réseau

Sécurité des workloads :

- Alertes

- Médecine légale
- Collecteurs
- Stratégies

ONTAP Essentials :

- Protection des données
- Sécurité
- Alertes
- Infrastructures
- Mise en réseau
- Workloads *VMware

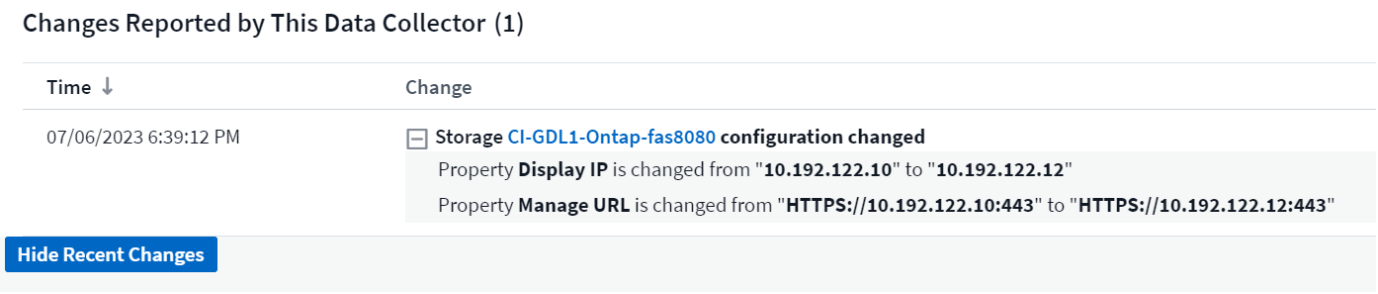
Admin :

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

Juillet 2023

Afficher les modifications récentes

Les pages d'accueil du Data Collector incluent désormais une liste des modifications récentes. Il vous suffit de cliquer sur le bouton « modifications récentes » en bas de toute page d'accueil du collecteur de données pour afficher les modifications récentes du collecteur de données.



Améliorations pour l'opérateur

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

- Option permettant de contourner la collection de mesures docker
- Possibilité d'ajouter et de personnaliser des tolérances à des démonstrateurs et des réplicajeux telegraf

Insight : récupération du stockage à froid

Le système "Récupération d'ONTAP Cold Storage Insight"prend désormais en charge FlexGroups et est désormais disponible pour tous les clients.

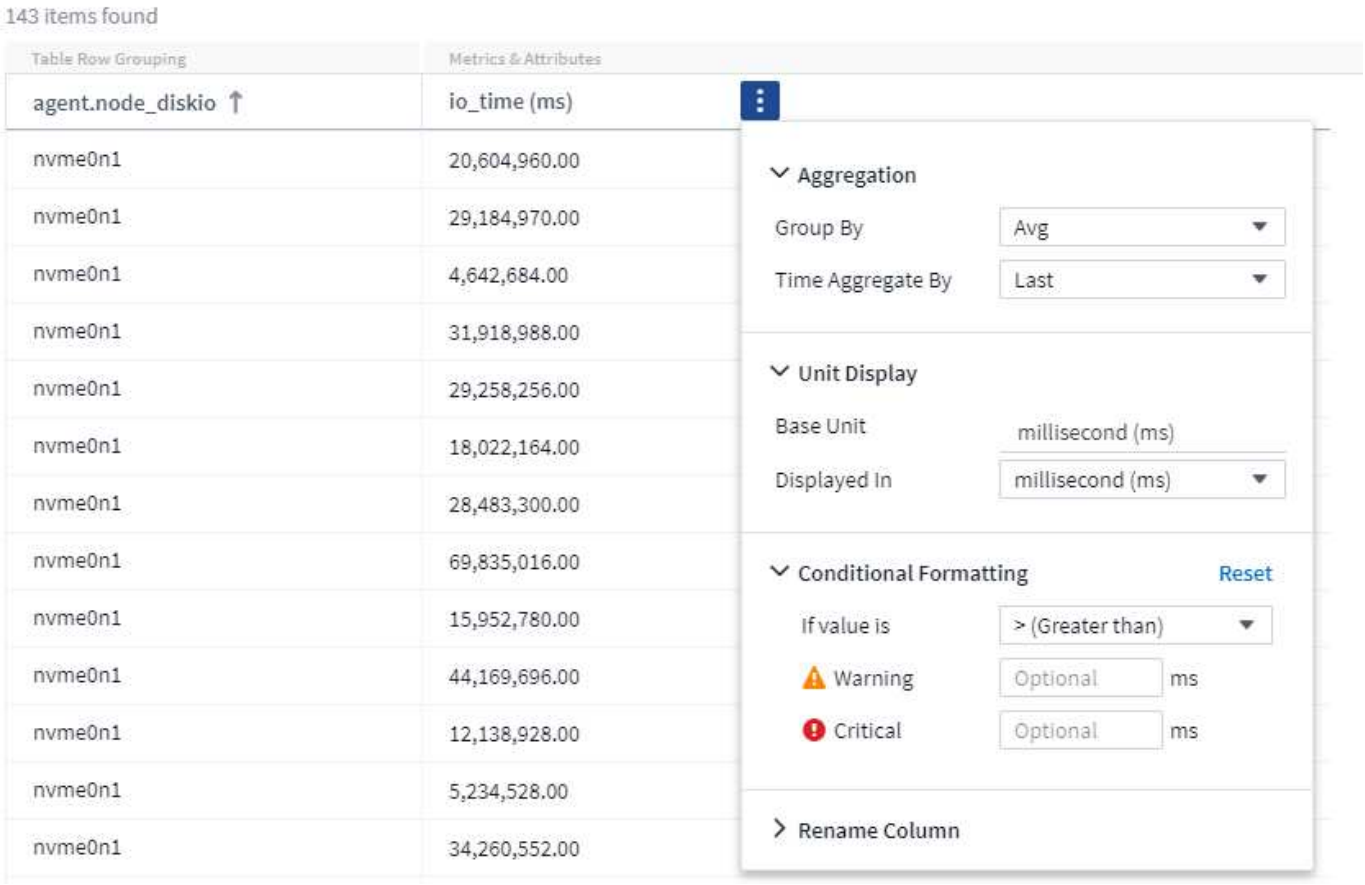
Signature de l'image de l'opérateur

Pour les clients qui utilisent un référentiel privé pour leur opérateur de surveillance Kubernetes NetApp, 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, etc. Pour les requêtes

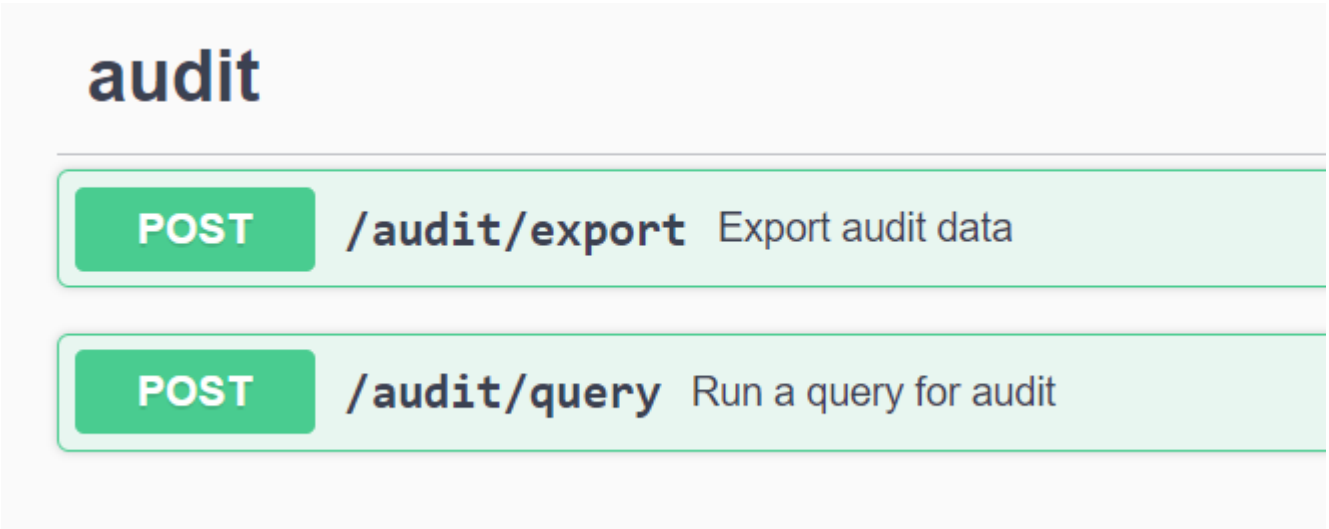
L'agrégation, la sélection d'unité, la mise en forme conditionnelle et le renommage de colonne sont parmi les fonctionnalités les plus utiles d'un widget de tableau de bord, et ces mêmes fonctionnalités sont maintenant disponibles pour "Requêtes".



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

API pour l'audit

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



Data Collector : économie de Trident

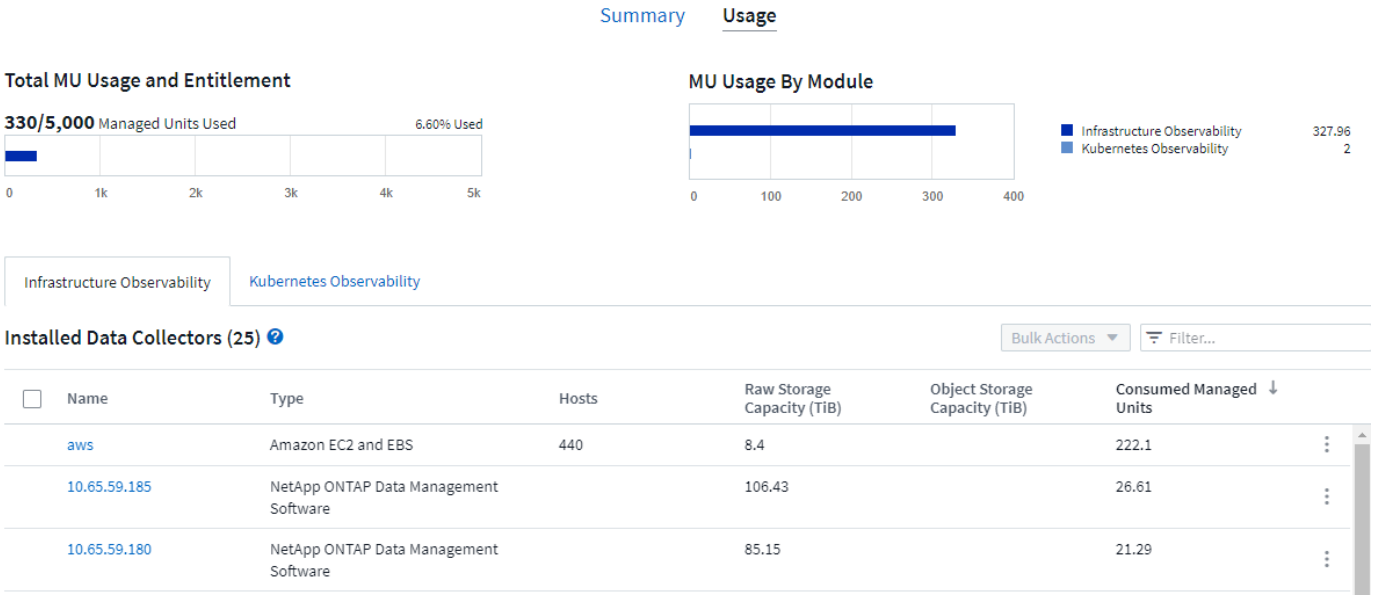
Cloud Insights prend désormais en charge le pilote d'économie Trident, en bénéficiant des avantages suivants :

- Visibilité sur le mappage qtree entre pods et ONTAP et les metrics de performance.
- Dépannage transparent et navigation aisée des pods Kubernetes vers le stockage back-end
- Détectez de manière proactive les problèmes de performances back-end à l'aide de moniteurs

Juin 2023

Découvrez votre utilisation

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



La surveillance et le mappage du réseau Kubernetes sont disponibles pour tous

"*Performances du réseau Kubernetes et mappage*"Simplifie la résolution des problèmes en mappant les dépendances entre les workloads Kubernetes, offrant ainsi une visibilité en temps réel sur les latences des performances du réseau et les anomalies pour identifier les problèmes de performance avant qu'ils n'affectent les utilisateurs. De nombreux clients l'ont trouvé utile lors de l'aperçu, et maintenant il est disponible pour tous les goûts.

Modifications du collecteur/de l'acquisition :

Les modifications suivantes du Data Collector/de l'unité d'acquisition sont en place :

- Les MU Data Domain et Cohesity sont mesurées à 40 Tio : 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 sont désormais disponibles dans les environnements de prévisualisation et sont désormais disponibles pour tous :

- Tableau de bord de sécurité
- Tableau de bord de protection des données (inclut les présentations 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

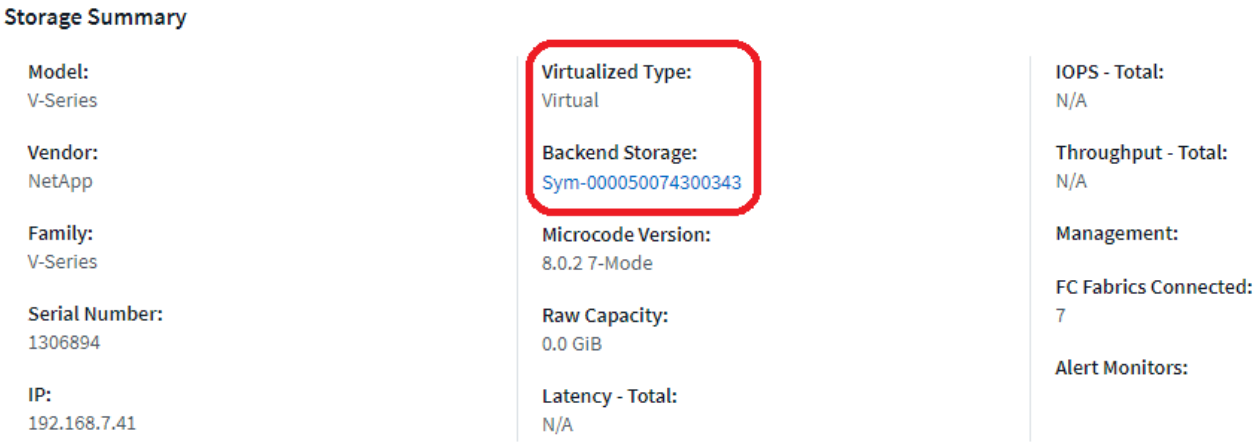
Amélioration de l'installation des opérateurs de surveillance Kubernetes

L'installation et la configuration du "Opérateur de surveillance NetApp Kubernetes" sont plus simples que jamais grâce aux améliorations suivantes :

- L'environnement "paramètres de configuration"se trouve dans un seul fichier de configuration auto-documenté.
- Instructions détaillées pour le téléchargement 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 système de contrôle Kubernetes tout en conservant des configurations personnalisées.
- Sécurité accrue : les clés d'API gèrent les secrets de manière sécurisée.
- Facilité d'intégration et de déploiement avec vos outils d'automatisation ci/CD.

Virtualisation du stockage

Cloud Insights peut différencier une baie de stockage dotée d'un stockage local ou d'une virtualisation d'autres baies de stockage. Vous pouvez ainsi établir le lien entre les coûts et distinguer les performances du stockage frontal et du stockage interne de votre infrastructure.



Nouveaux paramètres Webhook

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

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

Reporting sur les données Kubernetes

Les données Kubernetes collectées par Cloud Insights, y compris les volumes persistants (PV), les demandes de volume persistant, les workloads, les clusters et les namespaces, sont désormais disponibles pour le reporting, la facturation interne, les tendances, les prévisions, les calculs TTF et d'autres rapports métier sur les metrics pour Kubernetes.

Moniteurs système ONTAP par défaut activés pour les nouveaux clients

De nombreux moniteurs système ONTAP sont activés (c.-à-d. *repris*) par défaut dans les nouveaux environnements Cloud Insights. Auparavant, la plupart des moniteurs avaient par défaut l'état *Pause*. Étant donné que les besoins de l'entreprise varient d'une entreprise à l'autre, nous vous recommandons de toujours examiner le système dans votre environnement et de mettre en pause ou de reprendre chacun d'entre "moniteurs système"eux en fonction de vos besoins en matière d'alerte.

Avril 2023

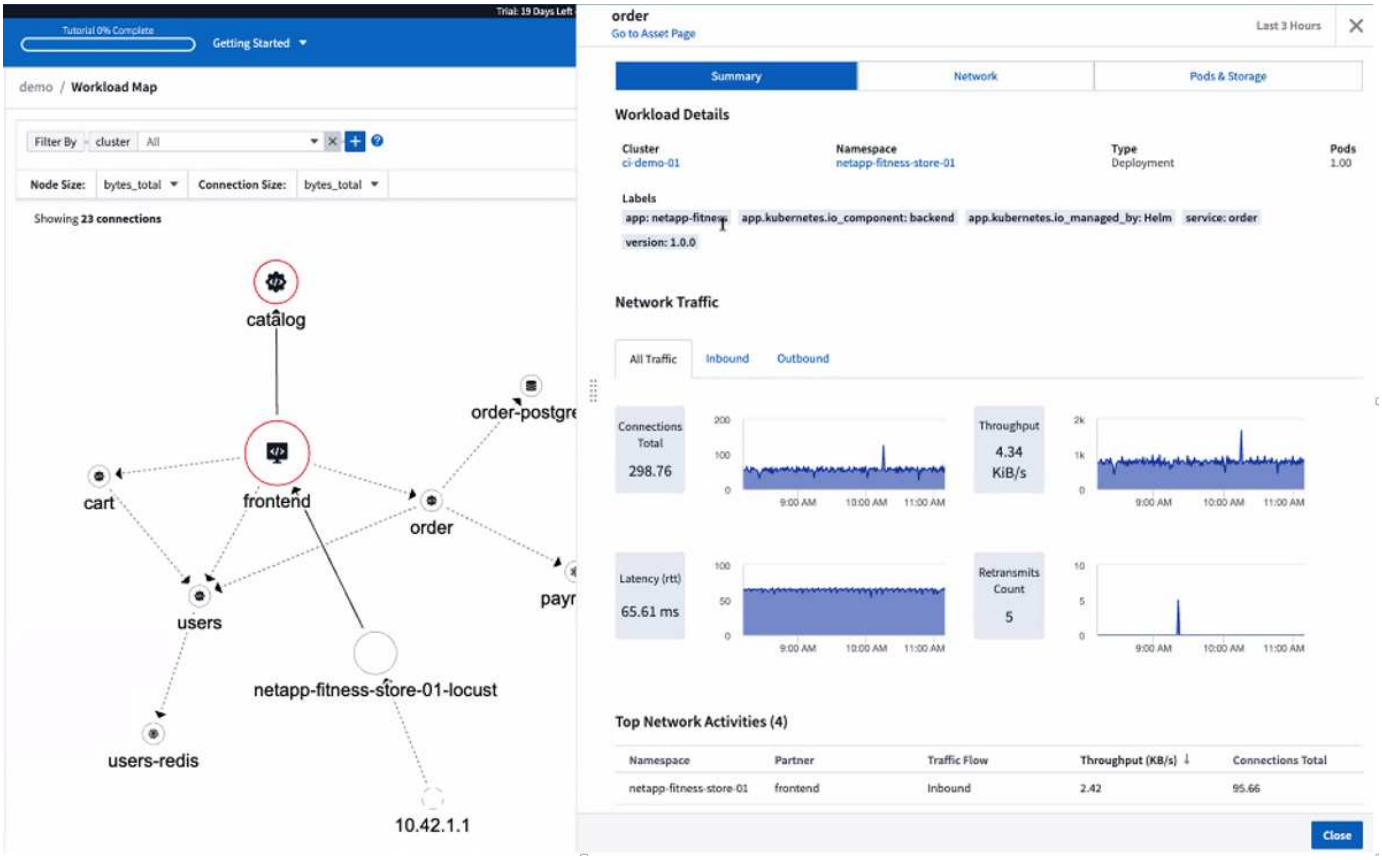
Contrôle des performances et mappage Kubernetes

"*Performances du réseau Kubernetes et mappage*"La fonctionnalité simplifie la résolution des problèmes en mappant les dépendances entre les workloads Kubernetes. Il fournit une visibilité en temps réel sur les latences et les anomalies des performances du réseau Kubernetes pour identifier les problèmes de performance avant qu'ils n'affectent les utilisateurs. Cette fonctionnalité aide les entreprises à réduire les coûts globaux grâce à l'analyse et à l'audit des flux de trafic Kubernetes.

Principales fonctionnalités : • la carte des workloads présente les dépendances et les flux des workloads Kubernetes, et souligne les problèmes de réseau et de performance. • Surveiller le trafic réseau entre les pods

Kubernetes, les workloads et les nœuds ; identifier la source des problèmes de trafic et de latence. • Réduire les coûts globaux en analysant les entrées, les sorties, le trafic interrégional et le trafic de réseau interzone.

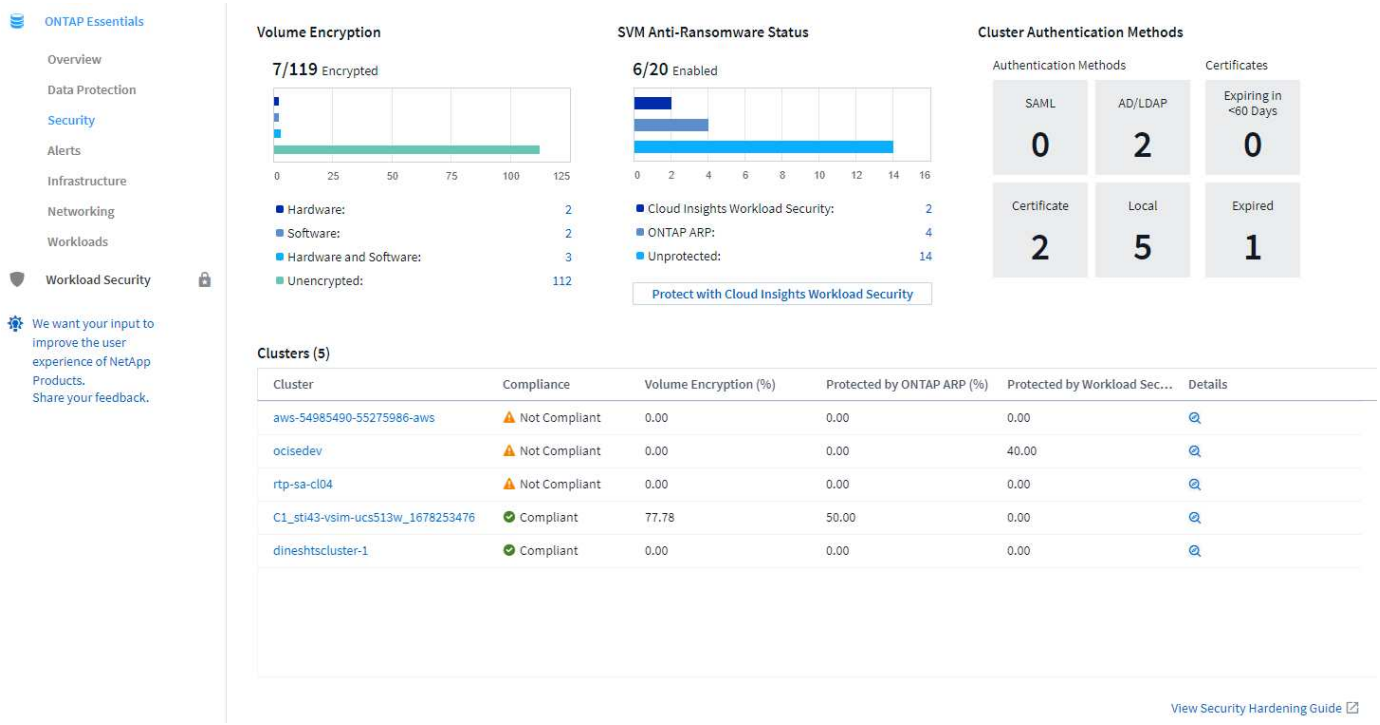
Carte des charges de travail affichant les détails de la diapositive :



Le contrôle et le mappage des performances Kubernetes sont disponibles en tant que "Aperçu"fonctionnalité.

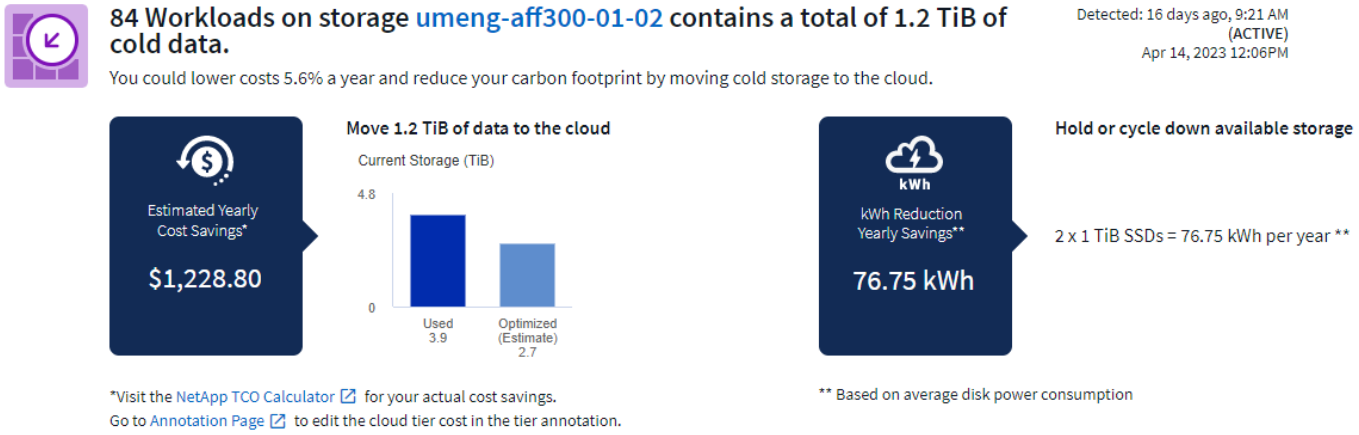
Tableau de bord de sécurité ONTAP Essentials

Vous offre une vue instantanée de votre situation en matière de sécurité et affiche des graphiques sur le "Tableau de bord de sécurité"chiffrement de volume matériel et logiciel, l'état anti-ransomware et les méthodes d'authentification du cluster. Le tableau de bord de sécurité est disponible en tant que "Aperçu"fonction.



Récupération du stockage à froid ONTAP

L'outil *Reclaim ONTAP Cold Storage* Insight fournit des données sur la capacité à froid, les économies potentielles en termes de coûts/d'énergie et les actions recommandées pour les volumes des systèmes ONTAP.



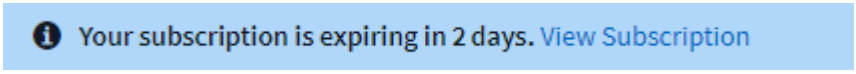
Grâce à Insight, vous pouvez répondre à des questions telles que :

- Quelle quantité de données inactives d'un cluster de stockage se trouve sur (a) des disques SSD à coût élevé, (b) des disques durs et (c) des disques virtuels ?
- Quelles charges de travail contribuent le plus en ce qui concerne le stockage non optimisé ?
- Quelle est la durée (en jours) pendant laquelle les données ont été inactives sur une charge de travail donnée ?

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

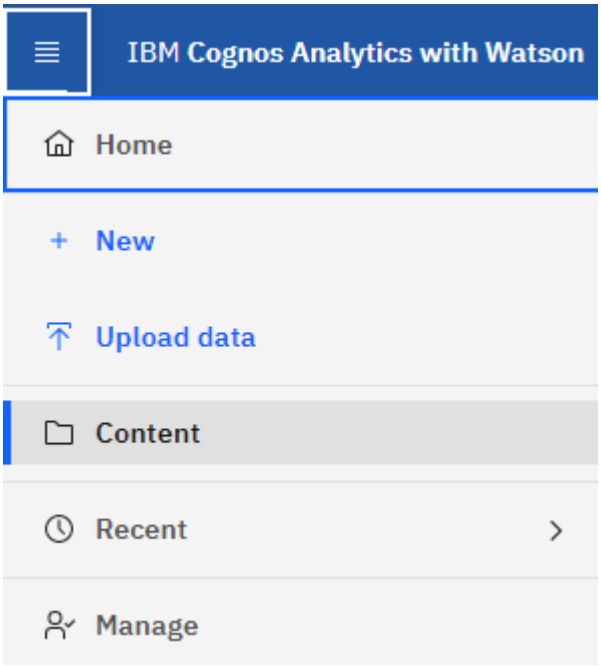
La notification d’abonnement contrôle également les messages de bannière

La définition des destinataires pour les notifications d’abonnement (Admin > Notifications) contrôle désormais également les personnes qui verront les notifications de bannière de produit liées aux abonnements.



Le reporting a une nouvelle apparence

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



Moniteurs en pause par défaut

Pour les nouveaux environnements Cloud Insights, n’oubliez pas que "moniteurs définis par le système"n’envoyez pas de notifications d’alerte par défaut. Vous devez activer les notifications pour tout moniteur que vous souhaitez vous alerter en ajoutant une ou plusieurs méthodes de remise pour le moniteur. Pour les environnements Cloud Insights existants, la liste des destinataires de notification *global* par défaut a été supprimée pour tous les moniteurs définis par le système actuellement à l’état *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 API ?

API Metering a été déplacé de la page Subscription à la page **Admin > API Access**.

Mars 2023

Cloud Connection pour ONTAP 9.9+ est obsolète

Le collecteur de données de Cloud Connection pour ONTAP 9.9+ est obsolète. À partir du 4 avril 2023, les collecteurs de données Cloud Connection de votre environnement ne collecteront plus les données et présenteront une erreur lors de l'interrogation. Le collecteur de données de Cloud Insights sera supprimé définitivement de 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 vous alerter des problèmes de liaisons d'interconnexion, de pulsation, etc. En outre, trois nouveaux moniteurs de journalisation de protection des données ont été ajoutés pour prévenir les modifications de resynchronisation automatique de SnapMirror, de la mise en miroir MetroCluster et de la resynchronisation des miroirs FabricPool.

Notez que certains de ces moniteurs seront *activés* par défaut ; vous devez les *mettre* en pause si vous ne souhaitez pas les alerter. Notez également que ces moniteurs ne sont pas configurés pour transmettre des notifications. Vous devez configurer les destinataires de notification sur ces moniteurs si vous souhaitez envoyer des alertes par e-mail ou via webhook.

Exportation .CSV pour tous les widgets de la table du tableau de bord

Il est essentiel d'assurer l'accessibilité à vos données, c'est pourquoi nous avons créé . Exportation CSV disponible pour toutes les requêtes métriques, les widgets de tableau de bord et les pages d'accueil 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 incluses dans la nouvelle fonctionnalité d'exportation.

Décembre 2022

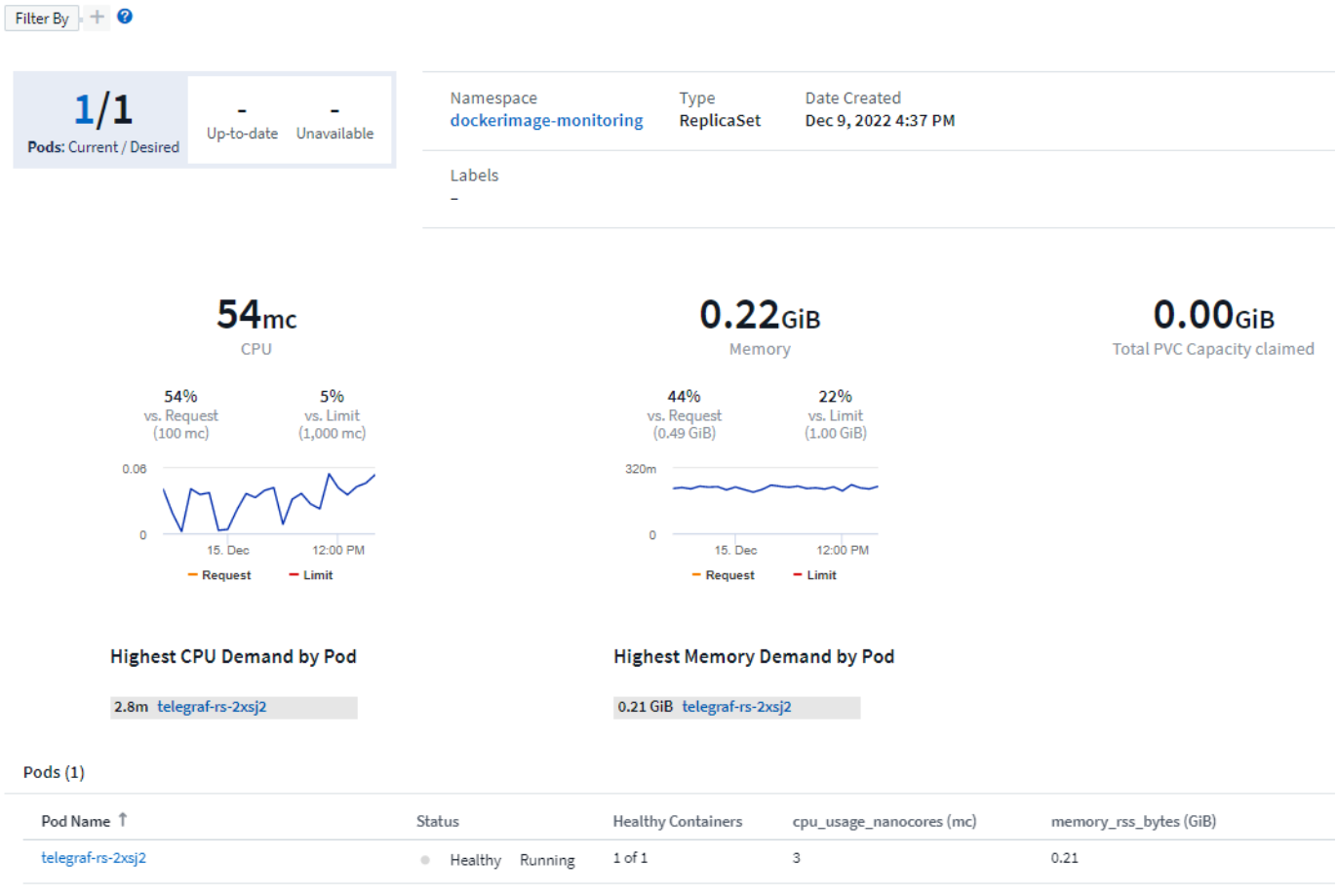
Découvrez les fonctionnalités de protection par ransomware et d'autres fonctionnalités de sécurité de Cloud Insights lors de l'essai

À partir d'aujourd'hui, vous vous inscrivez à un nouvel essai de Cloud Insights et explorez des fonctionnalités de sécurité telles que la détection des attaques par ransomware et la stratégie automatisée de réponse aux blocs par les utilisateurs. Si vous ne vous êtes pas inscrit à l'essai, faites-le dès aujourd'hui !

Les workloads Kubernetes ont leur propre page d'accueil

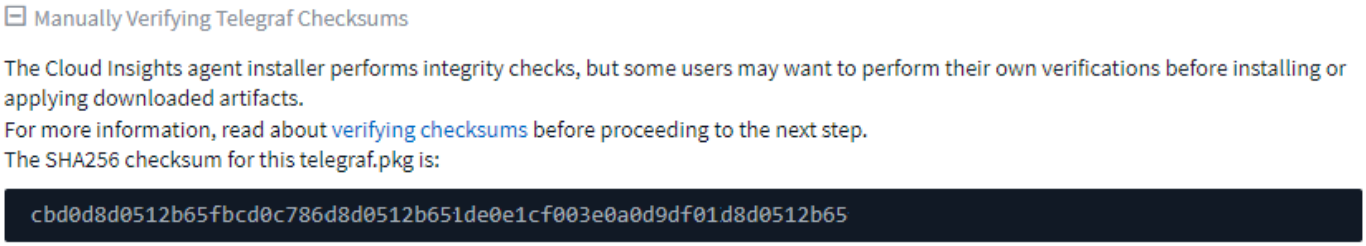
Les workloads constituent un élément clé de votre environnement Kubernetes, et Cloud Insights fournit donc désormais des pages d'accueil pour ces charges de travail. Vous pouvez y consulter, explorer et résoudre les

problèmes qui affectent vos workloads Kubernetes.



Vérifiez vos checksums

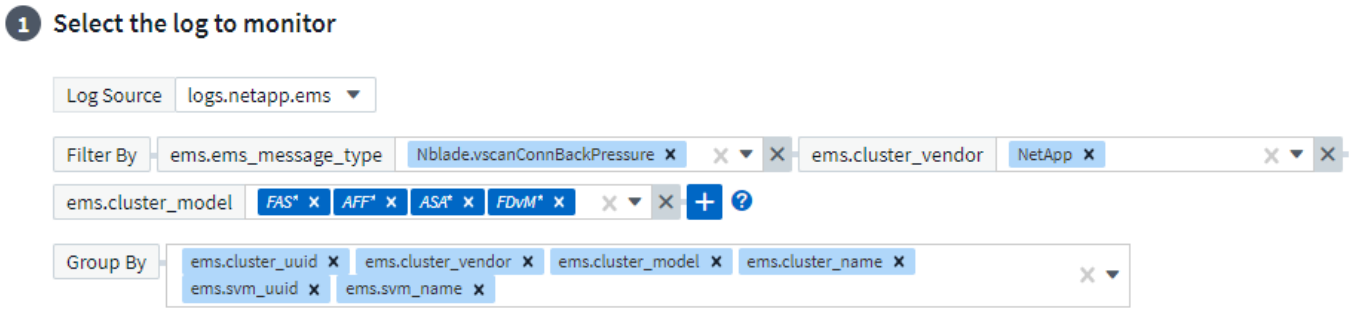
Vous nous avez demandé de vous fournir des valeurs de somme de contrôle lors de l'installation de l'agent pour Windows et Linux et nous pensons que c'est une excellente idée. Les voici donc :



Amélioration des alertes de journaux

Grouper par

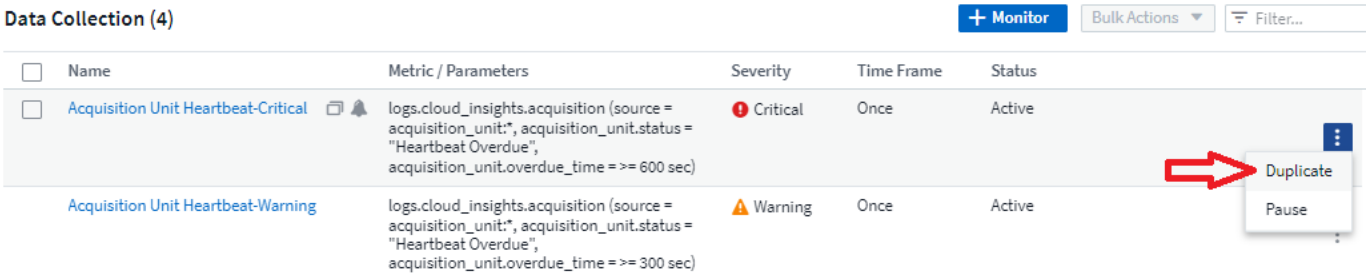
Lors de la création ou de la modification d'un moniteur de journal, vous pouvez désormais définir des attributs « Grouper par » pour permettre des alertes plus ciblées. Recherchez les attributs « Grouper par » sous les paramètres de « filtre » dans la définition de votre moniteur.



Cette modification permet d'intégrer les moniteurs métriques et les moniteurs de journaux à la parité des fonctions en normalisant l'aspect « regrouper par » des définitions de moniteur. Cette parité permet aux clients de cloner/dupliquer **tous** moniteurs par défaut définis par le système pour une personnalisation plus poussée.

Duplication

Vous pouvez à présent cloner (dupliquer) les moniteurs change Log, Kubernetes Log et Data Collector Log. Cela crée un nouveau moniteur de journaux personnalisé que vous pouvez modifier en fonction de vos définitions spécifiques.



11 nouveaux moniteurs ONTAP par défaut couvrant SnapMirror pour la continuité de l'activité

Nous avons ajouté près d'une douzaine de nouveautés "moniteurs système"pour SnapMirror for Business Continuity (SMBC), qui signalent 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 Cloud volumes ONTAP !

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

Octobre 2022

Détection plus précise et plus efficace des attaques par ransomware avec l'intégration autonome de ONTAP en cas de protection

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

Cloud Secure reçoit des événements ONTAP ARP sur les activités potentielles du chiffrement des fichiers de volume, et

- Met en corrélation les événements de cryptage des volumes avec l'activité des utilisateurs pour identifier qui est à l'origine des dommages,
- Mise en place de règles de réponse automatiques pour bloquer l'attaque,
- Identifie les fichiers affectés, ce qui permet de les récupérer plus rapidement et de mener des enquêtes sur les violations de données.

Septembre 2022

Moniteurs disponibles en édition de base

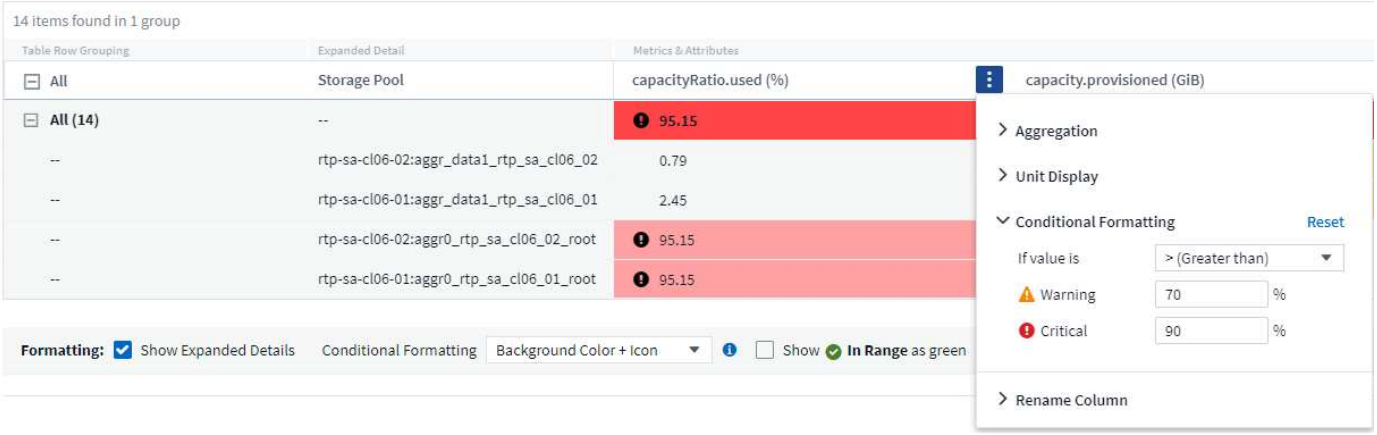
ONTAP "Moniteurs par défaut"est désormais disponible dans l'édition de base de Cloud Insights. Cela inclut plus de 70 moniteurs d'infrastructure et 30 exemples de charge de travail.

Tableaux de bord ONTAP Power and StorageGRID

La galerie de tableaux de bord inclut un nouveau tableau de bord pour l'alimentation et la température ONTAP ainsi que quatre tableaux de bord pour StorageGRID. Si votre environnement collecte des mesures de puissance ONTAP et/ou des données StorageGRID, importez ces tableaux de bord en sélectionnant **+dans Galerie**.

Visibilité des seuils d'un seul 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 ainsi une visibilité instantanée des valeurs aberrantes et des points de données exceptionnels.

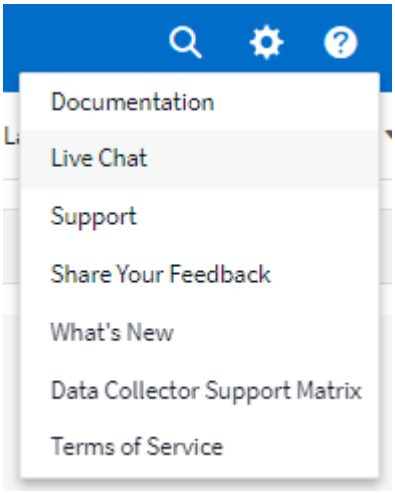


Moniteur de sécurité

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 regardez cet espace pour plus de moniteurs de sécurité, bientôt!

Discutez où vous voulez

Discutez avec un spécialiste du support NetApp depuis n'importe quel écran Cloud Insights en sélectionnant le nouveau **aide > chat en ligne**. L'aide est disponible à partir du « ? » dans le coin supérieur droit de l'écran.



Informations plus visibles

Si votre environnement subit des "Visibilité"contraintes telles que les *ressources partagées sous stress* ou *namespaces Kubernetes à court d'espace*, les pages d'accueil des ressources affectées incluent désormais des liens vers l'Insight proprement dit, ce qui accélère l'exploration et la résolution de problèmes.

Nouveaux collecteurs de données

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

Autres mises à jour du Data Collector

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

Systèmes d'exploitation pris en charge

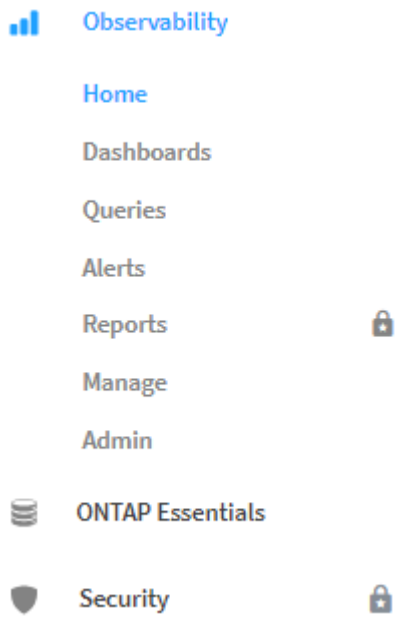
Les systèmes d'exploitation suivants sont pris en charge avec les unités d'acquisition Cloud Insights, en plus de ceux"déjà pris en charge"-ci :

- Red Hat Enterprise Linux 8.5, 8.6

Août 2022

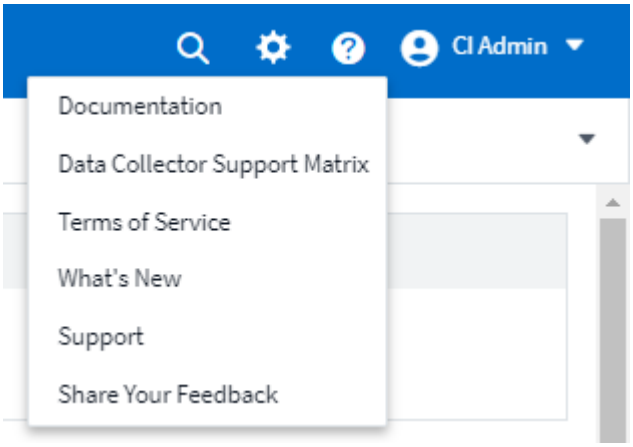
Le nouveau look de Cloud Insights !

À partir de ce mois-ci, "moniteur et optimisation" a été renommé **observabilité**. Vous trouverez ici toutes vos fonctionnalités préférées, comme Dashboards, requêtes, alertes et reporting. En outre, recherchez Cloud Secure dans le nouveau menu **sécurité**. Notez que seuls les menus ont changé ; la fonction reste la même.



Vous cherchez le menu **aide** ?

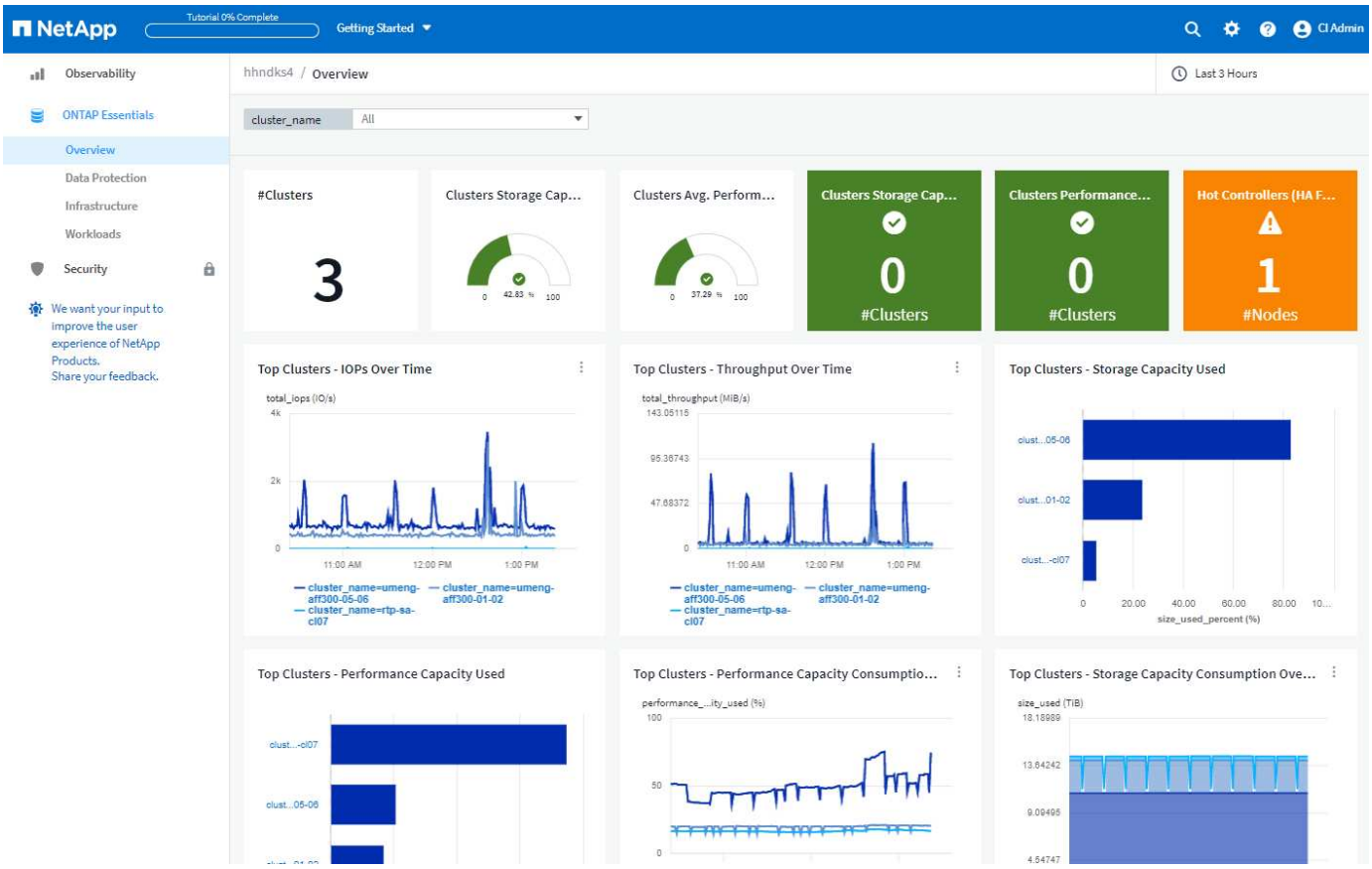
Aide maintenant vit dans le coin supérieur droit de l'écran.



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

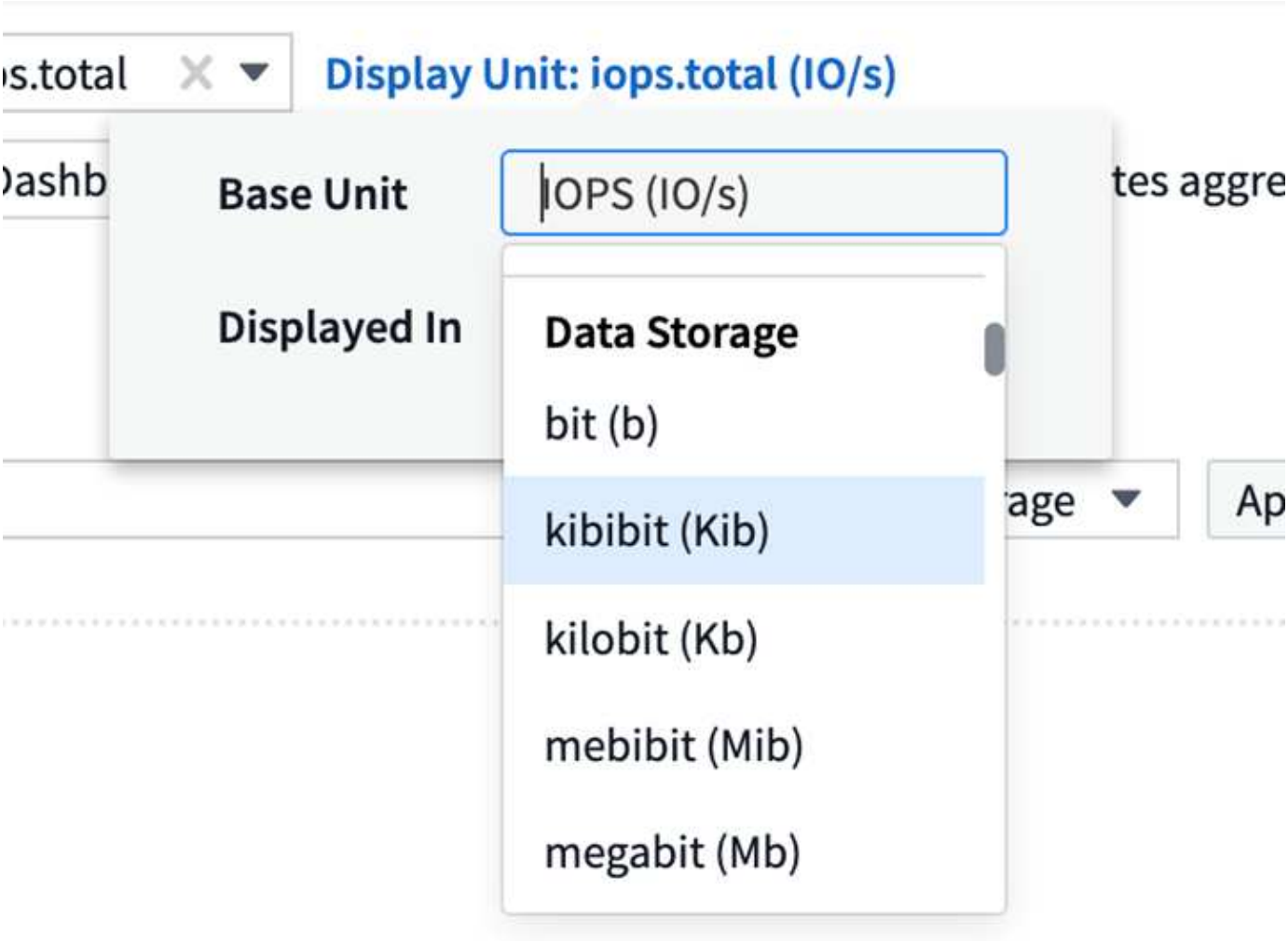
"Essentiels ONTAP" Est un ensemble de tableaux de bord et de workflows qui offrent des vues détaillées de vos inventaires NetApp ONTAP, des workloads et de la protection des données, et propose notamment des prévisions complètes concernant la capacité et les performances de stockage. Vous pouvez même voir si les contrôleurs fonctionnent à des taux d'utilisation élevés. 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 aux opérateurs et administrateurs ONTAP existants, ce qui simplifie la transition d'Active IQ Unified Manager vers les outils de gestion basés sur les services.



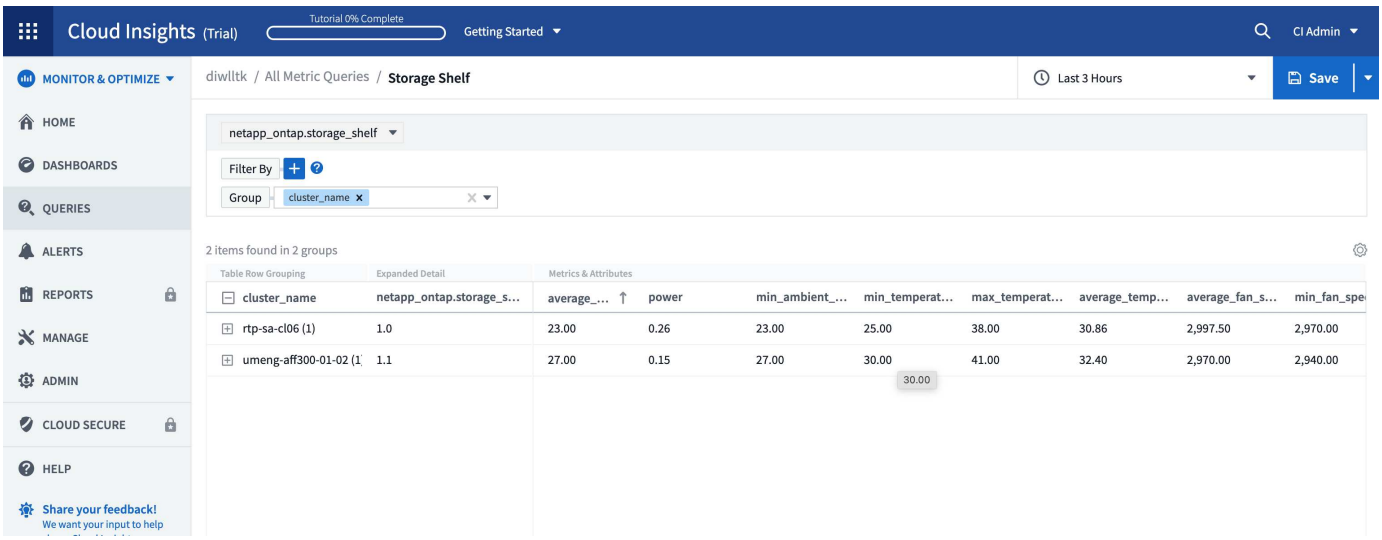
Les familles de données de stockage sont fusionnées

Vous en faites la demande, et maintenant vous l'avez. Les unités de données de base 2 et base-10 sont désormais combinées en une seule famille, des bits et octets aux tébibibits et téraoctets, ce qui facilite l'affichage des données sur vos tableaux de bord. Les taux de données représentent désormais une famille de personnes de taille.



Quelle est la puissance de mon stockage ?

Affichez et contrôlez la consommation électrique, la température et la vitesse des nœuds de stockage ONTAP à l'aide des metrics netapp_ontap.Storage_shelf, netapp_ontap.system_node et netapp_ontap.cluster (consommation électrique uniquement).



Fonctions avec un dégradé de l'aperçu

Les fonctionnalités suivantes ont été déaperçu et sont désormais disponibles pour tous les clients :

Fonctionnalité	Description
Espaces de noms Kubernetes manque d'espace	L'espace de noms *Kubernetes épuisé* Insight vous donne une vue d'ensemble des workloads des 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 contrainte	Les informations *ressource partagée soumise à stress* utilisent l'IA/ML pour identifier automatiquement les conflits de ressources qui entraînent une dégradation des performances dans votre environnement, surlignent toutes les charges de travail qui en sont affectées et proposent des actions recommandées pour les résoudre, ce qui vous permet de résoudre plus rapidement les problèmes de performance. "En savoir plus"
Cloud Secure – bloquer l'accès des utilisateurs aux attaques	Renforcez la protection de vos données stratégiques en vous permettant de bloquer l'accès des utilisateurs en cas d'attaque. L'accès peut être bloqué automatiquement, à l'aide des stratégies de réponse automatisée ou manuellement à partir des pages d'alerte ou de détails de l'utilisateur. "En savoir plus"

Comment ma collecte de données est-elle en bonne santé ?

Cloud Insights fournit deux nouveaux moniteurs de fréquence cardiaque pour vos unités d'acquisition, ainsi que deux moniteurs pour vous alerter des pannes de collecteur de données. Elles peuvent être utilisées pour vous alerter rapidement des problèmes liés à la collecte de données.

Les moniteurs suivants sont maintenant disponibles dans le groupe de moniteurs *Data Collection* :

- Unité d'acquisition Heartbeat-Critical
- Avertissement de pulsation de l'unité d'acquisition
- Echec du collecteur
- Avertissement du collecteur

Notez que ces moniteurs sont à l'état *Pause* par défaut. Activez-les pour être alerté des problèmes liés à la collecte des données.

Tokens de l'API de renouvellement automatique

Les tokens d'accès à l'API peuvent désormais être définis pour le renouvellement automatique. En activant cette fonction, les tokens d'accès API nouveaux/actualisés seront automatiquement générés pour les tokens arrivant à expiration. Les agents Cloud Insights qui utilisent un jeton expirant sont automatiquement mis à jour pour utiliser le token d'accès d'API correspondant, nouveau/actualisé, leur permettant ainsi de continuer à fonctionner en toute transparence. 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

s’exécutant sur la plateforme Kubernetes avec la dernière console de surveillance NetApp Kubernetes.

Basic Edition vous donne plus qu’avant

Votre période d’essai est terminée, mais vous n’êtes pas encore sûr de savoir si un abonnement vous convient ? 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 maintenant continuer à capturer la version VMware, la topologie et les données IOPS/débit/latence. Les clients NetApp bénéficiant d’un support Premium sur leurs systèmes de stockage pourront également bénéficier de la prise en charge de Cloud Insights.

Vous souhaitez en savoir plus dès maintenant ?

Consultez la section **Learning Center** de la page aide > support pour accéder aux liens vers les offres de cours NetApp University Cloud Insights !

Systèmes d’exploitation pris en charge

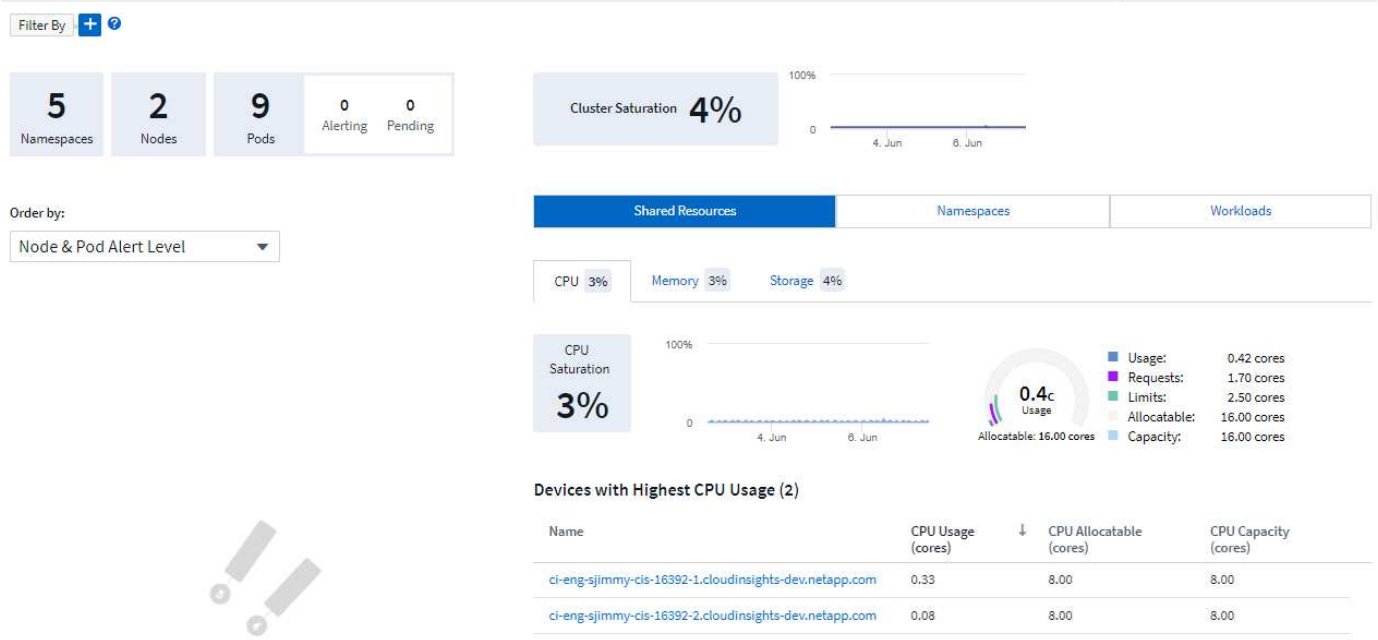
Le système d’exploitation suivant est pris en charge avec les unités d’acquisition Cloud Insights, en plus de ceux"déjà pris en charge"-ci :

- Windows 11

Juin 2022

La saturation du cluster Kubernetes et d’autres détails

Cloud Insights facilite plus que jamais l’exploration de votre environnement Kubernetes. Cette page de détails de cluster amélioré fournit des informations sur la saturation et un aperçu plus précis des espaces de noms et des charges de travail.



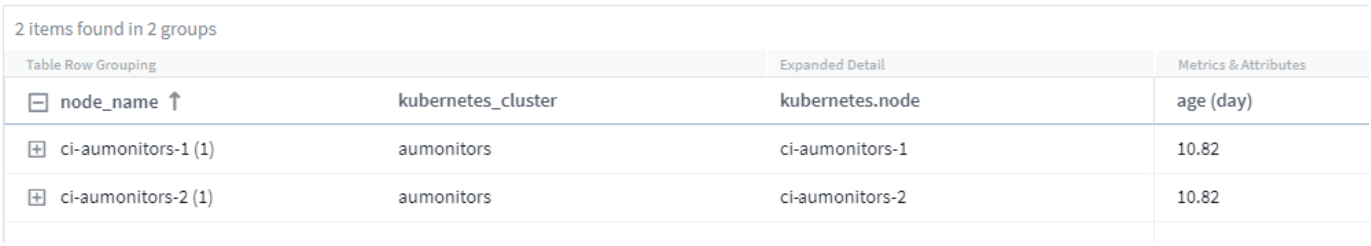
La page de liste des clusters vous offre également un aperçu rapide de la saturation en plus du nombre de

nœuds, de pods, d'espaces de noms et de workloads :



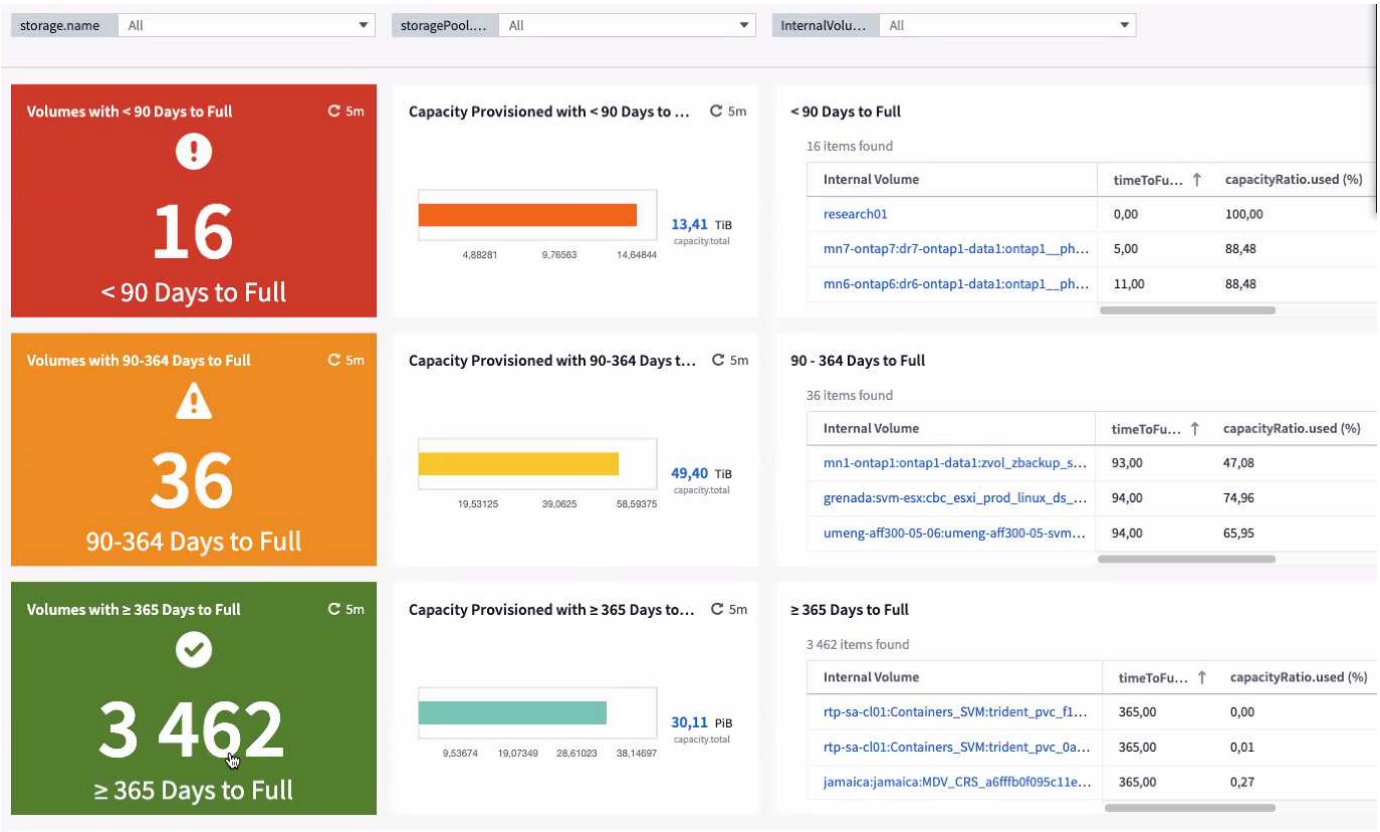
Quel est l'âge de votre cluster Kubernetes ?

Votre cluster vient-il de commencer au monde ou a-t-il connu une longue vie numérique ? *Age* a été ajouté sous forme de mesure de temps collectée pour les nœuds Kubernetes.



Prévision du délai avant utilisation de la capacité

Cloud Insights fournit un tableau de bord permettant de prévoir le nombre de jours avant que la capacité ne soit saturée pour chaque volume interne surveillé. Ces valeurs permettent de réduire considérablement le risque d'interruption.

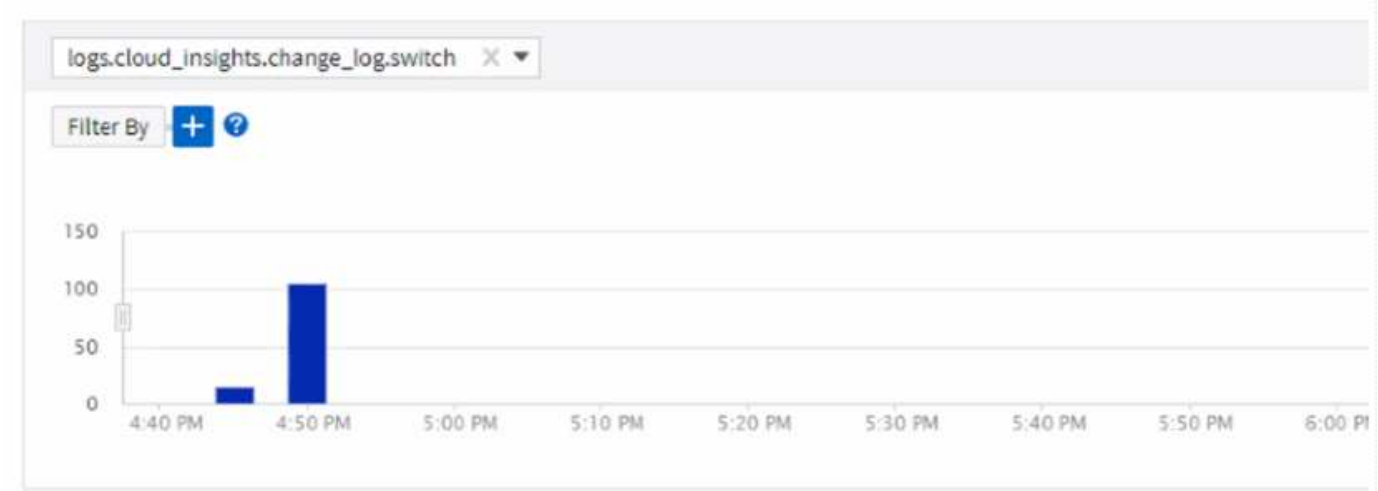


Des compteurs TTF sont également disponibles pour le stockage, le pool de stockage et le volume. Consultez régulièrement cet espace pour consulter d'autres tableaux de bord correspondant à ces objets.

Notez que les prévisions de temps à temps sont déintégrées de *Preview* et qu'elles seront mises en service à tous les clients.

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

Les entrées du journal des modifications ONTAP sont accessibles dans l'explorateur de journaux.



Log Entries

timestamp ↓	name	object_type	message
06/08/2022 4:52:51 PM	fc19	Port	Port with name:fc19 has been created
06/08/2022 4:52:51 PM	fc20	Port	Port with name:fc20 has been created
06/08/2022 4:52:51 PM	fc23	Port	Port with name:fc23 has been created
06/08/2022 4:52:51 PM	fc22	Port	Port with name:fc22 has been created

Systèmes d'exploitation pris en charge

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

- CentOS Stream 9
- Windows 2022

Agent Telegraf mis à jour

L'agent pour l'ingestion de données d'intégration de telegraf a été mis à jour vers la version **1.22.3**, avec des améliorations de performance et de sécurité. Les utilisateurs qui souhaitent mettre à jour peuvent se reporter à la section de mise à niveau appropriée de la "Installation de l'agent" documentation. Les versions précédentes de l'agent continueront de fonctionner sans qu'aucune action de l'utilisateur ne soit nécessaire.

Aperçu des fonctions

Cloud Insights met régulièrement en avant de nouvelles fonctionnalités exceptionnelles. Si vous souhaitez afficher un aperçu d'une ou de plusieurs de ces fonctionnalités, contactez votre "Équipe commerciale NetApp" pour plus d'informations.

Fonctionnalité	Description
Espaces de noms Kubernetes manque d'espace	L'espace de noms *Kubernetes épuisé* Insight vous donne une vue d'ensemble des workloads des 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 aux attaques	Renforcez la protection de vos données stratégiques en vous permettant de bloquer l'accès des utilisateurs en cas d'attaque. L'accès peut être bloqué automatiquement, à l'aide des stratégies de réponse automatisée ou manuellement à partir des pages d'alerte ou de détails de l'utilisateur. "En savoir plus"
Ressource partagée sous contrainte	Les informations *ressource partagée soumise à stress* utilisent l'IA/ML pour identifier automatiquement les conflits de ressources qui entraînent une dégradation des performances dans votre environnement, surlignent toutes les charges de travail qui en sont affectées et proposent des actions recommandées pour les résoudre, ce qui vous permet de résoudre plus rapidement les problèmes de performance. "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 > support, il vous suffit de cliquer sur l'icône Chat ou de cliquer sur *Chat* dans la section "Contactez-nous" pour démarrer une session Chat. L'assistance Chat est disponible en semaine pour les utilisateurs Standard et Premium Edition.



Opérateur Kubernetes

Nous avons facilité la mise en service de votre système grâce à la surveillance avancée de Kubernetes et à l'explorateur de clusters de Cloud Insights.

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

Cliquez sur le lien ci-dessus pour obtenir plus d'informations et les conditions préalables

Gestion des utilisateurs et des invitations à l'aide d'une API

Vous pouvez désormais gérer des utilisateurs et des invitations à l'aide de la puissante API de Cloud Insights. Pour en savoir plus, consultez le "Documentation API swagger".

Alertes de collecte de données

Ne manquez pas les mesures critiques en raison d'un collecteur défectueux !

Il n'a jamais été aussi simple de suivre vos collecteurs de données avec de nouveaux "alertes"défauts pour les unités d'acquisition et le collecteur de données. Notez que ces moniteurs sont *Pause* par défaut. Pour l'activer, accédez à la page moniteurs et localisez et reprenez "Arrêt de l'unité d'acquisition" et "échec du collecteur".

Alertes sur les modifications du stockage ONTAP

Ne laissez pas des modifications de stockage inattendues se traduire par des pannes !

Vous pouvez désormais configurer le Cloud Insights de manière à ce qu'il vous alerte lorsque des modifications ou des suppressions de volumes FlexVol, de nœuds et de SVM sont détectés sur les systèmes ONTAP.

Aperçu des fonctions

Cloud Insights met régulièrement en avant de nouvelles fonctionnalités exceptionnelles. Si vous souhaitez afficher un aperçu d'une ou de plusieurs de ces fonctionnalités, contactez votre "Équipe commerciale NetApp" pour plus d'informations.

Fonctionnalité	Description
Espaces de noms Kubernetes manque d'espace	L'espace de noms *Kubernetes épuisé* Insight vous donne une vue d'ensemble des workloads des 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"
Prévision de la durée totale de la capacité du volume et du volume interne	Cloud Insights est capable de programmer le nombre de jours jusqu'à ce que la capacité soit insuffisante pour chaque volume interne et volume surveillé. Cette valeur permet de réduire considérablement le risque d'interruption.
Cloud Secure : bloquer l'accès des utilisateurs aux attaques	Renforcez la protection de vos données stratégiques en vous permettant de bloquer l'accès des utilisateurs en cas d'attaque. L'accès peut être bloqué automatiquement, à l'aide des stratégies de réponse automatisée ou manuellement à partir des pages d'alerte ou de détails de l'utilisateur. "En savoir plus"

Ressource partagée sous contrainte	Les informations *ressource partagée soumise à stress* utilisent l'IA/ML pour identifier automatiquement les conflits de ressources qui entraînent une dégradation des performances dans votre environnement, surlignent toutes les charges de travail qui en sont affectées et proposent des actions recommandées pour les résoudre, ce qui vous permet de résoudre plus rapidement les problèmes de performance. "En savoir plus"

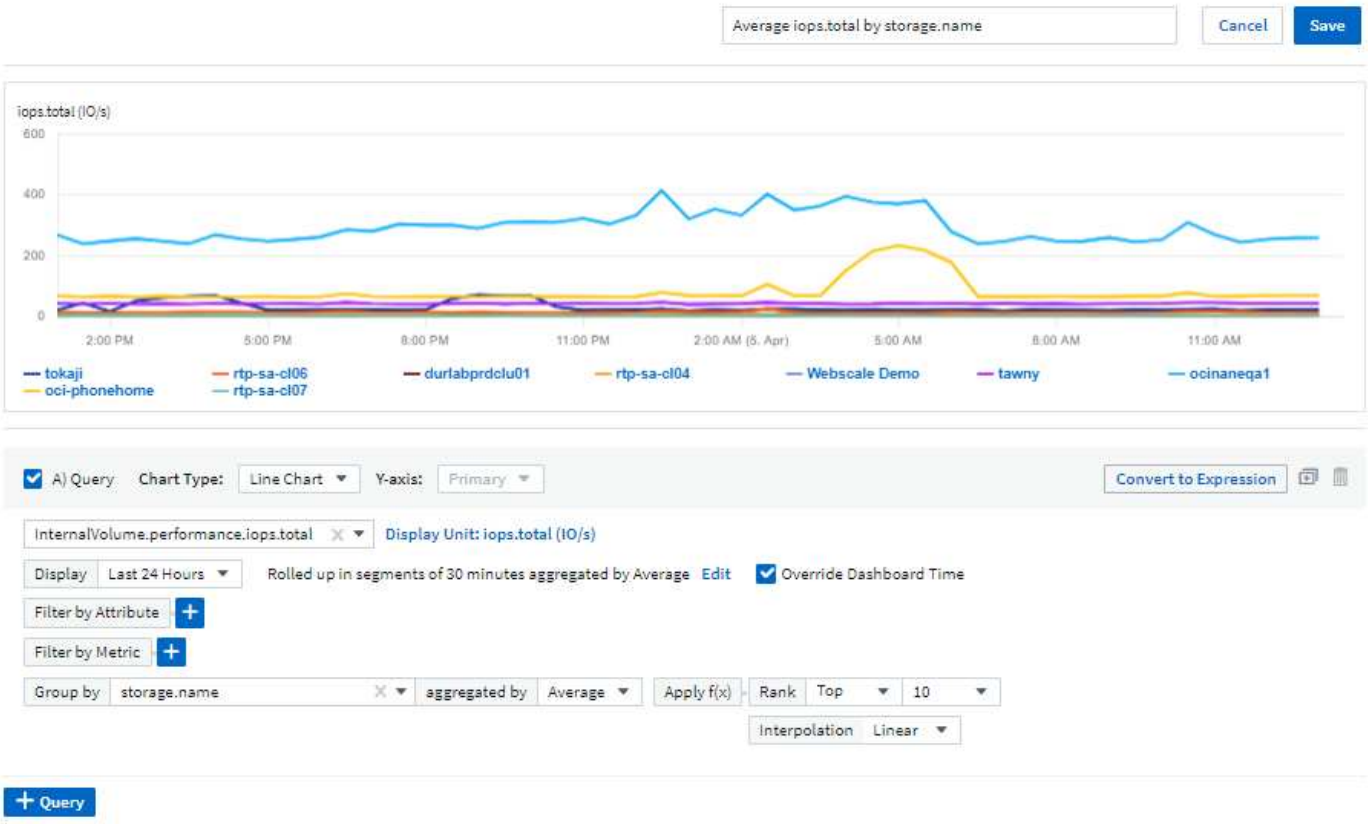
Avril 2022

Faites-nous part de vos commentaires !

Nous souhaitons que votre avis nous aide à façonner Cloud Insights. Gagnez des points et remportez des prix en participant au programme **Insights to action** de NetApp. **"Inscrivez-vous maintenant"**!

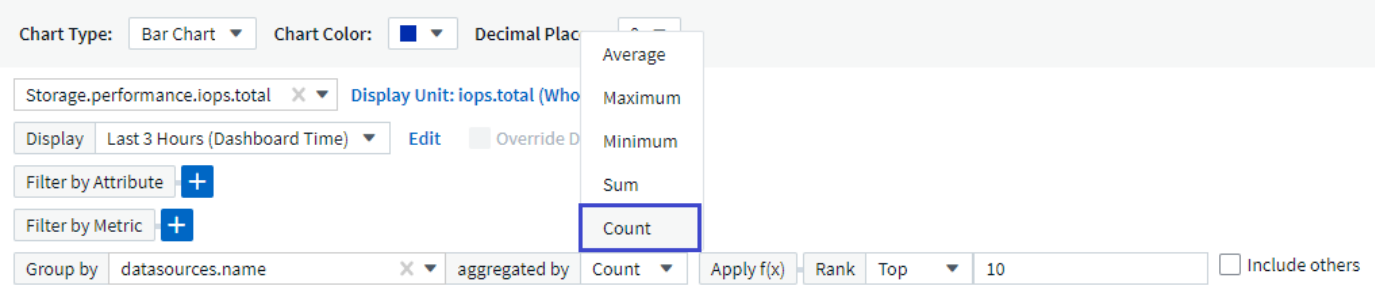
Editeur de tableau de bord mis à jour

Nous avons révisé nos outils de création de tableau de bord pour vous permettre de visualiser plus facilement 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 créez un nouveau tableau de bord de votre choix pour le consulter.



Une nouvelle méthode d'agrégation Count a également été introduite. Lors du regroupement de données dans

des graphiques à barres, des graphiques à colonnes et des widgets de graphique à secteurs, vous pouvez afficher rapidement et facilement le nombre d'objets pertinents pour la mesure sélectionnée.



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

- Aucun - aucune interpolation n'est effectuée
- Linéaire - interpole un point de données entre les points existants
- Stepper utilise le point de données précédent comme point de données interpolé

Amélioration de la surveillance de votre infrastructure Kubernetes

Cloud Insights vous tient au fait des modifications apportées à votre environnement Kubernetes en vous alertant lorsque des pods, des demi-déployer et des réplicats sont créés ou supprimés, ainsi que lorsque de nouveaux déploiements sont créés. Kubernetes surveille par défaut l'état *pause*. Vous devez donc activer uniquement ceux dont vous avez besoin.

Aperçu des fonctions

Cloud Insights met régulièrement en avant de nouvelles fonctionnalités exceptionnelles. Si vous souhaitez afficher un aperçu d'une ou de plusieurs de ces fonctionnalités, contactez votre "Équipe commerciale NetApp" pour plus d'informations.

Fonctionnalité	Description
Prévision de la durée totale de la capacité du volume et du volume interne	Cloud Insights est capable de programmer le nombre de jours jusqu'à ce que la capacité soit insuffisante pour chaque volume interne et volume surveillé. Cette valeur permet de réduire considérablement le risque d'interruption.
Cloud Secure : bloquer l'accès des utilisateurs aux attaques	Renforcez la protection de vos données stratégiques en vous permettant de bloquer l'accès des utilisateurs en cas d'attaque. L'accès peut être bloqué automatiquement, à l'aide des stratégies de réponse automatisée ou manuellement à partir des pages d'alerte ou de détails de l'utilisateur. "En savoir plus"

Ressource partagée sous contrainte	Les informations sur les ressources partagées soumises à des contraintes utilisent l'IA/ML pour identifier automatiquement les conflits de ressources qui causent la dégradation des performances dans votre environnement, identifier toutes les charges de travail impactées et proposer des actions recommandées pour résoudre les problèmes de performance plus rapidement. "En savoir plus"

Nouveau Data Collector

- **Cohesity SmartFiles** - ce collecteur BASÉ sur les API REST acquerra un cluster Cohesity, découvrant les « vues » (sous la forme de volumes internes ci), les différents nœuds, ainsi que les mesures de performance.

Autres mises à jour du Data Collector

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

- Brocade CLI
- Dell/EMC VPLEX, PowerStore, Isilon/PowerScale, VNX Block/CLARiiON CLI, XtremIO, Unity/VNXe
- FlashArray de Pure Storage

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

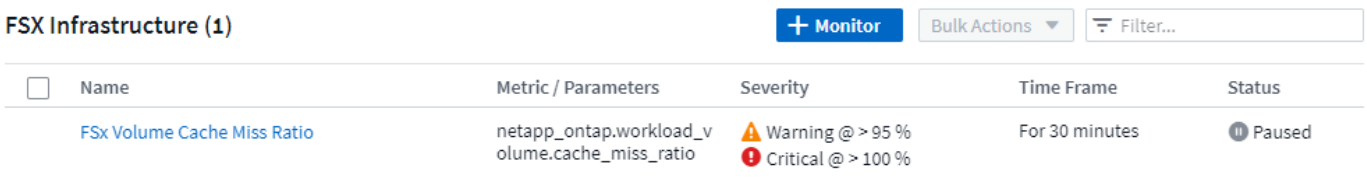
Mars 2022

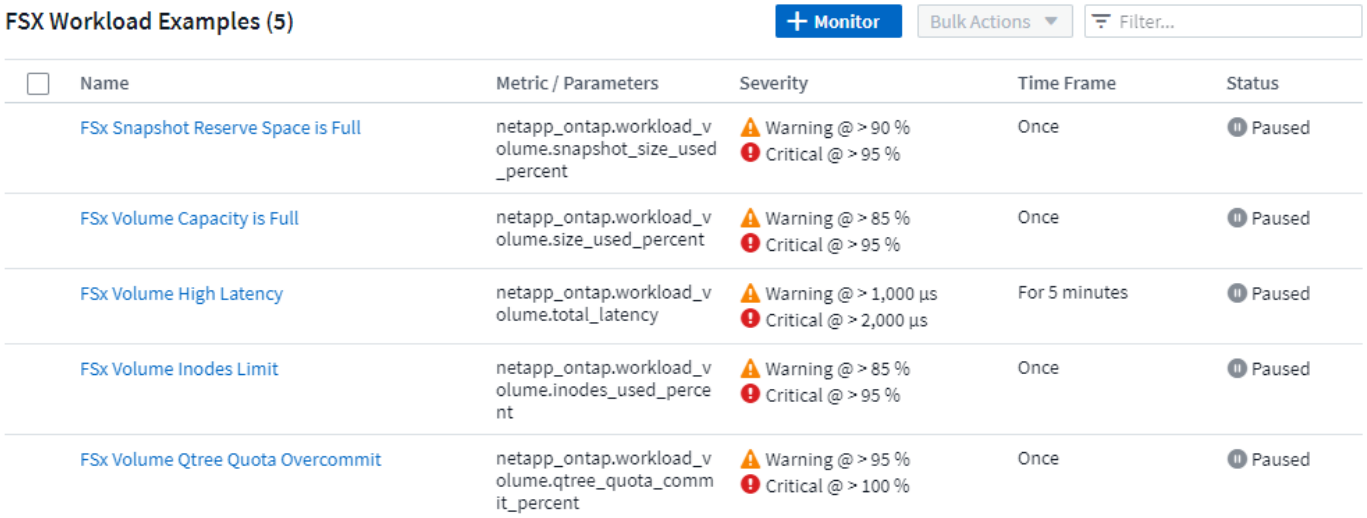
Connexion cloud pour ONTAP 9.9+

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

Nouveau FSX pour moniteurs ONTAP NetApp

La surveillance de votre environnement FSX pour NetApp ONTAP est simple grâce aux nouveautés à "moniteurs définis par le système"la fois pour l'infrastructure (metrics) et les workloads (journaux).





Nouvelles fonctionnalités de Cloud Secure disponibles à tous

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

Fonctionnalité	Description
Destruction de données – détection d'une attaque de suppression de fichier	Détectez les activités anormales de suppression de fichiers à grande échelle, bloquez l'accès aux fichiers malveillants par des utilisateurs malveillants et prenez des snapshots automatiques avec des règles de réponse automatiques.
Notifications séparées pour les avertissements et les alertes	Des notifications d'avertissement et d'alerte peuvent être envoyées à des destinataires distincts, ce qui permet à l'équipe appropriée de rester informée

Agent Telegraf mis à jour

L'agent pour l'ingestion de données d'intégration de telegraf a été mis à jour vers la version **1.21.2**, avec des améliorations de performance et de sécurité. Les utilisateurs qui souhaitent mettre à jour peuvent se reporter à la section de mise à niveau appropriée de la "Installation de l'agent" documentation. Les versions précédentes de l'agent continueront de fonctionner sans qu'aucune action de l'utilisateur ne soit nécessaire.

Mises à jour du Data Collector

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

Février 2022

Cloud Insights corrige les vulnérabilités Apache Log4j

La sécurité client est une priorité chez NetApp. Cloud Insights inclut des mises à jour de ses bibliothèques logicielles pour corriger les vulnérabilités Apache Log4j récentes.

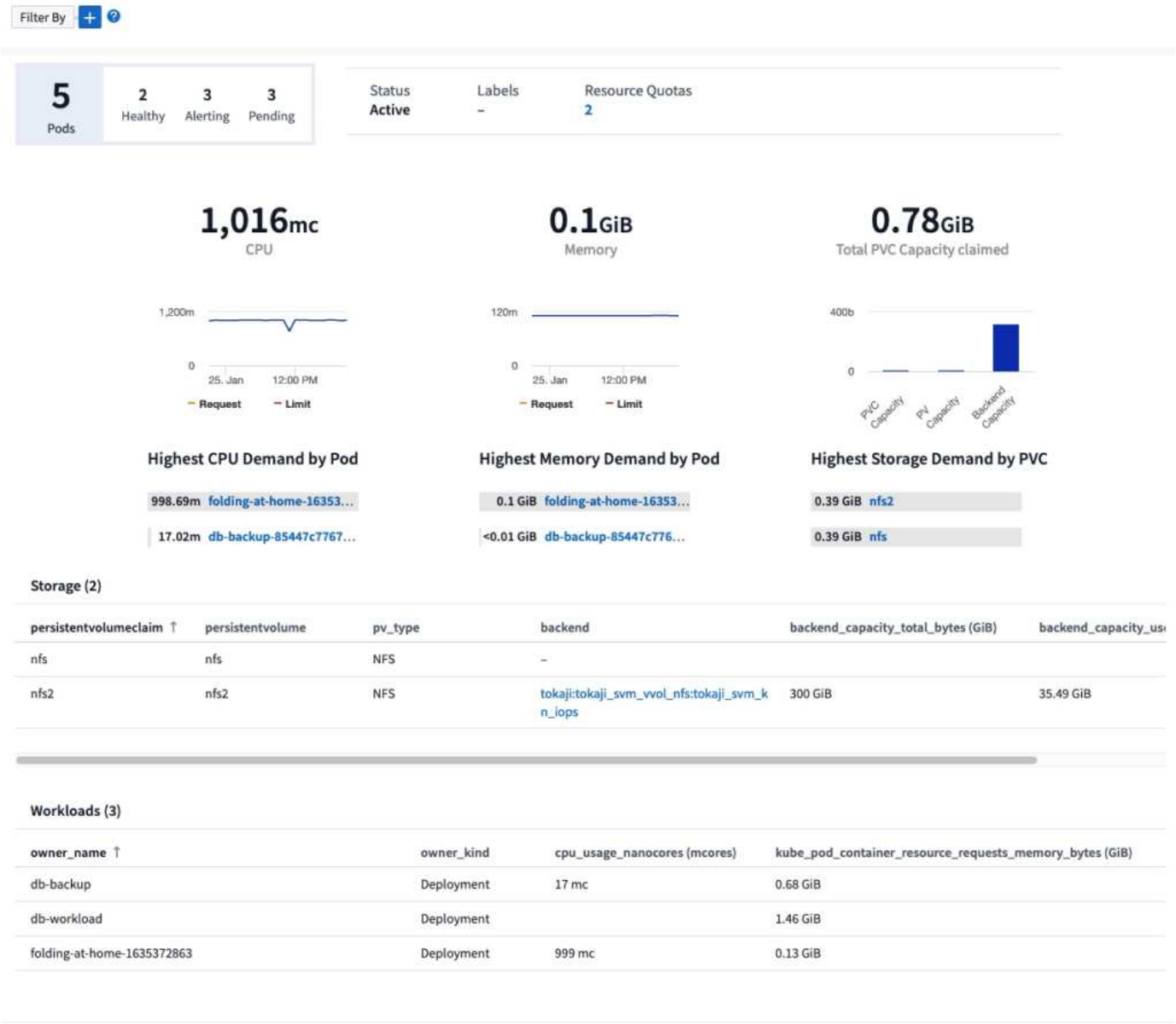
Reportez-vous à la liste suivante sur le site Web de l'avis de sécurité des produits de NetApp :

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

Pour en savoir plus sur ces vulnérabilités et la réponse de NetApp, consultez le "Communiqués NetApp".

Page de détails de l'espace de noms Kubernetes

Il vaut mieux étudier votre environnement Kubernetes, avec des pages détaillées pour les espaces de noms de votre cluster. La page de détails de l'espace de noms présente un récapitulatif de toutes les ressources utilisées par un espace de nom, notamment l'ensemble des ressources de stockage back-end et leur utilisation de la capacité.



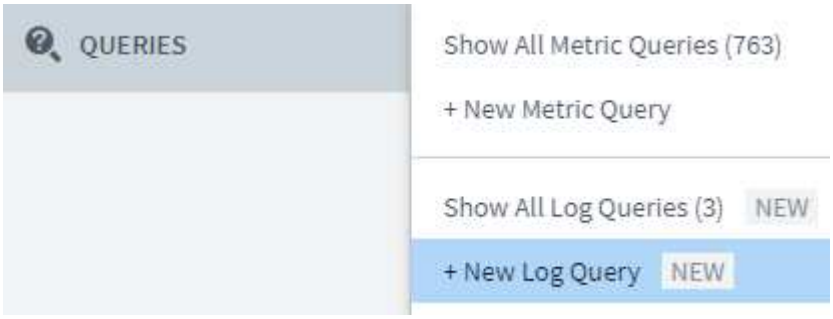
Décembre 2021

Intégration plus étroite pour les systèmes ONTAP

Simplifiez les alertes en cas de défaillances matérielles ONTAP et davantage grâce à une nouvelle intégration avec le système de gestion des événements (EMS) de NetApp. "Exploration et alerte" Messages ONTAP de bas niveau dans Cloud Insights pour informer et améliorer les workflows de résolution de problèmes 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", qui vous permet d'étudier et de dépanner facilement les entrées de journal EMS.



Notifications au niveau du Data Collector.

En plus des moniteurs définis par le système et personnalisés pour l'alerte, vous pouvez également définir des notifications d'alerte pour les collecteurs de données ONTAP, ce qui vous permet de spécifier des destinataires pour les alertes de niveau collecteur, indépendamment des autres alertes de moniteur.

Une plus grande flexibilité des rôles Cloud Secure

Les utilisateurs peuvent obtenir l'accès aux fonctions Cloud Secure en fonction d'"rôles"un ensemble défini par un administrateur :

Rôle	Accès à Cloud Secure
Administrateur	Peut exécuter toutes les fonctions Cloud Secure, y compris celles pour les alertes, les médico-événements, les collecteurs de données, les règles de réponse automatisées et les API pour Cloud Secure. Un administrateur peut également inviter d'autres utilisateurs, mais peut uniquement attribuer des rôles Cloud Secure.
Utilisateur	Peut afficher et gérer des alertes et afficher des informations judiciaires. Le rôle de l'utilisateur peut modifier l'état des alertes, ajouter une note, effectuer des snapshots manuellement et bloquer l'accès des utilisateurs.
Invité	Peut afficher les alertes et les analyses approfondies. Le rôle invité ne peut pas modifier le statut des alertes, ajouter une note, effectuer des snapshots manuellement ou bloquer l'accès des utilisateurs.

Systèmes d’exploitation pris en charge

Le support CentOS 8.x est remplacé par le support **CentOS 8 Stream**. CentOS 8.x atteindra fin de vie le 31 décembre 2021.

Mises à jour du Data Collector

Un certain nombre de noms de collecteurs de données Cloud Insights ont été ajoutés pour tenir compte des changements apportés au fournisseur :

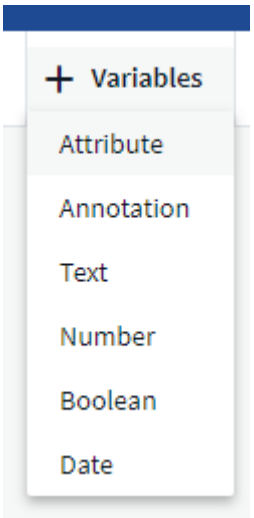
Fournisseur/modèle	Nom précédent
Dell EMC PowerScale	Isilon
HPE Alletra 9000 / Primera	3PAR
HPE Alletra 6000	Nimble

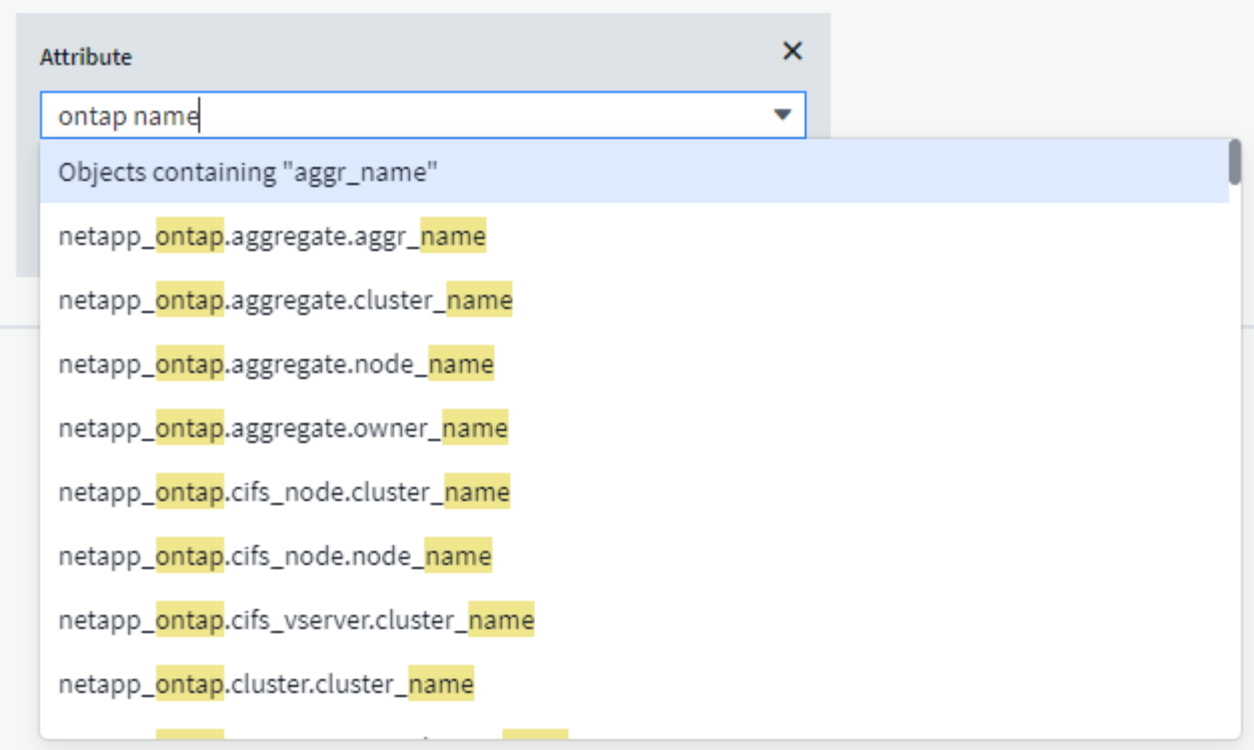
Novembre 2021

Tableaux de bord adaptatifs

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

Les tableaux de bord sont désormais plus puissants et plus flexibles que jamais. Créez des tableaux de bord adaptatifs avec des variables d’attributs pour filtrer rapidement les tableaux de bord à la volée. Grâce à ces outils et à d’autres outils préexistants"variables", vous pouvez désormais créer un tableau de bord de haut niveau pour consulter les mesures de votre environnement dans son ensemble et filtrer de manière transparente par nom de ressource, type, emplacement, etc. Utilisez des variables de nombre dans les widgets pour associer des métriques brutes à des coûts, par exemple le coût par Go pour le stockage à la demande.





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

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

Tableaux POD sur la page d'accueil de VM

Navigation transparente entre les machines virtuelles et les pods Kubernetes en utilisant ces pods : dans le cadre d'améliorations au niveau du dépannage et de la gestion de la marge de performances, un tableau des pods Kubernetes associés apparaîtra désormais sur les pages d'accueil des machines virtuelles.



Mises à jour du Data Collector

- ECS crée désormais des rapports sur le firmware pour le stockage et le nœud
- Isilon a amélioré la détection des invites
- Azure NetApp Files collecte plus rapidement les données de performances
- StorageGRID prend désormais en charge les authentifications uniques (SSO)
- L'CLI Brocade signale correctement le modèle pour X&-4

D’autres systèmes d’exploitation sont pris en charge

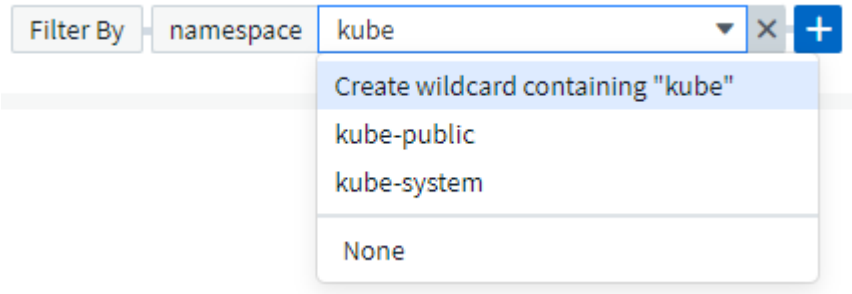
L’unité d’acquisition Cloud Insights prend en charge les systèmes d’exploitation suivants, en plus de ceux déjà pris en charge :

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

Octobre 2021

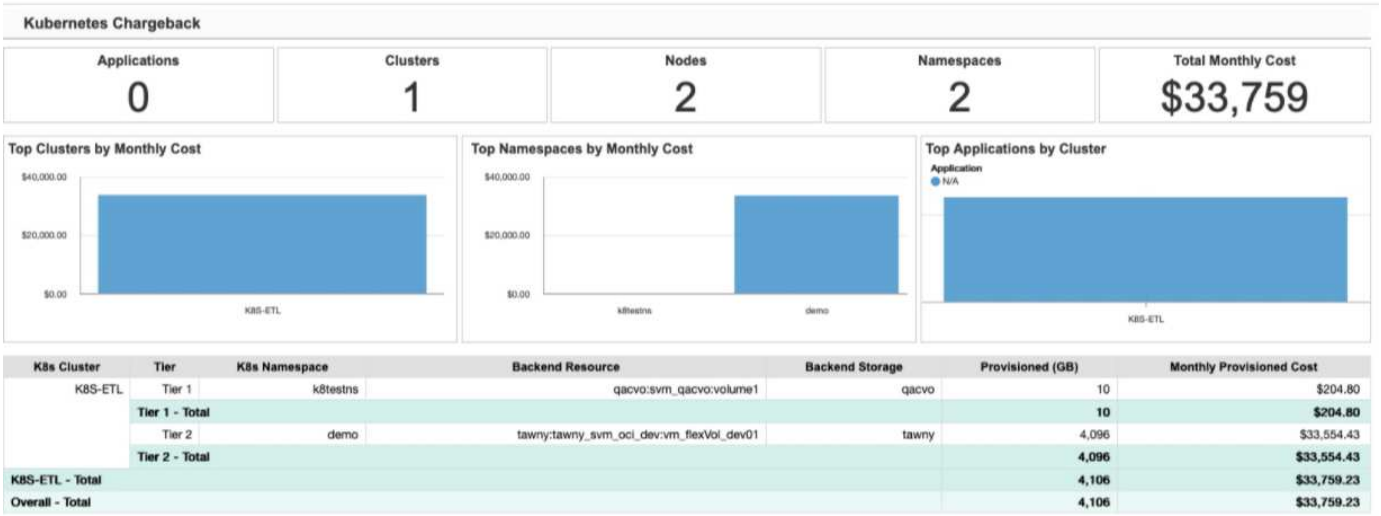
Filtres sur les pages de l’Explorateur K8S

"Kubernetes Explorer" Les filtres de page vous permettent de contrôler en priorité les données affichées pour votre cluster Kubernetes, l’exploration de nœuds et de pods.



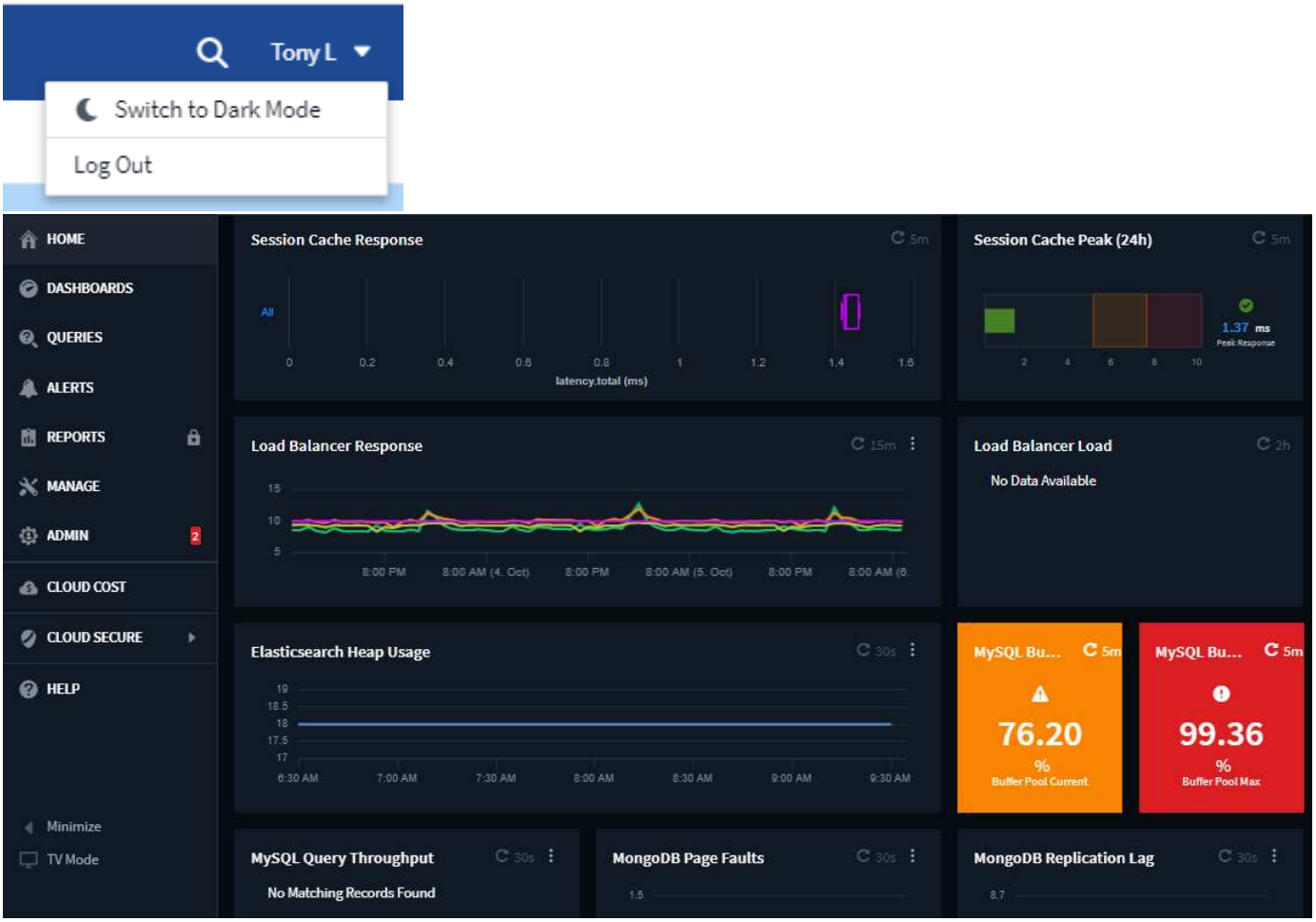
Données K8s pour la création de rapports

Les données Kubernetes sont désormais disponibles dans le reporting pour vous permettre de créer des rapports de refacturation ou d’autres rapports. Pour que les données de facturation interne Kubernetes soient transmises au service de reporting, vous devez disposer d’une connexion active à et Cloud Insights doit recevoir des données de, de votre cluster Kubernetes et de son stockage interne. Si aucune donnée n’est reçue du système de stockage interne, Cloud Insights ne peut pas envoyer les données d’objet Kubernetes au reporting.



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 la liste déroulante en regard de votre nom d'utilisateur.



Prise en charge du Data Collector

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

- Nouveau collecteur pour Amazon FSX pour ONTAP

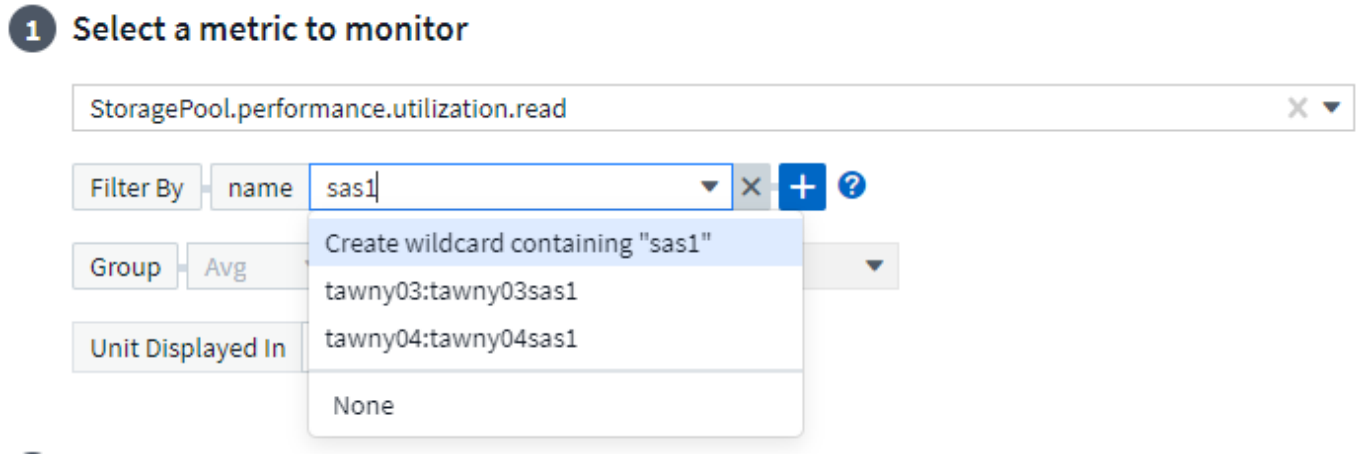
Septembre 2021

Les règles de performance sont désormais des moniteurs

Des moniteurs et des alertes ont supplanté les règles de performance et les violations dans l'ensemble de l'environnement Cloud Insights. "Alertes avec les moniteurs" offre une plus grande flexibilité et une meilleure visibilité sur les problèmes ou tendances potentiels de votre environnement.

Suggestions complètes, caractères génériques et expressions dans moniteurs

Lors de la création d'un contrôle des alertes, la saisie dans un filtre est désormais prédictive, ce qui vous permet de rechercher et de trouver facilement les mesures ou attributs de votre moniteur. En outre, vous avez la possibilité de créer un filtre générique basé sur le texte que vous saisissez.



Agent Telegraf mis à jour

L'agent pour l'ingestion de données d'intégration de telegraf a été mis à jour vers la version **1.19.3**, avec des améliorations de performance et de sécurité. Les utilisateurs qui souhaitent mettre à jour peuvent se reporter à la section de mise à niveau appropriée de la "Installation de l'agent" documentation. Les versions précédentes de l'agent continueront de fonctionner sans qu'aucune action de l'utilisateur ne soit nécessaire.

Prise en charge du Data Collector

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

- Le collecteur Hyper-V de Microsoft utilise désormais PowerShell à la place de WMI
- Les machines virtuelles Azure et le collecteur du VHD sont désormais 10 fois plus rapides en raison d'appels parallèles
- HPE Nimble prend désormais en charge les configurations fédérées et iSCSI

Et puisque nous améliorons toujours la collecte de données, voici d'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 générer des rapports sur les pools de structure
- ANF améliorée avec les performances du pool de stockage et des volumes
- EMC ECS amélioré avec les performances de stockage et de nœuds de stockage, ainsi que le nombre d'objets dans des compartiments
- EMC Isilon amélioré avec des mesures de nœud de stockage et qtree
- Amélioration d'EMC Symetrix avec des mesures de limite de QoS sur volume
- IBM SVC et EMC PowerStore amélioré avec le numéro de série parent des 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 d'exporter des événements d'audit vers un fichier .CSV.

Gestion améliorée des rôles utilisateur

Cloud Insights offre désormais une plus grande liberté pour l'attribution des rôles utilisateur et des contrôles d'accès. Les utilisateurs peuvent désormais se voir attribuer des autorisations granulaires pour la surveillance, le reporting et Cloud Secure séparément.

Vous pouvez ainsi autoriser davantage d'utilisateurs à accéder à des fonctions de surveillance, d'optimisation et de création de rapports tout en limitant l'accès à vos données d'activité et d'audit Cloud Secure sensibles à ceux qui en ont besoin.

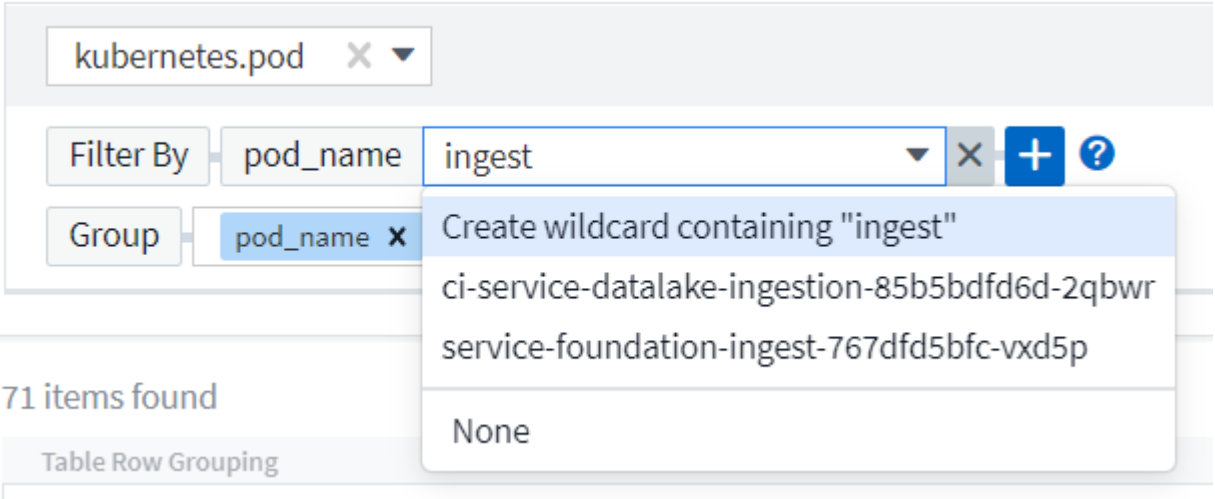
"En savoir plus" À propos des différents niveaux d'accès dans la documentation Cloud Insights.

Juin 2021

Suggestions, caractères génériques et expressions dans filtres

Avec cette version de Cloud Insights, vous n'avez plus besoin de connaître tous les noms et valeurs possibles pour filtrer les résultats d'une requête ou d'un widget. Lors du filtrage, il vous suffit de commencer à taper et Cloud Insights suggère des valeurs en fonction de votre texte. Fini les attentes liées aux applications et aux attributs Kubernetes à l'avance, juste pour trouver ceux que vous voulez afficher dans votre widget.

Lorsque vous tapez un filtre, le filtre affiche une liste intelligente des résultats que vous pouvez choisir, ainsi que l'option permettant de créer un **filtre générique** en fonction du texte actuel. Si vous sélectionnez cette option, tous les résultats correspondant à l'expression de caractère générique seront résélectionnés. Vous pouvez bien sûr sélectionner plusieurs valeurs individuelles que vous souhaitez ajouter au filtre.



En outre, vous pouvez créer **expressions** dans un filtre à l'aide DE NOT ou, ou 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

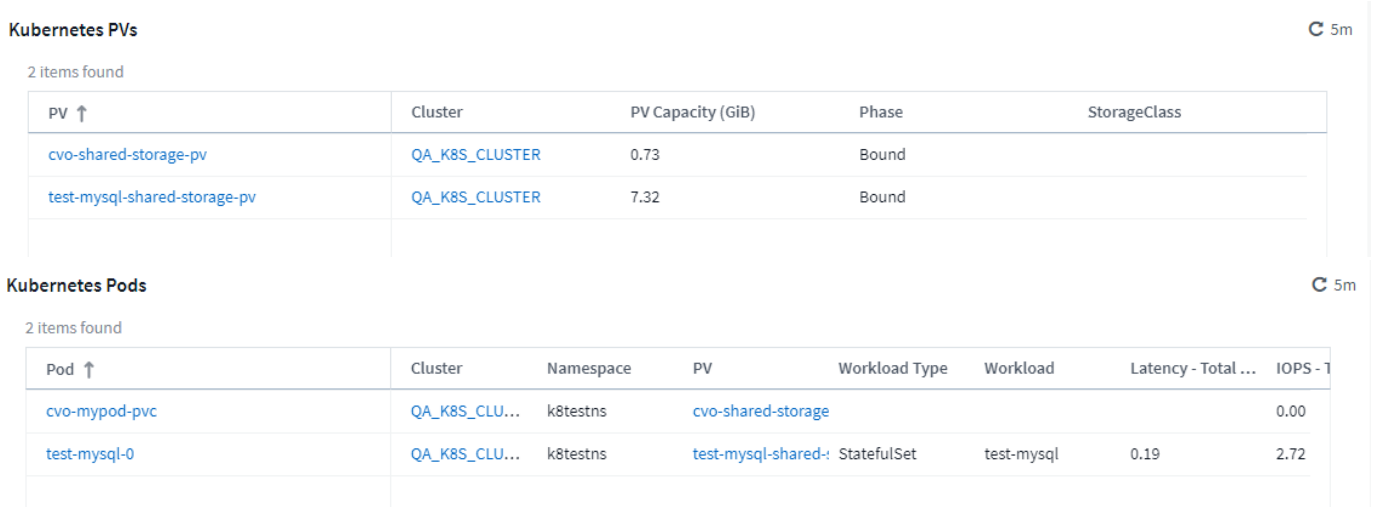
Les puissantes API de Cloud Insights sont plus accessibles que jamais, avec les API d'alertes désormais disponibles dans les éditions Standard et Premium. Les API suivantes sont disponibles pour chaque édition :

Catégorie API	Basique	Standard	Premium
Unité d'acquisition	✔	✔	✔
Collecte de données	✔	✔	✔
Alertes		✔	✔
Ressources		✔	✔
Ingestion des données		✔	✔

Visibilité sur les volumes persistants et pod pour Kubernetes

Cloud Insights fournit une visibilité sur le stockage back-end de vos environnements Kubernetes, ce qui vous donne des informations exploitables sur vos pods Kubernetes et vos volumes persistants. Vous pouvez désormais suivre les compteurs PV tels que les IOPS, la latence et le débit, depuis l'utilisation d'un seul pod via un compteur PV vers un PV et jusqu'au périphérique de stockage interne.

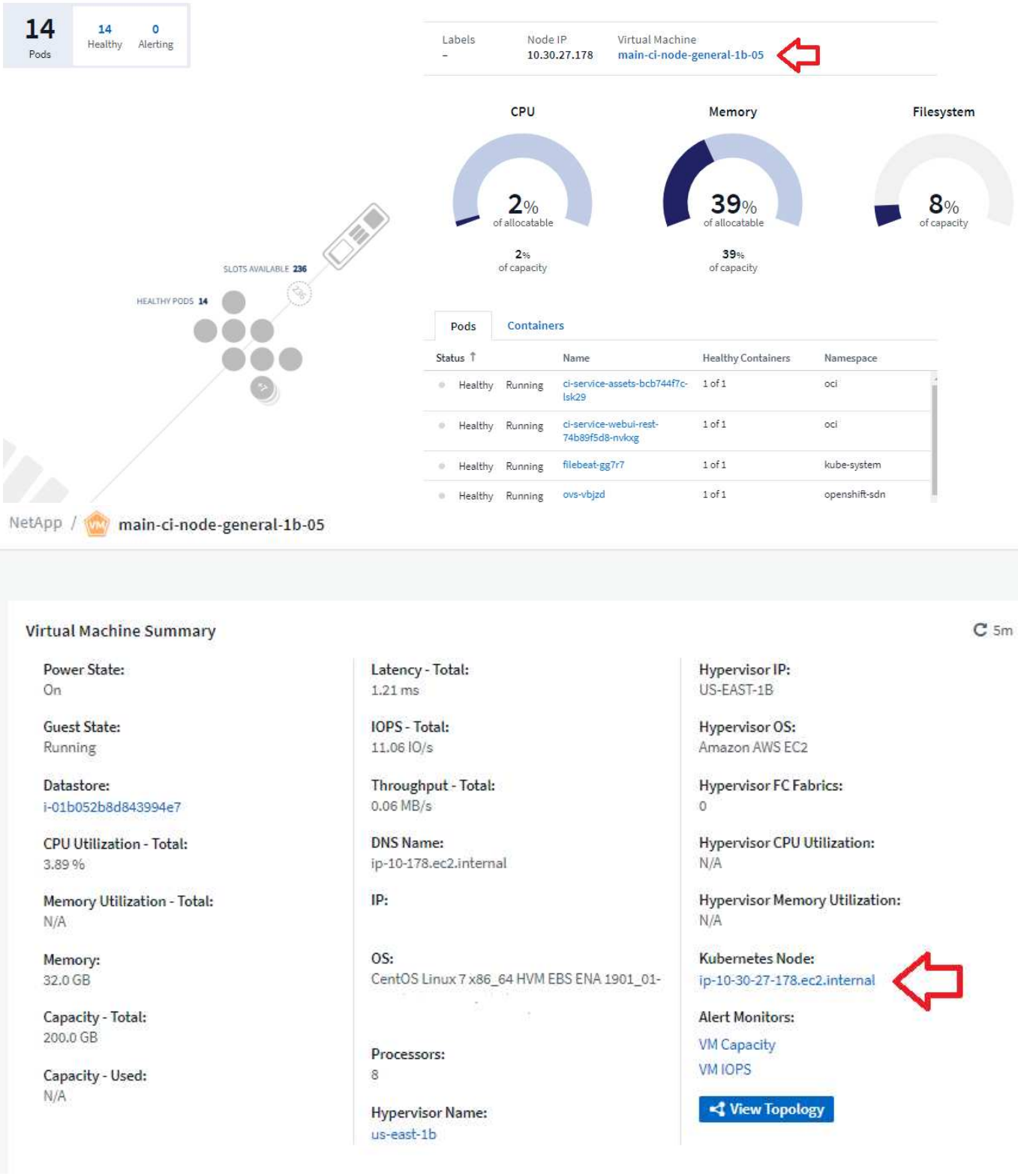
Sur une page d'accueil Volume ou Internal Volume, deux nouvelles tables sont affichées :



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

Liens entre un nœud Kubernetes et une machine virtuelle

Sur une page Kubernetes Node, vous pouvez maintenant cliquer sur pour ouvrir la page VM du nœud. La page VM comprend également un lien de retour vers le nœud lui-même.



Moniteurs d'alertes remplacement des règles de performance

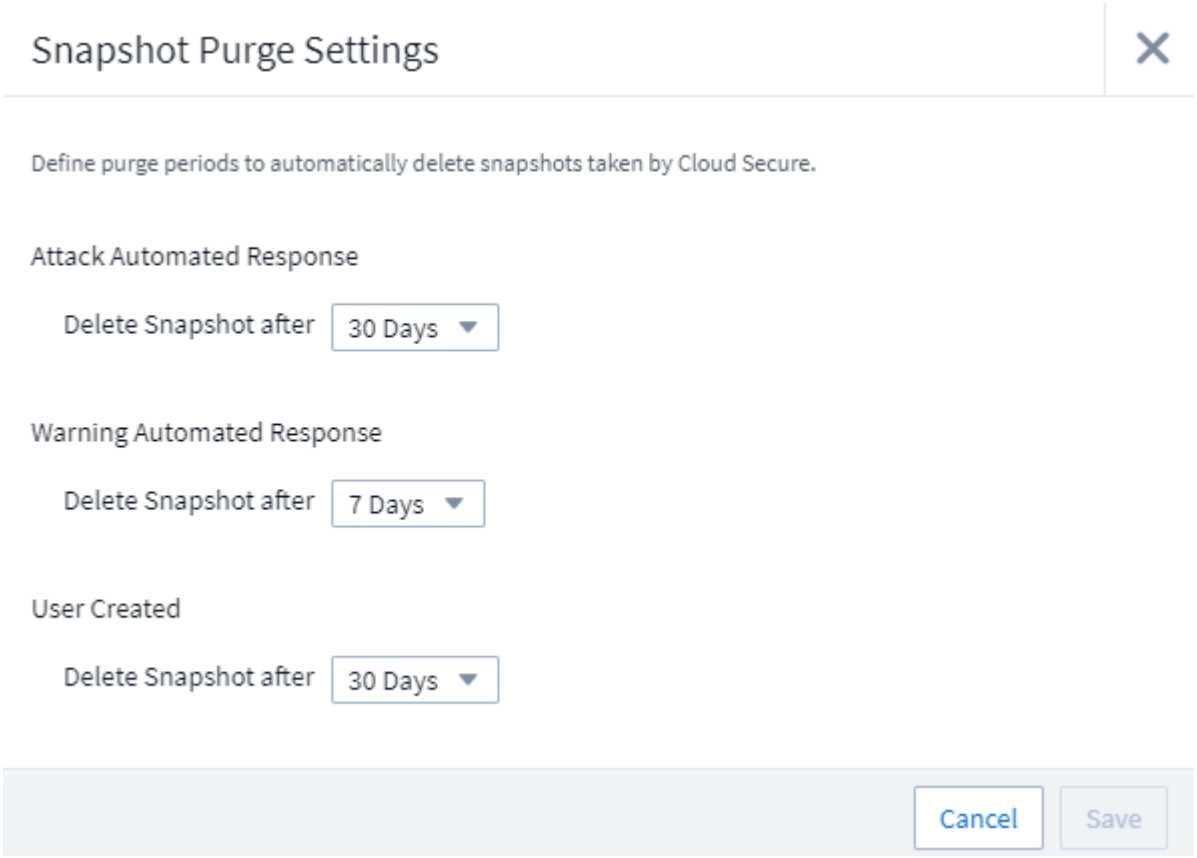
Pour bénéficier des avantages supplémentaires de la distribution de plusieurs seuils, de l'alerte Web et par e-mail, de l'alerte sur toutes les mesures à l'aide d'une interface unique, et plus encore, Cloud Insights convertit les clients de l'édition Standard et Premium de **stratégies de performance** en **moniteurs** pendant les mois de juillet et août 2021. En savoir plus sur "Alertes et moniteurs", et restez à l'affût 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 par ransomware. De plus, Cloud Secure prend en charge les répertoires des utilisateurs Active-Directory et LDAP pour la collecte d'attributs utilisateur NFS.

Suppression du snapshot Cloud Secure

Cloud Secure supprime automatiquement les snapshots en fonction des paramètres de purge des snapshots, pour économiser de l'espace de stockage et réduire la suppression manuelle des snapshots.



Vitesse de collecte des 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 apportés en avril :

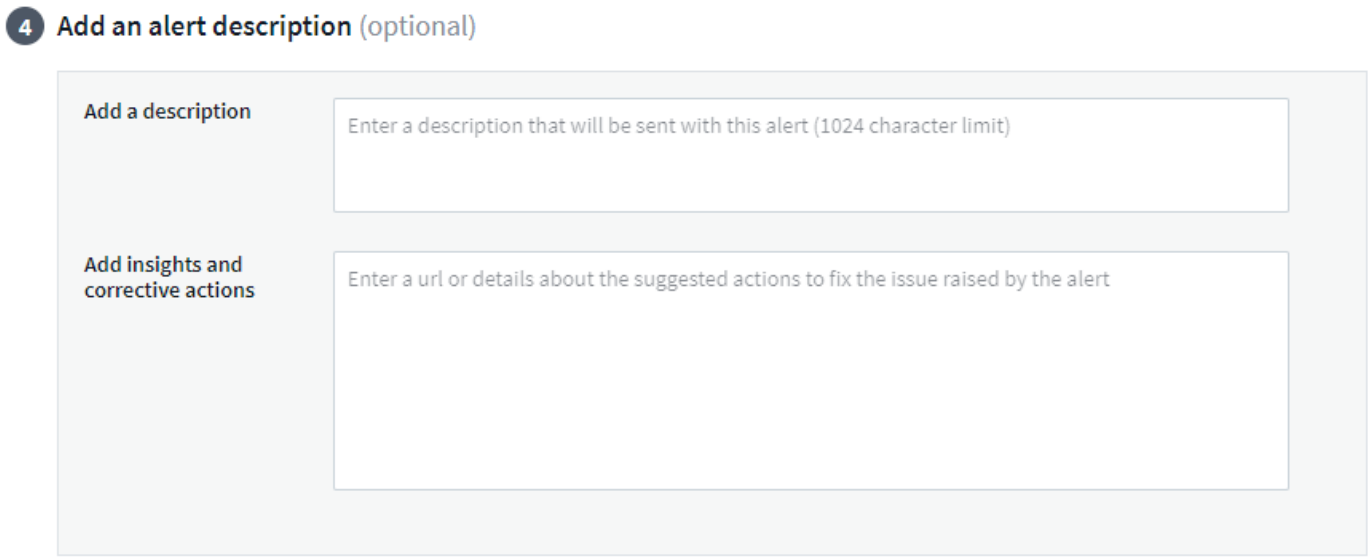
Agent Telegraf mis à jour

L'agent pour l'ingestion de données d'intégration de telegraf a été mis à jour vers la version 1.17.3, avec des améliorations de performance et de sécurité. Les utilisateurs qui souhaitent mettre à jour peuvent se reporter à

la section de mise à niveau appropriée de la "Installation de l'agent" documentation. Les versions précédentes de l'agent continueront de fonctionner sans qu'aucune action de l'utilisateur ne soit nécessaire.

Ajouter des actions correctives à une alerte

Vous pouvez maintenant 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 *Insights et actions correctives* peut fournir des étapes détaillées et des conseils sur la gestion des alertes et sera affiché dans la section récapitulative de la page d'arrivée de l'alerte.



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, tandis que les utilisateurs de l'édition Standard peuvent interroger des mesures et récupérer des mesures personnalisées. L'édition Premium continue d'autoriser l'utilisation complète de toutes les catégories d'API.

Catégorie API	Basique	Standard	Premium
Unité d'acquisition	✔	✔	✔
Collecte de données	✔	✔	✔
Ressources		✔	✔
Ingestion des données		✔	✔
Entrepôt de données			✔

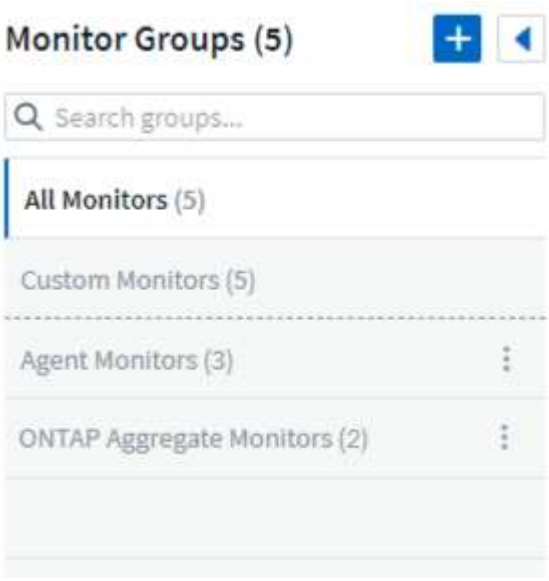
Pour plus d'informations sur l'utilisation de l'API, reportez-vous au "Documentation de l'API".

Avril 2021

Gestion simplifiée des moniteurs

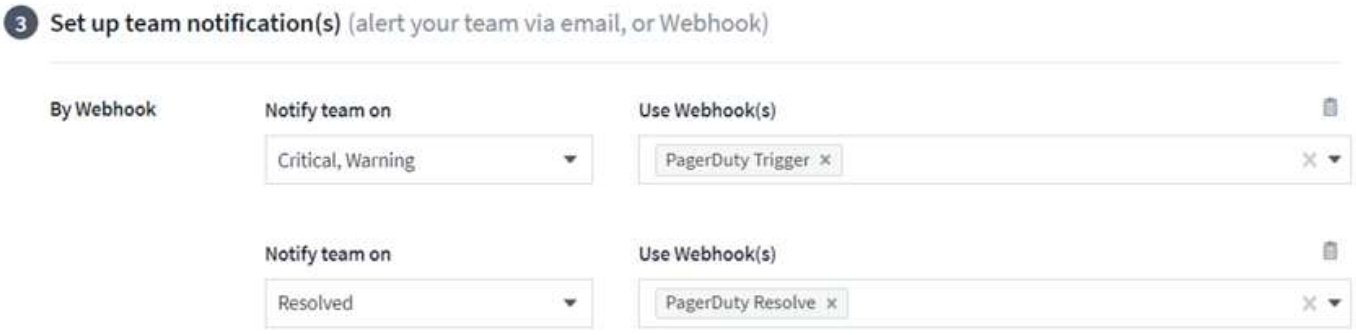
"Regroupement du moniteur" simplifie la gestion des moniteurs de votre environnement. Plusieurs moniteurs peuvent désormais être regroupés et mis en pause en un seul. Par exemple, si une mise à jour est effectuée sur une pile d'infrastructure, vous pouvez interrompre les alertes de tous ces périphériques en un clic.

Les groupes de moniteurs sont la première partie d'une nouvelle fonctionnalité intéressante qui améliore la gestion des périphériques ONTAP pour Cloud Insights.



Options d'alerte améliorées à l'aide de Webpatères

De nombreuses applications commerciales prennent en charge "Crochets en ligne" en tant qu'interface d'entrée standard. Cloud Insights prend désormais en charge la plupart de ces canaux de distribution, fournissant des modèles par défaut pour Slack, PagerDuty, Teams et discorde, en plus de fournir des crochets génériques personnalisables pour prendre en charge de nombreuses autres applications.



Identification améliorée des périphériques

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

Vous en avez demandé plus !

Les clients ont souvent demandé plus d'options par défaut pour visualiser la plage de données. Nous avons donc ajouté les cinq nouveaux choix suivants qui sont désormais disponibles dans tout le service via le sélecteur de plage horaire :

- Dernières 30 minutes
- Dernières 2 heures
- Dernières 6 heures
- Dernières 12 heures
- 2 derniers jours

Plusieurs abonnements dans un environnement Cloud Insights

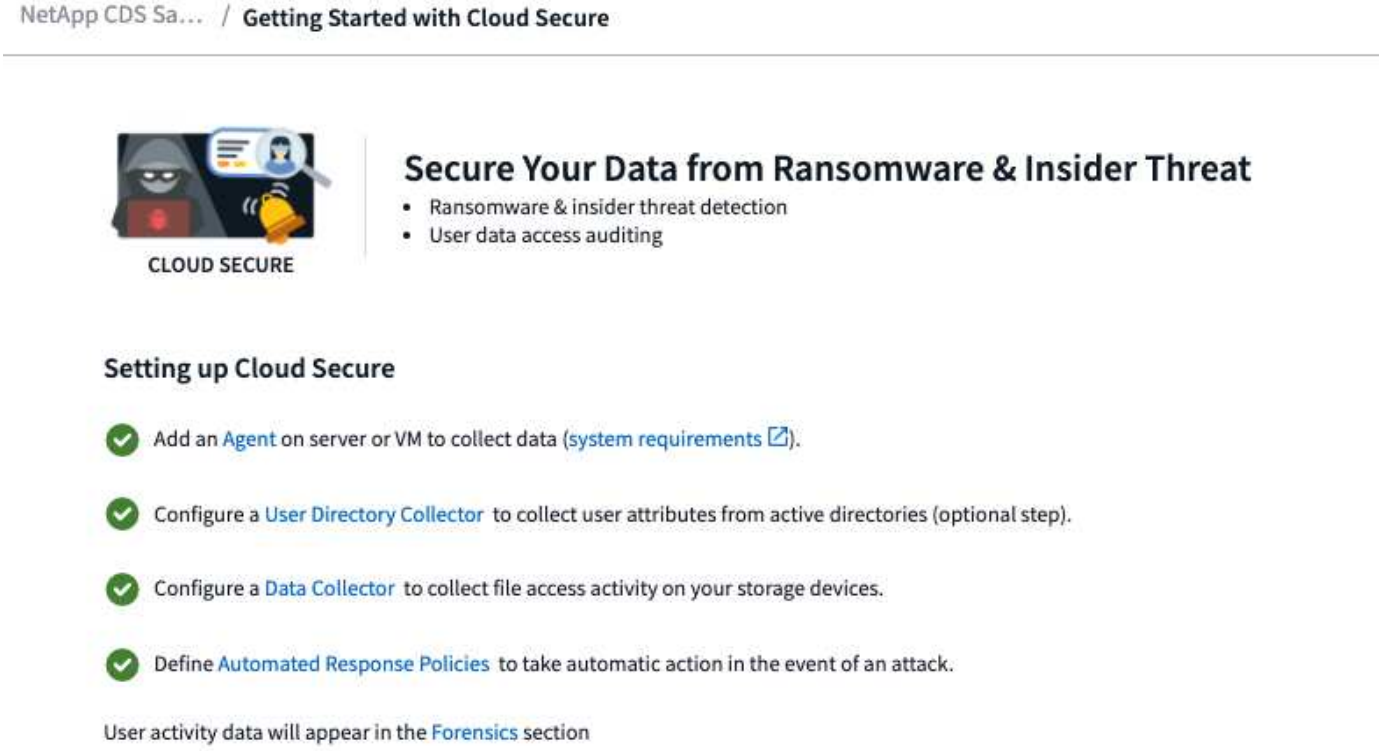
À partir du 2 avril, Cloud Insights prend en charge plusieurs abonnements du même type d'édition pour un client dans une seule instance Cloud Insights. Vous pouvez ainsi acquérir des éléments à terme de votre abonnement Cloud Insights en utilisant l'infrastructure. Contactez le service commercial NetApp pour obtenir de l'aide sur plusieurs abonnements.

Choisissez votre voie

Lors de la configuration de Cloud Insights, vous pouvez désormais choisir de commencer par surveiller et alertes ou par détection des attaques par ransomware et internes. Cloud Insights configurera votre environnement de départ en fonction du chemin que vous choisissez. Vous pouvez configurer l'autre chemin à tout moment.

Intégration Cloud Secure plus simple

En outre, vous pouvez commencer à utiliser Cloud Secure avec une nouvelle checklist de configuration détaillée.



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

Février 2021

Agent Telegraf mis à jour

L'agent pour l'ingestion de données d'intégration de telegraf a été mis à jour vers la version 1.17.0, qui inclut des correctifs de vulnérabilité et de bogues.

Analyseur de coût du cloud

Bénéficiez de la puissance de Spot by NetApp avec le coût du cloud, qui fournit une analyse détaillée des coûts des dépenses passées, présentes et estimées, afin de bénéficier d'une meilleure 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 ainsi qu'un aperçu détaillé des charges de travail, des comptes et des services individuels.

Le coût du cloud peut relever les défis majeurs suivants :

- Suivi et contrôle des dépenses liées au cloud
- Identification des déchets et des zones d'optimisation potentielles
- Livraison d'éléments d'action exécutables

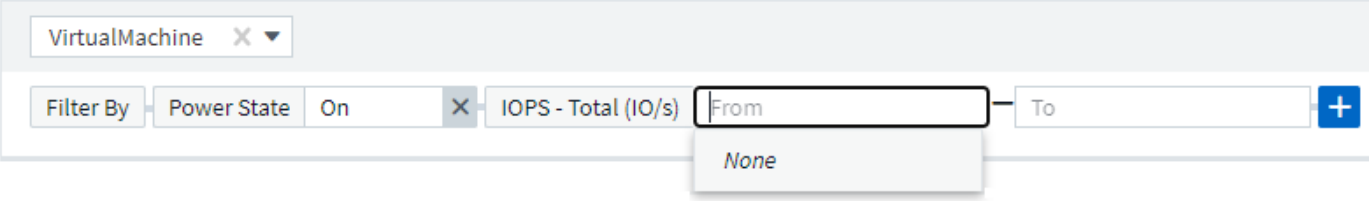
Le coût du cloud est axé sur la surveillance. Passez au compte point complet de NetApp pour réaliser des économies automatiques et optimiser l'environnement.

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

Cloud Insights permet désormais de rechercher des attributs et des mesures ayant des valeurs nulles/non via l'utilisation de filtres. Vous pouvez effectuer ce filtrage à tous les attributs/metrics dans les emplacements suivants :

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

Pour filtrer les valeurs NULL/None, il vous suffit de sélectionner l'option *None* lorsqu'elle apparaît dans la liste déroulante du filtre approprié.



Prise en charge multi-région

À partir d'aujourd'hui, nous proposons le service Cloud Insights dans différentes régions du monde, qui améliore les performances et la sécurité des clients situés en dehors des États-Unis. Cloud Insights/Cloud Secure stocke des 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 en vue d'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 de l'audit précédent	Nouveau nom de mesure
netapp_ontap.disque_composant.total_transferts	netapp_ontap.disk_composant.total_iops
netapp_ontap.disk.total_transferts	netapp_ontap.disk.total_iops
netapp_ontap.fcp_lif.read_data	netapp_ontap.fcp_lif.read_débit
netapp_ontap.fcp_lif.write_data	netapp_ontap.fcp_lif.débit_écriture

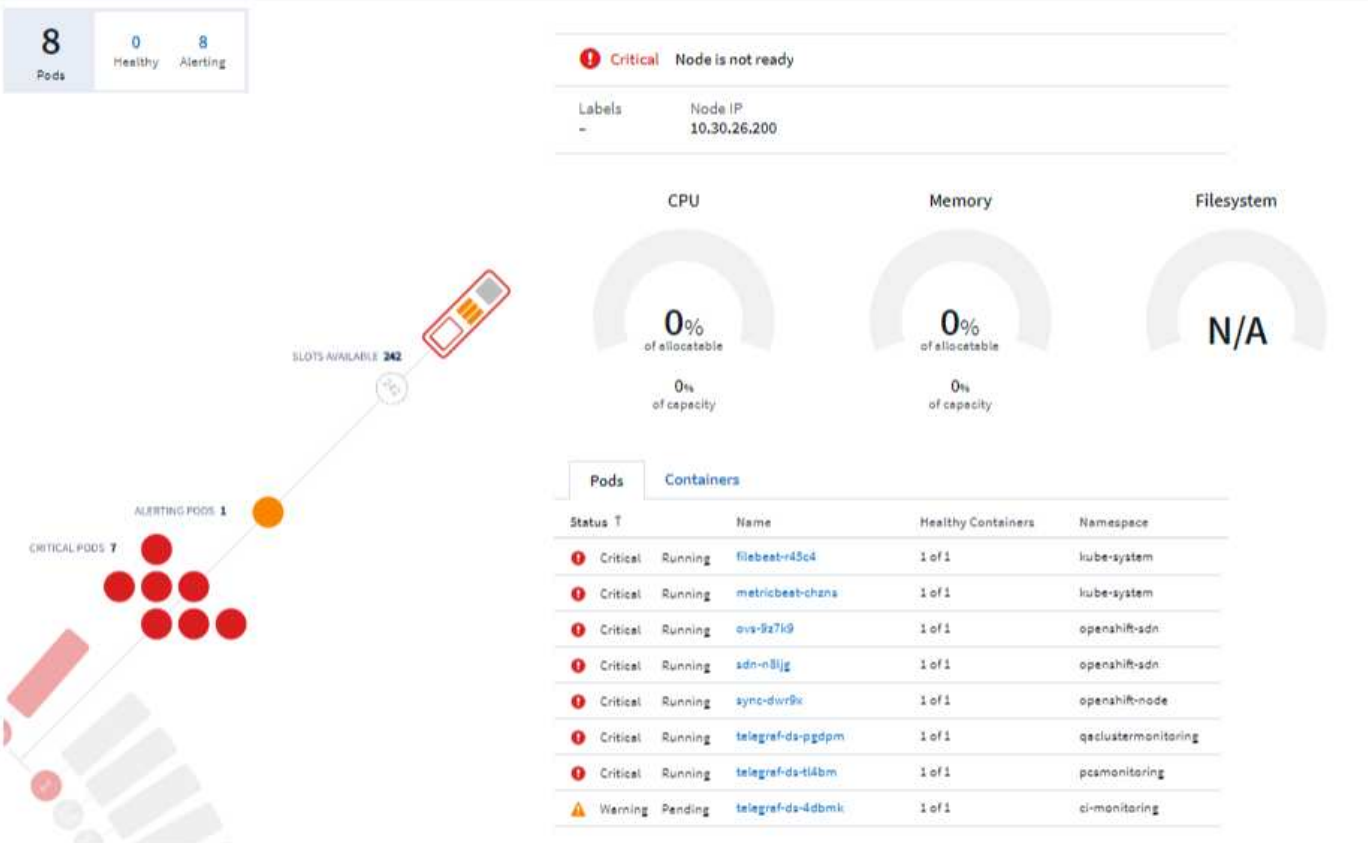
Nom de l'audit précédent	Nouveau nom de mesure
netapp_ontap.iscsi_lif.read_data	netapp_ontap.iscsi_lif.débit_lecture
netapp_ontap.iscsi_lif.write_data	netapp_ontap.iscsi_lif.débit_écriture
netapp_ontap.lif.recv_data	débit_netapp_ontap.lif.recv_recv
netapp_ontap.lif.sent_data	netapp_ontap.lif.sent_throughput
netapp_ontap.lun.read_data	netapp_ontap.lun.débit_lecture
netapp_ontap.lun.write_data	netapp_ontap.lun.débit_écriture
netapp_ontap.nic_common.rx_bytes	netapp_ontap.nic_common.rx_débit
netapp_ontap.nic_common.tx_bytes	netapp_ontap.nic_common.tx_débit
netapp_ontap.path.read_data	netapp_ontap.path.read_débit
netapp_ontap.path.write_data	netapp_ontap.path.write_débit
netapp_ontap.path.total_des_données	netapp_ontap.path.débit_total
netapp_ontap.policy_group.read_data	netapp_ontap.policy_group.débit_lecture
netapp_ontap.policy_group.write_data	netapp_ontap.policy_group.débit_écriture
netapp_ontap.policy_group.autres_données	netapp_ontap.policy_group.autre_débit
netapp_ontap.policy_group.total_data	netapp_ontap.policy_group.total_débit
netapp_ontap.system_node.disk_data_read	netapp_ontap.system_node.disk_débit_lecture
netapp_ontap.system_node.disk_data_wleged	netapp_ontap.system_node.disk_débit_écrit
netapp_ontap.system_node.hdd_data_read	netapp_ontap.system_node.hdd_débit_lecture
netapp_ontap.system_node.hdd_data_écrit	netapp_ontap.system_node.hdd_débit_écrit
netapp_ontap.system_node.ssd_data_read	netapp_ontap.system_node.ssd_débit_lecture
netapp_ontap.system_node.ssd_data_wleged	netapp_ontap.system_node.ssd_débit_écrit
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_recv
netapp_ontap.system_node.fcp_data_sent	netapp_ontap.system_node.fcp_débit_envoyé
netapp_ontap.volume_node.cifs_read_data	netapp_ontap.volume_node.cifs_read_débit
netapp_ontap.volume_node.cifs_write_data	netapp_ontap.volume_node.cifs_écriture_débit
netapp_ontap.volume_node.nfs_read_data	netapp_ontap.volume_node.nfs_read_débit
netapp_ontap.volume_node.nfs_write_data	netapp_ontap.volume_node.nfs_write_débit
netapp_ontap.volume_node.iscsi_read_data	netapp_ontap.volume_node.iscsi_read_débit
netapp_ontap.volume_node.iscsi_write_data	netapp_ontap.volume_node.iscsi_write_débit
netapp_ontap.volume_node.fcp_read_data	netapp_ontap.volume_node.fcp_read_débit
netapp_ontap.volume_node.fcp_write_data	netapp_ontap.volume_node.fcp_write_débit

Nom de l'audit précédent	Nouveau nom de mesure
netapp_ontap.volume.read_data	netapp_ontap.volume.débit_lecture
netapp_ontap.volume.write_data	netapp_ontap.volume.débit_écriture
netapp_ontap.workload.read_data	netapp_ontap.workload.débit_lecture
netapp_ontap.workload.write_data	netapp_ontap.workload.débit_écriture
netapp_ontap.workload_volume.read_data	netapp_ontap.workload_volume.débit_lecture
netapp_ontap.workload_volume.write_data	netapp_ontap.workload_volume.débit_écriture

Nouveau Kubernetes Explorer

"Kubernetes Explorer"Offre une vue topologique simple des clusters Kubernetes, ce qui permet même aux non-experts d'identifier rapidement les problèmes et les dépendances, du niveau du cluster au niveau du conteneur et du stockage.

Vous pouvez explorer de nombreuses informations à partir des informations détaillées de l'explorateur Kubernetes sur l'état, l'utilisation et l'état des clusters, des nœuds, des pods, des conteneurs et du stockage dans votre environnement Kubernetes.



Décembre 2020

Installation Kubernetes simplifiée

L'installation de Kubernetes Agent est rationalisée afin de réduire le nombre d'interactions entre l'utilisateur. "Installation de l'agent Kubernetes" Inclut désormais la collecte de données Kubernetes.

Novembre 2020

Tableaux de bord supplémentaires

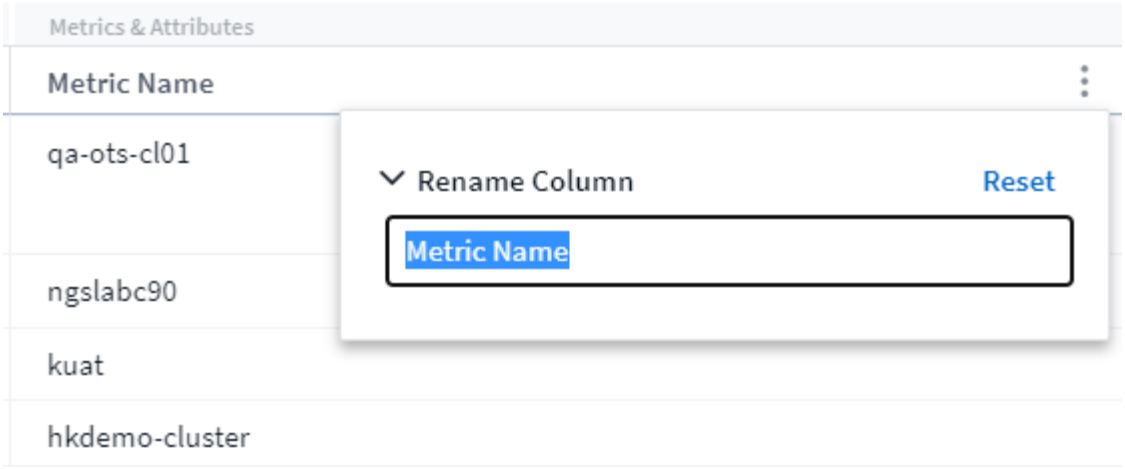
Les nouveaux tableaux de bord ONTAP suivants ont été ajoutés à la galerie et sont disponibles à l'importation :

- ONTAP : performances et capacité de l'agrégat
- FAS/AFF ONTAP - utilisation de la capacité
- Systèmes ONTAP FAS/AFF : capacité du cluster
- SYSTÈMES FAS/AFF ONTAP : EFFICACITÉ
- Systèmes FAS/AFF ONTAP - performances de FlexVol
- Systèmes FAS/AFF ONTAP - points opérationnels/optimaux des nœuds
- Systèmes FAS/AFF ONTAP : efficacité avant post-traitement de la capacité
- ONTAP : activité du port réseau
- ONTAP : performances des protocoles des nœuds
- ONTAP : performances des workloads de nœuds (front-end)
- ONTAP : processeur
- ONTAP : performances de charge de travail d'un SVM (front-end)
- ONTAP : performances des workloads de volumes (front-end)

Colonne Renommer dans les widgets du tableau

Vous pouvez renommer des colonnes dans la section *Metrics and Attributes* d'un widget de tableau en ouvrant le widget en mode Edition et en cliquant sur le menu en haut de la colonne. Entrez le nouveau nom et cliquez sur *Save*, ou cliquez sur *Reset* pour rétablir le nom d'origine de la colonne.

Notez que cela n'affecte que le nom d'affichage de la colonne dans le widget de table ; le nom de la mesure/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 l'extension par défaut des metrics Kubernetes, ONTAP Advanced Data et Agent Node. Par exemple, si vous regroupez Kubernetes *Nodes* par *Cluster*, vous verrez une ligne dans le tableau pour chaque cluster. Vous pouvez ensuite développer chaque ligne de cluster pour afficher la liste des objets noeud.

Assistance technique Edition de base

Le support technique est désormais disponible pour les abonnés à Cloud Insights édition de base en plus des éditions Standard et Premium. Cloud Insights a également simplifié le workflow de création d'un ticket de support NetApp.

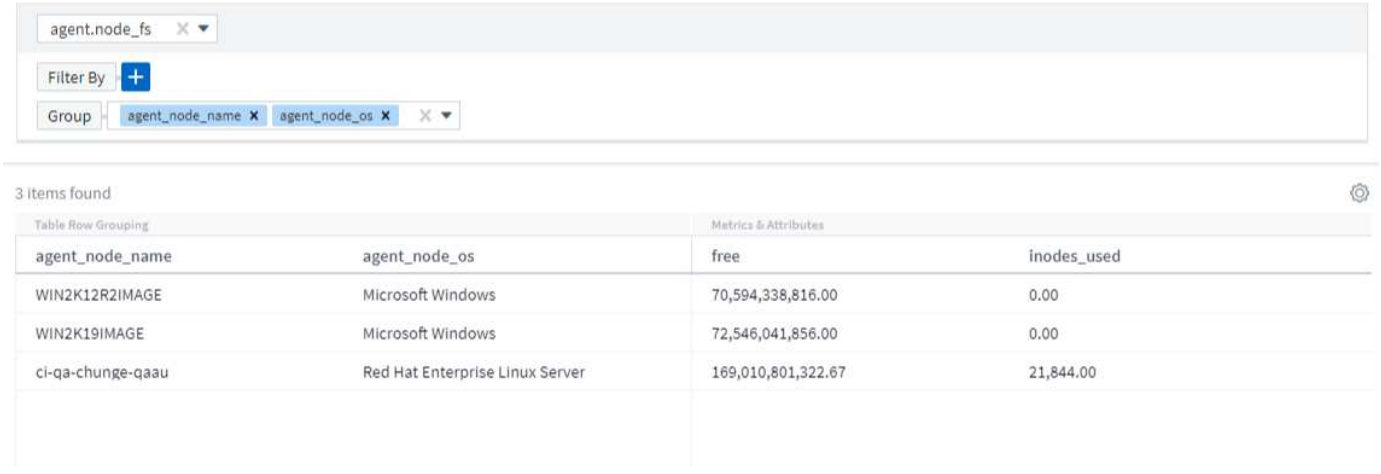
API publique Cloud Secure

Cloud Secure prend en charge l'"Les API REST"accès aux informations d'activité et d'alerte. Ce résultat est réalisé à l'aide de jetons d'accès d'API, créés via l'interface utilisateur d'administration de Cloud Secure, qui sont ensuite utilisées pour accéder aux API REST. La documentation swagger de ces API REST est intégrée à Cloud Secure.

Septembre 2020

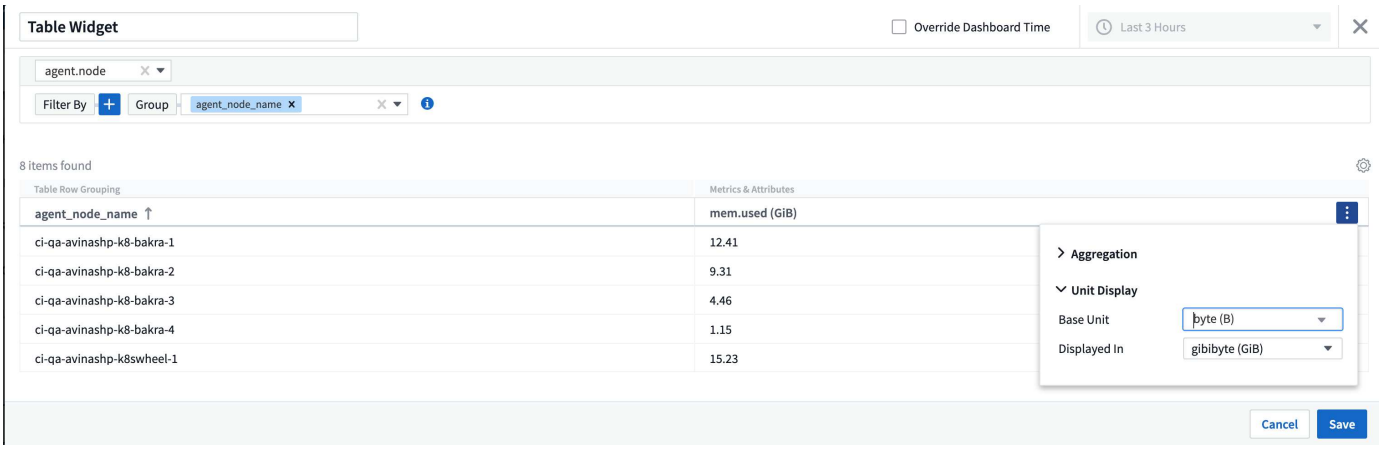
Page de requête avec données d'intégration

La page requête Cloud Insights prend en charge les données d'intégration (c'est-à-dire celles provenant de Kubernetes, des metrics avancés ONTAP, etc.). Lors de l'utilisation de données d'intégration, le tableau des résultats de la requête affiche une vue « écran fractionné », avec objet/regroupement sur le côté gauche et les données d'objet (attributs/metrics) sur la droite. Vous pouvez également choisir plusieurs attributs pour regrouper les données d'intégration.



Formatage de l'affichage de l'unité dans le widget de tableau

Le formatage de l'affichage de l'unité est désormais disponible dans les widgets du tableau pour les colonnes qui affichent des données métriques/compteur (par exemple, gigaoctets, Mo/seconde, etc.). Pour modifier l'unité d'affichage d'une mesure, cliquez sur le menu « trois points » dans l'en-tête de la colonne et sélectionnez « Affichage de l'unité ». Vous pouvez choisir parmi les 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 d'accueil, fournissant des détails utiles pour chaque au ainsi que des informations pour aider au dépannage. Le "Au page de détails" fournit des liens vers les collecteurs de données de l'au ainsi que des informations d'état utiles.

Dépendance vis-à-vis de Cloud Secure Docker supprimée

Cloud Secure n'a plus fait l'objet d'une dépendance vis-à-vis de Docker. Docker n'est plus nécessaire à l'installation de l'agent Cloud Secure.

Génération de rapports des rôles utilisateur

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

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

Rôle Cloud Insights	Rôle de génération de rapports	Autorisations liées aux rapports
Invité	Grand public	Permet d'afficher, de planifier et d'exécuter des rapports et de définir des préférences personnelles telles que celles pour les langues et les fuseaux horaires. Les clients ne peuvent pas créer de rapports ni effectuer des tâches administratives.
Utilisateur	Auteur	Peut exécuter toutes les fonctions de l'utilisateur ainsi que créer et gérer des rapports et des tableaux de bord.
Administrateur	Administrateur	Peut exécuter toutes les fonctions auteur ainsi que toutes les tâches administratives telles que la configuration des rapports et l'arrêt et le redémarrage des tâches de rapport.

Le reporting Cloud Insights est disponible pour les environnements de 500 UM ou plus.

Si vous êtes un client Premium Edition actuel et souhaitez conserver vos rapports, lisez ceci "remarque importante pour les clients existants".

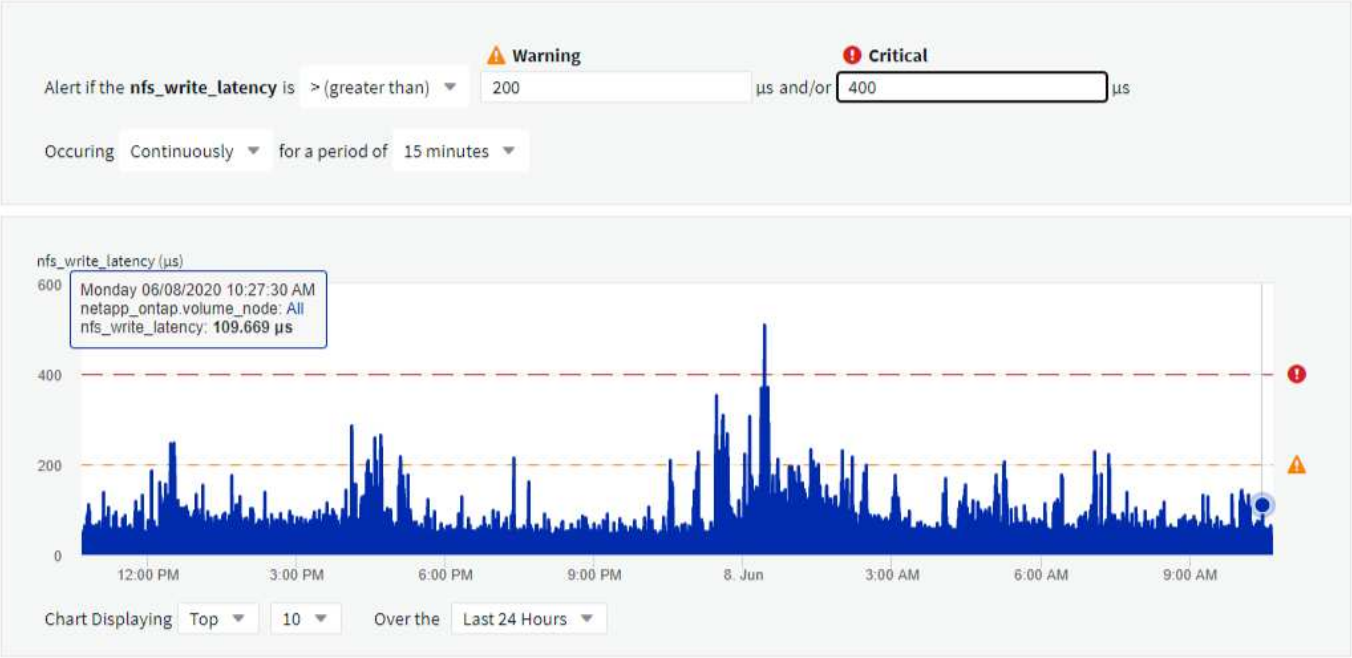
Nouvelle catégorie d'API pour l'acquisition de données

Cloud Insights a ajouté une catégorie API **Data ingestion**, vous donnant un meilleur contrôle sur les données et les agents personnalisés. Vous trouverez une documentation détaillée pour cette catégorie et d'autres catégories d'API dans Cloud Insights en accédant à **Admin > accès API** et en cliquant sur le lien *API Documentation*. Vous pouvez également joindre un commentaire à l'UA dans le champ Note qui s'affiche sur la page de détails de l'au ainsi que sur la page de liste de l'UA.

Août 2020

Surveillance et alertes

Outre la possibilité actuelle de définir des règles de performance pour les objets de stockage, les serveurs virtuels, EC2 et les ports, Cloud Insights Standard Edition inclut désormais la possibilité de définir "configurer les moniteurs"des seuils pour les données d'intégration pour Kubernetes, les metrics avancés ONTAP et les plug-ins Telegraf. Il vous suffit de créer un moniteur pour chaque mesure d'objet à déclencher des alertes, de définir les conditions des seuils de niveau d'avertissement ou de niveau critique et de spécifier le ou les destinataires d'e-mail souhaités pour chaque niveau. Vous pouvez ensuite "afficher et gérer les alertes"suivre les tendances ou résoudre les problèmes.



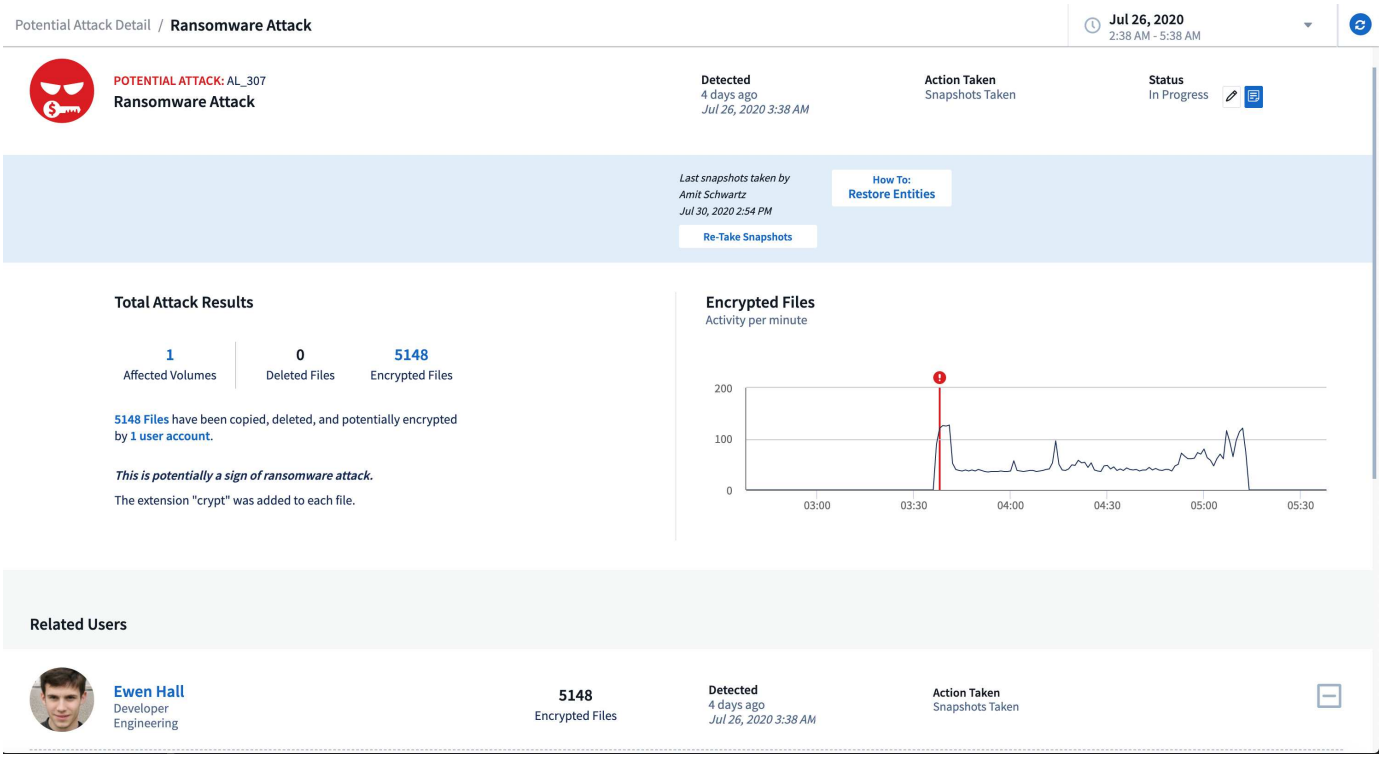
Juillet 2020

Cloud Secure *prendre une action instantané*

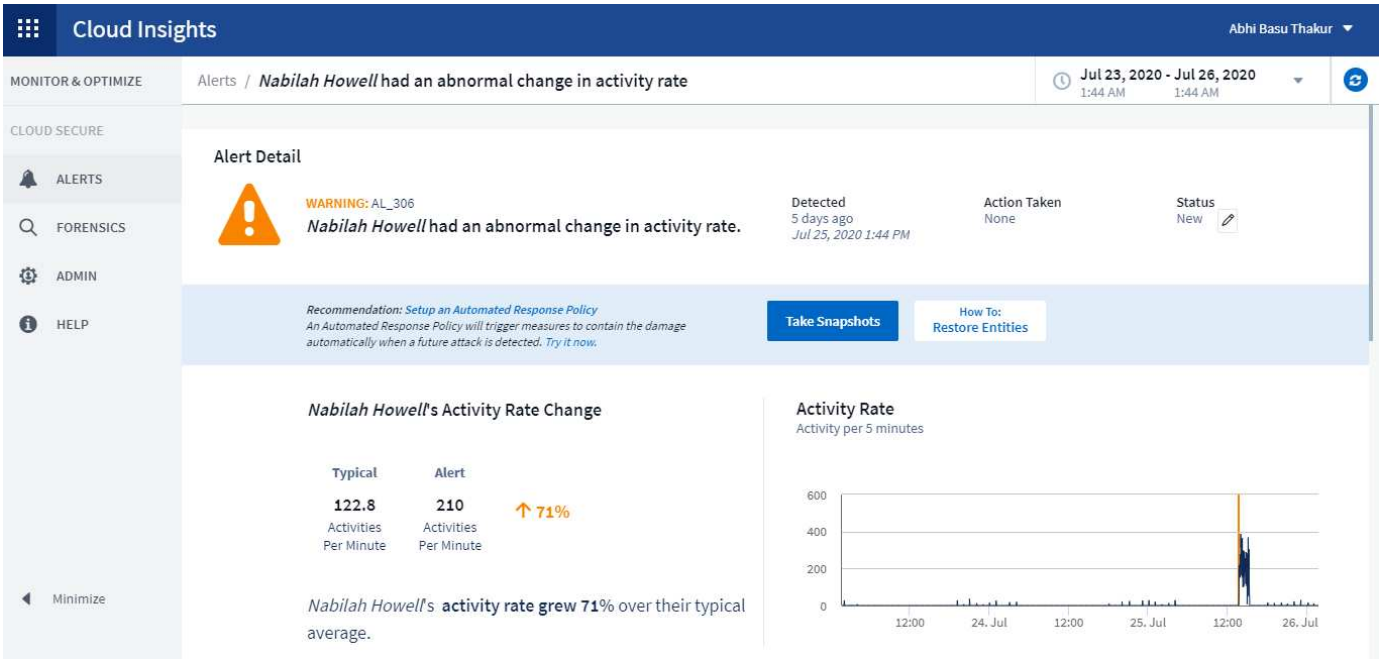
Cloud Secure protège vos données en effectuant automatiquement des copies Snapshot en cas de détection d'activités malveillantes, ce qui garantit la sauvegarde sécurisée de vos données.

Vous pouvez définir des règles de réponse automatisées qui prennent une copie Snapshot en cas d'attaque par ransomware ou d'autre activité anormale de l'utilisateur. Vous pouvez également prendre un instantané manuellement à partir de la page d'alerte.

Instantané automatique pris :



Instantané manuel :



Mises à jour des mesures/compteurs

Les compteurs de capacité suivants sont disponibles pour une utilisation dans l'interface utilisateur Cloud Insights et l'API REST. Auparavant, ces compteurs étaient uniquement disponibles pour l'entrepôt de données / les rapports.

Type d'objet	Compteur
Stockage	Capacité - capacité brute de réserve - défaillance brute

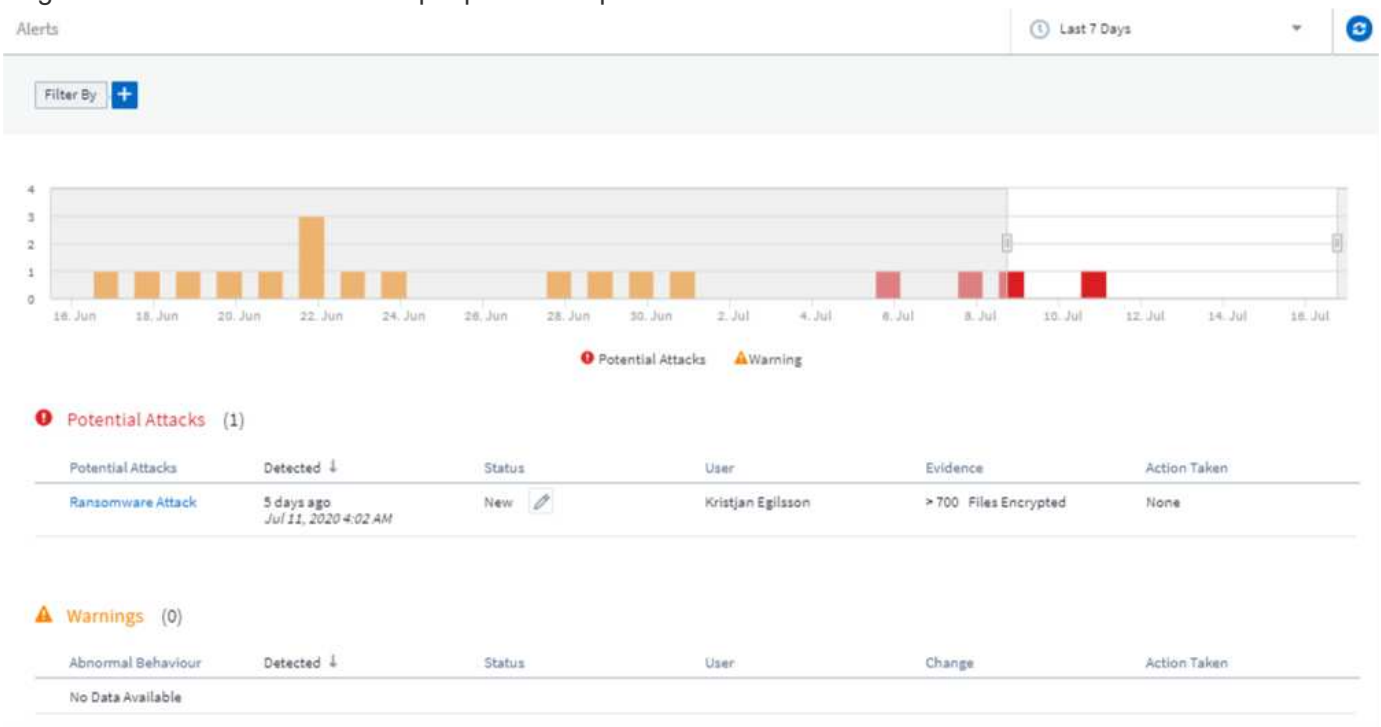
Type d'objet	Compteur
Pool de stockage	Capacité des données - capacité des données utilisées - Total des autres capacités - autre capacité utilisée - capacité totale - capacité brute - limite souple
Volume interne	Capacité des données - capacité des données utilisées - Total autre capacité - autre capacité utilisée - Total Clone Saved Capacity - Total

Détection des attaques potentielles au Cloud Secure

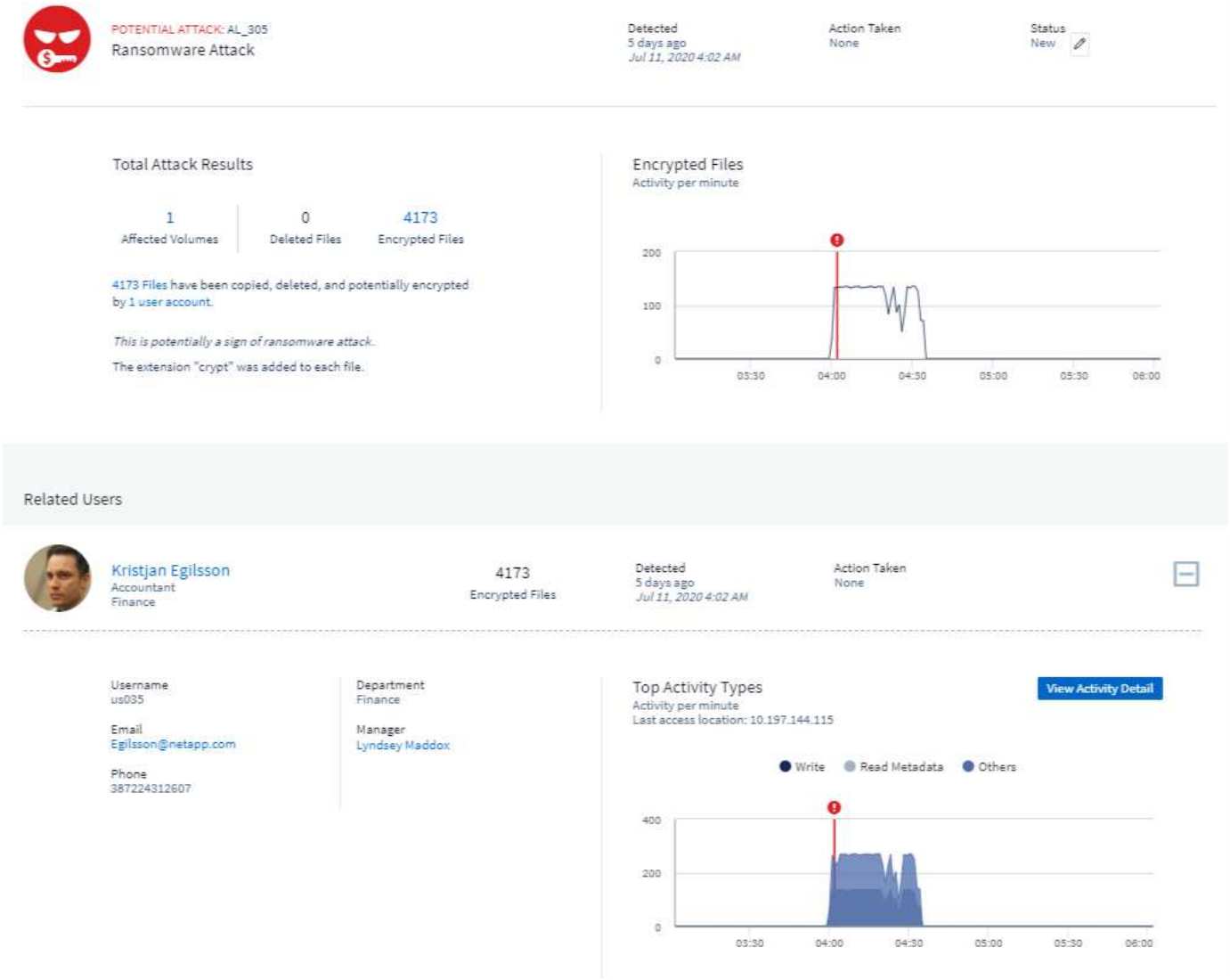
Cloud Secure détecte désormais les attaques potentielles telles que les ransomwares. Cliquez sur une alerte dans la page de liste alertes pour ouvrir une page de détails présentant les éléments suivants :

- Heure d'attaque
- Activité associée de l'utilisateur et du fichier
- Action entreprise
- Informations supplémentaires pour aider à effectuer le suivi des violations de sécurité possibles

Page d'alertes montrant une attaque potentielle par ransomware :



Page de détails des attaques par ransomware potentielles :



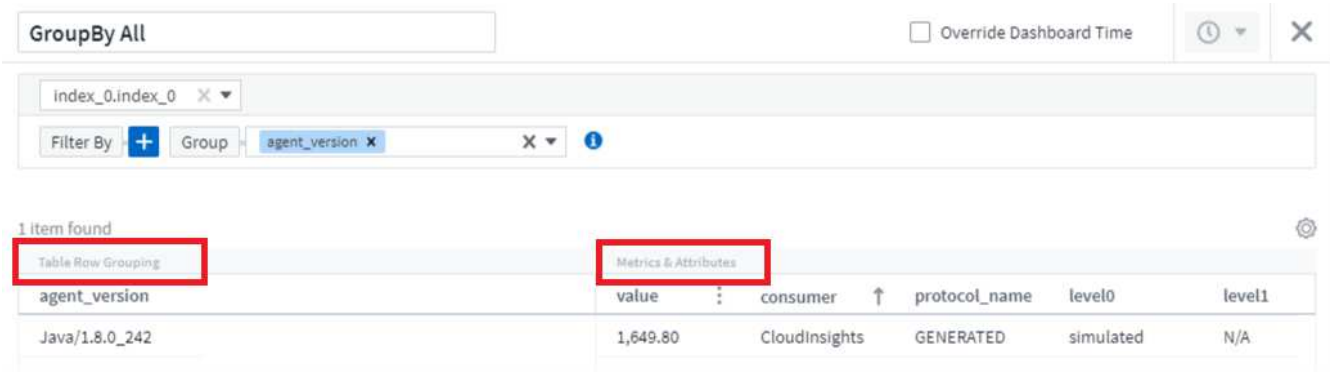
Abonnez-vous à Premium Edition via AWS

Pendant la version d'évaluation de Cloud Insights, vous pouvez "s'abonner vous-même" utiliser AWS Marketplace pour accéder à l'édition Standard ou Premium de Cloud Insights. Auparavant, vous pouviez uniquement vous abonner automatiquement à AWS Marketplace pour l'édition Standard.

Widget Table amélioré

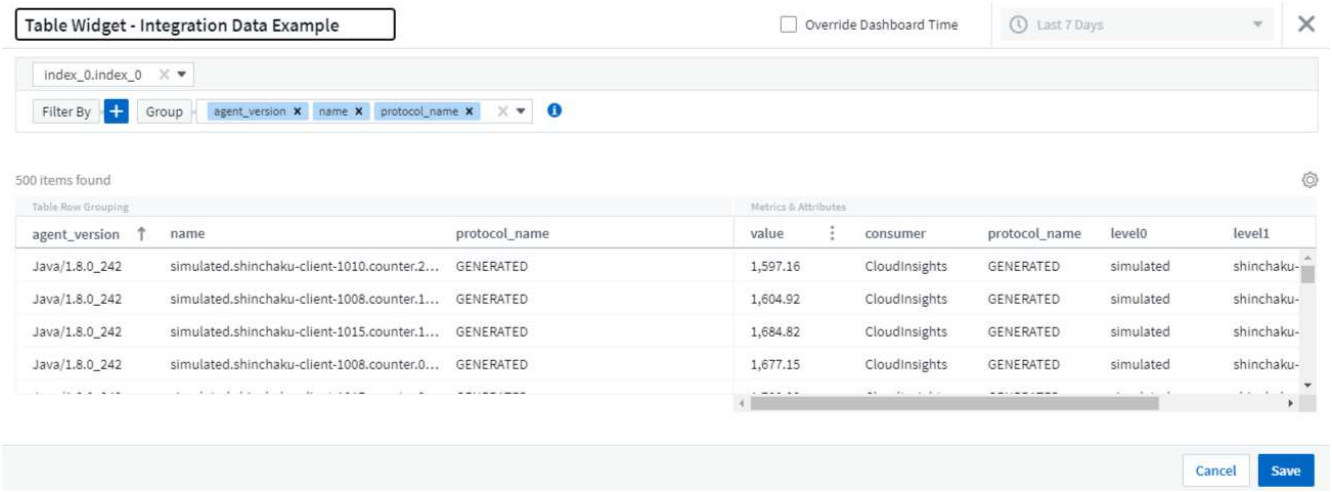
Le widget Tableau de bord/ressources comprend les améliorations suivantes :

- Vue « écran divisé » : les widgets de tableau affichent l'objet/le regroupement sur le côté gauche et les données d'objet (attributs/métriques) sur la droite.



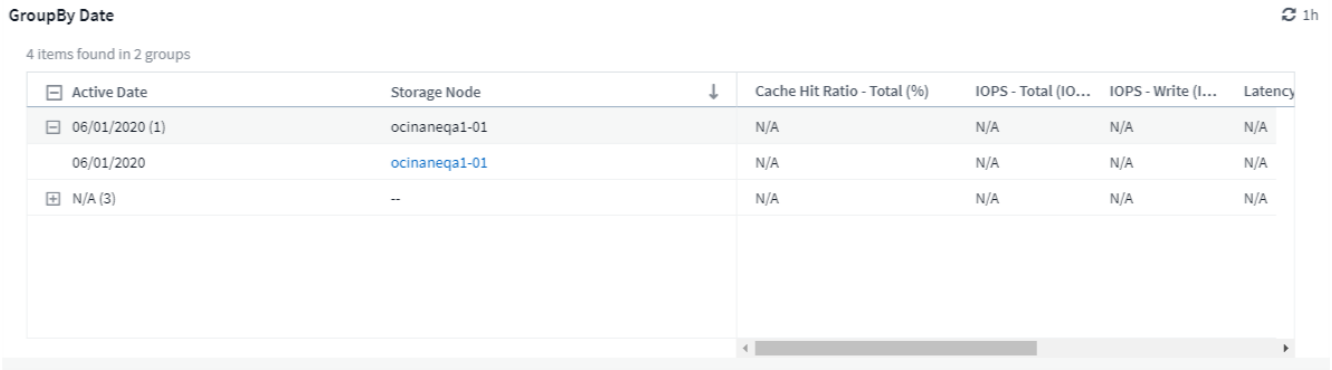
- Regroupement d'attributs multiples : pour les données d'intégration (Kubernetes, ONTAP Advanced Metrics, Docker, etc.), vous pouvez choisir plusieurs attributs pour le regroupement. Les données sont affichées en fonction des attributs de regroupement/que vous choisissez.

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



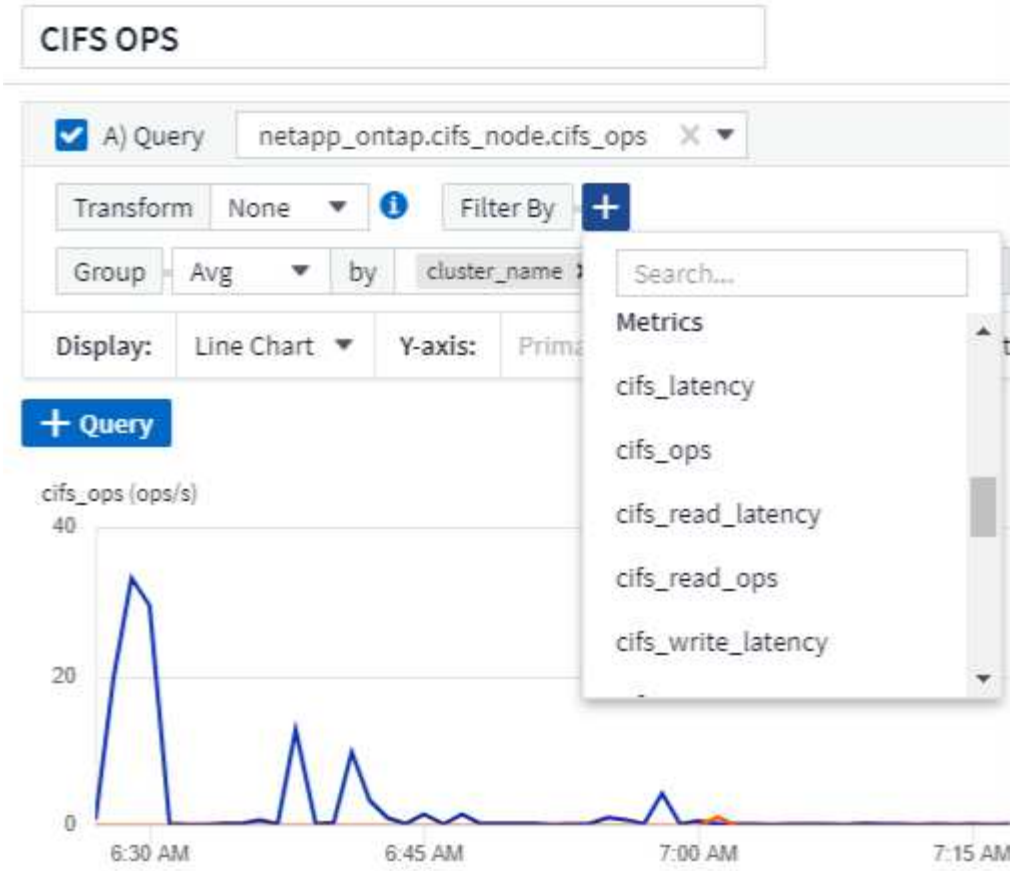
- Le regroupement des données d'infrastructure (stockage, EC2, VM, ports, etc.) se fait par un seul attribut, comme auparavant. Lors du regroupement par un attribut qui n'est pas l'objet, la table vous permet de développer la ligne du groupe pour voir tous les objets du groupe.

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

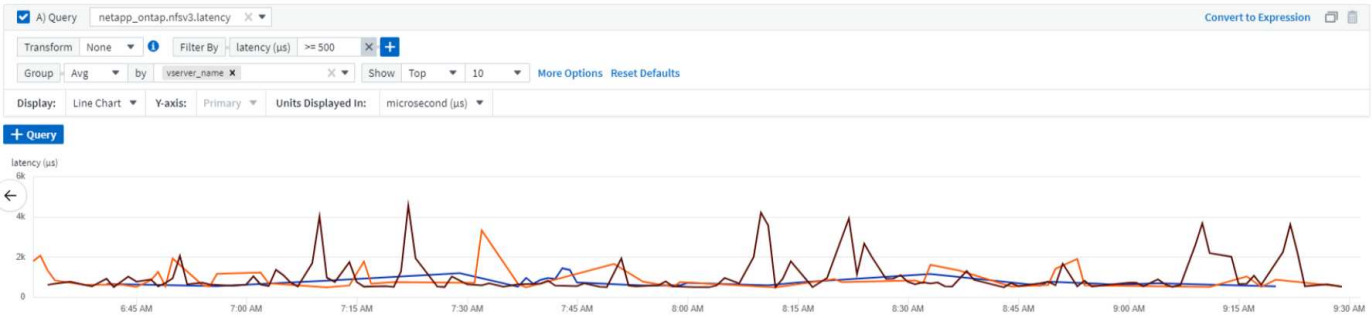


Filtrage de metrics

Outre le filtrage des attributs d'un objet dans un widget, vous pouvez désormais également filtrer les metrics.



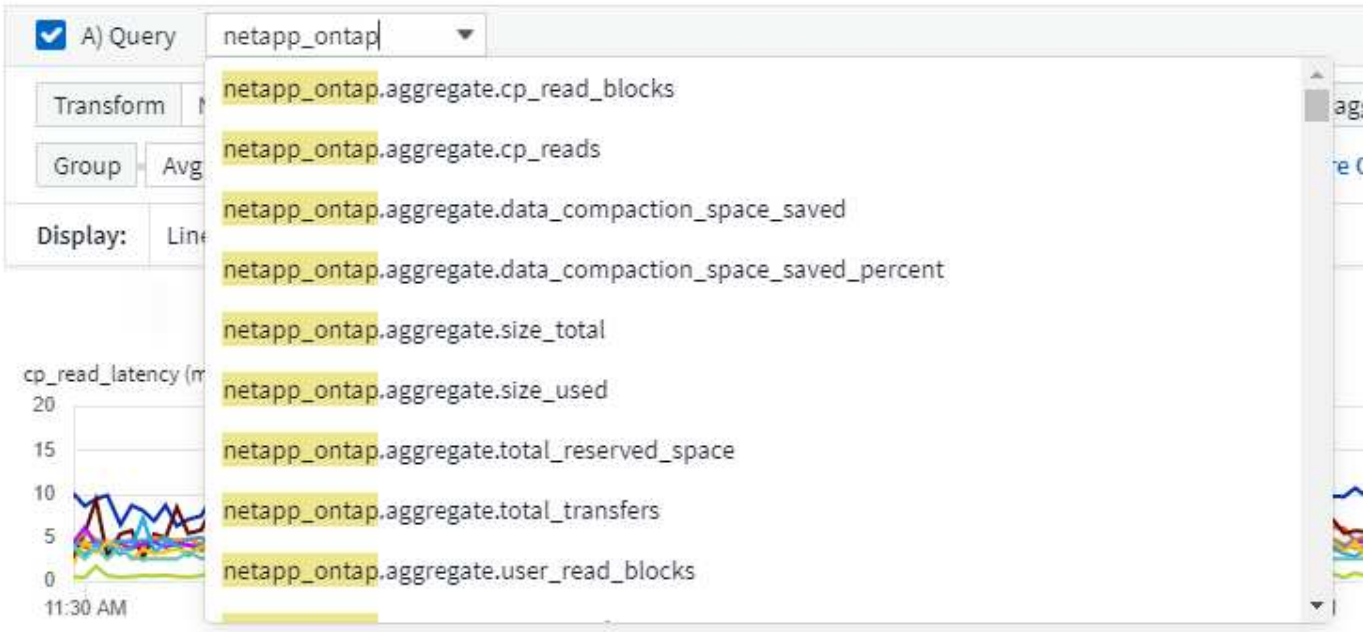
Lors de l'utilisation des données d'intégration (Kubernetes, ONTAP Advanced Data, etc.), le filtrage des mesures supprime les points de données individuels/non inégalés de la série de données tracées, contrairement aux données d'infrastructure (stockage, VM, ports, etc.), où les filtres fonctionnent sur la valeur agrégée de la série de données et peuvent potentiellement supprimer l'objet entier du graphique.



Données de compteur avancées ONTAP

Cloud Insights tire parti de la **Advanced Counter Data** propre à ONTAP, qui fournit une multitude de compteurs et de metrics collectés auprès des périphériques ONTAP. Les données de compteur avancé ONTAP sont disponibles pour tous les clients NetApp ONTAP. Ces indicateurs permettent une visualisation personnalisée et étendue dans les widgets et tableaux de bord Cloud Insights.

Pour trouver les compteurs avancés ONTAP, recherchez « netapp_ontap » dans la requête du widget et sélectionnez parmi les compteurs.



Vous pouvez affiner votre recherche en saisissant d'autres parties du nom du compteur. Par exemple :

- *lif*
- *agrégat*
- *offbox_vscan_server*
- entre autres



Veuillez noter ce qui suit :

- La collecte de données avancée 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 avancée des données n'est pas disponible pour les systèmes ONTAP 7-mode.

Tableaux de bord avancés

Cloud Insights est fourni avec une variété de tableaux de bord prédéfinis pour vous aider à commencer à visualiser les compteurs avancés ONTAP pour des sujets tels que *Aggregate Performance*, *Volume Workload*, *Processor Activity*, et bien plus encore. Si au moins un collecteur de données ONTAP est configuré, il est possible de les importer à partir de la galerie de tableaux de bord sur n'importe quelle page de liste de tableaux de bord.

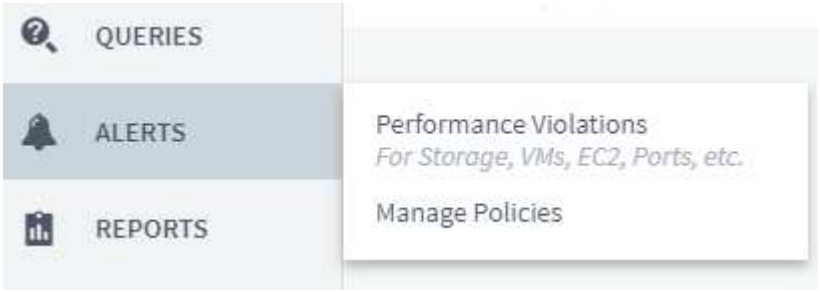
En savoir plus

Vous trouverez plus d'informations sur les données avancées de ONTAP dans les liens suivants :

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

Menu stratégies et violations

Les politiques de performance et les violations se trouvent désormais dans le menu **alertes**. Les règles et les violations de la fonctionnalité sont inchangées.



Agent Telegraf mis à jour

L'agent d'ingestion des données d'intégration telegraf a été mis à jour vers "version 1.14", qui inclut des correctifs de bogues, des correctifs de sécurité et de nouveaux plug-ins.

Remarque : lors de la configuration d'un collecteur de données Kubernetes sur la plateforme Kubernetes, une erreur « HTTP status 403 interdit » s'affiche dans le journal, en raison des autorisations insuffisantes dans l'attribut « clusterrole ».

Pour contourner ce problème, ajoutez les lignes mises en évidence suivantes à la section *rules:* du rôle cluster noeud final-accès, puis redémarrez les modules 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 du Data Collector simplifié

Le fait de signaler une erreur du collecteur de données est plus simple grâce au bouton *Send Error Report* de la page Data Collector. Cliquer sur le bouton envoie des informations de base sur l'erreur à NetApp et invite l'utilisateur à enquêter sur le problème. Une fois enfoncé, Cloud Insights reconnaît que NetApp a été notifié et que le bouton Rapport d'erreur est désactivé pour indiquer qu'un rapport d'erreur relatif à ce collecteur de données a été envoyé. Le bouton reste désactivé jusqu'à ce que la page du navigateur soit actualisée.

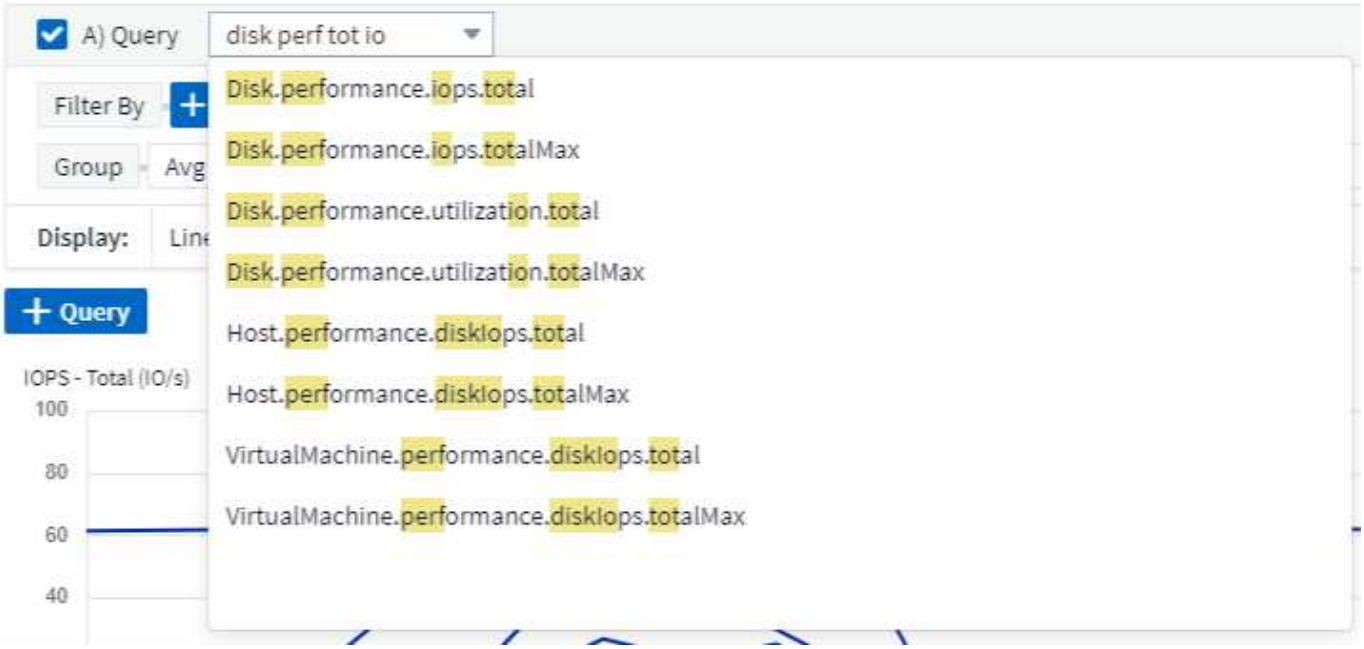


Améliorations des widgets

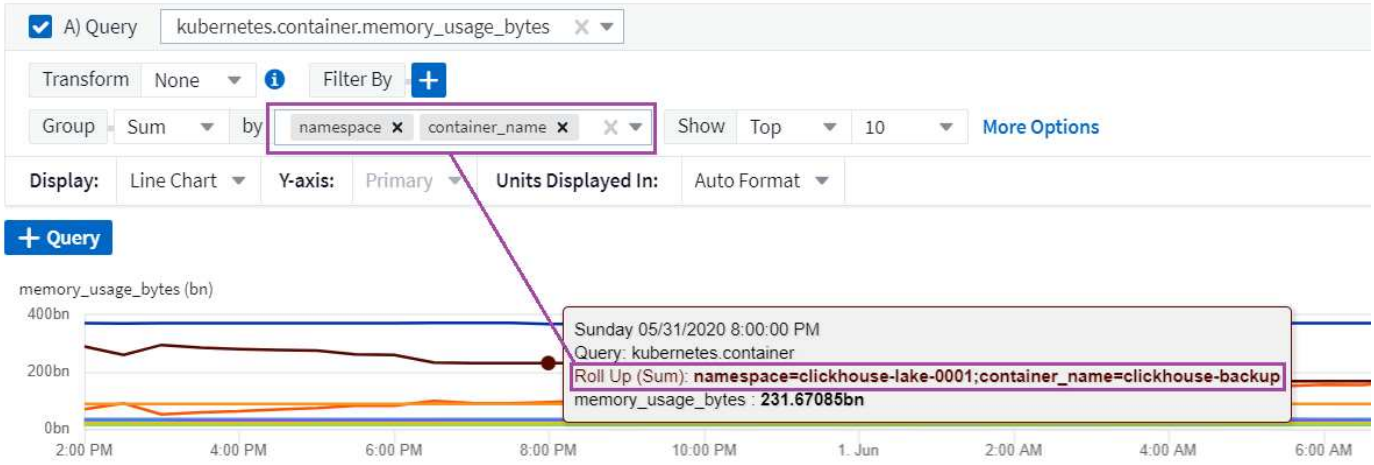
Les améliorations suivantes ont été apportées aux widgets du tableau de bord : Ces améliorations sont considérées comme une fonctionnalité d'aperçu et peuvent ne pas être disponibles pour tous les environnements Cloud Insights.

- Nouveau sélecteur d'objets/de mesures : les objets (stockage, disque, ports, nœuds, etc.) et les mesures associées (IOPS, latence, nombre de CPU, etc.) sont à présent disponibles dans des widgets dans une liste déroulante unique avec une fonctionnalité de recherche puissante. Vous pouvez entrer plusieurs

termes partiels dans la liste déroulante. Cloud Insights répertoriera tous les metrics d'objets répondant à ces termes.



- Regroupement de plusieurs balises : lorsque vous utilisez des données d'intégration (Kubernetes, etc.), vous pouvez regrouper les données par plusieurs balises/attributs. Par exemple, somme de l'utilisation de la mémoire par le namespace Kubernetes et le nom du conteneur.



Mai 2020

Génération de rapports des rôles utilisateur

Les rôles suivants ont été ajoutés pour le reporting :

- Consommateurs Cloud Insights : peut exécuter et afficher des rapports
- Auteurs Cloud Insights : peut exécuter les fonctions client ainsi que créer et gérer des rapports et des tableaux de bord

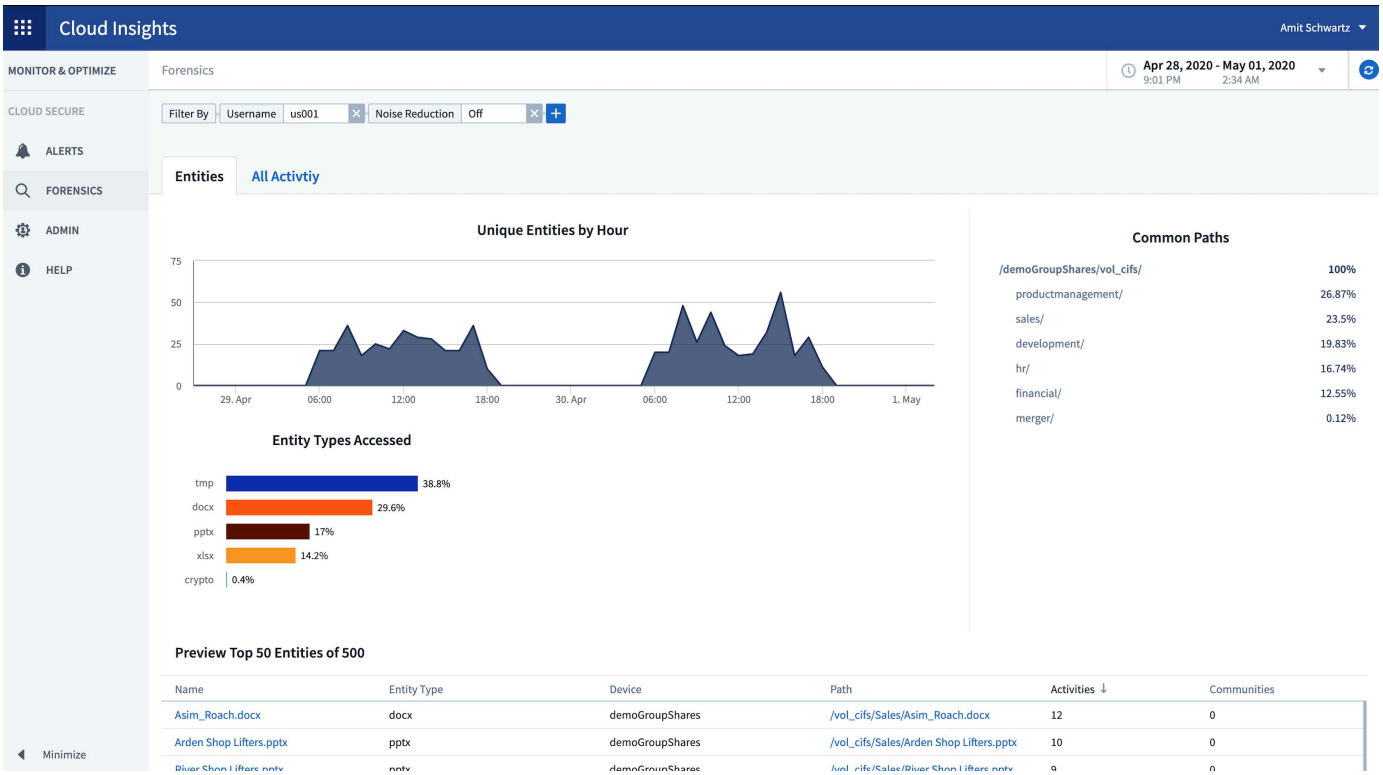
- Administrateurs Cloud Insights : permet d'effectuer les fonctions auteur ainsi que toutes les tâches administratives

Mises à jour Cloud Secure

Cloud Insights inclut les récentes modifications Cloud Secure suivantes.

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

- Vue d'activité axée sur l'activité des utilisateurs (quelle opération ? Où sont-elles effectuées ?)
- La vue entités, centrée sur les fichiers auxquels l'utilisateur a accédé.

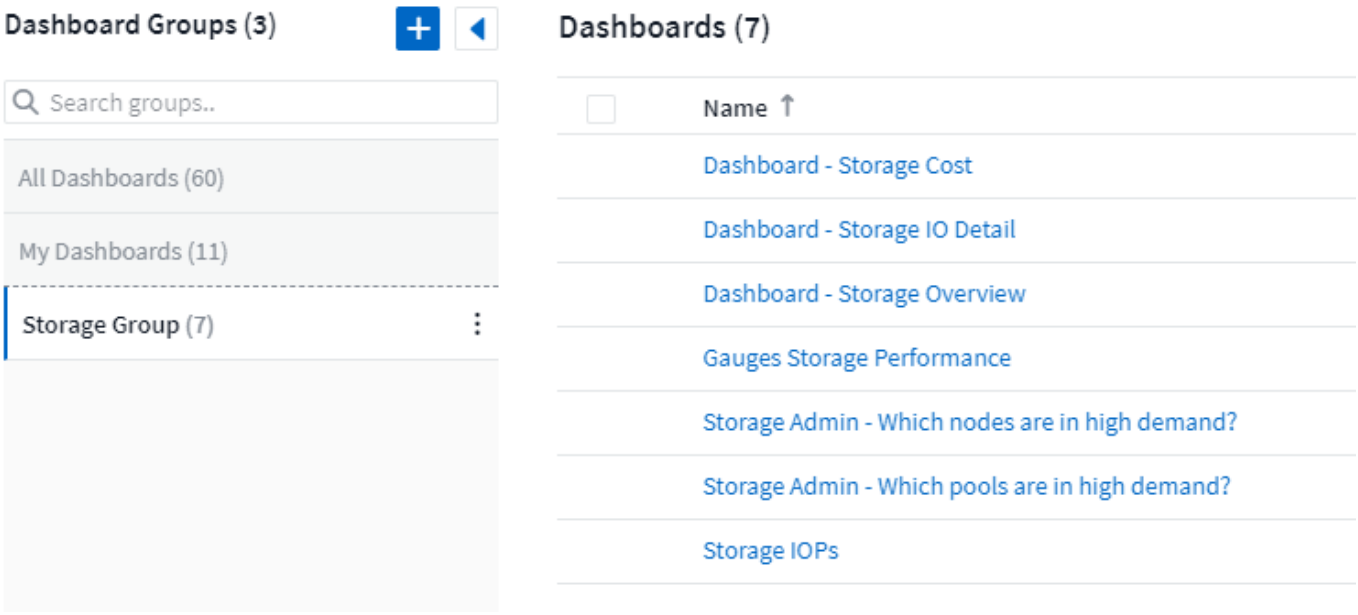


De plus, la notification par e-mail d'alerte contient désormais un lien direct vers la page d'alerte.

Regroupement du tableau de bord

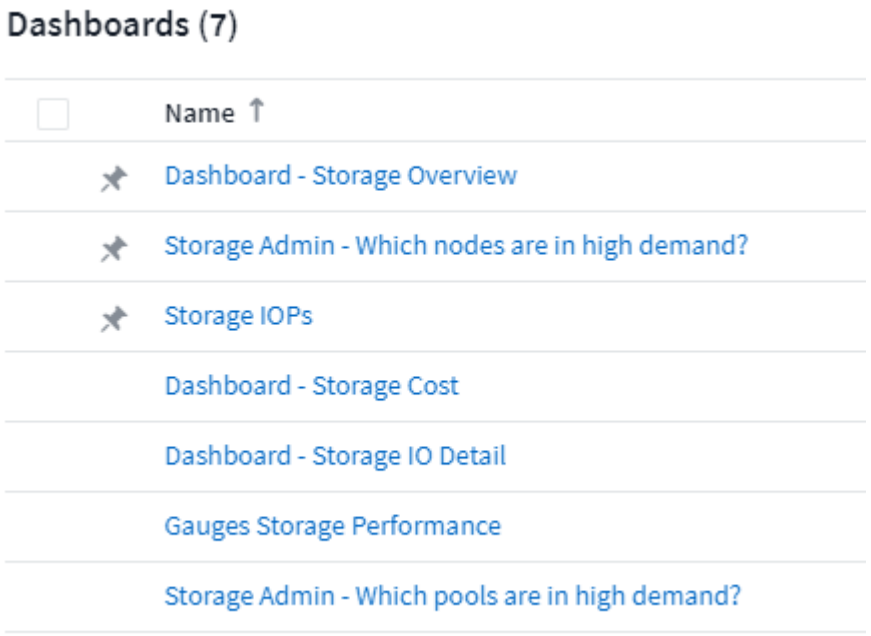
Le regroupement de tableaux de bord permet d'améliorer les "gestion des tableaux de bord"informations pertinentes pour vous. Vous pouvez ajouter des tableaux de bord associés à un groupe pour gérer en une seule étape la gestion de votre stockage ou de vos machines virtuelles, par exemple.

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



Épinglage du tableau de bord

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



Mode TV et actualisation automatique

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

- **Le mode TV** offre un affichage sans encombré; le menu de navigation est caché, offrant plus d'espace d'écran pour l'affichage de vos données.
- Données dans les widgets des tableaux de bord et des pages d'accueil des ressources **actualisation automatique** selon un intervalle de rafraîchissement (aussi peu que toutes les 10 secondes) déterminé

par la plage de temps du tableau de bord sélectionnée (ou la plage de temps du widget, si définie pour remplacer l'heure du tableau de bord).

Combiné, le mode TV et le rafraîchissement automatique offrent une vue en direct de vos données Cloud Insights, parfait pour des démonstrations fluides ou une surveillance en interne.

Avril 2020

Nouveaux choix de plage de temps du tableau de bord

Les choix de plage horaire pour les tableaux de bord et les autres pages Cloud Insights incluent désormais *les dernières 1 heure* et *les 15 dernières minutes*.

Mises à jour Cloud Secure

Cloud Insights inclut les récentes modifications Cloud Secure suivantes.

- Amélioration de la reconnaissance des modifications apportées aux métadonnées des fichiers et des dossiers pour détecter si l'utilisateur a modifié l'autorisation, le propriétaire ou la propriété du groupe.
- Exporter le rapport d'activité utilisateur au format CSV.

Cloud Secure contrôle et vérifie 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, le RGPD et HIPAA, et de mener des enquêtes sur les failles 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.

Optimisation des temps d'agrégation

Les intervalles optimisés "agrégation de temps"dans les widgets de séries chronologiques (graphiques ligne, Spline, surface et surface empilée) sont plus fréquents pour les plages de temps de tableau de bord/widget de 3 heures et 24 heures, ce qui permet une transcription plus rapide des données.

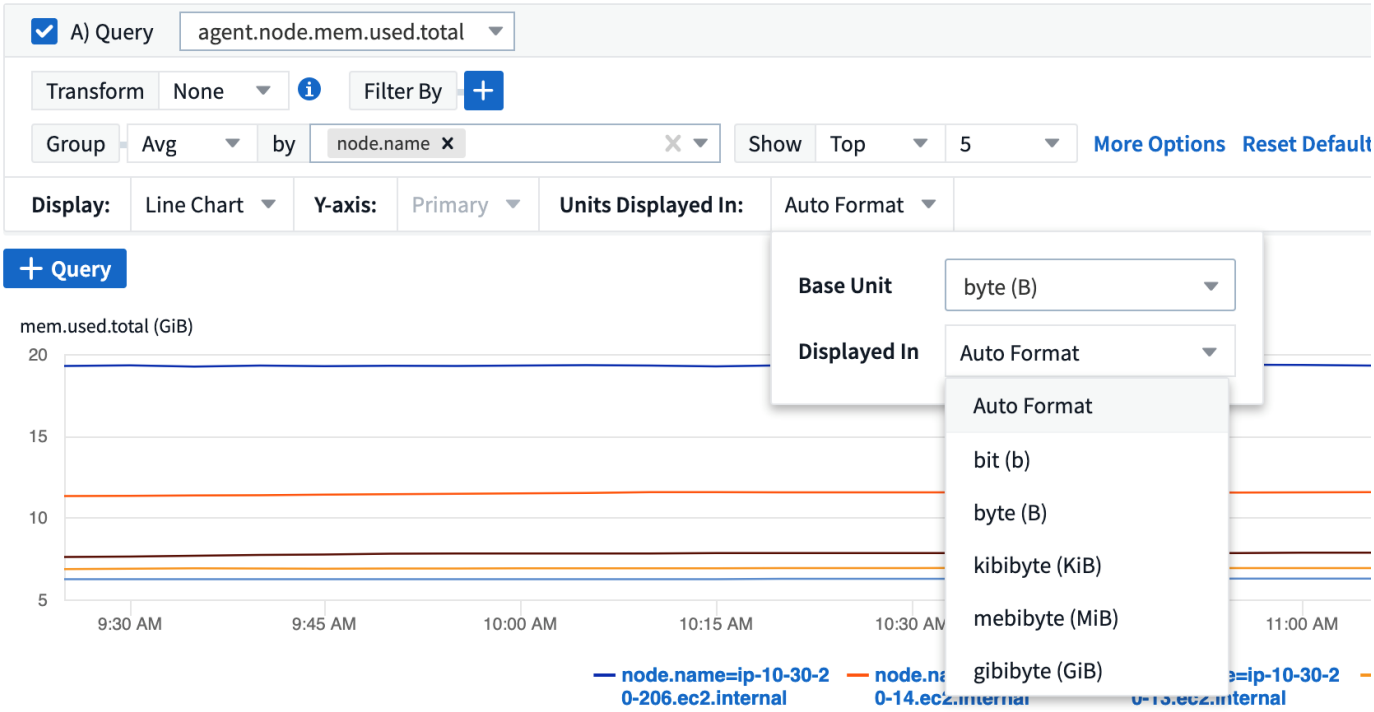
- la plage horaire de 3 heures optimise jusqu'à un intervalle d'agrégation de 1 minutes. Auparavant, c'était 5 minutes.
- la plage horaire de 24 heures optimise jusqu'à un intervalle d'agrégation de 30 minutes. Auparavant, c'était 1 heure.

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

Format 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 de l'unité la plus lisible. Par exemple, une valeur de données de 1,234,567,890 octets serait formatée automatiquement sur 1.23 gibioctets. Dans de nombreux cas, Cloud Insights connaît le format le plus adapté aux 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 de votre choix.



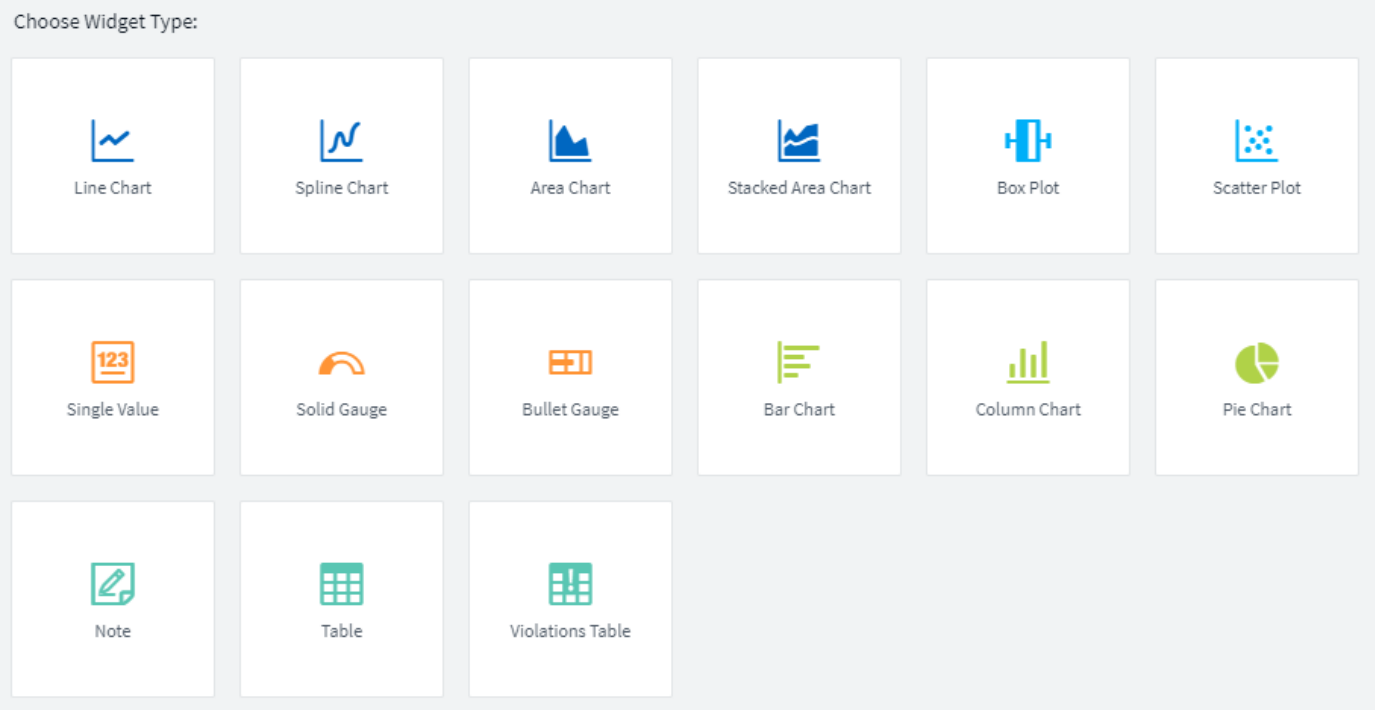
Importer des annotations à l'aide de l'API

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



Sélecteur de widget simplifié

Il est plus facile d'ajouter des widgets aux tableaux de bord et aux pages d'accueil des ressources grâce à un nouveau sélecteur de widgets qui affiche tous les types de widgets dans une seule vue tout-en-un. Ainsi, l'utilisateur n'a plus besoin de faire défiler 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.



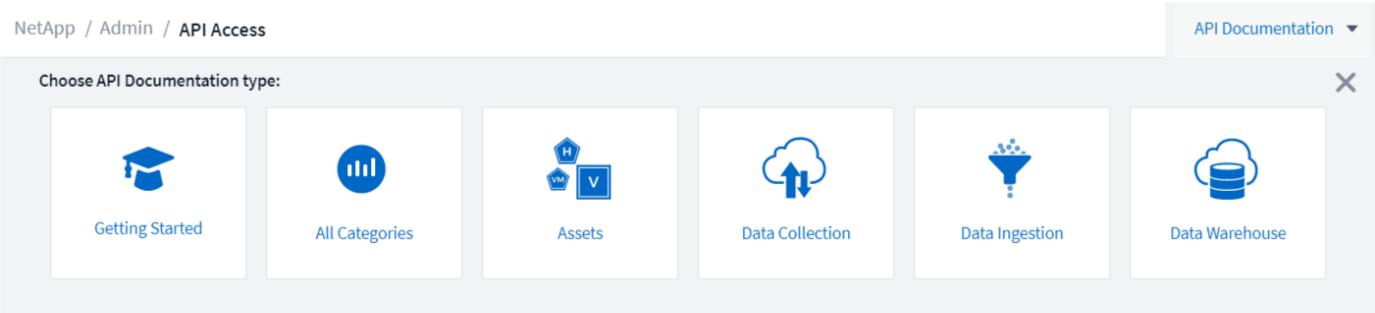
Février 2020

API avec édition Premium

Cloud Insights Premium Edition est fourni avec un "Puissance des API" qui peut être utilisé pour intégrer Cloud Insights avec d'autres applications, telles que des CMDB ou d'autres systèmes de gestion de tickets.

Des informations détaillées basées sur swagger sont disponibles dans **Admin > API accès**, sous le lien **API Documentation**. Swagger fournit une brève description et des informations d'utilisation de l'API, et vous permet de tester chaque API dans votre environnement.

L'API Cloud Insights utilise des jetons d'accès pour fournir un accès basé sur les autorisations aux catégories d'API, telles QUE LES RESSOURCES ou LES COLLECTIONS.



Interrogation initiale après ajout D'Un Data Collector

Auparavant, après avoir configuré un nouveau collecteur de données, Cloud Insights interroge immédiatement le collecteur de données pour recueillir *Inventory* data, mais il attend jusqu'à ce que l'intervalle d'interrogation de performance configuré (généralement 15 minutes) collecte des données initiales *performance*. Il attende

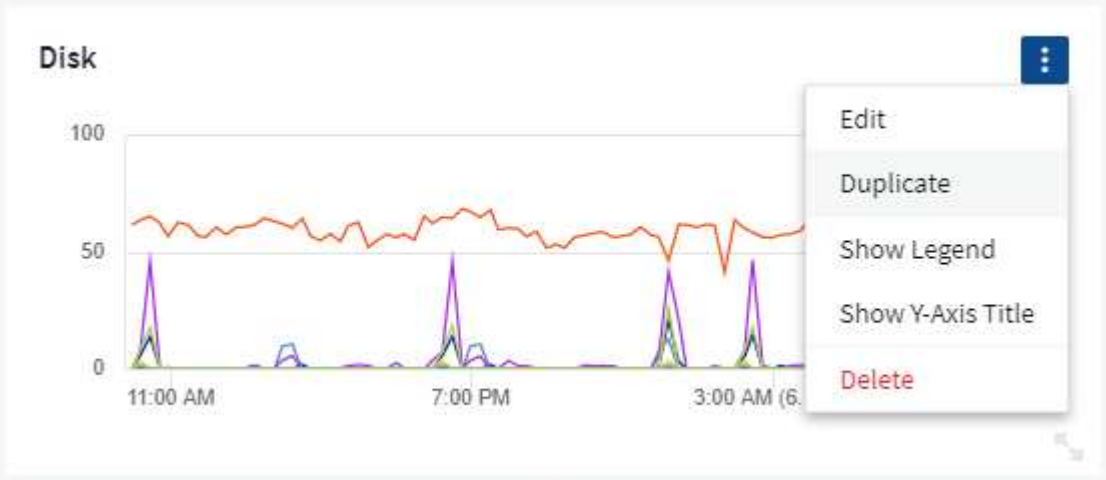
alors un autre intervalle avant de lancer le second sondage de performance, ce qui signifie qu'il faudrait jusqu'à *30 minutes* avant l'acquisition de données significatives à partir d'un nouveau collecteur de données.

Le collecteur de données "interrogation"a été considérablement amélioré, de sorte que l'enquête initiale de performance se produit immédiatement après l'enquête d'inventaire, le deuxième sondage de performance se produisant dans les quelques secondes qui suivent la fin du premier sondage de performance. Cela permet à Cloud Insights de commencer à afficher rapidement des données utiles sur les tableaux de bord et les graphiques.

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

Duplication simplifiée des widgets

Il est plus simple que jamais de créer une copie d'un widget depuis le tableau de bord ou une page d'accueil. En mode Tableau de bord, cliquez sur le menu du widget et sélectionnez **Dupliquer**. L'éditeur de widget est lancé, rempli avec la configuration du widget original 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 au bas de votre tableau de bord et vous pouvez le positionner selon les besoins. N'oubliez pas d'enregistrer votre tableau de bord lorsque toutes les modifications sont terminées.



Authentification unique (SSO)

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

SSO n'est disponible que dans Cloud Insights Premium Edition et doit être configuré avant de pouvoir être activé pour Cloud Insights. La configuration SSO inclut "Fédération des identités" via NetApp Cloud Central. La fédération permet aux utilisateurs de Single Sign-on d'accéder à vos comptes NetApp Cloud Central à l'aide des identifiants de votre annuaire d'entreprise.

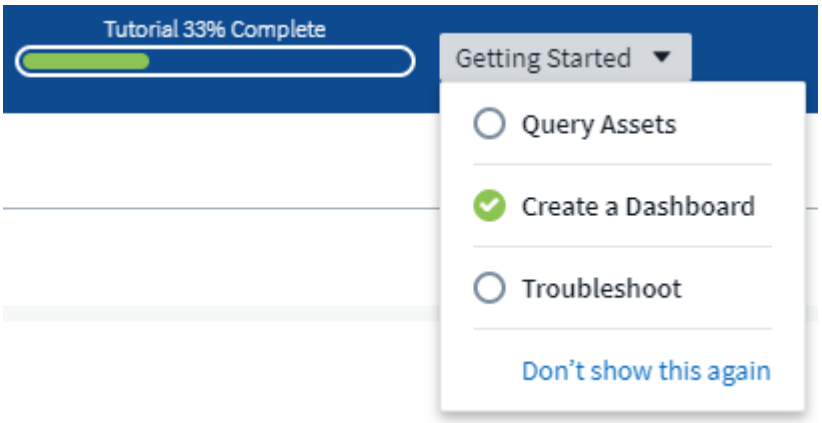
Janvier 2020

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 Tutoriels de fonctionnalités

La liste de contrôle des didacticiels de fonctionnalités a été déplacée vers la bannière supérieure et comporte désormais un indicateur de progression. Les didacticiels sont disponibles pour chaque utilisateur jusqu'à ce qu'ils soient ignorés, 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 VM portant le même nom qu'un au déjà installé, Cloud Insights garantit un nom unique en ajoutant le nom de l'UA à «_1 », «_2 », Etc. C'est également le cas lors de la désinstallation et de la réinstallation d'un au à partir de la même machine virtuelle sans le retirer d'abord de Cloud Insights. Vous voulez un autre nom au ? Aucun problème ; l'au peut être renommé après l'installation.

Agrégation de temps optimisée dans les widgets

Dans les widgets, vous pouvez choisir entre un intervalle d'agrégation de temps *optimisé* ou un intervalle *personnalisé* que vous avez défini. L'agrégation optimisée sélectionne automatiquement l'intervalle de temps approprié en fonction de la plage de temps sélectionnée sur le tableau de bord (ou de la plage de temps du widget, si l'on annule l'heure du tableau de bord). L'intervalle change dynamiquement au fur et à mesure de la modification de la plage de temps du tableau de bord ou du widget.

Processus simplifié « mise en route avec Cloud Insights »

Pour faciliter et simplifier la configuration initiale, le processus de mise en route de Cloud Insights a été simplifié. Il vous suffit de sélectionner un collecteur de données initial et de suivre les instructions. Cloud Insights vous fera découvrir la configuration du collecteur de données et tout agent ou unité d'acquisition requis. Dans la plupart des cas, il importe même un ou plusieurs tableaux de bord initiaux afin de pouvoir commencer à analyser rapidement votre environnement (mais permettez à 30 Cloud Insights de collecter des données significatives).

Autres améliorations :

- 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 améliorées du Data Collector sont plus faciles à suivre.
- Les utilisateurs expérimentés peuvent ignorer le processus de mise en route en cliquant sur un bouton.
- Une nouvelle barre de progression vous indique où vous êtes dans le processus.



Décembre 2019

L'entité métier peut être utilisée dans les filtres

Les annotations d'entité métier peuvent être utilisées dans des filtres pour les requêtes, les widgets, les règles de performance et les pages d'arrivée.

Informations détaillées disponibles pour les widgets à valeur unique et jauge, ainsi que pour tous les widgets ajoutés par « tous »

Un clic sur la valeur dans un widget à valeur unique ou jauge ouvre une page de requête affichant les résultats de la première requête utilisée dans le widget. En outre, si vous cliquez sur la légende d'un widget dont les données sont rassemblées par « All », une page de requête s'affiche également avec les résultats de la première requête utilisée dans le widget.

Période d'essai prolongée

Les nouveaux utilisateurs qui souhaitent bénéficier d'une version d'évaluation gratuite de Cloud Insights disposent désormais de 30 jours pour évaluer le produit. Il s'agit d'une augmentation par rapport à la période d'essai de 14 jours précédente.

Calcul de l'unité gérée

Le calcul des unités gérées (UM) dans Cloud Insights a été modifié comme suit :

- 1 unité gérée = 2 hôtes (toute machine virtuelle ou physique)
- 1 unité gérée = 4 To de capacité non formatée des disques physiques ou virtuels

Cette modification double de manière efficace la capacité de l'environnement que vous pouvez surveiller à l'aide de votre abonnement Cloud Insights existant.

Novembre 2019

Octobre 2019

Création de rapports

"Rapport Cloud Insights" est un outil de veille stratégique qui vous permet d'afficher des rapports prédéfinis ou de créer des rapports personnalisés. Avec le système de rapports, vous pouvez effectuer les tâches suivantes :

- Exécuter un rapport prédéfini
- Créer un rapport personnalisé
- Personnalisez le format du rapport et la méthode de livraison
- Planifiez l'exécution automatique des rapports
- Rapports par e-mail
- Utilisez des couleurs pour représenter des seuils sur les données

Les rapports Cloud Insights peuvent générer des rapports personnalisés dans des domaines tels que la refacturation, l'analyse de consommation et la prévision. Ils peuvent également répondre à des questions comme :

- Quel inventaire ai-je à faire ?
- Où est mon inventaire?
- Qui utilise nos ressources ?
- Quelle est la refacturation du stockage alloué à une unité commerciale ?
- Combien de temps me faut-il pour acquérir de la capacité de stockage supplémentaire ?
- Les unités commerciales sont-elles alignées sur les niveaux de stockage appropriés ?
- Dans quelle mesure les allocations de stockage sont-elles changeantes en un mois, un trimestre ou une année ?

Le reporting est disponible avec Cloud Insights **Édition Premium**.

Améliorations apportées à Active IQ

"Risques Active IQ" sont désormais disponibles en tant qu'objets pouvant être interrogés et utilisés dans les widgets de tableau de bord. Les attributs d'objet risques suivants sont inclus : * Catégorie * Catégorie d'atténuation * impact potentiel * détail du risque * gravité * Source * stockage * nœud de stockage * Catégorie d'interface utilisateur

---

Septembre 2019

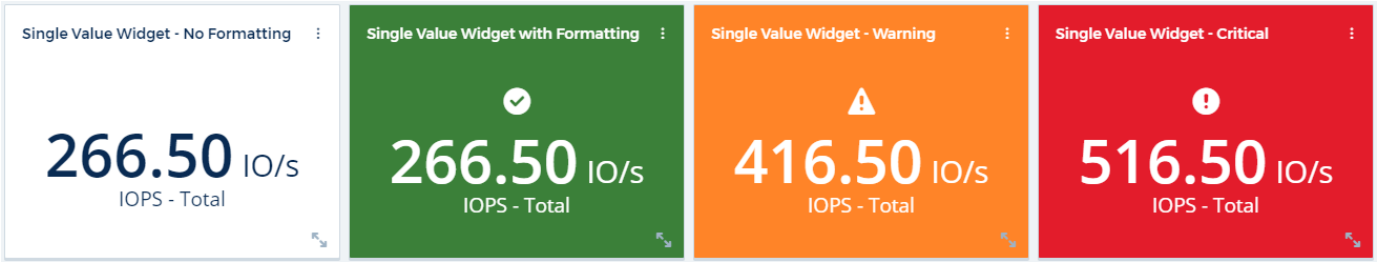
Nouveaux widgets Gauge

Deux nouveaux widgets permettent d'afficher des données à valeur unique sur vos tableaux de bord dans des couleurs accrocheuses en fonction des seuils spécifiés. Vous pouvez afficher les valeurs à l'aide d'une **jauge volumique** ou d'une **jauge à puce**. Les valeurs qui se trouvent dans la plage d'avertissement sont affichées en orange. Les valeurs de la plage critique sont affichées en rouge. Les valeurs inférieures au seuil d'avertissement sont affichées en vert.



Formatage conditionnel des couleurs pour le widget valeur unique

Vous pouvez maintenant afficher le widget valeur unique avec un arrière-plan coloré basé sur les seuils que vous avez définis.



Inviter des utilisateurs pendant l'intégration

À tout moment pendant le processus d'intégration, vous pouvez cliquer sur Admin > User Management > +User pour inviter d'autres utilisateurs à votre environnement Cloud Insights. Sachez que les utilisateurs disposant de rôles *invité* ou *utilisateur* bénéficieront d'un plus grand avantage une fois l'intégration terminée et les données recueillies.

Amélioration de la page de détails du Data Collector

La page de détails du collecteur de données a été améliorée pour afficher les erreurs dans un format plus lisible. Les erreurs sont désormais affichées dans un tableau distinct de la page, chaque erreur étant affichée sur une ligne distincte en cas d'erreurs multiples pour le collecteur de données.

Août 2019

Tous vs. Collecteurs de données disponibles

Lors de l'ajout de collecteurs de données à votre environnement, vous pouvez définir un filtre pour afficher uniquement les collecteurs de données disponibles pour vous en fonction de votre niveau d'abonnement, ou de tous les collecteurs de données.

Intégration d'ActiveIQ

Cloud Insights collecte les données d'ActiveIQ NetApp, qui fournit une série de visualisations, d'analyses et d'autres services de support associés à des clients NetApp et à leurs systèmes matériels/logiciels. Cloud Insights s'intègre aux systèmes de gestion des données ONTAP. Voir "Active IQ" pour plus d'informations.

Juillet 2019

Améliorations tableau de bord

Les tableaux de bord et les widgets ont été améliorés suite aux modifications suivantes :

- En plus de somme, min, Max et AVG, **Count** est maintenant une option de reprise dans les widgets à valeur unique. Lors de la mise en service par "nombre", Cloud Insights vérifie si un objet est actif ou non et ajoute uniquement les objets actifs au comptage. Le nombre qui en résulte est sujet à l'agrégation et aux filtres.
- Dans le widget valeur unique, vous avez maintenant la possibilité d'afficher le nombre obtenu avec 0, 1, 2, 3 ou 4 décimales.
- Les graphiques en ligne affichent une étiquette d'axe et des unités lorsqu'un seul compteur est tracé.
- **L'option Transform** est disponible pour les données d'intégration de services maintenant dans tous les widgets de séries chronologiques pour toutes les mesures. Pour tout compteur ou métrique d'intégration de services (Telegraf) dans les widgets de séries chronologiques (ligne, spline, zone, zone empilée), vous avez le choix de la façon dont vous voulez "Transformer les valeurs". Aucun (valeur d'affichage telle qu'elle est), somme, Delta, cumul, etc

Rétrograder à l'édition de base

La mise à niveau vers l'édition de base échoue et un message d'erreur s'affiche si aucun périphérique NetApp disponible n'a été configuré pour mener à bien un sondage au cours des 7 derniers jours.

Collecte des mesures Kube-State

Le système "Collecteur de données Kubernetes"collecte désormais des objets et des compteurs à partir du plug-in kube-state-metrics, ce qui augmente considérablement le nombre et la portée des mesures disponibles pour la surveillance dans Cloud Insights.

Juin 2019

Éditions Cloud Insights

Cloud Insights est disponible dans différentes éditions pour répondre à votre budget et aux besoins de votre entreprise. Les clients NetApp qui disposent d'un compte de support NetApp actif peuvent profiter de 7 jours de conservation des données et d'un accès aux collecteurs de données NetApp grâce à la version gratuite **Basic Edition**, ou encore bénéficier d'une conservation supérieure des données, de l'accès à tous les collecteurs de données pris en charge, au support technique par un expert et bien plus encore grâce à **Standard Edition**. Pour plus d'informations sur les fonctionnalités disponibles, consultez le site NetApp"Cloud Insights".

Nouveau collecteur de données d'infrastructure : NetApp HCI

- "Centre virtuel NetApp HCI" A été ajouté en tant que collecteur de données Infrastructure. Le collecteur de données HCI Virtual Center collecte les informations sur l'hôte NetApp HCI et requiert des privilèges en lecture seule sur tous les objets du Virtual Center.

Notez que le collecteur de données HCI fait l'acquisition auprès du Virtual Center HCI uniquement. Pour collecter des données du système de stockage, vous devez également configurer le collecteur de données NetApp"SolidFire".

Mai 2019

Nouveau collecteur de données de service : Kapacitor

- "Kapacitor" a été ajouté en tant que collecteur de données pour les services.

Intégration aux services via Telegraf

En plus de l'acquisition de données à partir de périphériques d'infrastructure tels que les commutateurs et le stockage, Cloud Insights collecte désormais des données à partir de divers systèmes d'exploitation et services, en les utilisant "Telegraf en tant qu'agent" pour la collecte des données d'intégration. Telegraf est un agent piloté par plug-in qui peut être utilisé pour collecter et signaler des mesures. Les plug-ins d'entrée sont utilisés pour recueillir les informations souhaitées dans l'agent en accédant directement au système/système d'exploitation, en appelant des API tierces ou en écoutant des flux configurés.

La documentation pour les intégrations actuellement prises en charge se trouve dans le menu de gauche sous **référence et support**.

Actifs Storage Virtual machine

- Les SVM (Storage Virtual machines) sont disponibles sous forme de ressources dans Cloud Insights. Les SVM disposent de leurs propres pages d'accueil Asset, et peuvent être affichées et utilisées dans les recherches, les requêtes et les filtres. Les SVM peuvent également être utilisés dans les widgets du tableau de bord, ainsi que dans les annotations.

Exigences du système de l'unité d'acquisition réduites

- Les besoins en processeur et mémoire du système pour le logiciel de l'unité d'acquisition (au) ont été

réduits. Ces nouvelles exigences sont les suivantes :

Composant	* Ancienne exigence*	Nouvelle exigence
Cœurs de processeurs	4	2
Mémoire	16 GO	8 Go

Autres plateformes prises en charge

- Les plates-formes suivantes ont été ajoutées à celles actuellement "Pris en charge pour Cloud Insights":

Linux	Fenêtres
CentOS 7.3 64 bits CentOS 7.4 64 bits CentOS 7.6 64 bits Debian 9 64 bits Red Hat Enterprise Linux 7.3 64 bits Red Hat Enterprise Linux 7.4 64 bits Red Hat Enterprise Linux 7.6 64 bits Ubuntu Server 18.04 LTS	Microsoft Windows 10 64 bits Microsoft Windows Server 2008 R2 Microsoft Windows Server 2019

Avril 2019

Filtrer les machines virtuelles par balises

Lors de la configuration des collecteurs de données suivants, vous pouvez filtrer pour inclure ou exclure des machines virtuelles de la collecte de données en fonction de leurs étiquettes ou étiquettes.

- "Amazon EC2"
- "Azure"
- "Google Cloud Platform"

Mars 2019

Notifications par e-mail pour les événements liés à un abonnement

- Vous pouvez sélectionner des destinataires pour les e-mails "notifications" lorsque des événements liés à l'abonnement se produisent, tels que l'expiration de l'essai à venir ou les modifications de compte auquel vous êtes abonné. Vous pouvez choisir des destinataires pour ces notifications parmi les suivantes :
  - Tous les propriétaires de compte
  - Tous les administrateurs
  - Adresses e-mail supplémentaires que vous spécifiez

Tableaux de bord supplémentaires

- Les nouveaux objectifs AWS suivants "tableaux de bord"ont été ajoutés à la galerie et sont disponibles à l'importation :
  - Administrateur AWS - quels EC2 sont le plus sollicités ?

◦ Performances de l'instance AWS EC2 par région

Février 2019

Collecte depuis les comptes enfants AWS

- Cloud Insights est pris en charge "Collection de comptes enfants AWS" dans un collecteur de données unique. Votre environnement AWS doit être configuré de sorte que Cloud Insights puisse collecter des données auprès de comptes enfants.

Dénomination du Data Collector

- Les noms de Data Collector peuvent maintenant inclure des points (.), des tirets (-) et des espaces ( ) en plus de lettres, des chiffres et des traits de soulignement. Les noms ne peuvent pas commencer ou se terminer par un espace, un point ou un tiret.

Unité d'acquisition pour Windows

- Vous pouvez configurer une unité d'acquisition Cloud Insights sur un serveur/machine virtuelle Windows. Vérifiez Windows "conditions préalables" avant d'installer "Logiciel de l'unité d'acquisition".

Janvier 2019

Le champ « propriétaire » est plus lisible

- Dans les listes de tableau de bord et de requête, les données du champ « propriétaire » étaient auparavant une chaîne d'ID d'autorisation au lieu d'un nom de propriétaire convivial. Le champ « propriétaire » affiche désormais un nom de propriétaire plus simple et plus lisible.

Répartition de l'unité gérée sur la page d'abonnement

- Pour chaque collecteur de données répertorié sur la page **Admin > abonnement**, vous pouvez maintenant voir une répartition des nombres d'unités gérées (UM) pour les hôtes et le stockage, ainsi que le total.

Décembre 2018

Amélioration du temps de chargement de l'interface utilisateur

- Le temps de chargement initial de l'interface utilisateur Cloud Insights a été considérablement amélioré. Le temps d'actualisation de l'interface utilisateur bénéficie également de cette amélioration dans les cas où les métadonnées sont chargées.

Edition groupée de collecteurs de données

- Vous pouvez modifier les informations de plusieurs collecteurs de données en même temps. Sur la page

observabilité > Collectors, sélectionnez les collecteurs de données à modifier en cochant la case à gauche de chaque et cliquez sur le bouton **Bulk actions**. Choisissez **Modifier** et modifiez les champs nécessaires.

Les collecteurs de données sélectionnés doivent être du même fournisseur et du même modèle et résident sur la même unité d'acquisition.

Des pages d'assistance et d'abonnement sont disponibles pendant l'intégration

- Pendant le flux de travail d'intégration, vous pouvez accéder aux pages **aide > support** et **Admin > abonnement**. Si vous retournez de ces pages, vous accédez au flux de travail d'intégration, à condition que vous n'ayez pas fermé l'onglet du navigateur.

Novembre 2018

Abonnez-vous via les équipes commerciales NetApp ou AWS Marketplace

- L'abonnement et la facturation Cloud Insights sont désormais disponibles directement auprès de NetApp. Outre l'abonnement en libre-service disponible sur AWS Marketplace, Un nouveau lien **Contact Sales** apparaît sur la page **Admin > abonnement**. Pour les clients dont les environnements disposent d'au moins 1,000 unités gérées ou qui doivent en disposer, il est recommandé de contacter l'équipe de vente NetApp via le lien contacter.

Liens hypertexte d'annotations de texte

- Les annotations de type texte peuvent désormais inclure des hyperliens.

Présentation de l'intégration

- Cloud Insights propose désormais une présentation d'intégration pour le premier utilisateur (administrateur ou propriétaire du compte) à se connecter à un nouvel environnement. L'inspection vous permet d'installer une unité d'acquisition, de configurer un collecteur de données initial et de sélectionner un ou plusieurs tableaux de bord utiles.

Importer des tableaux de bord à partir de la Galerie

- En plus de sélectionner des tableaux de bord pendant l'intégration, vous pouvez importer des tableaux de bord via **tableaux de bord > Afficher tous les tableaux de bord** et cliquer sur **+depuis la galerie**.

Duplication des tableaux de bord

- La possibilité de dupliquer un tableau de bord a été ajoutée à la page de liste de tableau de bord comme un choix dans le menu d'options pour chaque tableau de bord, et sur la page principale d'un tableau de bord elle-même à partir du menu *Save*.

Menu des produits Cloud Central

- Le menu vous permettant de basculer vers d'autres produits NetApp Cloud Central s'est déplacé en haut à droite de l'écran.

Intégration de données exploitables de l’infrastructure de données

Avant de commencer à travailler avec Data Infrastructure Insights, vous devez vous inscrire sur le portail **NetApp BlueXP** . Si vous disposez déjà d’un identifiant NetApp BlueXP , vous pouvez essayer gratuitement Data Infrastructure Insights en quelques étapes simples.

Création de votre compte NetApp BlueXP

Pour commencer à utiliser les services cloud de NetApp, rendez-vous sur **"NetApp BlueXP"** et cliquez sur **commencer**.

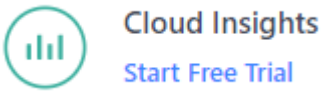
- Si vous n’êtes pas encore inscrit, sélectionnez **s’inscrire**
- Saisissez une adresse e-mail professionnelle valide et choisissez un mot de passe.
- Entrez le nom de votre entreprise, ainsi que votre nom complet.
- Acceptez les conditions générales et sélectionnez **Continuer**.
- BlueXP vous guidera tout au long de la mise en route.

Que se passe-t-il si je dispose déjà d’un identifiant de connexion NetApp BlueXP ?

Une fois que vous avez un compte NetApp BlueXP , il vous suffit de choisir **se connecter** sur la **"NetApp BlueXP"**page du portail.

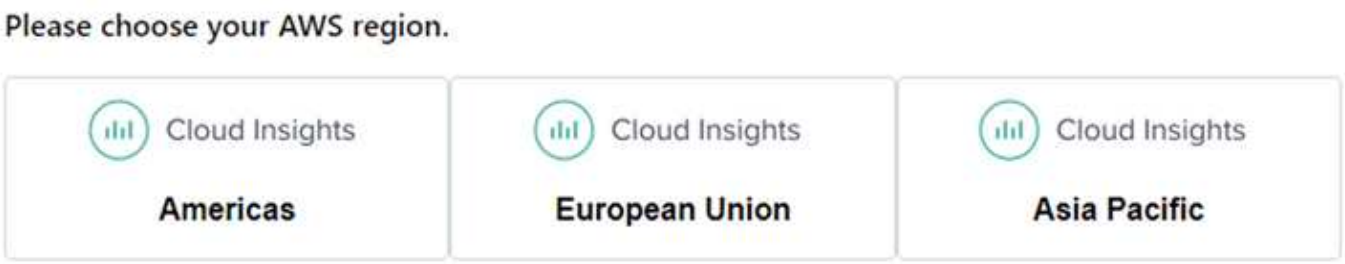
Entrez votre adresse e-mail et votre mot de passe. Vous serez ensuite redirigé vers la page d’offres clouds de NetApp.

Sélectionnez Data Infrastructure Insights.



Commencez l’essai gratuit de Data Infrastructure Insights

Si vous vous connectez pour la première fois à Data Infrastructure Insights, sous l’offre Data Infrastructure Insights, cliquez sur **commencer l’essai gratuit**. Les informations sur l’infrastructure de données vous aideront à créer le locataire de votre entreprise, notamment à sélectionner la région dans laquelle vous souhaitez placer votre locataire.



Une fois votre locataire créé, vous pouvez utiliser vos identifiants BlueXP pour vous connecter et commencer votre essai gratuit de 30 jours des informations exploitables sur l'infrastructure de données. Pendant la période d'essai, vous pouvez explorer les fonctionnalités offertes par Data Infrastructure Insights.

Pendant l'essai gratuit, vous pouvez "commencez votre abonnement" à tout moment accéder à la vue sur l'infrastructure de données. Lorsque vous êtes abonné, vous pouvez utiliser les fonctionnalités Data Infrastructure Insights basées sur votre abonnement actuel.

Connectez-vous et allez

Une fois votre locataire créé, il vous suffit à tout moment de vous connecter au portail NetApp BlueXP et de cliquer sur **aller à informations sur l'infrastructure de données**. Vous serez directement dirigé vers votre locataire Data Infrastructure Insights.

Vous pouvez également ouvrir un navigateur directement vers l'URL du locataire Data Infrastructure Insights, par exemple :

```
 \https://<tenant-prefix>.c01.cloudinsights.netapp.com/
L'URL sera également incluse dans l'e-mail d'invitation de chaque
utilisateur pour faciliter l'accès et le signet. Si l'utilisateur n'est
pas déjà connecté à BlueXP, il est invité à se connecter.
```

Les nouveaux utilisateurs doivent quand même s'inscrire pour accéder à BlueXP avant de pouvoir accéder à l'URL de leur locataire.

La première fois que vous vous connectez à un nouveau locataire, vous serez guidé lors de la configuration de **"commencer la collecte de données"**.

Déconnexion

Pour vous déconnecter de Data Infrastructure Insights, cliquez sur votre **Nom d'utilisateur** et sélectionnez **Fermer la session**. Vous revenez à l'écran de connexion BlueXP.

La déconnexion des informations d'infrastructure de données vous déconnecte de BlueXP . Vous serez également déconnecté des autres services cloud NetApp qui utilisent la connexion BlueXP.

Délai d'inactivité

Par défaut, BlueXP déconnecte un utilisateur s'il n'y a pas d'activité pendant six heures (360 minutes). Quelle

que soit l’activité, les utilisateurs seront déconnectés après sept jours.

Sécurité

Sécurité des informations exploitables de l'infrastructure de données

Chez NetApp, la sécurité des données des produits et des clients est au cœur de toute importance. Data Infrastructure Insights applique de bonnes pratiques de sécurité tout au long du cycle de vie des versions pour s'assurer que les informations et les données des clients bénéficient d'une sécurité optimale.

Présentation de la sécurité

Sécurité physique

L'infrastructure de production Data Infrastructure Insights est hébergée dans Amazon Web Services (AWS). Les contrôles de sécurité physiques et environnementaux des serveurs de production Data Infrastructure Insights, qui comprennent des bâtiments ainsi que des verrous ou des clés utilisés sur les portes, sont gérés par AWS. Conformément à AWS : « l'accès physique est contrôlé à la fois en périphérie et aux points d'entrée des bâtiments par du personnel de sécurité professionnel qui utilise la vidéosurveillance, les systèmes de détection d'intrusion et d'autres moyens électroniques. Le personnel autorisé utilise des mécanismes d'authentification multi-facteurs pour accéder aux sols des centres de données. »

Le service Data Infrastructure Insights respecte les bonnes pratiques de la "Modèle de responsabilité partagée" décrit par AWS.

Sécurité des produits

Data Infrastructure Insights suit un cycle de développement conforme aux principes agiles, ce qui nous permet de traiter plus rapidement tout défaut logiciel orienté sécurité, par rapport aux méthodologies de développement de cycle de lancement plus long. Grâce aux méthodologies d'intégration continue, nous sommes en mesure de répondre rapidement aux changements fonctionnels et de sécurité. Les procédures et les politiques de gestion du changement définissent le moment et la façon dont les changements se produisent et contribuent au maintien de la stabilité de l'environnement de production. Tout changement important est officiellement communiqué, coordonné, correctement examiné et approuvé avant leur libération dans l'environnement de production.

Sécurité réseau

L'accès réseau aux ressources dans l'environnement Data Infrastructure Insights est contrôlé par des pare-feu basés sur hôte. Chaque ressource (par exemple, 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 ports nécessaires à cette ressource pour exécuter sa fonction.

Data Infrastructure Insights utilise divers mécanismes, notamment des services de détection des intrusions, pour surveiller l'environnement de production à la recherche d'anomalies de sécurité.

Évaluation des risques

L'équipe Data Infrastructure Insights suit un processus d'évaluation des risques formalisé afin de fournir un moyen systématique et reproductible d'identifier et d'évaluer les risques afin qu'ils puissent être gérés de manière appropriée par le biais d'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 de calcul extrêmement disponible et redondante, les données stratégiques sont sauvegardées à intervalles réguliers et les restaurations sont régulièrement testées. Des politiques et procédures de sauvegarde formelles minimisent l'impact des interruptions d'activités commerciales et protègent les processus de l'entreprise contre les défaillances des systèmes d'information ou des incidents et assurent leur reprise en temps voulu et adéquate.

Authentification et gestion des accès

Tout accès client à Data Infrastructure Insights se fait via des interactions de l'interface du navigateur via https. L'authentification s'effectue via le service tiers, Auth0. NetApp a centralisé cette démarche en tant que couche d'authentification pour l'ensemble des services de données cloud.

Data Infrastructure Insights suit de bonnes pratiques du secteur, notamment le « privilège minimal » et le « contrôle d'accès basé sur des rôles » concernant l'accès logique à l'environnement de production Data Infrastructure Insights. L'accès est contrôlé selon un besoin strict et ne peut être accordé que par du personnel autorisé grâce à des mécanismes d'authentification multifacteur.

Collecte et protection des données clients

Toutes les données des clients sont chiffrées en transit sur des réseaux publics et chiffrées au repos. Data Infrastructure Insights utilise le chiffrement à divers points du système pour protéger les données des clients à l'aide de technologies telles que TLS (transport Layer Security) et l'algorithme AES-256 standard.

Déprovisionnement du client

Des notifications par e-mail sont envoyées à divers intervalles pour informer le client que son abonnement arrive à expiration. Une fois l'abonnement expiré, l'interface utilisateur est limitée et la collecte des données commence. Le client est alors averti par e-mail. Les abonnements d'essai bénéficient d'une période de grâce de 14 jours et les comptes d'abonnement payant bénéficient d'un délai de grâce de 28 jours. Une fois le délai de grâce expiré, le client est averti par e-mail que le compte sera supprimé dans 2 jours. Un client payant peut également demander directement de ne pas bénéficier du service.

Les locataires arrivés à expiration et toutes les données client associées sont supprimés par l'équipe Data Infrastructure Insights Operations (SRE) à la fin du délai de grâce ou après confirmation de la demande de résiliation du compte d'un client. Dans les deux cas, l'équipe SRE effectue un appel d'API pour supprimer le compte. L'appel d'API supprime l'instance de tenant 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

Ces données sont intégrées au processus d'équipe d'intervention en cas d'incident de sécurité des produits (PSIRT) de NetApp afin de détecter, d'évaluer et de résoudre les vulnérabilités connues. PSIRT affiche les informations de vulnérabilité provenant de plusieurs canaux, notamment les rapports clients, l'ingénierie interne et des sources largement reconnues comme la base de données CVE.

Si un problème est détecté par l'équipe d'ingénierie Data Infrastructure Insights, l'équipe lance le processus PSIRT, évalue et peut éventuellement résoudre le problème.

Il est également possible qu'un client ou un chercheur Data Infrastructure Insights identifie un problème de sécurité avec le produit Data Infrastructure Insights et le signale au support technique ou directement à l'équipe de réponse aux incidents de NetApp. Dans ce cas, l'équipe Data Infrastructure Insights lancera le

processus PSIRT, évaluera le problème et pourra éventuellement le résoudre.

Tests de vulnérabilité et de pénétration

Data Infrastructure Insights applique les bonnes pratiques du secteur et procède régulièrement à des tests de vulnérabilité et d'intrusion auprès de professionnels et d'entreprises de sécurité internes et externes.

Formation à la sensibilisation à la sécurité

Tous les membres du personnel Data Infrastructure Insights suivent une formation sur la sécurité, développée pour chaque rôle, afin de s'assurer que chaque employé est équipé pour gérer les défis spécifiques liés à la sécurité de son poste.

La conformité

La solution Data Infrastructure Insights confie à une entreprise externe détenant une licence CPA la réalisation d'un audit et de validations tiers indépendants portant sur la sécurité, les processus et les services, notamment l'exécution de l'audit SOC 2.

Avis de sécurité NetApp

Vous pouvez afficher les conseils de sécurité disponibles "ici"deNetApp .

Information et région

NetApp prend très au sérieux la sécurité des informations client. Voici comment et où les informations relatives à l'infrastructure de données sont stockées.

Quelles sont les informations stockées par Data Infrastructure Insights ?

Data Infrastructure Insights stocke les informations suivantes :

- Les données de performance

  Les données de performances sont des données de séries chronologiques fournissant des informations sur les performances de l'appareil/source surveillé. Cela inclut, par exemple, le nombre d'E/S fournies par un système de stockage, le débit d'un port FiberChannel, 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 l'appareil/la source surveillé et la façon 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 CPU, la RAM et les disques d'une machine virtuelle, les espaces de stockage d'une base de données, le nombre et le type de ports d'un commutateur SAN, les noms de répertoire/fichier (si la sécurité des charges de travail de stockage est activée), etc

- Données de configuration

  Cette section récapitule les données de configuration fournies par le client utilisées pour gérer l'inventaire et les opérations du client, par exemple les noms d'hôtes ou les adresses IP des périphériques surveillés, les intervalles d'interrogation, les valeurs de délai d'attente, etc

- Secrets

  Les secrets sont les références utilisées par l'unité d'acquisition Data Infrastructure Insights pour accéder aux appareils et services du client. Ces informations d'identification sont chiffrées 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 du client. Même les SRE Privileged Data Infrastructure Insights ne peuvent pas accéder aux secrets des clients en texte brut en raison de cette conception.

- Données fonctionnelles

  Il s'agit de données générées par NetApp avec le service de données cloud 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 ou de données personnelles.

- Données d'accès utilisateur

  Informations d'authentification et d'accès permettant à NetApp BlueXP de communiquer avec les sites régionaux d'informations sur l'infrastructure de données, y compris les données relatives aux autorisations des utilisateurs.

- Données du répertoire utilisateur pour la sécurité des charges de travail de stockage

  Lorsque la fonctionnalité de sécurité de la charge de travail est activée ET que le client choisit d'activer le collecteur d'annuaire de l'utilisateur, le système stocke les noms d'affichage des utilisateurs, les adresses e-mail de l'entreprise et d'autres informations collectées à partir d'Active Directory.

> ⓘ Les données de répertoire d'utilisateurs font référence aux informations de répertoire d'utilisateurs collectées par le collecteur de données de l'annuaire d'utilisateurs Workload Security, et non aux données relatives aux utilisateurs de Data Infrastructure Insights/Workload Security eux-mêmes.

Aucune donnée personnelle explicite n'est recueillie dans les ressources de l'infrastructure et des services. Les informations collectées concernent uniquement les mesures de performance, les informations de configuration et les métadonnées de l'infrastructure, comme bon nombre de fournisseurs de téléphonie, y compris le support automatique NetApp et ActiveIQ. Toutefois, en fonction des conventions de nom utilisées par le client, les données pour les partages, les volumes, les machines virtuelles, les qtrees, les applications, etc., peuvent contenir des informations personnelles identifiables.

Si la sécurité des charges de travail est activée, le système examine en outre 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'annuaire d'utilisateurs Workload Security (qui mappe essentiellement les SID Windows aux noms d'utilisateurs via Active Directory), le nom d'affichage, l'adresse e-mail d'entreprise et tous les attributs supplémentaires sélectionnés seront collectés et stockés par Data Infrastructure Insights.

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

Où mes informations sont-elles stockées ?

Les informations d'infrastructure de données stockent les informations en fonction de la région dans laquelle votre environnement est créé.

Les informations suivantes sont stockées dans la région hôte :

- Données de télémétrie et de ressources/objet, notamment compteurs et mesures de performances
- Informations sur l'unité d'acquisition
- Données fonctionnelles
- Informations d'audit sur les activités des utilisateurs dans Data Infrastructure Insights
- Informations Active Directory de sécurité des charges de travail
- Informations sur l'audit de sécurité de la charge de travail

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

- Informations sur le site de l'environnement (parfois appelées « locataire »), telles que le site ou le propriétaire du compte.
- Informations permettant à NetApp BlueXP de communiquer avec les sites d'informations stratégiques régionaux sur l'infrastructure de données, y compris tout ce qui a à voir avec les autorisations des utilisateurs.
- Informations relatives à la relation entre l'utilisateur Data Infrastructure Insights et le locataire.

Régions hôtes

Les régions hôtes sont les suivantes :

- ÉTATS-Unis : US-est-1
- EMEA : Europe centrale 1
- APAC : ap-Sud-est-2

Plus d'informations

Pour en savoir plus sur la confidentialité et la sécurité de NetApp, consultez les liens suivants :

- "Centre de confiance"
- "Transferts de données hors des frontières"
- "Règles de société contraignantes"
- "Répondre aux demandes de données tierces"
- "Principes de confidentialité de NetApp"

Outil SecurityAdmin

Les informations d'infrastructure de données incluent des fonctionnalités de sécurité qui permettent à votre environnement de fonctionner avec une sécurité renforcée. Ces fonctionnalités comprennent des améliorations au cryptage, au hachage de mot de passe et à la possibilité de modifier les mots de passe des utilisateurs internes ainsi que les paires de clés qui chiffrent 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 cryptés de la source de données sont stockés dans Data Infrastructure Insights, qui utilise

une clé publique pour chiffrer les mots de passe lorsqu'un utilisateur les saisit sur une page de configuration du collecteur de données. Data Infrastructure Insights ne dispose pas des clés privées requises pour décrypter les mots de passe du collecteur de données ; seules les unités d'acquisition (AUS) possèdent la clé privée du collecteur de données requise pour décrypter les mots de passe du collecteur de données.

Mise à niveau et installation

Si le système Insight contient des configurations de sécurité autres que celles par défaut (c'est-à-dire que vous avez des mots de passe avec clé de clés à clé), vous devez sauvegarder vos configurations de sécurité. L'installation de nouveaux logiciels ou, dans certains cas, la mise à niveau de logiciels restaure la configuration de sécurité par défaut de votre système. 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 de Data Infrastructure Insights et est exécuté sur le système d'unités d'acquisition. La gestion de la sécurité inclut la gestion des clés et des mots de passe, l'enregistrement et la restauration des configurations de sécurité que vous créez ou restaurez aux paramètres par défaut.

Avant de commencer

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

Après l'installation de au, l'outil SecurityAdmin se trouve sur le système d'unités d'acquisition à l'un des emplacements suivants :

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

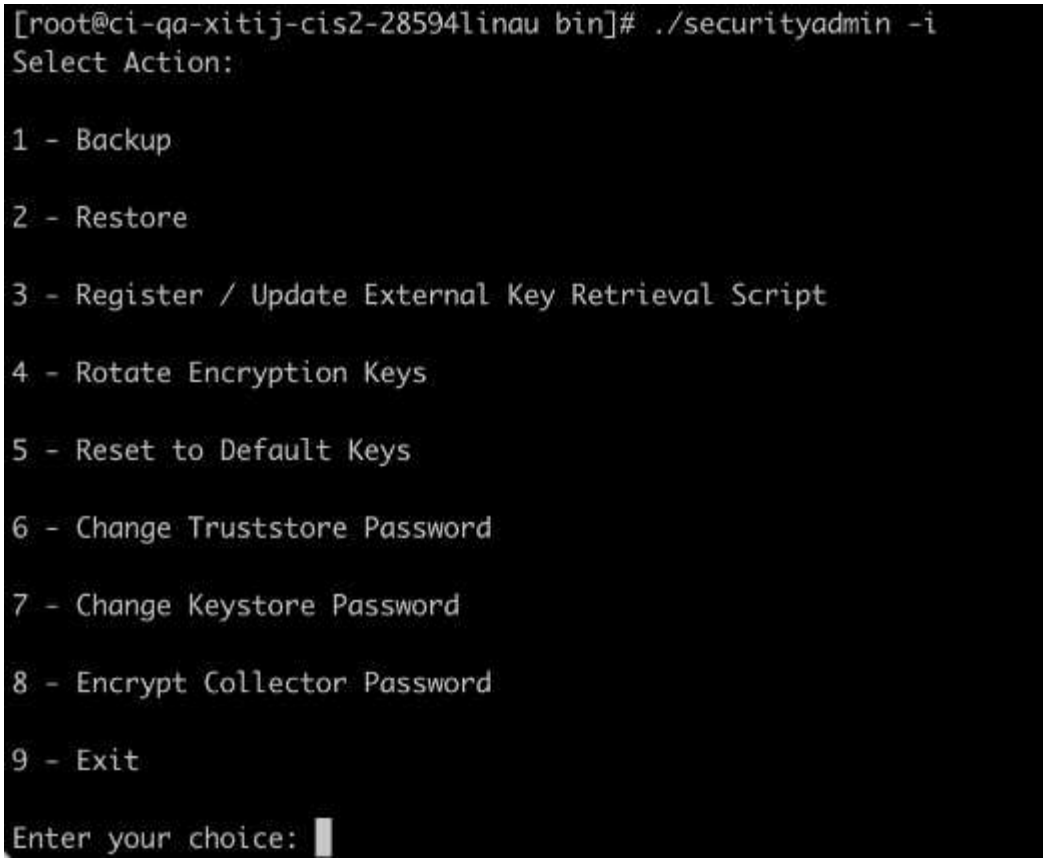
Utilisation de l'outil SecurityAdmin

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



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

Les options suivantes sont affichées :



1. **Sauvegarde**

   Crée un fichier zip de sauvegarde du coffre-fort contenant tous les mots de passe et clés et place le fichier à un emplacement spécifié par l'utilisateur ou aux 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 préserver la sécurité des sauvegardes de coffre-fort, car elles contiennent des informations sensibles.

2. **Restaurer**

   Restaure la sauvegarde zip du coffre-fort créé. Une fois restaurées, tous les mots de passe et clés sont rétablis dans les valeurs existantes au moment de la création de la sauvegarde.

   Restore peut être utilisé pour synchroniser les mots de passe et les clés sur plusieurs serveurs, par exemple en procédant comme suit : 1) modifiez les clés de cryptage sur l'au. 2) Créez une sauvegarde du coffre-fort. 3) restaurez la sauvegarde du coffre-fort sur chacun des États-Unis.

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

   Utilisez un script externe pour enregistrer ou modifier les clés de cryptage au utilisées pour crypter ou décrypter les mots de passe du terminal.

   Lorsque vous modifiez des clés de cryptage, sauvegardez votre nouvelle configuration de sécurité afin de

pouvoir la restaurer après une mise à niveau ou une installation.

Remarque cette option est uniquement disponible 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 publiques et privées cryptées.
- 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 cryptage**

   Faites pivoter vos clés de cryptage (désenregistre les clés actuelles et enregistre les nouvelles clés). Pour utiliser une clé d'un système de gestion externe des clés, 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 cryptage de l'utilisateur d'acquisition sur les valeurs par défaut. Les valeurs par défaut sont celles fournies lors de l'installation.

6. **Modifier le mot de passe de la banque de confiance**

   Modifiez le mot de passe du magasin de confiance.

7. **Changer le mot de passe de la base de stockage**

   Modifiez le mot de passe de la base de stockage de clés.

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

   Crypter le mot de passe du collecteur de données.

9. **Quitter**

   Quittez l'outil SecurityAdmin.

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

Spécification d'un utilisateur pour exécuter l'outil

Si vous vous trouvez dans un environnement contrôlé et soucieux de la sécurité, vous ne disposez peut-être pas du groupe *cisys* mais vous pouvez toujours demander à des utilisateurs spécifiques d'exécuter l'outil SecurityAdmin.

Pour ce faire, vous pouvez installer manuellement le logiciel au et spécifier l'utilisateur/le groupe auquel vous souhaitez accéder.

- À l'aide de l'API, téléchargez le programme d'installation d'EC sur le système au et décompressez-le.
  - Vous aurez besoin d'un jeton d'autorisation unique. Reportez-vous à la documentation API swagger (*Admin* > *API Access* et sélectionnez le lien *API Documentation*) et recherchez la section *GET*

/au/oneTimeToken API.

- Une fois que vous avez le jeton, utilisez l'API *GET /au/installateurs/{Platform}/{version}* pour télécharger le fichier d'installation. Vous devrez fournir une plate-forme (Linux ou Windows) ainsi qu'une 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 racine, en spécifiant l'utilisateur et le groupe :

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

Si l'utilisateur et/ou le groupe spécifié n'existe 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 des 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 la commande suivante :

```
 [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 clé externe

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 des clés.

Pour récupérer la clé, Data Infrastructure Insights exécute le script en passant deux paramètres : *Key ID* et *Key type*. *Key ID* peut être utilisé pour identifier la clé dans votre système de gestion des clés. *Key type* est "public" ou "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 de 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 se fermer avec un code de sortie de 0 ; tout autre code de retour est considéré comme une erreur.

Le script doit être enregistré avec l'unité d'acquisition à l'aide de l'outil SecurityAdmin, qui exécutera le script avec l'unité d'acquisition. Le script doit disposer des 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 avec l'unité d'acquisition.

paramètre d'entrée : id de clé	Identificateur de clé utilisé pour identifier la clé dans le système de gestion des clés du client.
paramètre d'entrée : type de clé	public ou privé.
sortie	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, format de clé publique PKCS8 PrivateKeyInfo RFC 5958 codé DER - PEM, X.509 PublictsubjecKeyInfo RFC 5280
code de sortie	Code de sortie de zéro pour réussir. Toutes les autres valeurs de sortie sont considérées comme ayant échoué.
autorisations de script	Le script doit disposer d'une autorisation de lecture et d'exécution pour l'utilisateur root et cisys.
journaux	Les exécutions de script sont consignées. Les journaux sont disponibles dans - /var/log/NetApp/cloudInsights/securityadmin/securityadmin.log /var/log/NetApp/cloudInsights/acq/acq.log

Cryptage d'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.

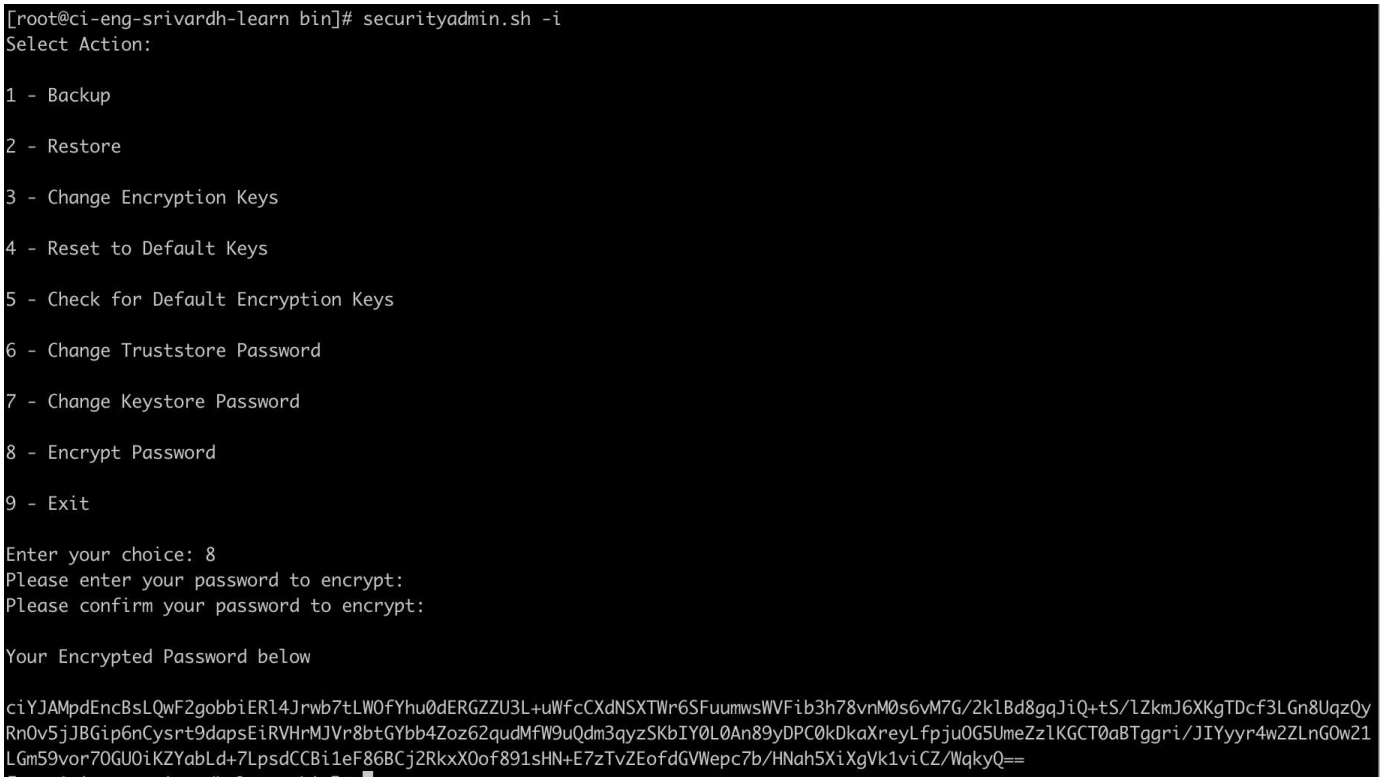
Démarrez l'outil SecurityAdmin en mode interactif et sélectionnez l'option 8 : *crypter le mot de passe*.

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

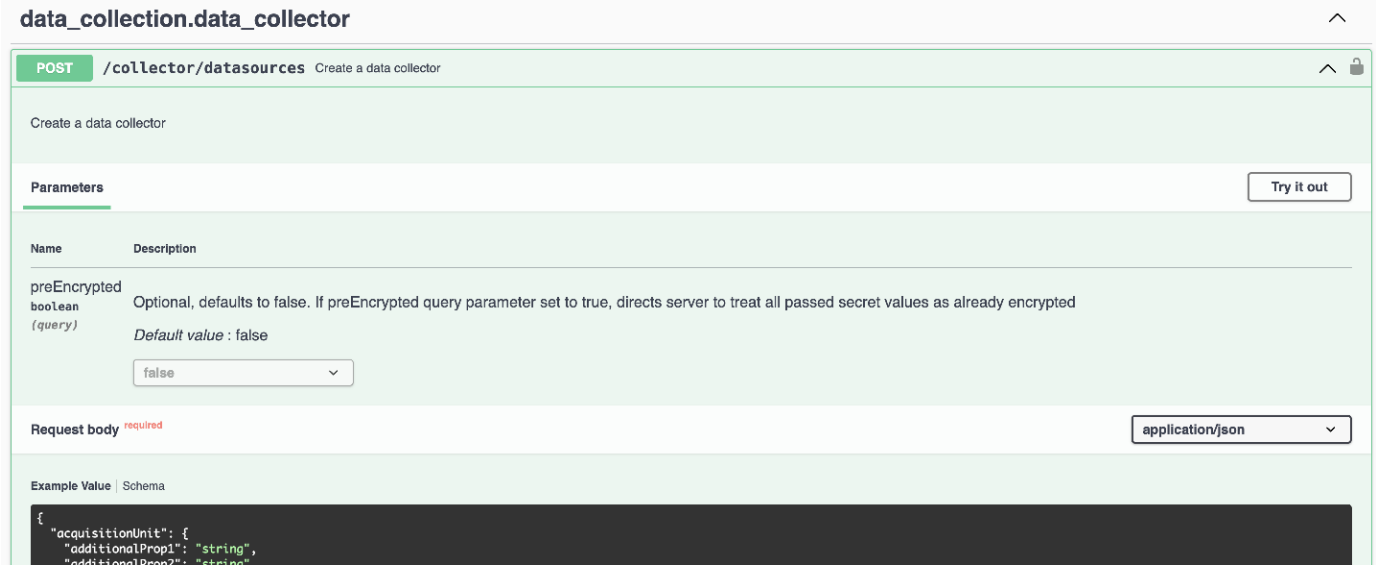
Sinon, si vous utilisez la commande dans un script, sur une ligne de commande, utilisez *securityadmin.sh* avec le paramètre "-enc", en transmettant votre mot de passe non chiffré :

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

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



Pour envoyer le mot de passe crypté à un collecteur de données, vous pouvez utiliser l'API de collecte de données. Le swagger pour cette API se trouve à l'adresse **Admin > API Access** 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 */Collector/datasources* POST pour cet exemple.



Si vous définissez l'option *preEncrypted* sur *True*, tout mot de passe que vous passez par la commande API sera traité comme **déjà crypté**; l'API ne recryptera pas le(s) mot(s) de passe. Lors de la création de votre API, il vous suffit de coller le mot de passe précédemment chiffré 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"
  }
}
```

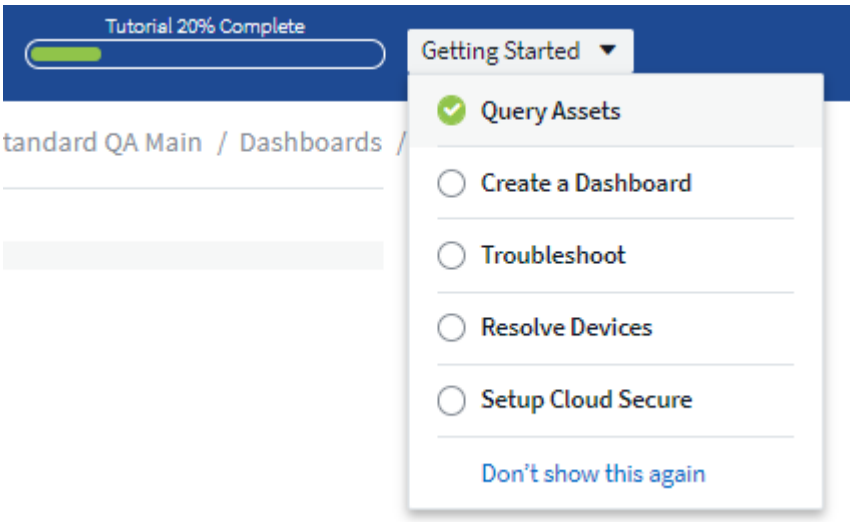
Mise en route

Tutoriels de fonctionnalités

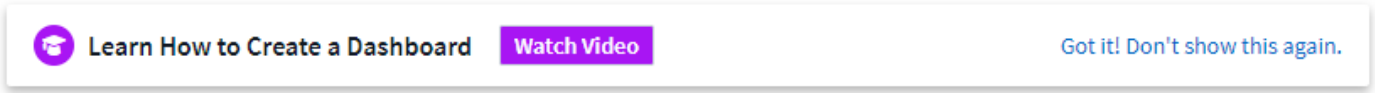
Les fonctionnalités utiles de Data Infrastructure Insights vous permettent de résoudre rapidement et facilement les problèmes et d'obtenir des informations sur votre environnement d'entreprise. Trouvez facilement des données grâce à des requêtes puissantes, visualisez des données dans des tableaux de bord et envoyez des alertes par e-mail pour les seuils de données que vous définissez.

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 de la checklist permet d'accéder à la page Data Infrastructure Insights appropriée pour ce concept. Par exemple, cliquer sur l'élément *Créer un tableau de bord* ouvre la page informations sur l'infrastructure de données **tableaux de bord**.



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



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

Vous pouvez afficher les didacticiels dans l'ordre de votre choix, autant de fois que vous le souhaitez jusqu'à ce que vous soyez congédié.

Rejet de la liste de contrôle

La liste de contrôle de démarrage s'affiche jusqu'à ce que vous cliquiez sur le lien *ne plus l'afficher* au bas de la liste de contrôle. Même après avoir rejeté la liste de contrôle, les didacticiels sont toujours disponibles sur chaque page Data Infrastructure Insights appropriée jusqu'à ce que vous les rejetez de la barre d'en-tête des messages.

Collecte des données

Début de la collecte des données

Une fois que vous vous êtes inscrit à Data Infrastructure Insights et que vous vous connectez pour la première fois à votre environnement, vous suivrez les étapes suivantes pour commencer à collecter et à gérer les données.

Les collecteurs de données détectent les informations provenant 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.

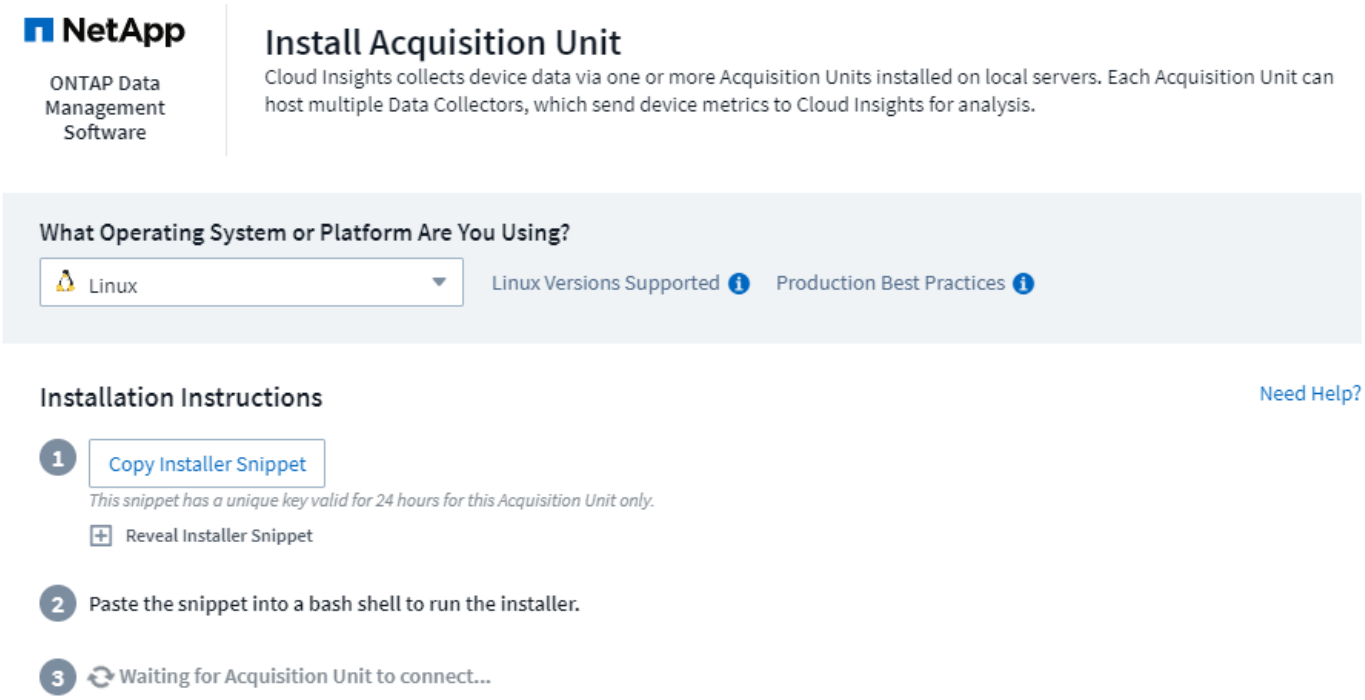
Data Infrastructure Insights dispose de trois types de collecteurs de données :

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

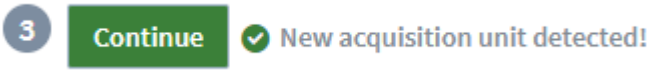
Sélectionnez votre premier collecteur de données parmi les fournisseurs et modèles pris en charge disponibles. Vous pouvez facilement ajouter des collecteurs de données supplémentaires ultérieurement.

Installer une unité d'acquisition

Si vous avez sélectionné un collecteur de données *Infrastructure*, une unité d'acquisition est nécessaire pour injecter des données dans les informations de l'infrastructure de données. Vous devrez télécharger et installer le logiciel acquisition Unit sur un serveur ou une machine virtuelle du centre de données à partir duquel vous allez recueillir. Une unité d'acquisition unique peut être utilisée pour plusieurs collecteurs de données.



- Suivez les "instructions"instructions affichées 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, différentes unités d'acquisition peuvent collecter des informations provenant de data centers situés dans différentes régions.

Configurer Data Collector - Infrastructure

Pour les collecteurs de données *Infrastructure*, on vous demandera 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 au périphérique, le cas échéant.
- Remplissez tous les autres champs obligatoires des sections *Configuration* et *Advanced Configuration*.
- Cliquez sur **Ajouter un collecteur** pour enregistrer le collecteur de données.

Vous pourrez configurer des collecteurs de données supplémentaires ultérieurement.

Configurer Data Collector - systèmes d'exploitation et services

Système d'exploitation :

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

etc

- Ouvrez un terminal ou une fenêtre de commande sur l'hôte de l'agent ou le VM, puis 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 vignette pour ouvrir la page d'instructions pour ce service.

- Choisissez une plate-forme et une clé d'accès Agent.
- Si aucun agent n'est installé sur cette plate-forme, suivez les instructions d'installation de 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 l'installation**.

Ajouter tableaux de bord

En fonction du 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 un sera défini comme votre page d'accueil 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 d'autres tableaux de bord ultérieurement, ou "créez la vôtre".

Ce n'est pas plus compliqué que cela

Une fois le processus de configuration initial terminé, votre environnement commence à collecter des données.

Si le processus de configuration initial est interrompu (par exemple, si vous fermez la fenêtre du navigateur), vous devez suivre les étapes manuellement :

- Choisissez un Data Collector
- Installez un agent ou une unité d'acquisition si vous y êtes invité
- Configurer le Data Collector

Définitions utiles

Les définitions suivantes peuvent être utiles lorsque vous parlez des collecteurs de données ou des fonctionnalités Data Infrastructure Insights :

- Cycle de vie du collecteur : un collecteur appartient à l'un des États suivants dans son cycle de vie :
  - **Aperçu** : disponible à une capacité limitée ou à un public limité. "Aperçu des fonctions" Et les collecteurs de données devraient devenir GA après la période de prévisualisation. Les périodes d'aperçu varient en fonction de l'audience ou de la fonctionnalité.
  - **GA** : une fonctionnalité ou un collecteur de données généralement disponible pour tous les clients, en fonction de l'édition ou du jeu de fonctions.
  - **Obsolète** : s'applique aux collecteurs de données qui ne sont, ou sont censés devenir, plus viables sur

le plan fonctionnel. Les collecteurs de données obsolètes sont souvent remplacés par de nouveaux collecteurs de données mis à jour de manière fonctionnelle.

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

- Unité d'acquisition : ordinateur dédié à l'hébergement de collecteurs de données, généralement une machine virtuelle. Cet ordinateur se trouve généralement dans le même centre de données/VPC que les éléments surveillés.
- Source de données : module de communication avec une pile matérielle ou logicielle. Il se compose d'une configuration et d'un code qui s'exécutent sur l'ordinateur au pour communiquer avec le périphérique.

Exigences relatives à l'unité d'acquisition

Vous devez installer une unité d'acquisition (au) afin d'obtenir des informations auprès de vos collecteurs de données d'infrastructure (stockage, VM, port, EC2, etc.). Avant d'installer l'unité d'acquisition, assurez-vous que votre locataire répond aux exigences en matière de système d'exploitation, de processeur, de mémoire et d'espace disque.

De formation

Composant	Configuration Linux requise	Configuration Windows requise
Système d'exploitation	Un ordinateur exécutant une version sous licence de l'un des systèmes d'exploitation suivants : * AlmaLinux 9.3 à 9.5 * Centos (64 bits) : 7.2 à 7.9, 8.1 à 8.4, Stream 8, Stream 9 * Debian (64 bits) : 9 à 12 * OpenSUSE Leap 15.1 à 15.6 * Oracle Enterprise Linux (64 bits) : 7.5 à 7.9, 8.1 à 8.10, 9.3 à 9.6 * Red Hat (64 bits) : 7.2 à 7.9, 8.1 à 8.10, 9.1 à 9.6 * Rocky 9.0 à 9.5 * SUSE Linux Enterprise Server 15, 15 SP2 à 15 SP6 * Ubuntu Server : 18.04, 20.04, 22.04, 24.04 LTS * SELinux sur les plates-formes ci-dessus Cet ordinateur ne doit exécuter aucun autre logiciel au niveau de l'application. Un serveur dédié est recommandé. Si vous utilisez SELinux, il est recommandé d'exécuter les commandes suivantes sur le système d'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'une des versions suivantes : * Microsoft Windows 10 64 bits * Microsoft Windows 11 * Microsoft Windows Server 2012 * Microsoft Windows Server 2012 R2 * Microsoft Windows Server 2016 * Microsoft Windows Server 2019 * Microsoft Windows Server 2022 * Microsoft Windows Server 2025 cet ordinateur ne doit pas exécuter d'autre logiciel au niveau de l'application. Un serveur dédié est recommandé.
CPU	2 cœurs de processeurs	Identique
Mémoire	8 GO DE RAM	Identique

Espace disque disponible	50 Go (100 Go recommandés) pour Linux, l'espace disque doit être alloué de la manière suivante : /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
Le réseau	Une connexion Ethernet 100 Mbit/s/1 Gbit/s, une adresse IP statique et une connectivité port 80 ou 443 (sortante) de l'unité d'acquisition vers *.cloudInsights.NetApp.com ou votre locataire Data Infrastructure Insights (https://<tenant_id>.c01.cloudInsights.NetApp.com) sont requis. Pour connaître les exigences entre l'unité d'acquisition et chaque Data Collector, reportez-vous aux instructions du "Collecteur de données". Si votre entreprise a besoin d'un proxy pour accéder à Internet, vous devrez peut-être comprendre le comportement du proxy de votre entreprise 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 ou domaines Web spécifiques par exception ? Si c'est le cas, vous devrez ajouter le domaine suivant à la liste d'exceptions : *.cloudInsights.NetApp.com pour plus d'informations, lisez à propos de Proxies "Ici (Linux)" ou "Ici (Windows)". Notez que le port 443 doit être ouvert « sortant » de l'au vers Data Infrastructure Insights.	Identique
Autorisations	Autorisations sudo sur le serveur de l'unité d'acquisition. /tmp doit être monté avec les fonctions exec.	Autorisations d'administrateur sur le serveur de l'unité d'acquisition

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

Recommandations supplémentaires

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

Par rapport au dimensionnement

Vous pouvez commencer avec une unité d'acquisition Data Infrastructure Insights qui dispose de 8 Go de mémoire et 50 Go d'espace disque. Toutefois, pour les environnements plus volumineux, vous devez vous poser les questions suivantes :

Vous vous attendez à :

- Découvrez plus de 2500 machines virtuelles ou 10 clusters ONTAP de grande taille (> 2 nœuds), Symmetrix ou HDS/HPE VSP/XP sur cette unité d'acquisition ?
- Déployer 75 collecteurs de données ou plus 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. Donc, par exemple, si vous avez répondu « Oui » aux deux, vous devriez déployer un système de 24 Go avec 150 Go ou plus d'espace disque. Sous Linux, l'espace disque à ajouter à l'emplacement du journal.

Pour toute question sur le dimensionnement, contactez le support NetApp.

Configuration des unités d'acquisition

Data Infrastructure Insights collecte les données des périphériques à l'aide d'une ou de plusieurs unités d'acquisition installées sur les serveurs locaux. Chaque unité d'acquisition peut héberger plusieurs collecteurs de données, qui envoient des mesures de périphérique 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 un reporting précis des données, il est fortement recommandé de synchroniser l'heure sur la machine de l'unité d'acquisition à l'aide de **Network Time Protocol (NTP)** ou **simple Network Time Protocol (SNTP)**.

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

Ajout d'une unité d'acquisition Linux

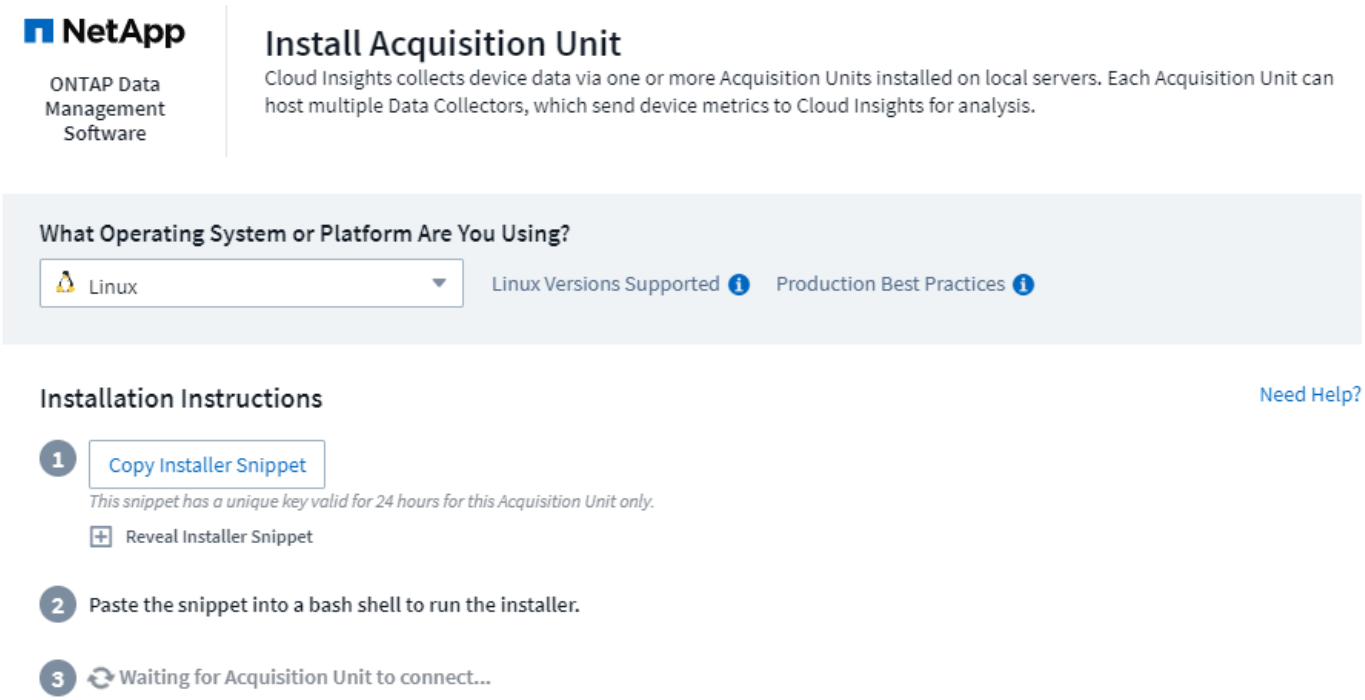
Avant de commencer

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

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

1. Connectez-vous en tant qu'administrateur ou responsable 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 *Install acquisition Unit*. Choisissez Linux.



1. Vérifiez que le serveur ou le VM hébergeant l'unité d'acquisition répond à la configuration système recommandée.
2. Vérifiez que le serveur exécute une version prise en charge de Linux. Cliquez sur *OS versions supportées (i)* pour obtenir la liste des versions prises en charge.
3. Copiez l'extrait de code de la commande installation dans 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.

Une fois que vous avez terminé

- Cliquez sur **observabilité > collecteurs > unités d'acquisition** pour vérifier l'état des unités d'acquisition.
- Les journaux des unités d'acquisition sont accessibles 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 utilisant un proxy, vous devez définir les variables d'environnement 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 *avoir un serveur proxy?*
2. Copiez les commandes dans un éditeur de texte et définissez vos variables proxy si nécessaire.

   Remarque : tenez compte des restrictions relatives aux caractères spéciaux dans les champs nom d'utilisateur et mot de passe du proxy : '%' et '!' sont autorisées dans le champ nom d'utilisateur. ':', '%' et '!' sont autorisées dans le champ 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 transférer la demande https au serveur Data Infrastructure Insights sans déchiffrer les données.

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

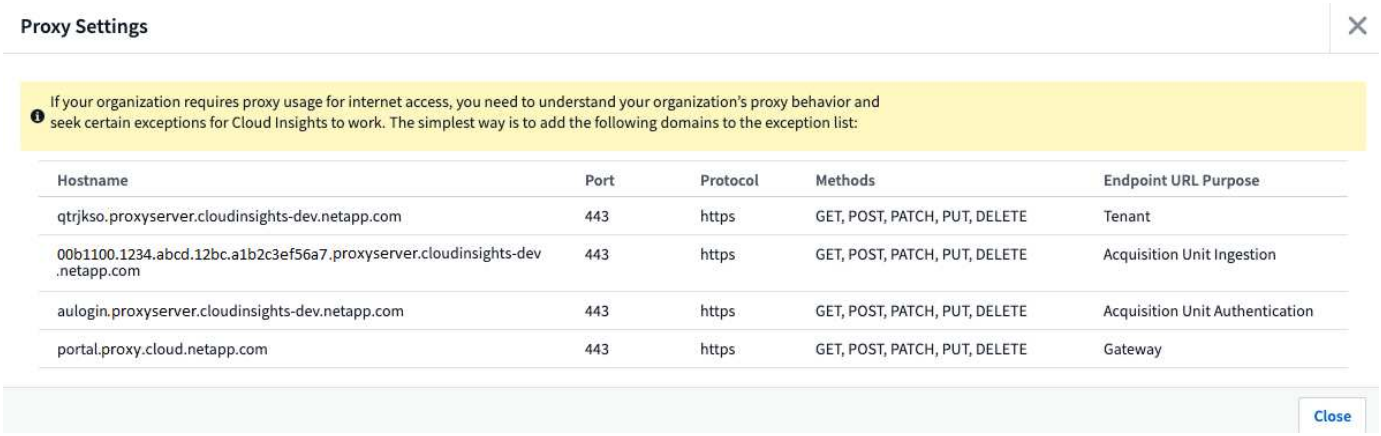
```
*.cloudinsights.netapp.com
```

L'utilisation d'un astérisque (*) pour le caractère générique est courante, mais votre configuration proxy/pare-feu peut utiliser un format différent. Consultez la documentation de votre proxy pour vous assurer que les spécifications des caractères génériques sont correctes dans votre environnement.

Pour plus d'informations sur la configuration du proxy"Base de connaissances", consultez le NetApp .

Affichage des URL du proxy

Vous pouvez afficher les URL de votre point final proxy en cliquant sur le lien **Paramètres proxy** lorsque vous choisissez un collecteur de données pendant l'intégration, ou sur le lien sous *Paramètres proxy* de la page **aide > support**. Un tableau comme celui ci-dessous s'affiche.



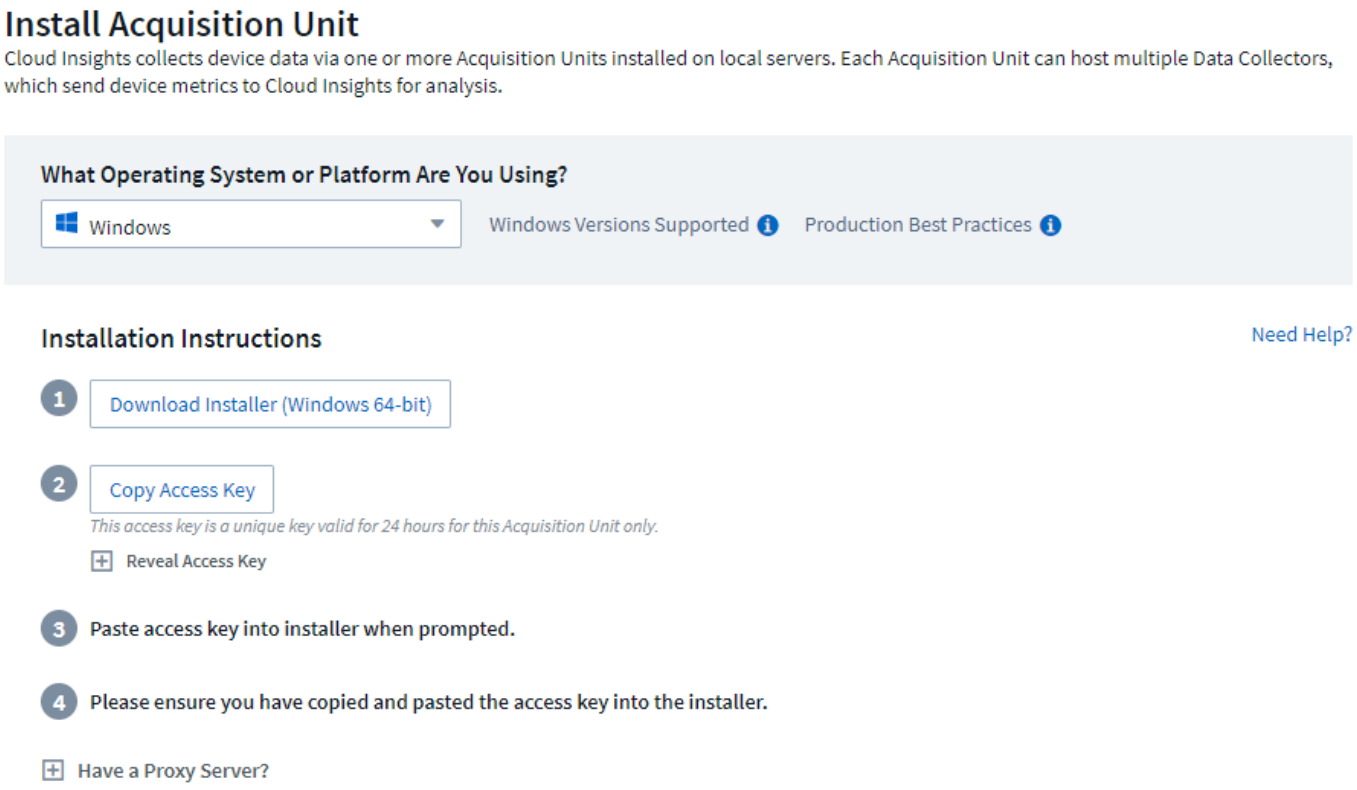
Si votre locataire dispose de Workload Security, les URL de point de terminaison configurées seront également affichées dans cette liste.

Ajout d'une unité d'acquisition Windows

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

1. Connectez-vous au serveur/VM de l'unité d'acquisition en tant qu'utilisateur disposant des 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 responsable de compte.
3. Cliquez sur **observabilité > collecteurs > unités d'acquisition > +unité d'acquisition** .

   Le système affiche la boîte de dialogue *Install acquisition Unit*. Choisissez Windows.



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

recommandée.

2. Vérifiez que le serveur exécute une version prise en charge de Windows. Cliquez sur *OS versions supportées (i)* pour obtenir la liste des versions prises en charge.
3. Cliquez sur le bouton **Download installer (Windows 64 bits)**.
4. Copiez la clé d'accès. Vous en aurez besoin pendant l'installation.
5. Sur le serveur/VM 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. Au cours de l'installation, vous aurez la possibilité de fournir les paramètres de votre serveur proxy.

Une fois que vous avez 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 <dossier 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 transférer la demande https au serveur Data Infrastructure Insights sans déchiffrer les données.

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

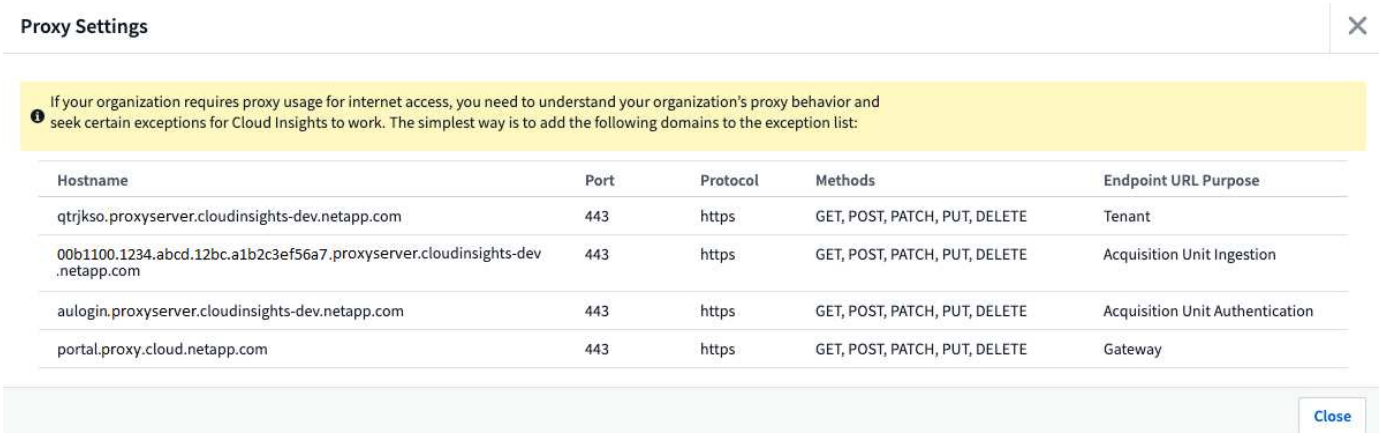
```
*.cloudinsights.netapp.com
```

> L'utilisation d'un astérisque (*) pour le caractère générique est courante, mais votre configuration proxy/pare-feu peut utiliser un format différent. Consultez la documentation de votre proxy pour vous assurer que les spécifications des caractères génériques sont correctes dans votre environnement.

Pour plus d'informations sur la configuration du proxy"Base de connaissances", consultez le NetApp .

Affichage des URL du proxy

Vous pouvez afficher les URL de votre point final proxy en cliquant sur le lien **Paramètres proxy** lorsque vous choisissez un collecteur de données pendant l'intégration, ou sur le lien sous *Paramètres proxy* de la page **aide > support**. Un tableau comme celui ci-dessous s'affiche.



Si votre locataire dispose de Workload Security, 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 :

Windows:

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

1. Sur le serveur/VM de l'unité d'acquisition, ouvrez le panneau de configuration et choisissez **Désinstaller un programme**. Sélectionnez le programme Data Infrastructure Insights acquisition Unit à supprimer.
2. Cliquez sur Désinstaller et suivez les invites.

Linux:

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

1. Sur le serveur/VM 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 désinstallation de l'au:

1. Dans Data Infrastructure Insights, accédez à **observabilité > Collectors et sélectionnez l'onglet**

***acquisition Units**.

2. Cliquez sur le bouton Options à droite de l'unité d'acquisition que vous souhaitez désinstaller, puis sélectionnez *Delete*. Vous pouvez supprimer une unité d'acquisition uniquement si aucun collecteur de données n'y est affecté.

> Vous ne pouvez pas supprimer une unité d'acquisition (au) avec des collecteurs de données connectés. Déplacez tous les collecteurs de données de l'au vers un autre au (modifiez le collecteur et sélectionnez simplement un au différent) avant de supprimer l'au d'origine.

Une unité d'acquisition avec une étoile à côté de celle-ci est utilisée pour la résolution de l'appareil. Avant de supprimer cette au, vous devez sélectionner un autre au à utiliser pour la résolution du périphérique. Passez le curseur sur un autre au et ouvrez le menu « trois points » pour sélectionner « utiliser pour la résolution du périphérique ».



Réinstallation d'une unité d'acquisition

Pour réinstaller une unité d'acquisition sur le même serveur/VM, vous devez procéder comme suit :

Avant de commencer

Une unité d'acquisition temporaire doit être configurée sur un serveur/VM 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 > Collectors**.
3. Pour chaque collecteur de données, cliquez sur le menu Options à droite et sélectionnez *Edit*. 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 groupées**. Choisissez *Edit* et affectez les collecteurs de données à l'unité d'acquisition temporaire.

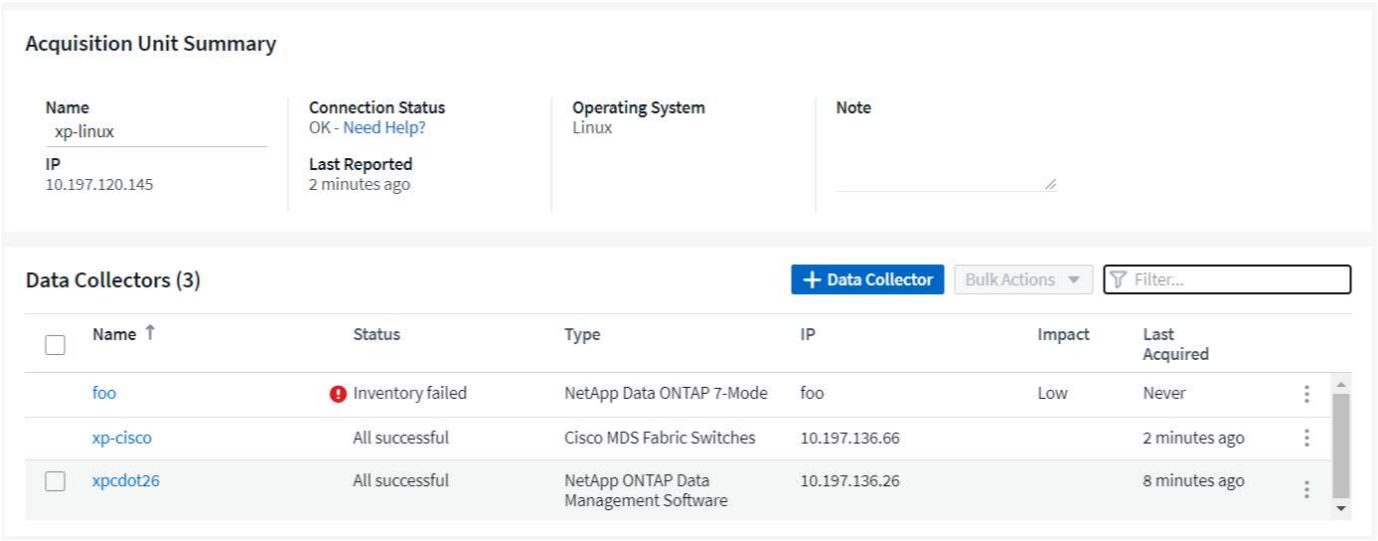
4. Une fois que tous les collecteurs de données ont été déplacés vers l'unité d'acquisition temporaire, allez dans **observabilité > collecteurs** et sélectionnez l'onglet **unités d'acquisition**.
5. Cliquez sur le bouton Options à droite de l'unité d'acquisition que vous souhaitez réinstaller, puis sélectionnez *Delete*. Vous pouvez supprimer une unité d'acquisition uniquement si aucun collecteur de données n'y est affecté.
6. Vous pouvez maintenant réinstaller le logiciel acquisition Unit 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 que l'unité d'acquisition a été réinstallée, affectez vos collecteurs de données à l'unité d'acquisition.

Affichage des détails au

La page de détails de l'unité d'acquisition (au) fournit des informations utiles pour un au, ainsi que des

informations d'aide pour le dépannage. La page de détails au contient les sections suivantes :

- Une section **résumé** montrant les éléments suivants :
  - **Nom** et **IP** de l'unité d'acquisition
  - Connexion actuelle **État** de l'au
  - **Dernier rapporté** temps d'interrogation réussi du collecteur de données
  - Le **système d'exploitation** de la machine au
  - Toute * Note* actuelle pour l'UA. Utilisez ce champ pour saisir un commentaire pour l'UA. Le champ affiche la note ajoutée la plus récente.
- Un tableau des **collecteurs de données** de l'UA, pour chaque collecteur de données :
  - **Nom** - cliquez sur ce lien pour accéder à la page détaillée du collecteur de données avec des informations supplémentaires
  - **Statut** - informations de réussite ou d'erreur
  - **Type** - fournisseur/modèle
  - **Adresse IP** du collecteur de données
  - Niveau actuel **impact**
  - **Dernière acquisition** heure - 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, Sondage ou Supprimer le collecteur de données. Vous pouvez également sélectionner plusieurs collecteurs de données dans cette liste pour effectuer des actions en bloc sur eux.

Pour redémarrer l'unité d'acquisition, cliquez sur le bouton **redémarrer** en haut de la page. Faites descendre ce bouton pour tenter de **rétablir la connexion** à l'UA en cas de problème de connexion.

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

L'"Télégraf"agent Data Infrastructure Insights sert de collecte de données d'intégration. Telegraf est un agent serveur piloté par plug-in qui peut être utilisé pour collecter et signaler des mesures, des événements et des journaux. Les plug-ins d'entrée sont

utilisés pour recueillir les informations souhaitées dans l'agent en accédant directement au système/système d'exploitation, en appelant des API tierces ou en écoutant des flux configurés (c.-à-d. Kafka, statsD, etc.). Les plug-ins de sortie permettent d'envoyer les metrics, les événements et les journaux collectés à partir de l'agent vers Data Infrastructure Insights.

Pour plus d'informations sur l'installation sur Kubernetes, rendez-vous sur la "Opérateur de surveillance NetApp Kubernetes" page.

Pour un audit et un reporting précis des données, il est fortement recommandé de synchroniser l'heure sur l'ordinateur Agent à l'aide de **NTP (Network Time Protocol)** ou **SNTP (simple Network Time Protocol)**.

Si vous souhaitez vérifier les fichiers d'installation avant d'installer l'agent, reportez-vous à la section ci-dessous à la Vérification des sommes de contrôle du package Telegraf.

Installation d'un agent

Si vous installez un collecteur de données de service et que vous n'avez pas encore configuré un agent, vous êtes invité à installer 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 :

- Fenêtres
- RHEL et CentOS
- Ubuntu et Debian

Pour installer un agent, quelle que soit la plate-forme 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 > Collectors**.
3. Cliquez sur **+Data Collector** et choisissez un collecteur de données à installer.
4. Choisir la plate-forme appropriée pour votre hôte (Windows, Linux)
5. Suivez les étapes restantes pour chaque plate-forme.

Une fois que vous avez installé un agent sur un hôte, vous n'avez pas besoin d'installer de 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 metrics à partir de ce système en plus de collecter les données des collecteurs que vous configurez. Ces mesures sont collectées comme "Metrics de nœud".

Si vous utilisez un proxy, lisez les instructions du proxy de votre plate-forme 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

Fenêtres

Conditions préalables :

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

Configuration du support de proxy pour Windows

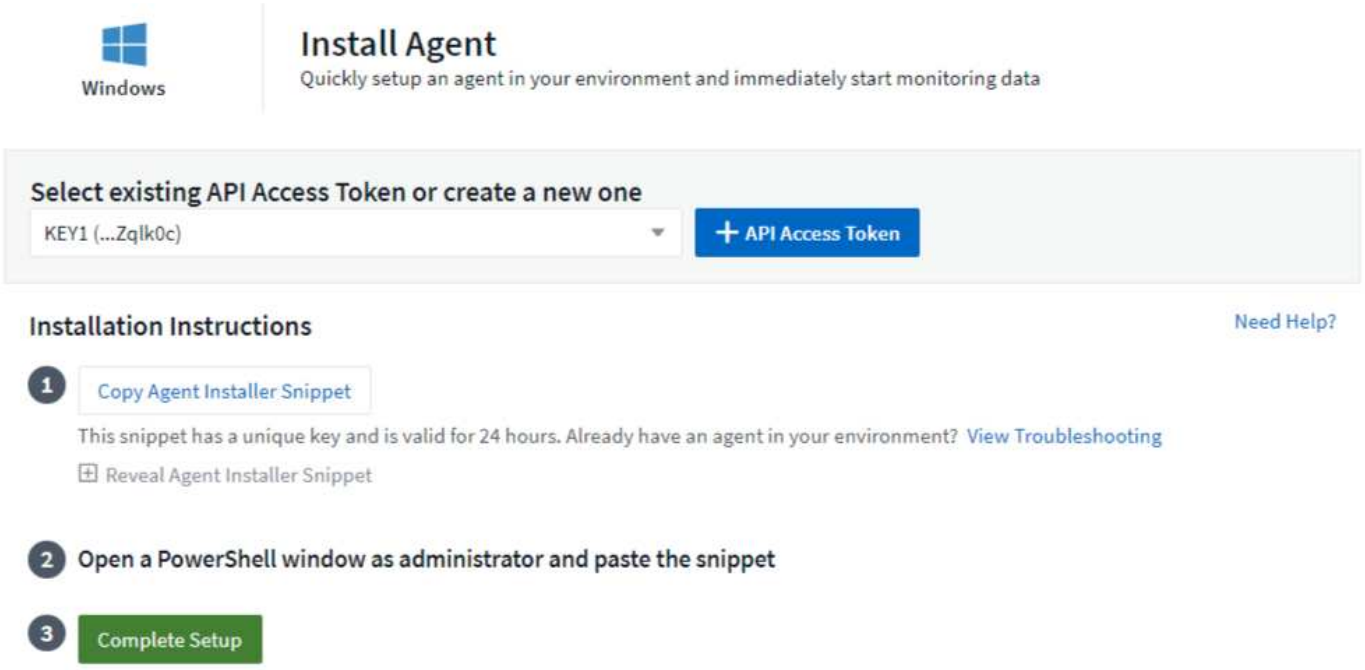
Si votre environnement utilise un proxy, lisez cette section avant de procéder à l'installation.

Les étapes ci-dessous présentent 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 *no_proxy Environment*.

Pour les systèmes résidant derrière un proxy, procédez comme suit pour définir la ou les variables d'environnement *https_proxy* et/ou *http_proxy* **ANTÉRIEURES** à l'installation de l'agent Telegraf :

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

Installation de l'agent



Procédure d'installation de l'agent sous 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. Ouvrez une fenêtre PowerShell
4. Collez la commande dans la fenêtre PowerShell, puis appuyez sur entrée.
5. La commande télécharge le programme d'installation de l'agent approprié, l'installe et définit une configuration par défaut. Une fois l'opération terminée, le service agent redémarre. La commande a une clé unique et est valide pendant 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. Arrêtez et supprimez le service Telegraf :

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

2. Retirez le certificat du magasin de la vérité :

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

3. Supprimez le dossier *C:\Program Files\telegraf* pour supprimer le fichier binaire, les journaux et les fichiers de configuration
4. Supprimez la clé *SYSTÈME\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 *SYSTÈME\CurrentControlSet\Services\EventLog\application\telegraf* du Registre
3. Supprimer *C:\Program Files\telegraf\telegraf.conf*
4. Supprimer *C:\Program Files\telegraf\telegraf.exe*
5. "Installez le nouvel agent".

RHEL et CentOS

Conditions préalables :

- 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 du support proxy pour RHEL/CentOS**.

Configuration de la prise en charge de Proxy pour RHEL/CentOS

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

Les étapes ci-dessous présentent 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 *no_proxy Environment*.

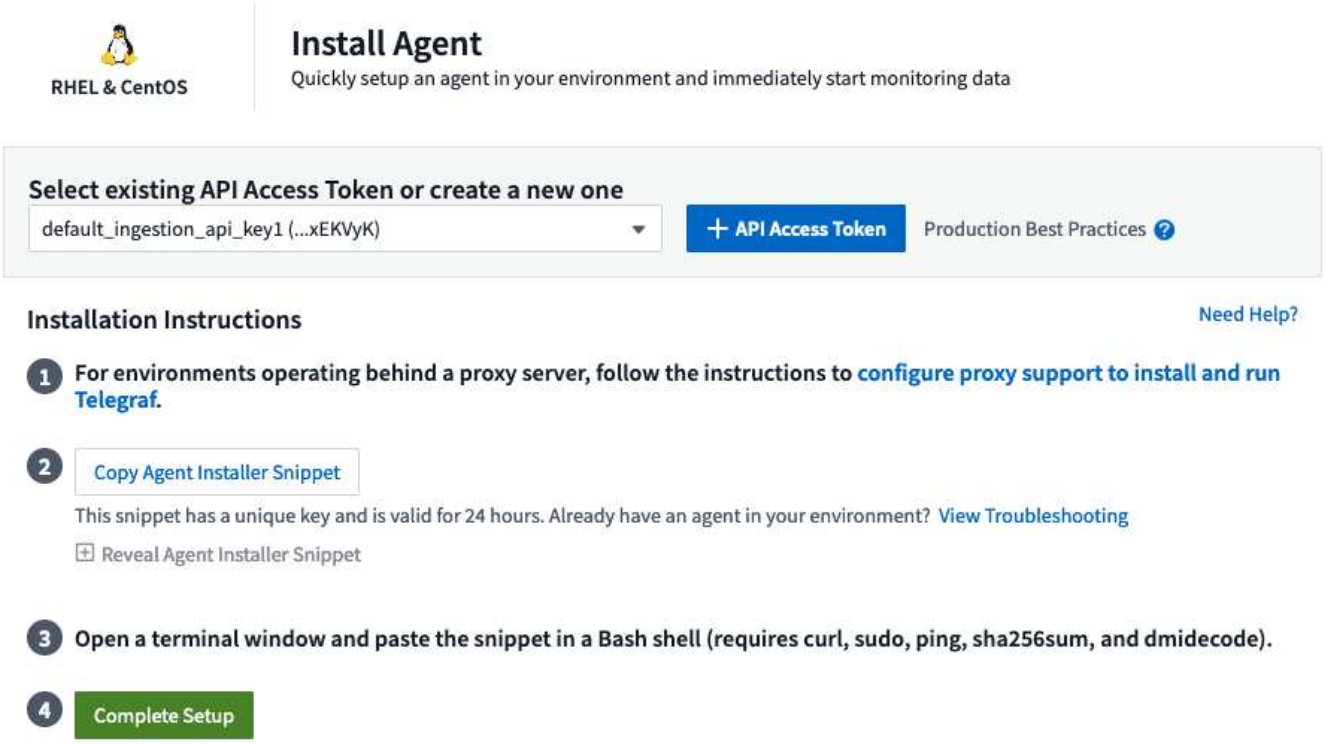
Pour les systèmes résidant derrière un proxy, effectuez les opérations suivantes **ANTÉRIEUR** à l'installation de l'agent Telegraf :

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 des définitions pour les
variables _https_proxy_ et/ou _http_proxy_ :
```

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

Installation de l'agent



Étapes d'installation de 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. Ouvrez une fenêtre de jeu
4. Collez la commande dans la fenêtre Bash et appuyez sur entrée.
5. La commande télécharge le programme d'installation de l'agent approprié, l'installe et définit une configuration par défaut. Une fois l'opération terminée, le service agent redémarre. La commande a une clé unique et est valide pendant 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 le système (CentOS 7+ et RHEL 7+) :

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

Si votre système d'exploitation n'utilise pas le système (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. Supprimez l'agent Telegraf :

   ```
    yum remove telegraf
   . Supprimez tous les fichiers de configuration ou de journal qui peuvent
   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. Supprimez l'agent telegraf précédent :

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

Ubuntu et Debian

Conditions préalables :

- 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 de proxy pour Ubuntu/Debian

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

Les étapes ci-dessous présentent 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 *no_proxy Environment*.

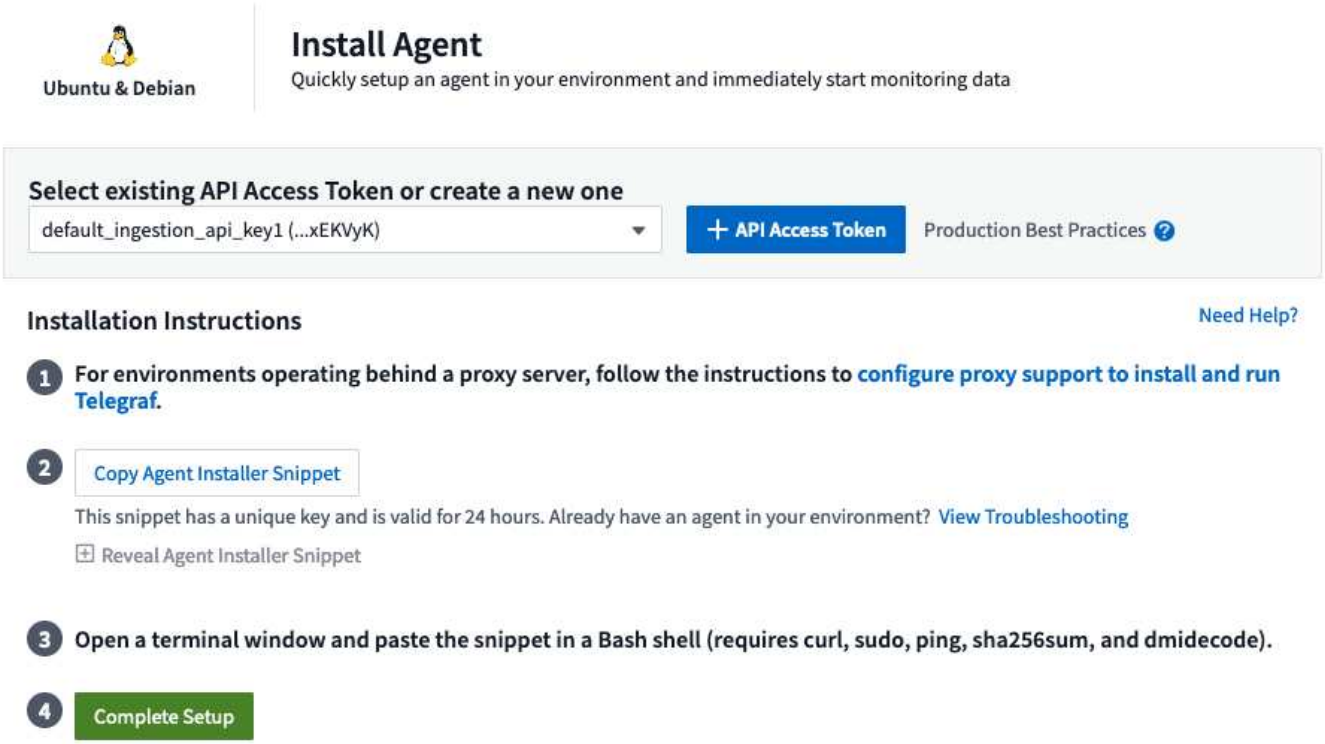
Pour les systèmes résidant derrière un proxy, effectuez les opérations suivantes **ANTÉRIEUR** à l'installation de l'agent Telegraf :

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 des définitions pour les
variables _https_proxy_ et/ou _http_proxy_ :
```

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

Installation de l'agent



Étapes pour installer un 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. Ouvrez une fenêtre de jeu
4. Collez la commande dans la fenêtre Bash et appuyez sur entrée.
5. La commande télécharge le programme d'installation de l'agent approprié, l'installe et définit une configuration par défaut. Une fois l'opération terminée, le service agent redémarre. La commande a une clé unique et est valide pendant 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 le système :

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

Désinstallation de l'agent

Pour désinstaller l'agent sur Ubuntu/Debian, dans un terminal Bash, exécutez les opérations suivantes :

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. Supprimez l'agent Telegraf :

```
 dpkg -r telegraf
. Supprimez tous les fichiers de configuration ou de journal qui peuvent
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. Supprimez l'agent telegraf précédent :

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

Vérification des sommes de contrôle du package Telegraf

Le programme d'installation de l'agent Data Infrastructure Insights effectue des vérifications d'intégrité, mais certains utilisateurs peuvent vouloir effectuer leurs propres vérifications avant d'installer le binaire Telegraf téléchargé. Pour ce faire, téléchargez le programme d'installation et générez une somme de contrôle pour le package téléchargé, puis comparez la somme de contrôle à la valeur indiquée dans les instructions d'installation.

Téléchargez le programme d'installation sans l'installer

Pour effectuer une opération de téléchargement uniquement (par opposition à la commande de téléchargement et d'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 ».

Voici la procédure à suivre :

1. Copiez l'extrait de code Agent installer comme indiqué.
2. Au lieu de coller le fragment dans une fenêtre de commande, collez-le dans un éditeur de texte.
3. Supprimez la commande de fin « --install » (Linux) ou « -install » (Windows).
4. Copiez la commande entière à partir de l'éditeur de texte.
5. Ensuite, collez-la dans votre fenêtre de commande (dans un répertoire de travail) et exécutez-la.

Non Windows (ces exemples sont pour Kubernetes ; les noms réels de scripts peuvent varier) :

- Téléchargement et installation (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
```

Windows :

- Téléchargement et installation (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 télécharge tous les artefacts requis depuis Data Infrastructure Insights vers le répertoire de travail. Les artefacts incluent, mais ne se limitent pas aux éléments suivants :

- un script d'installation
- un fichier d'environnement
- Binaire Telegraf

- Une signature pour le binaire Telegraf
- un certificat public pour vérifier la signature binaire

Le snippet d'installation téléchargé et copié depuis DII contrôle 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 checksum, exécutez la commande suivante pour votre plateforme appropriée :

- RHEL/Ubuntu :

```
 sha256sum <package_name>
* Windows :
```

```
Get-FileHash telegraf.zip -Algorithm SHA256 | Format-List
```

Installez l'image téléchargée

Une fois tous les artefacts vérifiés de manière satisfaisante, l'installation de l'agent peut être lancée en exécutant :

Non Windows :

```
 sudo -E -H ./<installation_script_name> --install
Windows :
```

```
.\cloudinsights-windows.ps1 -install
```

Création et utilisation de tokens d'accès d'API

Pour créer un jeton d'accès API pour l'ingestion de données Telegraf, effectuez l'une des opérations suivantes :

Créer via la page d'installation du Data Collector

1. Accédez à la page d'installation du Data Collector correspondant à la plate-forme que vous souhaitez utiliser (Windows, Linux).
2. Créez un jeton à l'aide du bouton + jeton d'accès API.
3. Entrez 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.

Créez manuellement un jeton d'accès API

1. Accédez à Admin> API Access.
2. Cliquez sur + jeton d'accès API.
3. Entrez un nom et éventuellement une description.
4. Sous « quel type d'API ce token sera-t-il utilisé pour appeler ? », sélectionnez « ingestion des données » uniquement, puis désélectionnez « unité d'acquisition ».
5. Sous autorisations, sélectionnez lecture/écriture.
6. Désélectionnez « faire pivoter automatiquement les tokens pour Kubernetes ».

Pour utiliser votre jeton d'accès à l'API nouvellement créé, sélectionnez-le dans la liste déroulante « Sélectionner un jeton d'accès à l'API existant ou en créer un nouveau » de la page du programme d'installation. Veuillez noter que seuls les jetons possédant les propriétés suivantes peuvent être utilisés :

- Type d'API : uniquement « Data ingestion »
- Autorisations : lecture/écriture
- Rotation automatique Kubernetes : désactivée

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes lors de la configuration d'un agent :

Problème :	**Essayer :**
Après avoir configuré un nouveau plug-in et redémarré Telegraf, Telegraf ne démarre pas. Les journaux indiquent qu'une erreur semblable à celle qui suit : "[telegraf] erreur d'exécution de l'agent : erreur lors du chargement du fichier de configuration /etc/telegraf/telegraf.d/cloudInsights-default.conf : sorties du plug-in.http: Line <linenumber>: Configuration a spécifié les champs ["use_system_proxy"], mais ils n'ont pas été utilisés"	La version installée de Telegraf est obsolète. Suivez les étapes de 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 pas de données	Désinstallez l'agent telegraf, puis relancez le script d'installation. Suivez les étapes **mettre à niveau l'agent** de cette page pour votre plate-forme appropriée.
J'ai déjà installé un agent à l'aide de Data Infrastructure Insights	Si vous avez déjà installé un agent sur votre hôte/machine virtuelle, il n'est pas nécessaire d'installer l'agent à nouveau. Dans ce cas, il vous suffit de choisir la plate-forme et la clé appropriées dans l'écran installation de l'agent, puis de cliquer sur **Continuer** ou **Terminer**.
Un agent est déjà installé, mais pas en utilisant le programme d'installation de Data Infrastructure Insights	Supprimez l'agent précédent et exécutez l'installation de l'agent Data Infrastructure Insights pour vous assurer que les paramètres par défaut du fichier de configuration sont corrects. Lorsque vous avez terminé, cliquez sur **Continuer** ou **Terminer**.

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en

charge du Data Collector".

Configuration des collecteurs de données

Vous configurez les collecteurs de données dans votre environnement Data Infrastructure Insights pour collecter les données des terminaux du data Center.

Avant de commencer

- Vous devez avoir configuré une unité d'acquisition pour pouvoir commencer à collecter des données.
- Vous avez besoin d'informations d'identification pour les périphériques à partir desquels vous recueillez des données.
- Les adresses réseau du périphérique, les informations de compte et les mots de passe sont requis pour tous les périphériques à partir de qui vous recueillez des données.

Étapes

1. Dans le menu Data Infrastructure Insights, cliquez sur **observabilité > Collectors**

   Le système affiche les collecteurs de données disponibles classés par fournisseur.

2. Cliquez sur **+ Collector** 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. Entrez 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 une 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 prendre jusqu'à deux périodes d'interrogation avant que les données du service soient affichées dans les tableaux de bord ou disponibles pour les requêtes.

- 1er sondage d'inventaire : immédiatement
- 1er sondage de données sur les performances pour établir une ligne de base : immédiatement après l'inventaire des stocks
- 2e sondage de performance : dans les 15 secondes après la fin du 1er sondage de performance

L'interrogation se poursuit ensuite en fonction des intervalles d'inventaire et d'interrogation des performances configurés.

Détermination de l'état d'acquisition du collecteur de données

Comme les collecteurs de données sont la principale source d'informations pour les informations d'infrastructure de données, il est impératif de rester en cours d'exécution.

L'état du collecteur de données s'affiche dans le coin supérieur droit de n'importe quelle page de ressources sous forme de message « acquis il y a N minutes », où N indique la durée d'acquisition la plus récente du ou des collecteurs de données du bien. L'heure/la date d'acquisition s'affiche également.

Un clic sur le message affiche un tableau avec le nom, l'état et la dernière heure d'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 détaillée de ce collecteur de données.

Gestion des collecteurs de données configurés

La page collecteurs de données installés permet d'accéder aux collecteurs de données qui ont été configurés pour Data Infrastructure Insights. Vous pouvez utiliser cette page pour modifier des collecteurs de données existants.

Étapes

1. Dans le menu Data Infrastructure Insights, cliquez sur **observabilité > Collectors**

   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, son état, l'adresse IP à laquelle le collecteur accède et quand les données ont été acquises pour la dernière fois depuis le périphérique A. Les actions pouvant être effectuées sur cet écran sont les suivantes :

   - Contrôle de l'interrogation
   - Modifier les informations d'identification du collecteur de données
   - Collecteurs de données de clonage

Contrôle de l'interrogation du Data Collector

Après avoir apporté une modification à un collecteur de données, vous pouvez interroger immédiatement pour vérifier vos modifications ou reporter la collecte de données sur un collecteur de données pendant un, trois ou cinq jours pendant que vous travaillez sur un problème.

Étapes

1. Dans le menu Data Infrastructure Insights, cliquez sur **observabilité > Collectors**
2. Cliquez sur **collecteurs de données installés**
3. Cochez la case à gauche du Data Collector que vous souhaitez modifier
4. Cliquez sur **actions groupées** et sélectionnez l'action d'interrogation que vous souhaitez effectuer.

   Les actions en bloc peuvent être exécutées simultanément sur plusieurs collecteurs de données. Sélectionnez les collecteurs de données et choisissez l'action à effectuer dans le menu **action groupée**.

Modification des informations du collecteur de données

Vous pouvez modifier les informations de configuration existantes du collecteur de données.

Pour modifier un collecteur de données unique :

1. Dans le menu Data Infrastructure Insights, cliquez sur **observabilité > Collectors** pour ouvrir la liste des Data Collectors 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. Entrez 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 groupées** 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 résident sur la même unité d'acquisition.

Lors de l'édition 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 sur les collecteurs de données sélectionnés affichent les valeurs actuelles et peuvent être modifiés.

Lors de l'édition de plusieurs collecteurs de données, le bouton **Test Configuration** n'est pas disponible.

Clonage des collecteurs de données

La fonction de clonage permet d'ajouter rapidement une source de données dotée des mêmes identifiants et attributs qu'une autre source de données. Le clonage vous permet de configurer facilement plusieurs instances d'un même type de périphérique.

Étapes

1. Dans le menu Data Infrastructure Insights, cliquez sur **observabilité > Collectors**.
2. Cliquez sur **collecteurs de données installés**.
3. Cochez la case 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 **Clone**.

   La boîte de dialogue Cloner le Data Collector s'affiche.

5. Entrez de nouvelles informations dans les champs obligatoires.
6. Cliquez sur **Enregistrer**.

Une fois que vous avez terminé

L'opération de clonage copie tous les autres attributs et paramètres pour créer le nouveau collecteur de données.

Exécution d'actions en bloc sur des collecteurs de données

Vous pouvez modifier simultanément certaines informations pour plusieurs collecteurs de données. Cette fonction vous permet de lancer un sondage, de reporter l'interrogation et de reprendre l'interrogation sur plusieurs collecteurs de données. En outre, vous pouvez supprimer plusieurs collecteurs de données.

Étapes

1. Dans le menu Data Infrastructure Insights, cliquez sur **observabilité > Collectors**
2. Cliquez sur **collecteurs de données installés**
3. Cochez la case 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.

Une fois que vous avez terminé

L'opération que vous avez sélectionnée est exécutée sur les collecteurs de données. Lorsque vous avez choisi de supprimer des collecteurs de données, une boîte de dialogue vous demande de vous conformer à l'action.

Recherche d'un collecteur de données défectueux

Si un collecteur de données a 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.

Procédez comme suit pour déterminer la cause de l'échec des collecteurs de données. Les messages d'échec du collecteur de données s'affichent dans le menu **Admin** et sur la page **Data Collectors installés**.

Étapes

1. Cliquez sur **Admin** > **Data Collectors** > **Data Collectors installés**.
2. Cliquez sur le nom lié du collecteur de données défaillant pour ouvrir la page Résumé.
3. Sur la page Summary, vérifiez dans la zone Comments les remarques qui auraient pu être laissées par un autre ingénieur pour compte.
4. Notez tous les messages de performance.
5. Déplacez le pointeur de la 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 affiché 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 en cours d'utilisation et les suggestions sur ce qui peut être tenté de corriger le problème.

7. Dans la zone périphériques signalés par ce Data Collector, vous pouvez filtrer la liste pour n'afficher que les périphériques qui vous intéressent et cliquer sur le **Nom** lié d'un périphérique pour afficher la page de ressources de ce périphérique.
8. Lorsque vous revenez à la page de résumé du collecteur de données, vérifiez la zone **Afficher les changements récents** en bas de la page pour voir si des modifications récentes pourraient avoir causé le problème.

Importation à partir de la galerie de tableaux de bord

Data Infrastructure Insights fournit un certain nombre de tableaux de bord recommandés pour fournir des informations stratégiques sur vos données. Chaque tableau de bord contient des widgets conçus pour vous aider à répondre à une question particulière ou à résoudre un problème particulier concernant les données actuellement collectées sur votre locataire.

Pour importer un tableau de bord à partir de la galerie, procédez comme suit :

1. Sélectionnez **tableaux de bord > tableaux de bord**
2. Cliquez sur **+dans Galerie**

   Une liste de **tableaux de bord recommandés** s'affiche. Chaque tableau de bord est nommé avec une question spécifique que le tableau de bord peut vous aider à résoudre. Des tableaux de bord permettent de répondre aux questions concernant différents types d'objets, notamment AWS, NetApp, le stockage, VMware, et autres

3. Sélectionnez un ou plusieurs tableaux de bord dans la liste et cliquez sur **Ajouter tableaux de bord**. Ces tableaux de bord s'affichent à présent dans votre liste de bord.

En plus des tableaux de bord recommandés, vous pouvez également choisir d'importer **tableaux de bord supplémentaires** qui ne sont pas pertinents pour vos données actuelles. Par exemple, si aucun collecteur de données de stockage n'est actuellement installé mais que vous prévoyez de le configurer ultérieurement, vous pouvez toujours choisir d'importer les tableaux de bord pertinents pour le stockage. Ces tableaux de bord seront disponibles à l'affichage mais ne peuvent pas afficher les données pertinentes tant qu'au moins un collecteur de données de stockage n'est pas configuré.

L'importation à partir de la galerie du tableau de bord est accessible aux utilisateurs ayant le rôle Administrateur ou propriétaire du compte.

Comptes utilisateur et rôles

Data Infrastructure Insights fournit jusqu'à quatre rôles de compte utilisateur : propriétaire de compte, administrateur, utilisateur et invité. Chaque compte se voit attribuer des niveaux d'autorisation spécifiques, comme indiqué dans le tableau ci-dessous. Les utilisateurs "invités"accèdent aux informations de l'infrastructure de données et se voient attribuer un rôle spécifique, ou peuvent se connecter via "Autorisation SSO (Single Sign-On)" 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 des privilèges d'administrateur pour créer ou modifier des comptes d'utilisateur. Un rôle est attribué à chaque compte utilisateur pour chaque fonctionnalité Data Infrastructure Insights à partir des niveaux d'autorisation suivants.

Rôle	Observabilité	Sécurité des workloads	Création de rapports	Admin
Propriétaire du compte	Identique à Administrateur	Identique à Administrateur	Identique à Administrateur	Identique à Administrator, et gère la configuration de l'authentification SSO et de la fédération des identités. Peut également attribuer des propriétaires supplémentaires.

Rôle	Observabilité	Sécurité des workloads	Création de rapports	Admin
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, les analyses approfondies, les collecteurs de données, les stratégies de réponse automatisées et les jetons d'API pour la sécurité. Un administrateur peut également inviter d'autres utilisateurs, mais peut uniquement attribuer des rôles de sécurité.	Peut exécuter toutes les fonctions utilisateur/auteur, y compris la gestion des tokens API Reporting, ainsi que toutes les tâches administratives telles que la configuration des rapports, l'arrêt et le redémarrage des tâches de reporting. Un administrateur peut également inviter d'autres utilisateurs, mais peut uniquement attribuer des rôles de rapport.	Peut inviter d'autres utilisateurs, mais ne peut affecter que des rôles d'observabilité. Peut afficher, mais pas modifier la configuration SSO. Peut créer et gérer des jetons d'accès aux API. Peut afficher les informations d'audit. Permet d'afficher les informations d'abonnement, l'utilisation et l'historique. Peut gérer les listes de destinataires des notifications d'alertes globales et des notifications d'abonnement.
Utilisateur	Peut afficher et modifier les tableaux de bord, les requêtes, les alertes, les annotations, les règles d'annotation, et des applications, et gérez la résolution des périphériques.	Peut afficher et gérer des alertes et afficher des informations judiciaires. Le rôle de l'utilisateur peut modifier l'état des alertes, ajouter une note, effectuer des instantanés manuellement et gérer l'accès des utilisateurs limité.	Peut exécuter toutes les fonctions invité/consommateur ainsi que créer et gérer des rapports et des tableaux de bord.	Non disponible

Rôle	Observabilité	Sécurité des workloads	Création de rapports	Admin
Invité	Dispose d'un accès en lecture seule aux pages de ressources, aux tableaux de bord, aux alertes et peut afficher et exécuter des requêtes.	Peut afficher les alertes et les analyses approfondies. Le rôle invité ne peut pas modifier le statut des alertes, ajouter une note, effectuer des instantanés manuellement ou restreindre l'accès des utilisateurs.	Permet d'afficher, de planifier et d'exécuter des rapports et de définir des préférences personnelles telles que celles pour les langues et les fuseaux horaires. Les clients/clients ne peuvent pas créer de rapports ni effectuer des 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 celui des comptes utilisateur ou invités.

Autorisations d'accès aux informations sur l'infrastructure de données par rôle d'utilisateur

Le tableau suivant présente les autorisations Data Infrastructure Insights accordées à chaque rôle d'utilisateur.

Fonction	Administrateur/propriétaire du compte	Utilisateur	Invité
Unités d'acquisition : ajouter/Modifier/Supprimer	Y	N	N
Alertes* : créer/Modifier/Supprimer	Y	Y	N
Alertes*: Affichage	Y	Y	Y
Règles d'annotation : créer/Exécuter/Modifier/Supprimer	Y	Y	N
Annotations : créer/Modifier/affecter/Afficher/Supprimer/Supprimer	Y	Y	N
Accès API* : créer/Renommer/Désactiver/révoquer	Y	N	N
Applications : créer/Afficher/Modifier/Supprimer	Y	Y	N
Pages de ressources : modifier	Y	Y	N
Pages de ressources : afficher	Y	Y	Y

Audit : afficher	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/Sondage/ 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 du périphérique	Y	Y	N
Rapports* : afficher/Exécuter	Y	Y	Y
Rapports* : créer/Modifier/Supprimer/ planifier	Y	Y	N
Abonnement : afficher/Modifier	Y	N	N
Gestion des utilisateurs : inviter/Ajouter/Modifier/Désactiver	Y	N	N

*Nécessite Premium Edition

Créer des comptes en invitant des utilisateurs

La création d'un compte utilisateur est possible via BlueXP. Un utilisateur peut répondre à l'invitation envoyée par e-mail, mais s'il ne dispose pas d'un compte BlueXP, il doit s'inscrire auprès de BlueXP pour accepter l'invitation.

Avant de commencer

- Le nom d'utilisateur est l'adresse électronique de l'invitation.
- Comprendre les rôles utilisateur que vous allez attribuer.
- Les mots de passe sont définis par l'utilisateur pendant le 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**

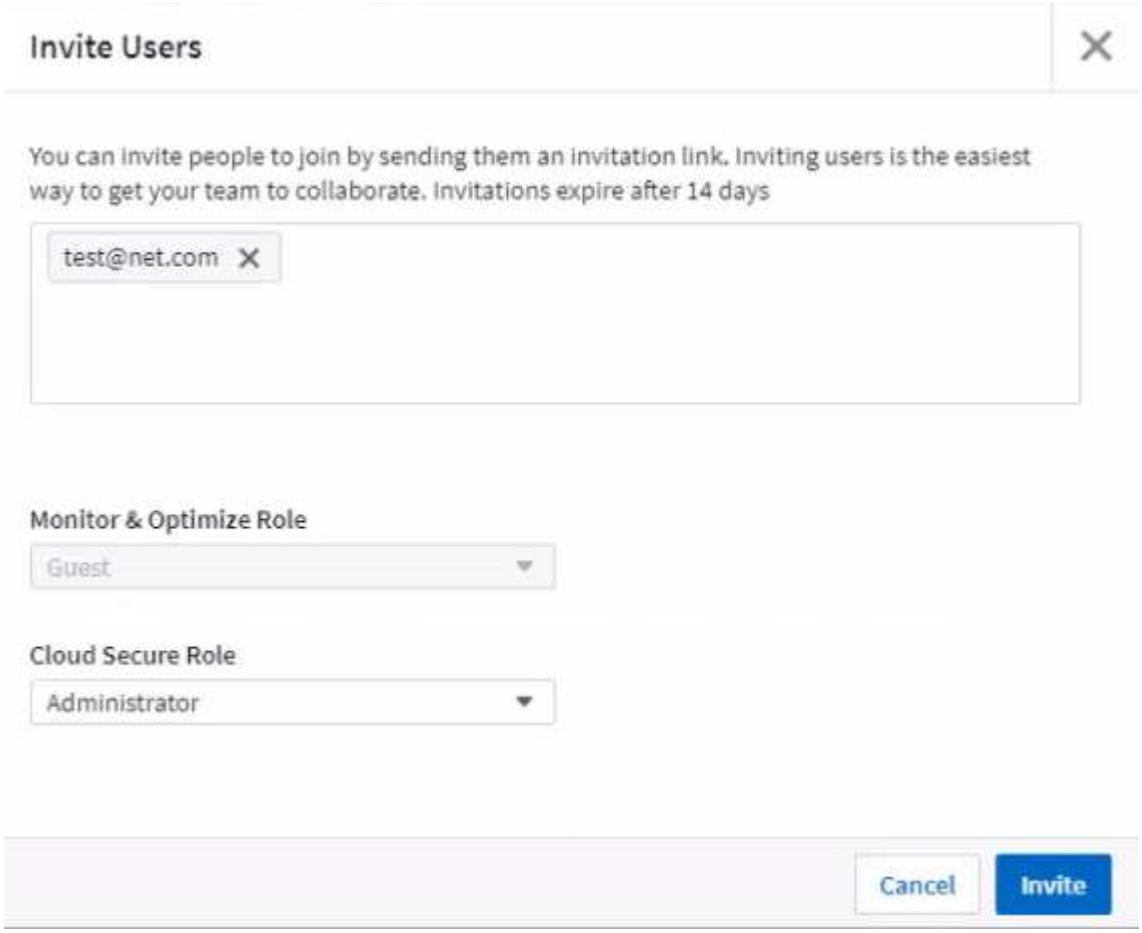
   L'écran **inviter utilisateur** s'affiche.

4. Entrez 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 fonctions et les rôles que vous pouvez choisir dépendent des fonctionnalités auxquelles vous avez accès dans votre rôle d'administrateur particulier. Par exemple, si vous avez un rôle d'administrateur uniquement pour Reporting, vous serez en mesure d'affecter des utilisateurs à n'importe quel rôle dans Reporting, mais vous ne pourrez pas attribuer de rôles à des fins d'observabilité ou de sécurité.



6. Cliquez sur **inviter**

   L'invitation est envoyée à l'utilisateur. Les utilisateurs auront 14 jours pour accepter l'invitation. Une fois l'invitation acceptée, l'utilisateur sera redirigé vers le portail NetApp Cloud Portal où il utilisera l'adresse e-mail de l'invitation. S'il dispose déjà d'un compte pour cette adresse e-mail, il lui suffit de se connecter pour

accéder à son environnement Data Infrastructure Insights.

Modification du rôle d'un utilisateur existant

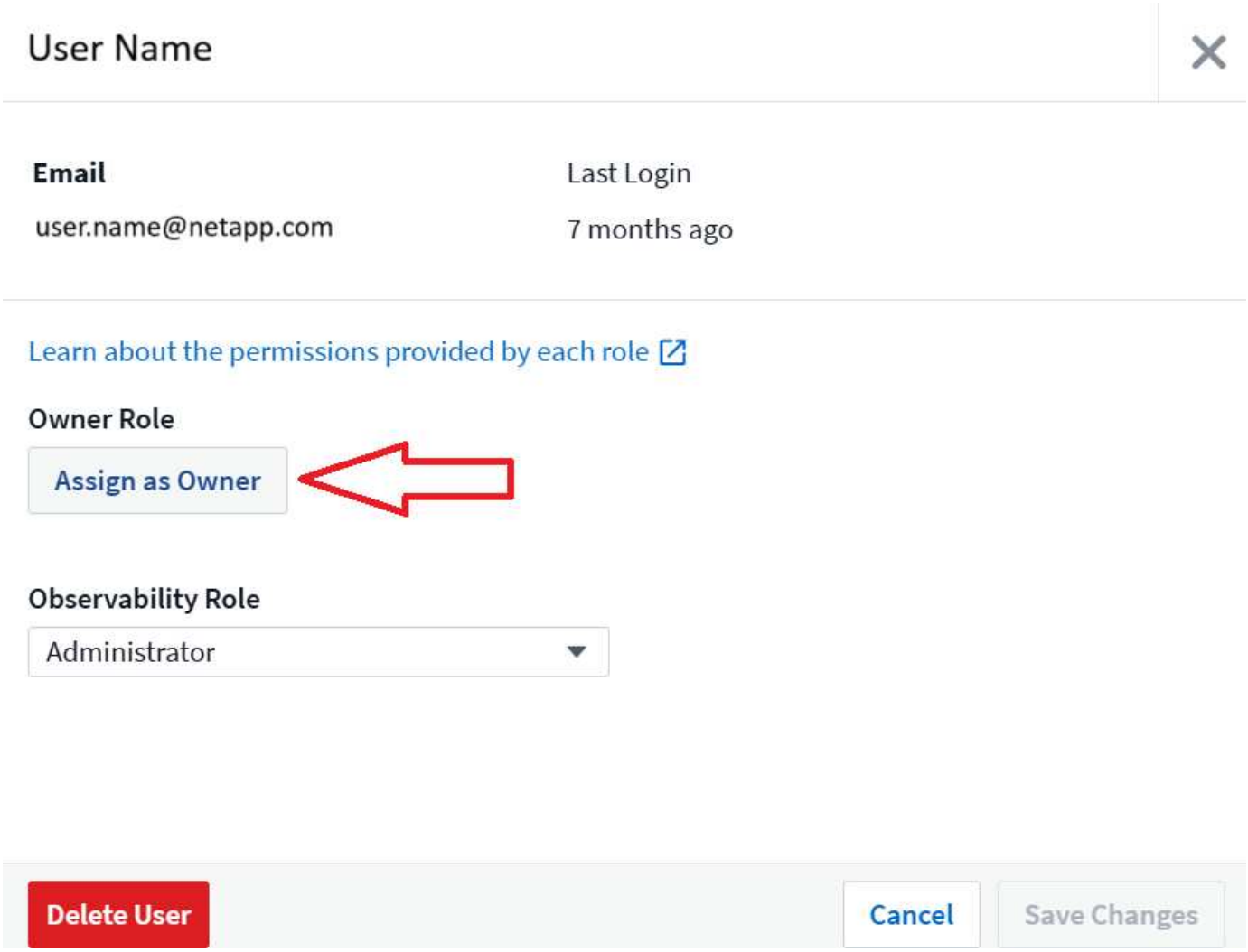
Pour modifier le rôle d'un utilisateur existant, y compris l'ajouter en tant que **propriétaire de compte secondaire**, procédez comme suit.

1. Cliquez sur **Admin > gestion des utilisateurs**. L'écran affiche la 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 Data Infrastructure Insights si nécessaire.
4. Cliquez sur *Enregistrer les modifications*.

Pour attribuer un propriétaire de compte secondaire

Vous devez être connecté en tant que propriétaire de compte pour l'observabilité afin d'affecter le rôle propriétaire du 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 seulement sélectionner des personnes.

Suppression d'utilisateurs

Un utilisateur avec le rôle Administrateur peut supprimer un utilisateur (par exemple, quelqu'un n'ayant plus la société) 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 restent disponibles dans l'environnement Data Infrastructure Insights même après la suppression de l'utilisateur.

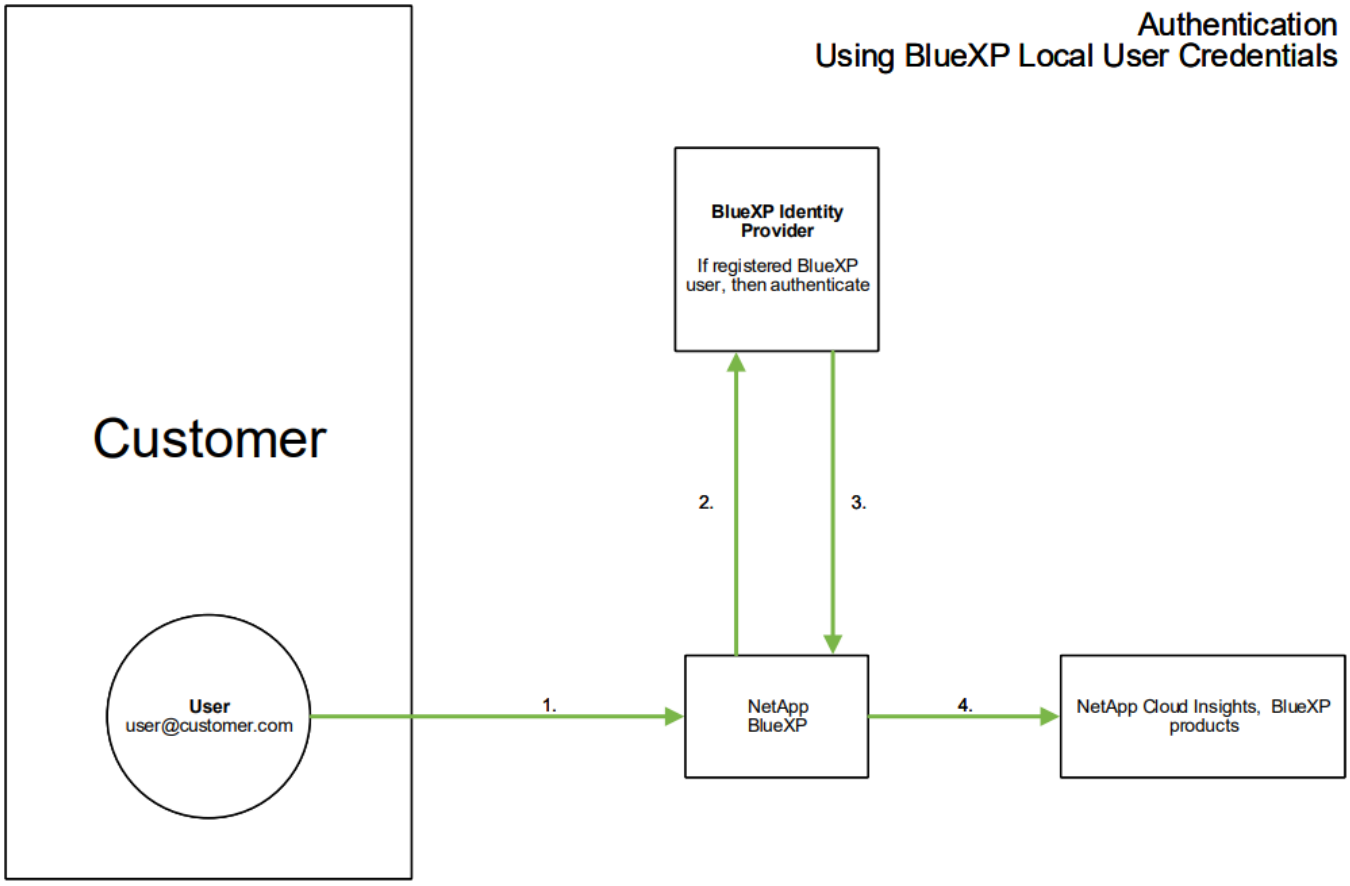
Authentification unique (SSO) et fédération des identités

Qu'est-ce que la fédération des identités ?

Avec la fédération des identités :

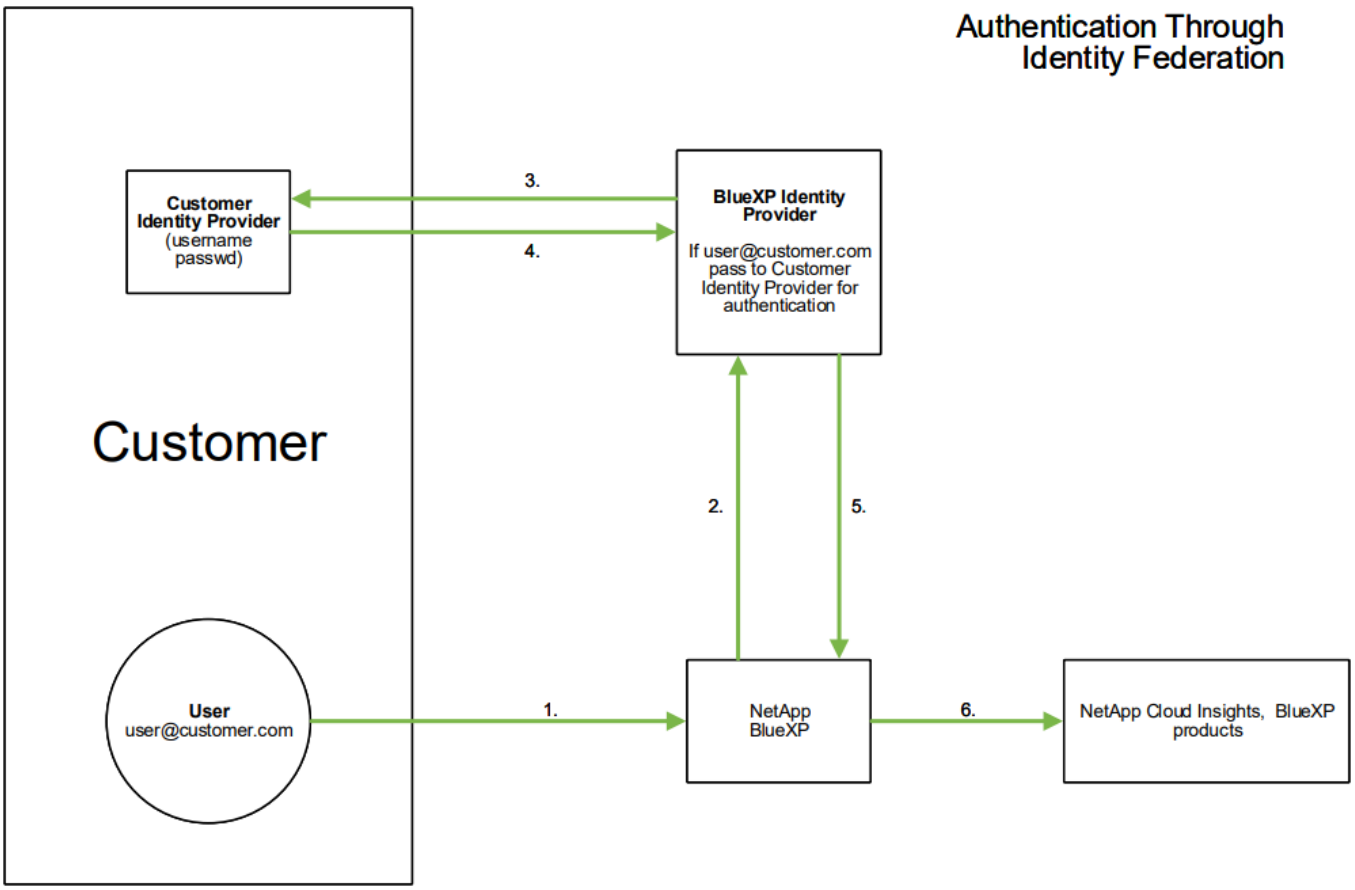
- L'authentification est déléguée au système de gestion des identités du client, en utilisant les informations d'identification du client de votre annuaire d'entreprise et les stratégies d'automatisation telles que l'authentification multifacteur (MFA).
- Les utilisateurs se connectent une seule fois à tous les services NetApp BlueXP (authentification unique).

Les comptes utilisateur sont gérés dans NetApp BlueXP pour tous les services cloud. Par défaut, l'authentification s'effectue à l'aide d'un profil utilisateur local BlueXP. Voici une présentation simplifiée de ce processus :



Cependant, certains clients souhaitent utiliser leur propre fournisseur d'identité pour authentifier leurs utilisateurs afin de bénéficier des informations exploitables de l'infrastructure de données et de leurs autres services NetApp BlueXP . Grâce à la fédération des identités, les comptes NetApp BlueXP sont authentifiés à l'aide d'informations d'identification provenant 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 à des fins d'authentification. Une fois le compte authentifié, l'utilisateur est dirigé vers l'URL du locataire Data Infrastructure Insights.

Activation de la fédération des identités

BlueXP utilise Auth0 pour implémenter la fédération des identités et intégrer des services tels que ADFS (Active Directory Federation Services) et Active Directory de Microsoft Azure. Pour configurer la fédération des identités, reportez-vous au "Instructions de fédération BlueXP".

Vous devez configurer la fédération des identités BlueXP avant de pouvoir utiliser SSO avec les informations d'infrastructure de données.

Il est important de comprendre que la modification de la fédération des identités dans BlueXP s'appliquera non seulement aux informations exploitables sur l'infrastructure de données, mais aussi à tous les services NetApp BlueXP . Le client doit discuter de ce changement avec l'équipe NetApp de chaque produit BlueXP qu'il possède pour s'assurer que la configuration qu'il utilise fonctionnera avec la fédération des identités ou si des ajustements doivent être effectués sur les comptes. Le client devra également faire appel à son équipe interne SSO pour modifier la fédération des identités.

Il est également important de réaliser qu'une fois la fédération des identités activée, toute modification du fournisseur d'identité de l'entreprise (comme le passage de SAML à Microsoft AD) nécessitera probablement des dépannages/modifications/une attention particulière dans BlueXP pour mettre à jour les profils des utilisateurs.

Pour ce problème de fédération ou pour tout autre problème de fédération, vous pouvez ouvrir un ticket de support à l'adresse https://mysupport.netapp.com/site/help et sélectionner la catégorie « BlueXP .NetApp.com

> problèmes de fédération ».

Mise en service automatique par l'utilisateur 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. Lorsque SSO est activé, tout utilisateur possédant 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 utilisateur SSO inclut "Fédération des identités" via NetApp BlueXP comme décrit dans la section ci-dessus. La fédération permet aux utilisateurs d'authentification unique d'accéder à vos comptes NetApp BlueXP à l'aide d'identifiants de votre répertoire d'entreprise, en utilisant des normes ouvertes telles que le langage SAML (Security assertion Markup Language 2.0) et OpenID Connect (OIDC).

Pour configurer *SSO User Auto-Provisioning*, vous devez d'abord avoir configuré BlueXP Identity Federation sur la page **Admin > User Management**. Sélectionnez le lien **configurer la fédération** dans la bannière pour passer à la fédération BlueXP. Une fois configuré, les administrateurs Data Infrastructure Insights peuvent activer la connexion utilisateur SSO. Lorsqu'un administrateur active *SSO User Auto-Provisioning*, il choisit un rôle par défaut pour tous les utilisateurs SSO (comme invité ou utilisateur). Les utilisateurs qui se connectent via SSO possèdent ce rôle par défaut.



Il arrive parfois qu'un administrateur souhaite promouvoir un utilisateur unique à partir du rôle SSO par défaut (par exemple, pour lui faire un administrateur). Ils peuvent le faire sur la page **Admin > User Management** en cliquant sur le menu de droite de l'utilisateur et en sélectionnant *Assign role*. Les utilisateurs auxquels un rôle explicite est attribué de cette façon continuent d'avoir accès à Data Infrastructure Insights même si *SSO User Auto-Provisioning* est désactivé par la suite.

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.

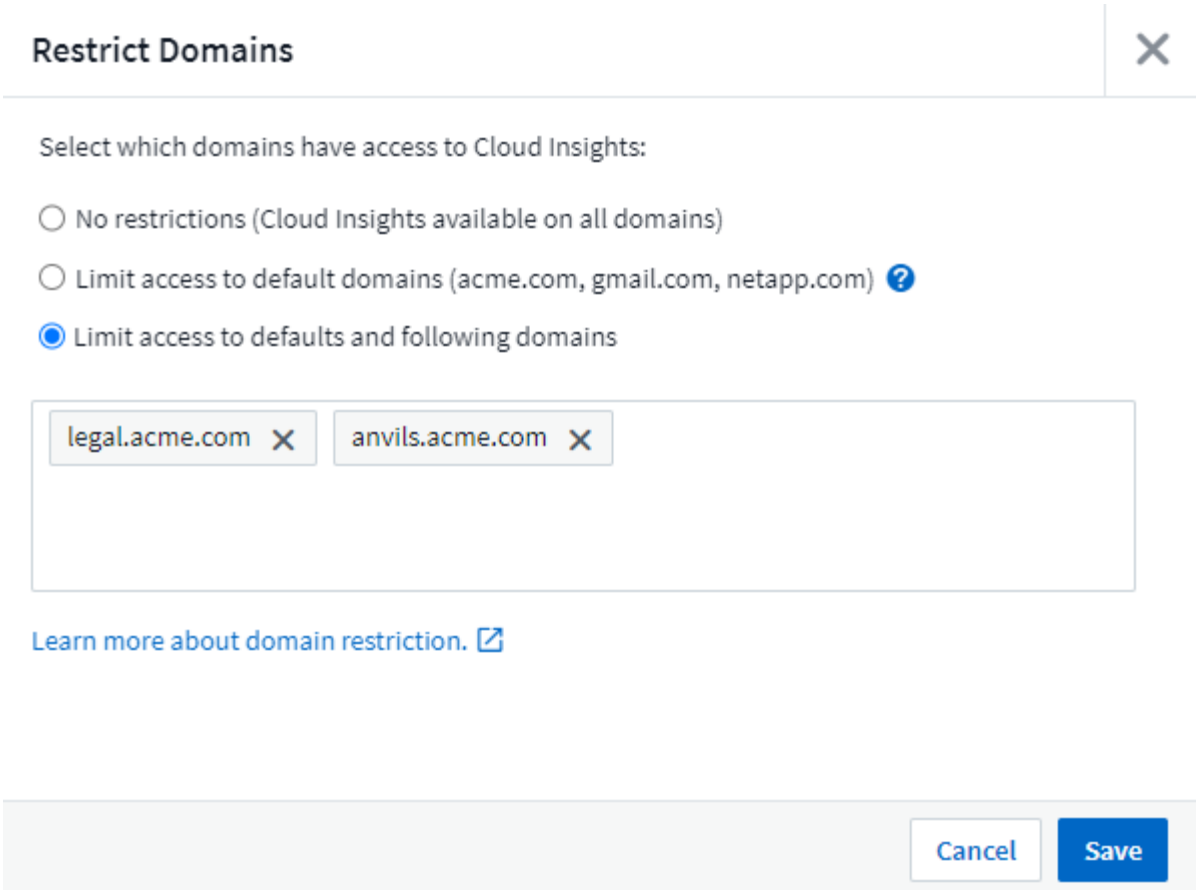
Vous pouvez choisir de masquer les utilisateurs SSO en décochant la case **Afficher les utilisateurs SSO**.

Cependant, n'activez pas l'option *SSO User Auto-Provisioning* si l'un de ces éléments est vrai :

- Votre entreprise dispose de plusieurs locataires Data Infrastructure Insights
- Votre entreprise 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 dans le temps, nous n'avons pas la possibilité d'utiliser des groupes pour contrôler l'accès aux rôles avec cette option*.

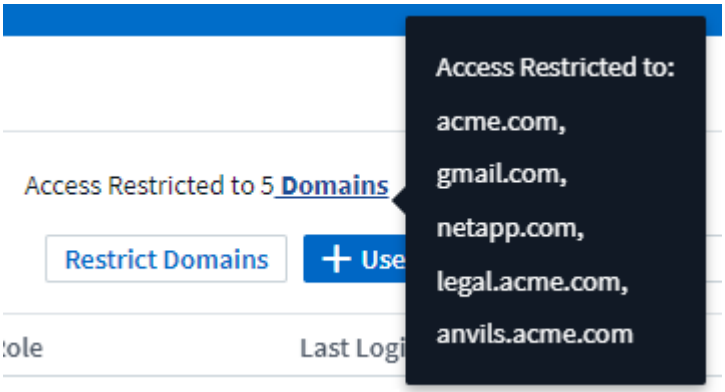
Restriction de l'accès par domaine

Les informations sur l'infrastructure de données peuvent limiter l'accès des utilisateurs aux seuls domaines que vous spécifiez. Sur la page **Admin > gestion des utilisateurs**, sélectionnez « restreindre les domaines ».



Les choix suivants s'offrent à vous :

- Aucune restriction : les informations concernant l'infrastructure de données restent accessibles 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 d'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 que vous souhaitez avoir accès à votre environnement Data Infrastructure Insights, en plus des domaines par défaut.



Liste Data Collector de Data Infrastructure Insights

Informations exploitables sur l'infrastructure de données prend en charge une variété de collecteurs de données de nombreux fournisseurs et services.

Les collecteurs de données sont classés selon les types suivants :

- Infrastructure : acquisition auprès de dispositifs du fournisseur tels que les baies de stockage, les commutateurs, les hyperviseurs ou les dispositifs de sauvegarde.
- Service : acquis auprès de services tels que Kubernetes ou Docker. Également appelé *Integration*.

Liste alphabétique des collecteurs de données pris en charge par Data Infrastructure Insights :

Collecteur de données	Type
"Amazon EC2 et EBS"	Infrastructures
"AWS S3 en tant que système de stockage"	Infrastruture
"Amazon FSX pour NetApp ONTAP"	Infrastructures
"Apache"	Service
"Azure NetApp Files"	Infrastructures
"Les machines virtuelles Azure et les VHD"	Infrastructures
"Brocade Network Advisor (BNA)"	Infrastructures
"Commutateurs Fibre Channel Brocade"	Infrastructures
"Brocade FOS REST"	Infrastructures
"Commutateurs de structure Cisco MDS"	Infrastructures
"Consul"	Service
"Couchbase"	Service
"CouchDB"	Service
"Cohesity SmartFiles"	Infrastructures
"Dell EMC Data Domain"	Infrastructures
"Dell EMC ECS"	Infrastructures
"Dell EMC PowerScale (auparavant Isilon)"	Infrastructures
"Dell EMC Isilon / POWERSCALE REST"	Infrastructures
"Dell EMC PowerStore"	Infrastructures
"Dell EMC RecoverPoint"	Infrastructures
"Dell EMC ScaleIO/PowerFlex"	Infrastructures
"Dell EMC Unity"	Infrastructures
"DELL EMC Unisphere REST"	Infrastructures

Collecteur de données	Type
"Gamme de périphériques Dell EMC VMAX/PowerMax"	Infrastructures
"Stockage de blocs Dell EMC VNX"	Infrastructures
"Fichier Dell EMC VNX"	Infrastructures
"Stockage unifié Dell EMC VNX"	Infrastructures
"Dell EMC VPLEX"	Infrastructures
"Dell EMC XtremIO"	Infrastructures
"Série Dell XC"	Infrastructures
"Docker"	Service
"ElasticSearch"	Service
"Encre"	Service
"ETERNUS DX de Fujitsu"	Infrastructures
"Google Compute et Storage"	Infrastructures
"Google Cloud NetApp volumes"	Infrastructures
"Hadoop"	Service
"HABProxy"	Service
"Plate-forme de contenu Hitachi (HCP)"	Infrastructures
"Suite de commande Hitachi Vantara"	Infrastructures
"Plateforme NAS Hitachi Vantara"	Infrastructures
"Hitachi Ops Center"	Infrastructures
"Solution de stockage HP Enterprise Alletra 6000 (anciennement Nimble)"	Infrastructures
"Système de stockage HP Enterprise Alletra 9000 / Primera (auparavant 3PAR"	Infrastructures
"HP Enterprise Command View"	Infrastructures
"Périphériques Huawei OceanStor et Dorado"	Infrastructures
"IBM Cleversafe"	Infrastructures
"Gamme IBM CS"	Infrastructures
"IBM PowerVM"	Infrastructures
"Contrôleur de volume SAN IBM (SVC)"	Infrastructures
"Gamme IBM System Storage DS8000"	Infrastructures
"Storages IBM XIV et A9000"	Infrastructures
"Infinidat Box d'Infinidat"	Infrastructures
"Java"	Service

Collecteur de données	Type
"Kafka"	Service
"Kapacitor"	Service
"Kibana"	Service
"Kubernetes"	Service
"Lenovo HX Series"	Infrastructures
"Mise en mémoire cache"	Service
"Microsoft Azure NetApp Files"	Infrastructures
"Microsoft Hyper-V"	Infrastructures
"MongoDB"	Service
"MySQL"	Service
"NetApp Cloud Volumes ONTAP"	Infrastructures
"NetApp Cloud volumes Services pour AWS"	Infrastructures
"Connexion cloud NetApp pour ONTAP 9.9+"	Infrastructures
"NetApp Data ONTAP 7-mode"	Infrastructures
"NetApp E-Series"	Infrastructures
"NetApp E-Series REST"	Infrastructures
"Amazon FSX pour NetApp ONTAP"	Infrastructures
"Centre virtuel NetApp HCI"	Infrastructures
"Logiciel de gestion des données NetApp ONTAP"	Infrastructures
"Collecteur de REPOS NetApp ONTAP"	Infrastructures
"Collecteur de baies SAN 100 % Flash (ASA) NetApp ONTAP"	Infrastructures
"NetApp ONTAP Select"	Infrastructures
"Baies 100 % Flash NetApp SolidFire"	Infrastructures
"NetApp StorageGRID"	Infrastructures
"Netstat"	Service
"Nginx"	Service
"Nœud"	Service
"Gamme Nutanix NX"	Infrastructures
"OpenZFS"	Service
"Oracle ZFS Storage Appliance"	Infrastructures
"PostgreSQL"	Service
"Agent Puppet"	Service

Collecteur de données	Type
"Solution FlashArray de Pure Storage"	Infrastructures
"Red Hat Virtualization"	Infrastructures
"Redis"	Service
"RethinkDB"	Service
"RHEL ; CentOS"	Service
"Stockage CDM Rubrik"	Infrastructures
"Ubuntu Debian"	Service
"VASTE stock de données"	Infrastructures
"VMware vSphere"	Infrastructures
"Fenêtres"	Service
"Zookeeper"	Service

Abonnement à Data Infrastructure Insights

La mise en route de Data Infrastructure Insights se fait en trois étapes simples :

1. Créez un compte sur **"NetApp BlueXP"** pour accéder à toutes les offres cloud de NetApp.
2. Inscrivez-vous pour essayer gratuitement Data Infrastructure Insights et découvrir les fonctionnalités disponibles. Pour vous inscrire à un essai gratuit :
   - Accédez à https://netapp.com
   - Sélectionnez **choisir un partenaire** en haut de la page.
   - Sélectionnez **demander un essai**. Si vous n'êtes pas encore inscrit à BlueXP , saisissez vos coordonnées et inscrivez-vous. Sinon, connectez-vous.
   - Planifiez une réunion ou attendez qu'un représentant vous contacte au sujet de votre version d'évaluation.
3. **Abonnez-vous** à Data Infrastructure Insights pour un accès continu et ininterrompu à vos données grâce à une variété d'options d'abonnement flexibles :
   - "Ventes directes NetApp"
   - Place de marché AWS :
     - "Abonnement à durée déterminée"
     - "Abonnement avec paiement à l'utilisation"
     - "Abonnement base fixe + dépassements à la carte"
   - "Azure Marketplace" (toutes les options d'abonnement)

Lors du processus d'enregistrement, vous pouvez choisir la région globale dans laquelle héberger votre environnement Data Infrastructure Insights. Pour en savoir plus, consultez la rubrique informations sur l'infrastructure de données "Information et région".

Pour une comparaison complète des fonctionnalités disponibles dans Data Infrastructure Insights Basic Edition et Premium Edition, reportez-vous à la "Éditions Data Infrastructure Insights" page.

> Les environnements inactifs Data Infrastructure Insights Basic Edition sont supprimés et leurs ressources sont récupérées. Un environnement est considéré comme inactif s'il n'y a aucune activité utilisateur pendant 30 jours consécutifs, si aucune donnée n'est ingérées pendant 7 jours consécutifs. Data Infrastructure Insights envoie une notification et fournit un délai de grâce de quatre jours avant la suppression d'un environnement.

Lorsque vous utilisez Data Infrastructure Insights, si vous voyez une icône de cadenas  , cela signifie que la fonction n'est pas disponible dans votre abonnement actuel ou est disponible sous une forme limitée. Abonnez-vous à cette fonction pour un accès complet. Certaines fonctionnalités sont disponibles Évaluation du module avant l'abonnement.

Version d'essai

En vous inscrivant pour accéder à des informations exploitables sur l'infrastructure de données et que votre environnement est actif, vous pouvez participer à un essai gratuit de 30 jours de Data Infrastructure Insights. Pendant la période d'essai, vous pouvez explorer les fonctionnalités que Data Infrastructure Insights peut offrir, dans votre propre environnement.

Vous pouvez à tout moment pendant la période d'essai vous abonner à Data Infrastructure Insights. En vous abonnant à Data Infrastructure Insights, vous bénéficiez d'"**support produit**"un accès ininterrompu à vos données ainsi que d'options étendues.

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 abonnement.

Si vous avez besoin de plus de temps pour évaluer les informations stratégiques de votre infrastructure de données et que votre version d'évaluation expire dans 4 jours ou moins, vous pouvez prolonger votre période d'essai de 30 jours supplémentaires. Vous ne pouvez prolonger l'essai qu'une seule fois. Vous ne pouvez pas prolonger si votre période d'essai a expiré.

Essai via AWS Marketplace

Vous pouvez également vous inscrire pour essayer gratuitement sur 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 se passe-t-il si mon essai a expiré ?

Si votre essai gratuit a expiré et que vous n'avez pas encore souscrit à Data Infrastructure Insights, vous bénéficierez de fonctionnalités limitées jusqu'à votre abonnement. L'ingestion des données peut s'arrêter et au bout de quelques semaines, vos données seront supprimées conformément à notre politique de conservation des données.

Que se passe-t-il si mon abonnement a expiré ?

Si vous avez souscrit un abonnement à Data Infrastructure Insights, mais que cet abonnement a expiré, vous disposez d'un délai de grâce de cinq jours pour renouveler votre abonnement. Toutes les fonctionnalités Data Infrastructure Insights restent actives pendant ce délai de grâce.

Une fois le délai de grâce écoulé, la fonctionnalité Data Infrastructure Insights est suspendue jusqu'au renouvellement. Pour renouveler votre abonnement, consultez la page **Admin > abonnement** ou contactez le service commercial de NetApp.

Vos données Data Infrastructure Insights restent intactes pendant les 30 jours suivant le délai de grâce. Si vous renouvelez votre abonnement dans ce délai, toutes vos données jusqu'au moment où le délai de grâce s'est écoulé seront disponibles.

Évaluation du module

Vous pouvez également profiter des **évaluations de module**. Par exemple, si vous êtes déjà abonné à l'observabilité de l'infrastructure, mais que vous ajoutez Kubernetes à votre environnement, vous passez automatiquement une évaluation de 30 jours de l'observabilité Kubernetes, à partir de l'installation de l'opérateur de surveillance Kubernetes NetApp. Vous ne serez facturé que pour l'utilisation de votre unité gérée d'observabilité Kubernetes à la fin de la période d'évaluation.

Gardez à l'esprit que vous serez facturé pour une nouvelle utilisation d'unité gérée (MU) après l'évaluation, assurez-vous donc de planifier en conséquence. À la fin de l'évaluation de votre module, vous serez informé si vous devrez ajouter d'autres unités de gestion pour éviter toute interruption de service.

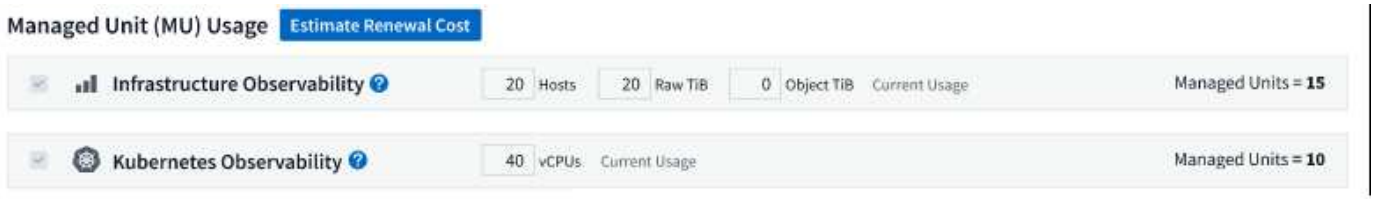
Vous pouvez contrôler l'utilisation de votre unité gérée sur la page **Admin > abonnement** de l'onglet **usage**.



Une *évaluation de module* n'est pas une *version d'essai* - nous utilisons la version d'essai lorsque nous fournissons aux clients une période d'essai gratuite d'utilisation du service Data Infrastructure Insights pour confirmer l'adéquation et activer l'achat. Une évaluation de module est différente. C'est lorsque nous permettons à un client payant de tester un module 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 annulés. L'environnement de travail du client est toujours sous abonnement et n'a pas rétabli la version d'évaluation. L'abonnement n'a pas changé.

Estimateur

Lors d'une évaluation du module, vous n'êtes pas facturé pour l'utilisation des UM pour les ressources consommées pour le module, mais vous pouvez ouvrir le **estimateur** (dans l'onglet *Summary*) pour voir comment les UM seront facturées après l'évaluation, ainsi que jouer avec les scénarios « What if » avec le nombre d'UM dont vous aurez besoin à l'avenir. Réinitialisez les chiffres en quittant l'estimateur.



Cochez la case en regard d'un module pour ajouter ou supprimer les UM du module entier du coût estimé.

L'estimateur vous permet également de voir comment les numéros se positionnent soit pour un module complémentaire, où vous conservez votre abonnement actuel et augmentez le nombre d'unités gérées sous licence, soit pour une option Renew pour un abonnement de renouvellement que vous achèterez lors de votre

abonnement actuel fin du terme.

Notez que les clients ne peuvent bénéficier d'une évaluation de module qu'une seule fois par abonnement.

Options d'abonnement

Pour vous abonner, accédez à **Admin → abonnement**. En plus des boutons **Subscribe**, vous pourrez voir vos collecteurs de données installés et calculer votre mesure estimée. Dans un environnement classique, vous pouvez cliquer sur le bouton AWS Marketplace en libre-service. Si votre environnement comprend ou devrait inclure au moins 1,000 unités gérées, vous pouvez bénéficier de la tarification en volume.

Mesure de l'observabilité

L'observabilité Data Infrastructure Insights est mesurée de deux manières :

- Mesure de la capacité
- Mesure d'unité gérée (héritée)

Votre abonnement sera mesuré par l'une de ces méthodes, selon que vous avez un abonnement existant ou que vous langiez un nouvel abonnement.

Mesure de la capacité

Informations sur l'infrastructure de données : l'observabilité mesure l'utilisation en fonction du Tier de stockage de votre locataire. Vous pouvez avoir des stockages qui entrent dans une ou plusieurs de ces catégories :

- Primaire brut
- 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 usage = Raw TiB + (0.1 x Object Tier Raw TiB) + (0.25 x Cloud
Tier Provisioning TiB)
Pour faciliter cette tâche, DII calcule un seul numéro *pondéré de droit*
basé sur les quantités _souscrites_. Il calcule ensuite ce même nombre en
fonction du stockage _découvert_ et déclare la violation uniquement si la
capacité découverte est supérieure au droit pondéré. Vous avez ainsi la
possibilité de surveiller les quantités qui varient en fonction des
montants souscrits pour chaque niveau, ce que DII autorise tant que le
stockage total découvert est compris dans le droit pondéré souscrit.
```

Mesure d'unité gérée (héritée)

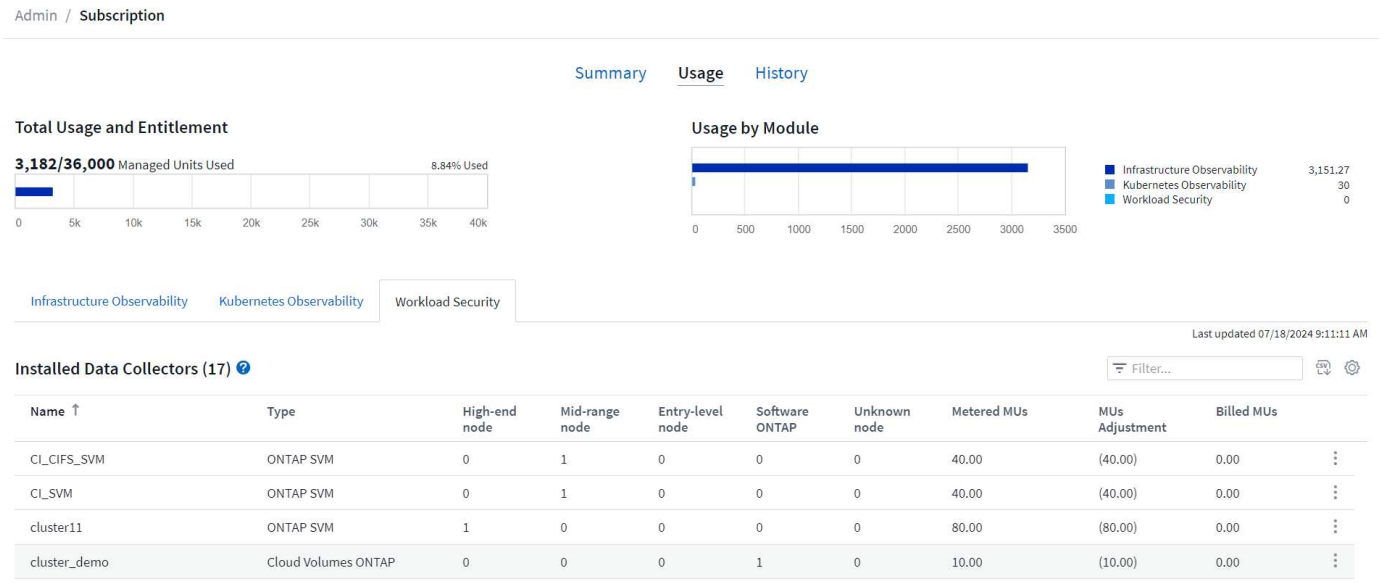
Informations sur l'infrastructure de données observabilité de l'infrastructure et utilisation du compteur d'observabilité Kubernetes par **unité gérée**. L'utilisation de vos unités gérées est calculée en fonction du nombre de **hôtes ou machines virtuelles** et de la quantité de **capacité non formatée** 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 des 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 ajustement des K8s d'une unité gérée = 2 nœuds ou hôtes également surveillés par l'infrastructure.

Mesure de la sécurité des charges de travail

La mesure de la sécurité des workloads est effectuée par Cluster selon la même approche que la mesure de l'observabilité.

Vous pouvez afficher votre utilisation de Workload Security dans la page **Admin > Subscription** de l'onglet **Workload Security**.



L'utilisation des UM des abonnements Workload Security existants est ajustée de sorte que l'utilisation des nœuds ne consomme pas les unités gérées. Data Infrastructure Insights mesure l'utilisation pour garantir la conformité avec l'utilisation sous licence.

Comment s'inscrire ?

Si votre nombre d'unités gérées est inférieur à 1,000, vous pouvez vous abonner via l'équipe de vente NetApp ou s'abonner vous-même via AWS Marketplace.

Abonnez-vous via NetApp Sales Direct

Si le nombre d'unités gérées que vous prévoyez d'utiliser est supérieur ou égal à 1,000, cliquez sur le **"Contactez-nous"** bouton pour vous abonner à l'équipe de vente NetApp.

Vous devez fournir vos informations de l'infrastructure de données **Numéro de série** à votre ingénieur commercial NetApp pour 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 se trouve sur la page **Admin > abonnement**.

Vous pouvez vous inscrire via AWS Marketplace

> Vous devez être titulaire d'un compte ou administrateur pour appliquer un abonnement AWS Marketplace à votre compte d'essai Data Infrastructure Insights existant. Vous devez également disposer d'un compte Amazon Web Services (AWS).

Cliquez sur le lien Amazon Marketplace pour ouvrir la "Informations exploitables sur l'infrastructure de données" page d'abonnement AWS, où vous pouvez terminer votre abonnement. Notez que les valeurs saisies dans le calculateur ne sont pas renseignées dans la page d'abonnement AWS ; vous devez entrer le nombre total d'unités gérées sur cette page.

Après avoir saisi le nombre total d'unités gérées et choisi soit 12 mois, soit 36 mois, cliquez sur **configurer votre compte** pour terminer le processus d'abonnement.

Une fois l'abonnement à AWS terminé, vous serez à nouveau redirigé vers votre environnement Data Infrastructure Insights. De plus, si l'environnement n'est plus actif (par exemple, vous vous êtes déconnecté), vous accédez à la page de connexion de NetApp BlueXP. Lorsque vous vous reconnectez à Data Infrastructure Insights, votre abonnement est actif.

> Après avoir cliqué sur **configurer votre compte** sur la page AWS Marketplace, vous devez terminer le processus d'abonnement AWS en une heure. Si vous ne le terminez pas dans l'heure, vous devrez cliquer de nouveau sur **configurer votre compte** pour terminer le processus.

En cas de problème et si le processus d'abonnement ne s'effectue pas correctement, la bannière « version d'évaluation » s'affiche toujours lorsque vous vous connectez à votre environnement. Dans ce cas, vous pouvez accéder à **Admin > abonnement** et répéter le processus d'abonnement.

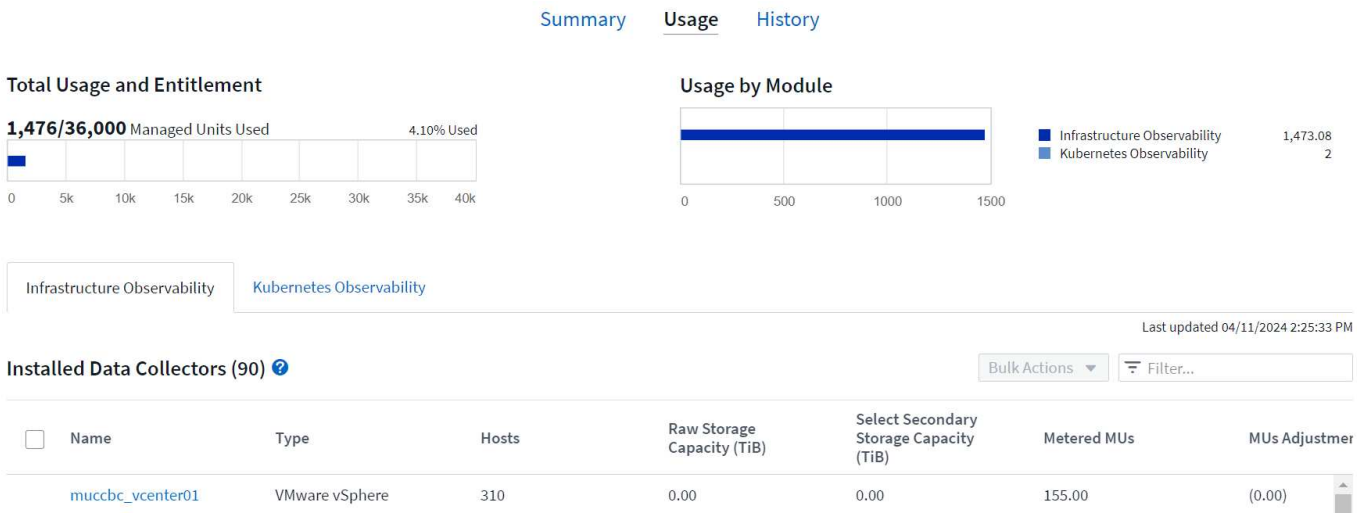
Afficher l'état de votre abonnement

Une fois votre abonnement actif, vous pouvez afficher l'état de votre abonnement et l'utilisation de l'unité gérée à partir de la page **Admin > abonnement**.

L'onglet Subscription **Summary** affiche les éléments suivants :

- Édition actuelle
- Numéro de série de l'abonnement
- Droits UM actuels

L'onglet **usage** vous indique votre utilisation actuelle des UM et la manière dont cette utilisation se divise par collecteur de données.



L'onglet **Historique** vous donne un aperçu de votre utilisation des UM au cours des 7 à 90 derniers jours. Passez le curseur sur une colonne du graphique pour une répartition par module (observabilité, Kubernetes).



Affichez votre gestion de l'utilisation

L'onglet gestion de l'utilisation présente un aperçu de l'utilisation des unités gérées, ainsi que les onglets qui dépanne la consommation des unités gérées par collecteur ou cluster Kubernetes.

Le nombre d'unités gérées capacité non formatée correspond à la somme de la capacité brute totale dans 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 Résumé. C'est parce que les nombres d'unités gérées sont arrondis à l'unité gérée la plus proche. La somme de ces nombres dans la liste collecteurs de données peut être légèrement supérieure au total des unités gérées dans la section d'état. La section Synthèse indique le nombre réel d'unités gérées pour votre abonnement.

Si votre utilisation approche ou dépasse le montant souscrit, vous pouvez réduire l'utilisation en supprimant des 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 l'utilisation de votre unité gérée dépasse 80 %, 90 % et 100 % du montant total de votre abonnement :

Lorsque l'utilisation dépasse:	Ceci se produit / action recommandée:
80 %	Une bannière informative s'affiche. Aucune action n'est nécessaire.
90 %	Une bannière d'avertissement s'affiche. Vous pouvez augmenter le nombre d'unités gérées souscrites.
100 %	Une bannière d'erreur s'affiche jusqu'à ce que vous effectuez l'une des opérations suivantes : • Supprimez les collecteurs de données pour que votre utilisation de l'unité gérée soit égale ou inférieure au montant souscrit • Modifiez votre abonnement pour augmenter le nombre d'unités gérées souscrites

Inscrivez-vous directement et ignorez l'essai

Vous pouvez également vous abonner à Data Infrastructure Insights directement à partir du "Marketplace AWS", sans avoir à créer au préalable un environnement d'essai. Une fois votre abonnement terminé et votre environnement configuré, vous êtes immédiatement abonné.

Ajout d'un ID de droit

Si vous possédez un produit NetApp valide fourni avec Data Infrastructure Insights, vous pouvez ajouter ce numéro de série à votre abonnement Data Infrastructure Insights existant. Par exemple, si vous avez acheté NetApp Astra Control Center, le numéro de série de licence Astra Control Center peut être utilisé pour identifier l'abonnement dans Data Infrastructure Insights. Les informations sur l'infrastructure de données font référence à ceci : *ID de licence*.

Pour ajouter un ID de droit à votre abonnement à Data Infrastructure Insights, sur la page **Admin > abonnement**, cliquez sur *+ID de droit*.

Subscription Summary

NetApp Serial Number: 95001014387268156333
Active Edition: Premium
+ Entitlement ID

Usage and Entitlement

5,122 out of 18,000 Managed Units

0 18,000

Hosts: 1,388 Managed Units (2,776 Hosts)
Unformatted Capacity: 3,734 Managed Units (14,934 TB)

Subscription Details

36 Months (Premium Edition)
Expires: March 3rd, 2022

NetApp

Modify Subscription Estimate Cost

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 un grand nombre de widgets, chacun offrant une grande flexibilité d'affichage et de transcription de vos données.

Les exemples présentés dans ces sections sont fournis à des fins d'explication uniquement et ne couvrent pas tous les scénarios possibles. Les concepts et étapes dans ce document peuvent être utilisés pour créer vos propres tableaux de bord afin de mettre en évidence les données spécifiques à vos besoins spécifiques.

Création d'un tableau de bord

Vous créez un nouveau tableau de bord à deux endroits :

- **Tableaux de bord > [+Nouveau tableau de bord]**
- **Tableaux de bord > Afficher tous les tableaux de bord >** cliquez sur le bouton **[+Dashboard]**

Commandes du tableau de bord

L'écran Tableau de bord comporte plusieurs commandes :

- **Time Selector** : permet d'afficher les données du tableau de bord pendant une période 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 de temps 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.

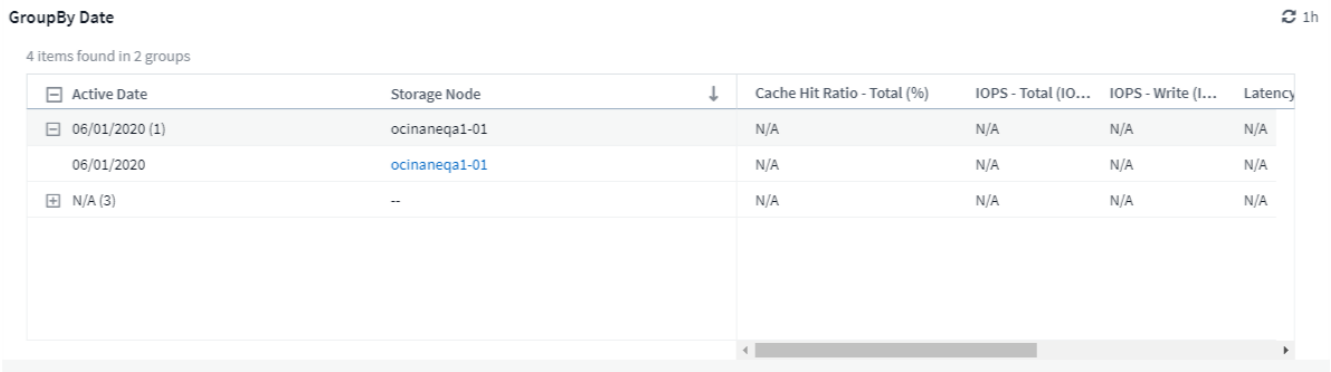
  Les widgets peuvent être redimensionnés et déplacés vers différentes positions dans le tableau de bord pour vous fournir une vue optimale de vos données selon vos besoins actuels.

- **+ bouton Ajouter une variable**, qui vous permet d'utiliser des variables pour filtrer activement les données du tableau de bord.

Types de widget

Vous pouvez choisir parmi les types de widget suivants :

- **Widget Table** : tableau affichant les données en fonction des filtres et des colonnes que vous choisissez. Les données de table peuvent être combinées dans des groupes qui peuvent être réduits et développés.



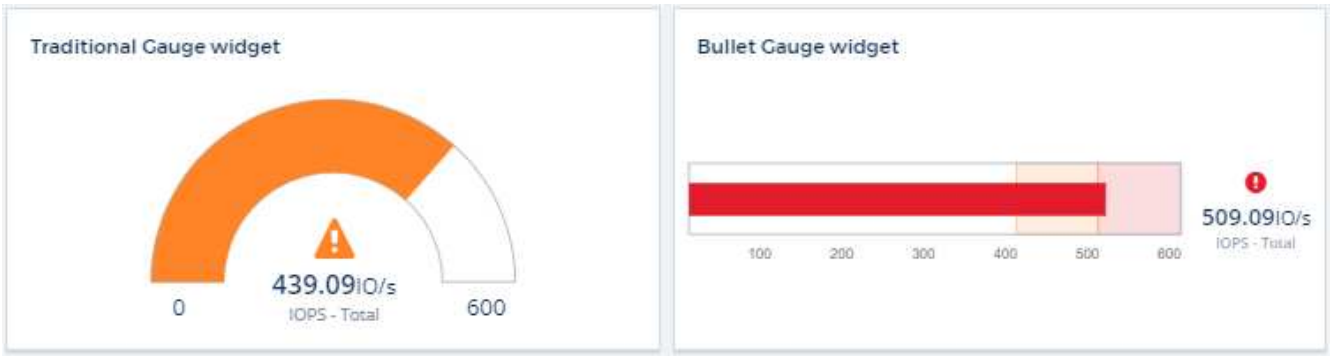
- **Graphiques ligne, Spline, surface, surface empilée** : il s'agit de widgets graphiques de séries chronologiques sur lesquels vous pouvez afficher les performances et d'autres données au fil du temps.



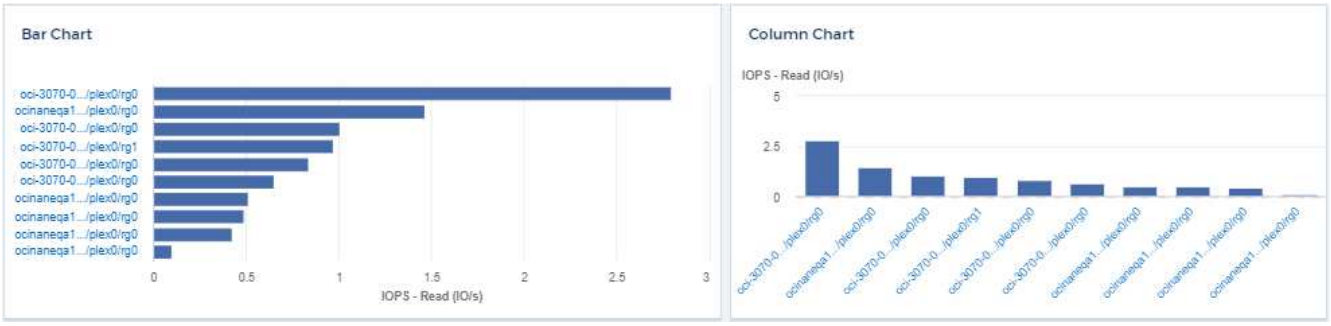
- **Widget valeur unique** : widget permettant d'afficher une valeur unique qui peut être dérivée directement d'un compteur ou calculée à l'aide d'une requête ou d'une expression. Vous pouvez définir des seuils de mise en forme des couleurs pour indiquer si la valeur est dans la plage attendue, avertissement ou critique.



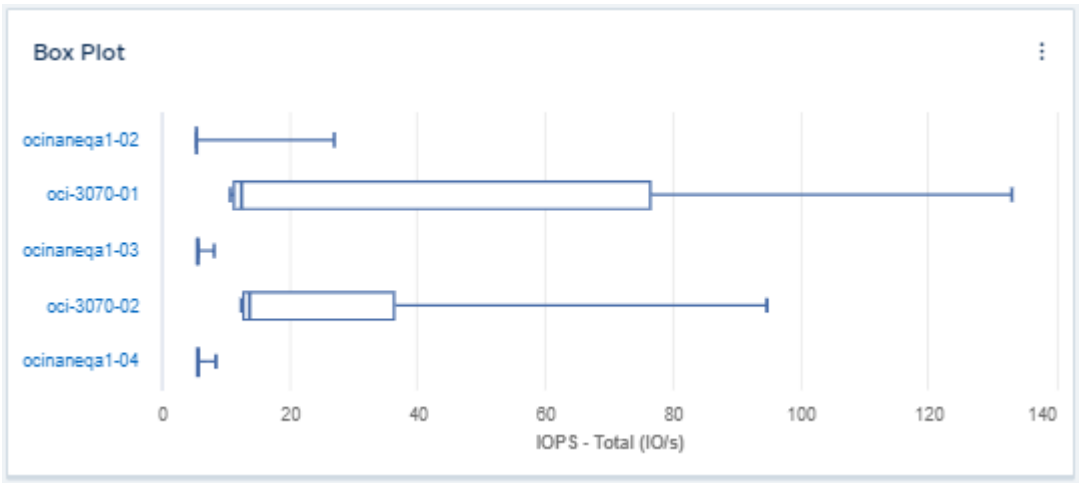
- **Widget jauge**: Affiche les données à valeur unique dans une jauge classique (solide) ou une jauge à puce, avec des couleurs basées sur les valeurs "Avertissement" ou "critique" vous "personnaliser".



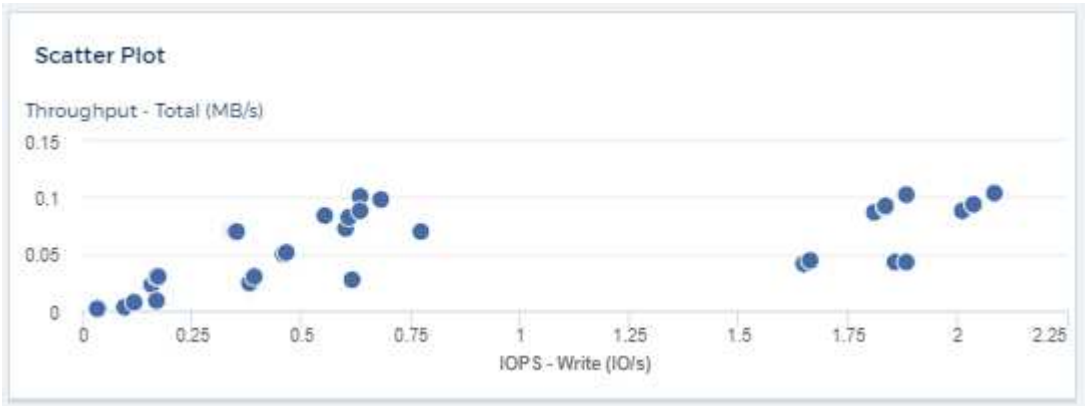
- **Bar, colonnes graphiques** : affiche les valeurs N supérieures ou inférieures, par exemple, les 10 premiers stockages par capacité ou les 5 volumes inférieurs par IOPS.



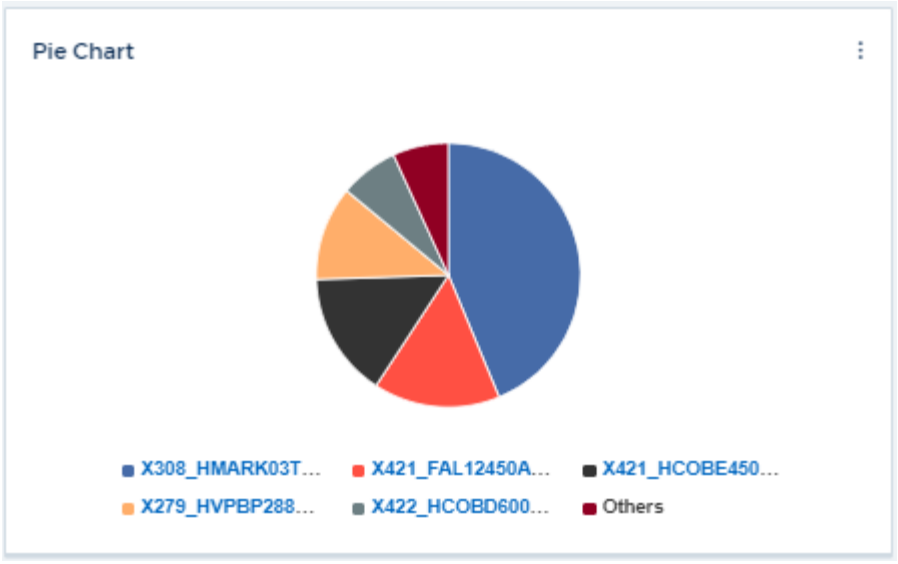
- **Diagramme de tracé de boîte** : tracé de la valeur minimale, maximale, médiane et de la plage entre le quartile inférieur et le quartile supérieur des données dans un seul graphique.



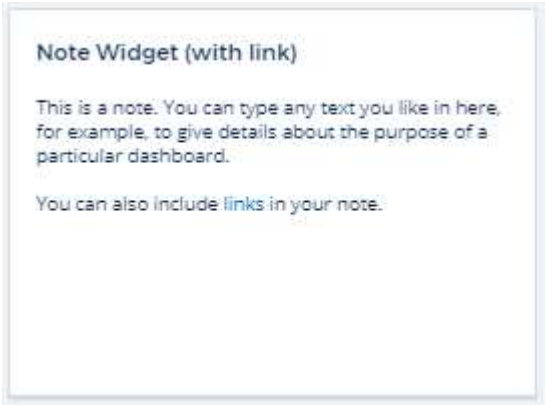
- **Diagramme de tracé Scatter** : trace les données associées en points, par exemple, les IOPS et la latence. Dans cet exemple, vous pouvez localiser rapidement des ressources bénéficiant d'un débit élevé et d'IOPS faibles.



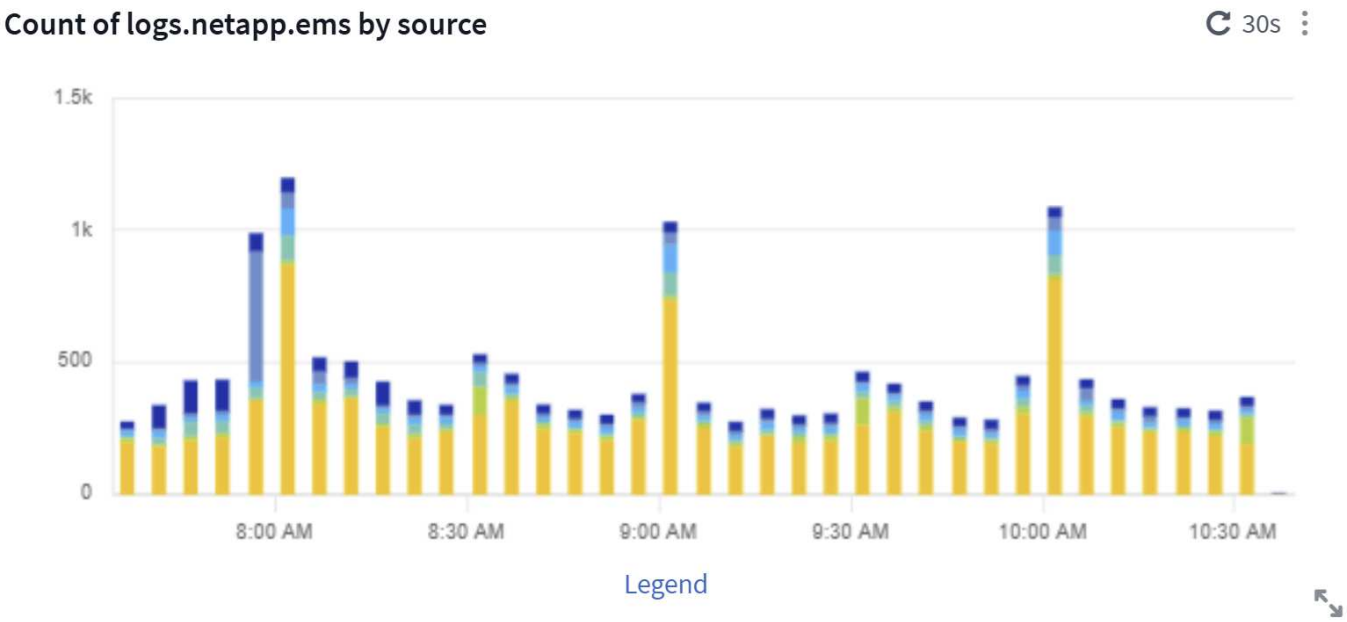
- **Pie Chart**: Un diagramme circulaire traditionnel pour afficher les données en tant que pièce du total.



- **Note widget** : jusqu'à 1000 caractères de texte libre.



- **Graphique à barres temporelles** : affiche les données de log ou de métrique dans le temps.



- **Tableau des alertes** : affiche jusqu'aux 1,000 dernières alertes.

Pour des explications plus détaillées sur ces fonctions et d'autres fonctions du tableau de bord, "cliquez ici".

Définition d'un tableau de bord comme page d'accueil

Vous pouvez choisir le tableau de bord à définir comme **page d'accueil** de votre locataire à l'aide de 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 dans la liste pour ouvrir le tableau de bord. Cliquez sur le menu déroulant dans le coin supérieur et sélectionnez **définir comme page d'accueil**.

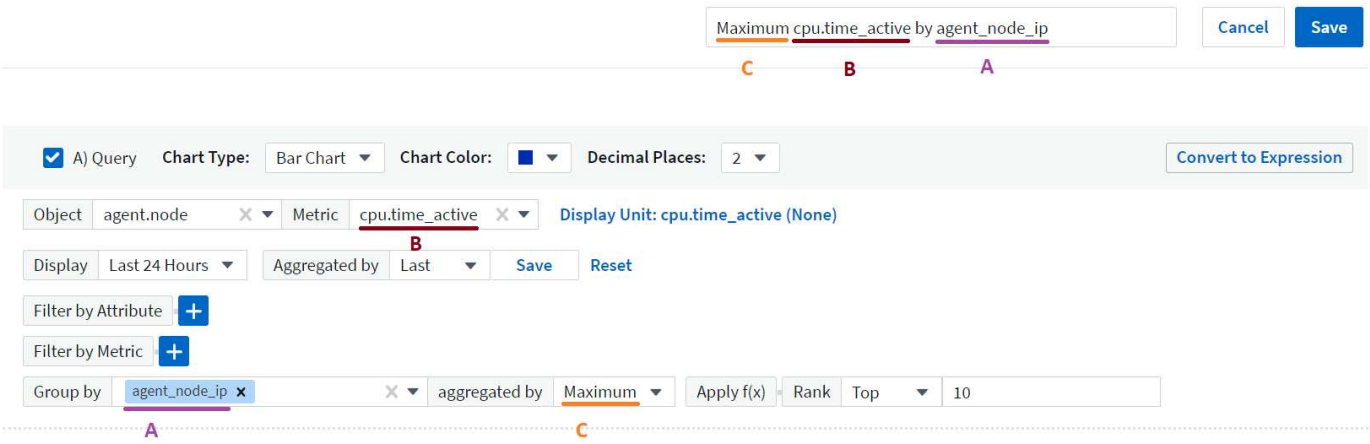
Fonctionnalités du tableau de bord

Les tableaux de bord et les widgets offrent une grande flexibilité dans le mode d'affichage des données. Voici quelques concepts qui vous aideront à tirer le meilleur parti de vos tableaux de bord personnalisés.

sommaire :[]

Dénomination des widgets

Les widgets sont automatiquement nommés en fonction de l'objet, de la mesure 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 entrer un nouveau nom.

Positionnement et taille des widgets

Tous les widgets de tableau de bord peuvent être positionnés et dimensionnés en fonction de vos besoins pour chaque tableau de bord spécifique.

Duplication d’un widget

En mode Tableau de bord, cliquez sur le menu du widget et sélectionnez **Dupliquer**. L’éditeur de widget est lancé, rempli avec la configuration du widget original 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 au bas de votre tableau de bord et vous pouvez le positionner selon les besoins. N’oubliez pas d’enregistrer votre tableau de bord lorsque toutes les modifications sont terminées.

Affichage des légendes du widget

La plupart des widgets des tableaux de bord peuvent être affichés avec ou sans légendes. Les légendes des widgets peuvent être activées ou désactivées sur un tableau de bord à l’aide de l’une des méthodes suivantes :

- Lorsque vous affichez le tableau de bord, cliquez sur le bouton **Options** du widget et sélectionnez **Afficher légendes** dans le menu.

Au fur et à mesure que les données affichées dans le widget changent, la légende de ce widget est mise à jour dynamiquement.

Lorsque des légendes sont affichées, si la page d’accueil de la ressource indiquée par la légende peut être navigué vers, la légende s’affiche sous forme de lien vers cette page de ressources. Si la légende affiche « tous », cliquer sur le lien pour afficher une page de requête correspondant à la première requête dans le widget.

Transformation des mesures

Data Infrastructure Insights fournit différentes options de **transformation** pour certaines mesures dans des widgets (en particulier, les metrics appelés « personnalisés » ou les metrics d’intégration, telles que Kubernetes, les données avancées ONTAP, les plug-ins Telegraf, etc.), ce qui vous permet d’afficher les données de différentes manières. Lorsque vous ajoutez des mesures transformables à un widget, une liste déroulante vous propose les options de transformation suivantes :

Aucune : les données sont affichées telles qu’elles sont, sans manipulation.

Taux : valeur actuelle divisée par la plage horaire depuis l’observation précédente.

Cumulatif : accumulation de la somme des valeurs précédentes et de la valeur actuelle.

Delta : différence entre la valeur d’observation précédente et la valeur actuelle.

Delta rate : valeur Delta divisée par la plage de temps depuis l’observation précédente.

Taux cumulatif : valeur cumulée divisée par la plage horaire depuis l’observation précédente.

Notez que la transformation des mesures ne modifie pas les données sous-jacentes, mais uniquement la façon dont elles sont affichées.

Requêtes et filtres du widget du tableau de bord

Requêtes

La requête dans un widget de tableau de bord est un outil puissant de gestion de l’affichage de vos données. Voici quelques points à noter sur les requêtes de widget.

Certains widgets peuvent avoir jusqu'à cinq requêtes. Chaque requête trace son propre ensemble de lignes ou de graphiques dans le widget. La configuration de l'agrégation, du regroupement, des résultats supérieurs/inférieurs, etc. Sur une requête n'affecte pas les autres requêtes du widget.

Vous pouvez cliquer sur l'icône œil pour masquer temporairement une requête. L'affichage du widget est automatiquement mis à jour lorsque vous masquez ou affichez une requête. Cela vous permet de vérifier les données affichées pour les requêtes individuelles au fur et à mesure de la création de votre widget.

Les types de widget suivants peuvent avoir plusieurs requêtes :

- Graphique de zone
- Graphique de zone empilée
- Graphique en courbes
- Graphique de spline
- Widget à valeur unique

Les types de widget restants ne peuvent avoir qu'une seule requête :

- Tableau
- Graphique à barres
- Tracé de zone
- Tracé de dispersion

Filtrage dans les requêtes widget du tableau de bord

Voici quelques choses que vous pouvez faire pour tirer le meilleur parti de vos filtres.

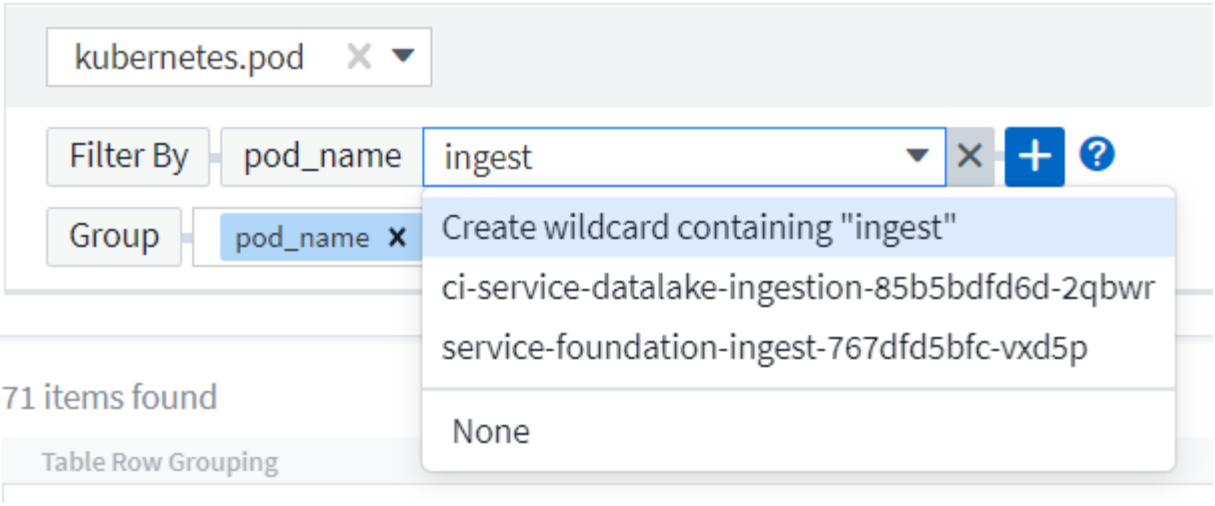
Filtrage de correspondance exacte

Si vous placez une chaîne de filtre entre deux guillemets, Insight traite tout entre le premier et le dernier devis comme une correspondance exacte. Tous les caractères spéciaux ou opérateurs situés dans les guillemets seront traités comme des littéraux. Par exemple, le filtrage pour **"*"** renvoie des résultats qui sont un astérisque littéral ; l'astérisque ne sera pas traité comme un caractère générique dans ce cas. Les opérateurs ET, OU, et NON SERONT également traités comme des chaînes littérales lorsqu'ils sont entourés de guillemets doubles.

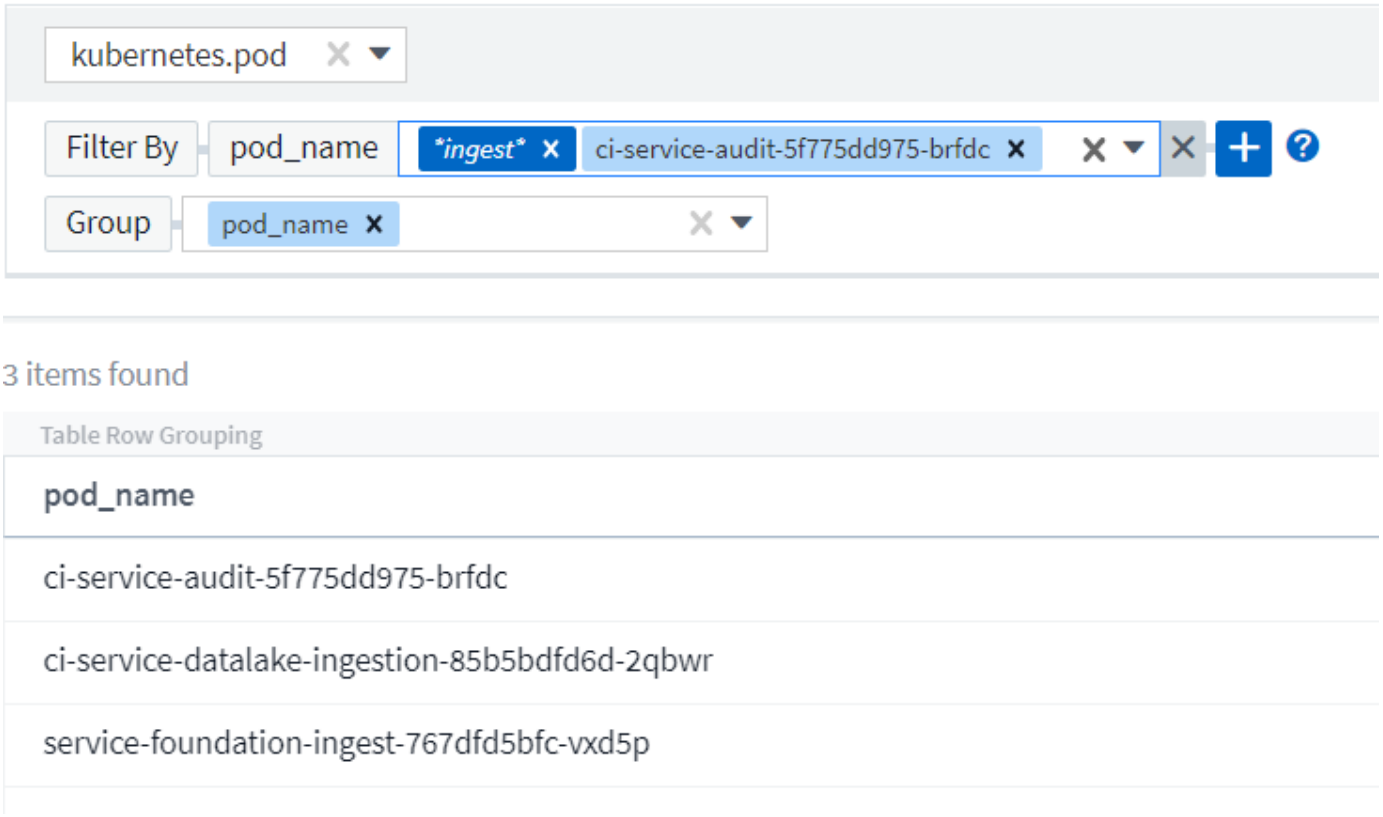
Vous pouvez utiliser des filtres de correspondance exacte pour trouver des ressources spécifiques, par exemple nom d'hôte. Si vous voulez trouver uniquement le nom d'hôte « marketing » mais exclure « marketing01 », « marketing-boston », etc., il suffit de placer le nom « marketing » dans des guillemets doubles.

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 taper, vous avez la possibilité de créer un **filtre générique** basé sur le texte en cours. Si vous sélectionnez cette option, tous les résultats correspondant à l'expression de caractère générique seront résélectionnés. Vous pouvez également créer **expressions** à l'aide DE NOT ou OU, ou sélectionner l'option "aucun" pour filtrer les valeurs nulles dans le champ.



Filtres basés sur des caractères génériques ou des expressions (par exemple NON, OU « aucun », etc.) s'affiche en bleu foncé dans le champ du filtre. Les éléments que vous sélectionnez directement dans la liste s'affichent en bleu clair.



Notez que le filtrage des caractères génériques et des expressions fonctionne avec du texte ou des listes, mais pas avec des valeurs numériques, des dates ou des valeurs booléennes.

Filtrage avancé du texte avec des suggestions contextuelles de type avance

Le filtrage dans les requêtes de widget est *Contextual* ; lorsque vous sélectionnez une valeur de filtre ou des valeurs pour un champ, les autres filtres pour cette requête affichent les valeurs pertinentes pour ce filtre. Par exemple, lors de la définition d'un filtre pour un objet spécifique *Name*, le champ à filtrer pour *Model* affiche uniquement les valeurs pertinentes pour ce nom d'objet.

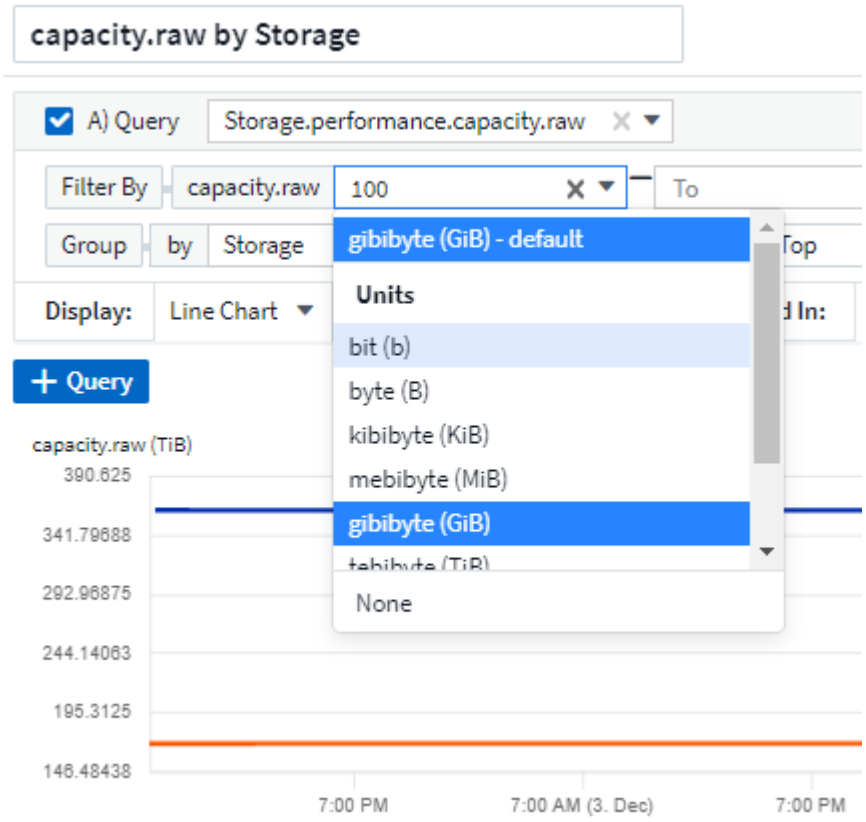
Le filtrage contextuel s'applique également aux variables de page du tableau de bord (attributs de type texte ou annotations uniquement). Lorsque vous sélectionnez une valeur de fichier pour une variable, toutes les autres variables utilisant des objets associés n'afficheront que les valeurs de filtre possibles en fonction du contexte de ces variables associées.

Notez que seuls les filtres de texte affichent des suggestions contextuelles de type à l'avance. La date, Enum (liste), etc. N'affichera pas de suggestions de type à l'avance. Cela dit, vous pouvez *CAN* définir un filtre dans un champ Enum (c.-à-d. liste) et avoir d'autres champs de texte à filtrer dans le contexte. Par exemple, la sélection d'une valeur dans un champ Enum comme Data Center, les autres filtres n'affichent que les modèles/noms dans ce centre de données), mais pas l'inverse.

La plage de temps sélectionnée fournit également un contexte pour les données affichées dans les filtres.

Choix des unités de filtre

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 la capacité brute et choisir d'afficher dans le Gio par défaut, ou sélectionner un autre format tel que Tio. Ceci est utile si vous disposez d'un certain nombre de graphiques sur votre tableau de bord affichant les valeurs en Tio et que vous souhaitez que tous vos graphiques affichent des valeurs cohérentes.



Améliorations supplémentaires du filtrage

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 commençant par "vol" et se terminant par "rhel".

- Le point d'interrogation permet de rechercher un nombre spécifique de caractères. Par exemple :

```
BOS-PRD??-S12
```

Affiche *BOS-PRD12-S12*, *BOS-PRD13-S12*, etc.

- L'opérateur OU vous permet de spécifier plusieurs entités. Par exemple :

```
FAS2240 OR CX600 OR FAS3270
```

identification des nombreux modèles de stockage

- L'opérateur NOT permet d'exclure du texte des résultats de la recherche. Par exemple :

```
NOT EMC*
```

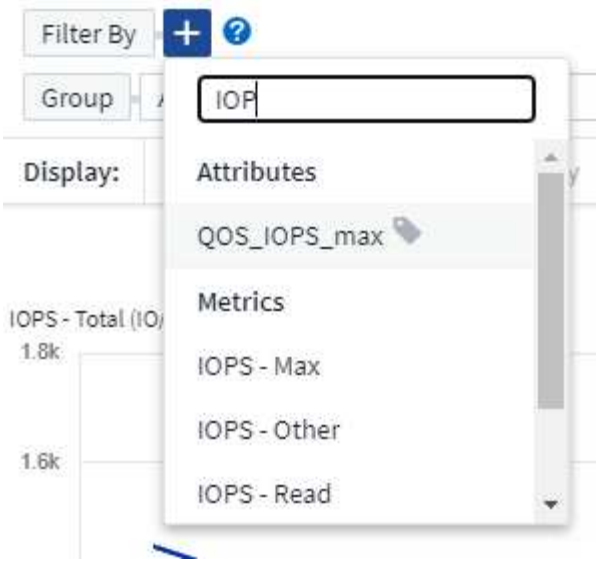
Trouve tout ce qui ne commence pas par « EMC ». Vous pouvez utiliser

```
NOT *
```

pour afficher les champs ne contenant aucune valeur.

Identification des objets renvoyés par des requêtes et des filtres

Les objets renvoyés par des requêtes et des filtres ressemblent à ceux affichés dans l'illustration suivante. Les objets avec des « balises » qui leur sont attribués sont des annotations, tandis que les objets sans balises sont des compteurs de performance ou des attributs d'objet.



Regroupement et agrégation

Regroupement (reprise)

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 avez un widget graphique en lignes qui affiche les IOPS de stockage au fil du temps, il est possible que vous souhaitiez afficher une ligne distincte pour chacun de vos data centers, afin d'obtenir une comparaison rapide. Vous pouvez choisir de regrouper ces données de différentes manières :

- **Moyenne** : affiche chaque ligne comme la *moyenne* des données sous-jacentes.
- **Maximum** : affiche chaque ligne sous la forme *maximum* des données sous-jacentes.
- **Minimum** : affiche chaque ligne comme le *minimum* des données sous-jacentes.
- **Somme** : affiche chaque ligne sous la forme *sum* des données sous-jacentes.
- **Count** : affiche un *count* d'objets qui ont des données déclarées dans la période spécifiée. Vous pouvez choisir la *fenêtre de temps entière* déterminée par la plage de temps du tableau de bord.

Étapes

Pour définir la méthode de regroupement, procédez comme suit.

1. Dans la requête de votre widget, choisissez un type et une mesure de ressource (par exemple *Storage*) et une mesure (par exemple *Performance IOPS Total*).
2. Pour **Groupe**, choisissez une méthode de synthèse (comme *Average*) et sélectionnez les attributs ou les métriques par lesquels vous souhaitez synthétiser les données (par exemple *Data Center*).

   Le widget se met automatiquement à jour et affiche les données de chacun de vos data centers.

Vous pouvez également choisir de regrouper *tous* des données sous-jacentes dans le graphique ou la table. Dans ce cas, vous obtenez une ligne unique pour chaque requête dans le widget, qui affiche la moyenne, min, max, somme ou nombre de la ou des mesures choisies pour toutes les ressources sous-jacentes.

Si vous cliquez sur la légende d'un widget dont les données sont regroupées par "All", une page de requête affiche 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.

Notez que lorsque vous choisissez de regrouper un widget par n'importe quel champ (par exemple, *Model*), vous devrez toujours filtrer par ce champ pour afficher correctement les données de ce champ sur le graphique ou la table.

Agrégation des données

Vous pouvez aligner davantage vos graphiques de séries chronologiques (ligne, zone, etc.) en regroupant les points de données en compartiments minute, heure ou jour avant que ces données ne soient ensuite regroupées par attribut (si vous le souhaitez). Vous pouvez choisir d'agréger des points de données en fonction de leur *moyenne, maximum, minimum, somme* ou *Count*.

Un petit intervalle combiné à une longue plage de temps peut entraîner un avertissement « l'intervalle d'agrégation a entraîné un nombre trop important de points de données. » Vous pouvez le voir si vous avez un petit intervalle et augmenter la durée du tableau de bord à 7 jours. Dans ce cas, Insight augmente temporairement l'intervalle d'agrégation jusqu'à ce que vous sélectionniez une période plus petite.

Vous pouvez également agréger les données dans le widget de graphique à barres et à valeur unique.

La plupart des compteurs d'actifs sont agrégés à *moyenne* par défaut. Certains compteurs sont agrégés par défaut à *Max, min* ou *sum*. Par exemple, les erreurs de port sont agrégées à *sum* par défaut, où Storage IOPS Aggregate to *moyenne*.

Affichage des résultats supérieurs/inférieurs

Dans un widget graphique, vous pouvez afficher les résultats **Haut** ou **Bas** pour les données cumulées et choisir le nombre de résultats affiché dans la liste déroulante. Dans un widget de tableau, vous pouvez trier par colonne.

Haut/bas du widget graphique

Dans un widget graphique, lorsque vous choisissez de regrouper des données par un attribut spécifique, vous avez la possibilité d'afficher les résultats N du haut ou N du bas. Notez que vous ne pouvez pas choisir les résultats supérieurs ou inférieurs lorsque vous choisissez de faire un cumul par attributs *All*.

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 tableau, vous pouvez sélectionner le nombre de résultats affichés dans le tableau des résultats. Vous n'avez pas la possibilité de choisir les résultats supérieurs ou inférieurs car le tableau vous permet de trier les résultats par ordre croissant ou décroissant en fonction d'une colonne à la demande.

Vous pouvez choisir le nombre de résultats à afficher dans la table du tableau de bord en sélectionnant une valeur dans le champ **Afficher les entrées** de la requête.

Regroupement dans un widget de tableau

Les données d'un widget de tableau peuvent être regroupées par n'importe quel attribut disponible, ce qui vous permet d'afficher une vue d'ensemble de vos données et d'en explorer les données pour plus de détails. Les mesures de la table sont rassemblées pour faciliter l'affichage dans chaque ligne réduite.

Les widgets de tableau vous permettent de regrouper vos données en fonction des attributs que vous avez

définis. Par exemple, votre tableau peut afficher les IOPS de stockage totales regroupées en fonction des data centers dans lesquels ces stockages sont actifs. Vous pouvez également afficher un tableau des machines virtuelles regroupées en fonction de l'hyperviseur qui les héberge. Dans la liste, vous pouvez développer chaque groupe pour afficher les ressources de ce groupe.

Le regroupement n'est disponible que dans le type de widget Table.

Exemple de regroupement (avec cumul expliqué)

Les widgets de tableau vous permettent de regrouper les données pour faciliter leur affichage.

Dans cet exemple, nous allons créer un widget de tableau répertoriant toutes les machines virtuelles regroupées par Data Center.

Étapes

1. Créez ou ouvrez un tableau de bord et ajoutez un widget **Table**.
2. Sélectionnez *Virtual machine* comme type d'actif pour ce widget.
3. Cliquez sur le sélecteur de colonne et choisissez *Hypervisor name* et *IOPS - Total*.

   Ces colonnes sont maintenant affichées dans le tableau.

4. Ignorez toutes les machines virtuelles sans IOPS et incluez uniquement les machines virtuelles pour lesquelles les IOPS totales sont supérieures à 1. Cliquez sur le bouton **Filter by [+]** et sélectionnez *IOPS - Total*. Cliquez sur *any*, et dans le champ **de**, saisissez **1**. Laissez le champ **à** vide. Appuyez sur entrer sans cliquer sur le champ de filtre pour appliquer le filtre.

   Le tableau indique désormais toutes les machines virtuelles dont le nombre total d'IOPS est supérieur ou égal à 1. Notez qu'il n'y a pas de regroupement dans la table. Toutes les VM sont affichées.

5. Cliquez sur le bouton **Grouper par [+]**.

   Vous pouvez grouper par n'importe quel attribut ou annotation affiché. Choisissez *All* pour afficher toutes les machines virtuelles d'un même groupe.

   Tout en-tête de colonne pour une mesure de performance affiche un menu "trois points" contenant une option **Roll up**. La méthode par défaut est *Average*. Cela signifie que le nombre indiqué pour le groupe correspond à la moyenne de toutes les IOPS totales indiquées pour chaque machine virtuelle du groupe. Vous pouvez choisir de faire rouler cette colonne vers le haut par *moyenne, somme, minimum* ou *maximum*. Toutes les colonnes qui contiennent des mesures de performance peuvent être synthétisés individuellement.



6. Cliquez sur *All* et sélectionnez *Hypervisor name*.

   La liste des machines virtuelles est désormais groupée par hyperviseur. Vous pouvez développer chaque hyperviseur pour afficher les VM hébergées par celui-ci.

7. Cliquez sur **Enregistrer** pour enregistrer la table 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 synthèse pour cette colonne. La méthode de défilement par défaut consiste à afficher la moyenne (*avg*) des données sous-jacentes de la ligne du 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 des données de votre tableau de bord. Seules les données relatives à la plage horaire sélectionnée s'affichent dans les widgets du tableau de bord. Vous pouvez sélectionner l'une des plages de temps suivantes :

- Dernières 15 minutes
- Dernières 30 minutes
- Dernières 60 minutes
- Dernières 2 heures
- Les 3 dernières heures (il s'agit de la valeur par défaut)
- Dernières 6 heures
- Dernières 12 heures
- Dernières 24 heures

- 2 derniers jours
- 3 derniers jours
- 7 derniers jours
- 30 derniers jours
- Plage horaire personnalisée

  La plage de temps 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 12:00 AM le premier jour sélectionné et l'heure de fin par défaut est 11:59 PM le dernier jour sélectionné. Cliquez sur **appliquer** pour appliquer la plage de temps personnalisée au tableau de bord.

Zoom avant sur une plage de temps

Lors de l'affichage d'un widget de séries chronologiques (ligne, spline, zone, zone empilée)--ou d'un graphique sur une page d'accueil—vous pouvez faire glisser la souris sur le graphique pour effectuer un zoom avant. Dans le coin supérieur droit de l'écran, vous pouvez verrouiller cette plage de temps pour que les graphiques des autres pages reflètent les données de cette plage de temps verrouillée. Pour déverrouiller, sélectionnez une plage horaire différente dans la liste.

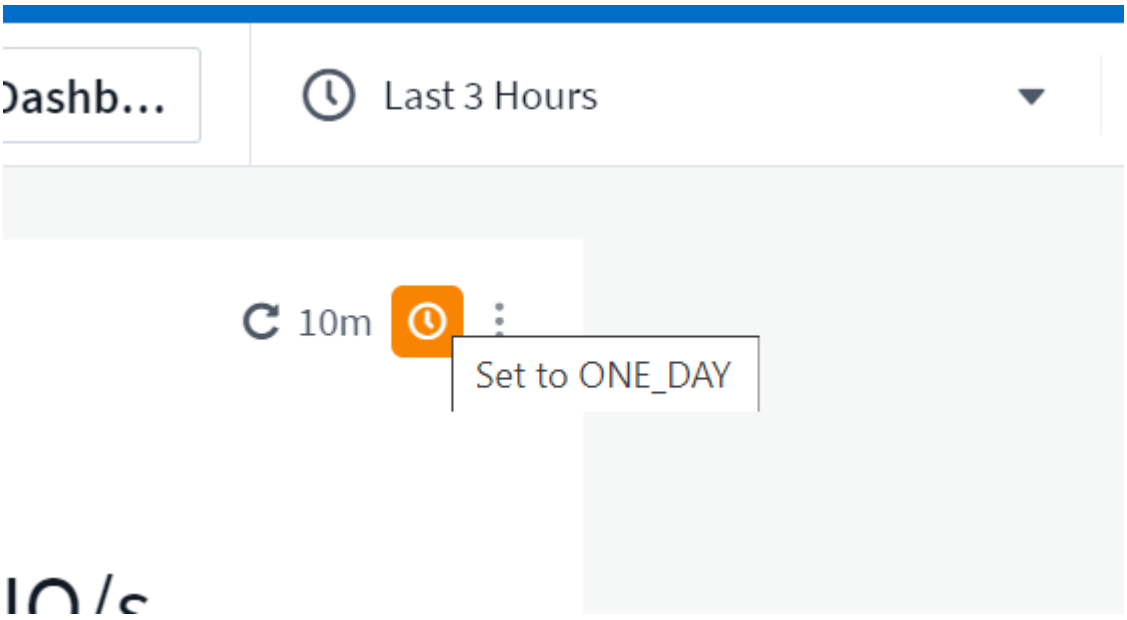
Remplacement de l'heure du tableau de bord dans des widgets individuels

Vous pouvez remplacer le paramètre de plage horaire principal du tableau de bord dans des widgets individuels. Ces widgets affichent des données en fonction de leur période définie, et non pas de l'heure du tableau de bord.

Pour annuler 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 dérisée et enregistrez le widget dans le tableau de bord.

Le widget affichera ses données en fonction de la période définie, indépendamment du délai sélectionné sur le tableau de bord lui-même.

La période que vous définissez pour un widget n'affectera pas les autres widgets du tableau de bord.



Axes principal et secondaire

Les différentes mesures utilisent différentes unités de mesure pour les données qu'elles indiquent dans un graphique. Par exemple, dans le cas des IOPS, l'unité de mesure correspond au nombre d'opérations d'E/S par seconde de temps (E/S), tandis que la latence mesure uniquement le temps (millisecondes, microsecondes, secondes, etc.). Lors de la transcription des deux mesures sur un graphique à ligne unique à l'aide d'un ensemble unique de valeurs a pour l'axe y, les nombres de latence (en général quelques millisecondes) sont transcrits sur la même échelle avec les IOPS (généralement la numérotation des milliers) et la ligne de latence est perdue à cette échelle.

Mais il est possible de tracer les deux ensembles de données sur un seul graphique significatif, en définissant 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 saisie à sa propre échelle.

Étapes

Cet exemple illustre le concept des axes principal et secondaire dans un widget graphique.

1. Créez ou ouvrez un tableau de bord. Ajoutez un graphique linéaire, un graphique spline, un graphique de zone ou un widget de graphique à zone empilée au tableau de bord.
2. Sélectionnez un type de ressource (par exemple *Storage*) et choisissez *IOPS - Total* pour votre première mesure. Définissez les filtres que vous souhaitez et choisissez une méthode de déploiement si vous le souhaitez.

   La ligne IOPS s'affiche sur le tableau, avec son échelle affichée à gauche.

3. Cliquez sur **[+Query]** pour ajouter une seconde ligne au graphique. Pour cette ligne, choisissez *latence - Total* pour la mesure.

   Notez que la ligne est affichée à plat en bas du graphique. C'est parce qu'elle est *à la même échelle* que la ligne IOPS.

4. Dans la requête latence, sélectionnez **axe y : secondaire**.

   La ligne latence est maintenant tracée à sa propre échelle, qui est affichée à droite du graphique.



Expressions dans les widgets

Dans un tableau de bord, n'importe quel widget de séries chronologiques (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 du widget de tableau). Les exemples suivants utilisent des expressions pour résoudre des problèmes spécifiques. Dans le premier exemple, nous souhaitons afficher les IOPS en lecture sous forme de pourcentage des IOPS totales pour toutes les ressources de stockage de votre locataire. Le deuxième exemple offre une visibilité sur les IOPS système ou indirectes qui se produisent sur votre locataire, à savoir les IOPS qui ne sont pas directement lues ou écrites les données.

Vous pouvez utiliser des variables dans des expressions (par exemple, *$Var1 * 100*)

Expressions exemple : pourcentage d'IOPS en lecture

Dans cet exemple, nous allons afficher les IOPS en lecture sous forme de pourcentage du nombre total d'IOPS. Vous pouvez considérer ceci comme la formule suivante :

```
 Read Percentage = (Read IOPS / Total IOPS) x 100
Ces données peuvent s'afficher dans un graphique en courbes sur votre
tableau de bord. Pour ce faire, procédez comme suit :
```

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 **diagramme de zone**.

   Le widget s'ouvre en mode édition. Par défaut, une requête est affichée avec *IOPS - Total* pour *Storage* Assets. Si vous le souhaitez, sélectionnez un autre type d'actif.

3. Cliquez sur le lien **convertir en expression** à droite.

   La requête en cours est convertie en mode expression. Vous ne pouvez pas modifier le type de ressource en mode expression. Lorsque vous êtes en mode expression, le lien devient **revenir à requête**. Cliquez sur ce bouton si vous souhaitez revenir au mode requête à tout moment. N'oubliez pas que le passage d'un mode à l'autre réinitialise les champs à leur valeur par défaut.

   Pour l'instant, restez en mode expression.

4. La mesure **IOPS - Total** se trouve maintenant dans le champ de variable alphabétique "**a**". Dans le champ variable "**b**", cliquez sur **Select** et choisissez **IOPS - lecture**.

   Vous pouvez ajouter jusqu'à cinq variables alphabétiques pour votre expression en cliquant sur le bouton + en suivant les champs des variables. Pour notre exemple de pourcentage de lecture, nous n'avons besoin que des IOPS totales ("**a**") et des IOPS de lecture ("**b**").

5. Dans le champ **expression**, vous utilisez les lettres correspondant à chaque variable pour créer votre expression. Nous savons que Read Percentage = (Read IOPS / Total IOPS) x 100, nous écrivons cette expression comme suit :

   ```
    (b / a) * 100
   . Le champ *Label* identifie l'expression. Remplacez l'étiquette par «
   pourcentage de lecture », ou quelque chose de tout aussi significatif
   pour vous.
   . Définissez le champ *unités* sur " %" ou sur "pourcentage".
   ```

Le graphique affiche le pourcentage de lecture des IOPS dans le temps pour les périphériques de stockage sélectionnés. Si vous le souhaitez, vous pouvez définir un filtre ou choisir une autre méthode d'agrégation. Sachez que si vous sélectionnez somme comme méthode de cumul, toutes les valeurs de pourcentage sont ajoutées ensemble, qui peuvent être supérieures à 100 %.

6. Cliquez sur **Enregistrer** pour enregistrer le graphique dans votre tableau de bord.

Expressions exemple : E/S « système »

Exemple 2 : parmi les mesures collectées à partir des sources de données sont la lecture, l'écriture et le nombre total d'IOPS. Toutefois, le nombre total d'IOPS indiqué par une source de données inclut parfois des IOPS « système », ce qui ne fait pas partie directement des opérations de lecture ou d'écriture des données. Ces E/S du système peuvent également être considérées comme des E/S « surcharges » qui sont nécessaires au bon fonctionnement du système, mais pas directement liées aux opérations de données.

Pour afficher ces E/S système, vous pouvez limiter le nombre d'IOPS de lecture et d'écriture du total indiqué lors de l'acquisition. La formule peut ressembler à ceci :

```
 System IOPS = Total IOPS - (Read IOPS + Write IOPS)
Ces données peuvent ensuite être affichées dans un graphique en courbes
sur votre tableau de bord. Pour ce faire, procédez comme suit :
```

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 de lignes**.

   Le widget s'ouvre en mode édition. Par défaut, une requête est affichée avec *IOPS - Total* pour *Storage* Assets. Si vous le souhaitez, sélectionnez un autre type d'actif.

3. Dans le champ **cumul**, choisissez *sum* by *All*.

   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.

   Une copie de la requête est ajoutée sous l'original.

5. Dans la deuxième requête, cliquez sur le bouton **convertir en expression**.

   La requête en cours est convertie en mode expression. Cliquez sur **revenir à la requête** si vous souhaitez revenir au mode requête à tout moment. N'oubliez pas que le passage d'un mode à l'autre réinitialise les champs à leur valeur par défaut.

   Pour l'instant, restez en mode expression.

6. La mesure *IOPS - Total* se trouve maintenant dans le champ de variable alphabétique "**a**". Cliquez sur *IOPS - Total* et remplacez-le par *IOPS - Read*.
7. Dans le champ variable "**b**", cliquez sur **Select** et choisissez *IOPS - Write*.
8. Dans le champ **expression**, vous utilisez les lettres correspondant à chaque variable pour créer votre expression. Nous écrivons notre expression simplement comme :

```
a + b
```

Dans la section Affichage, choisissez **diagramme de zone** pour cette expression.

9. Le champ **Label** identifie l'expression. Remplacez ce label par « IOPS système », ou quelque chose de tout aussi utile pour vous.

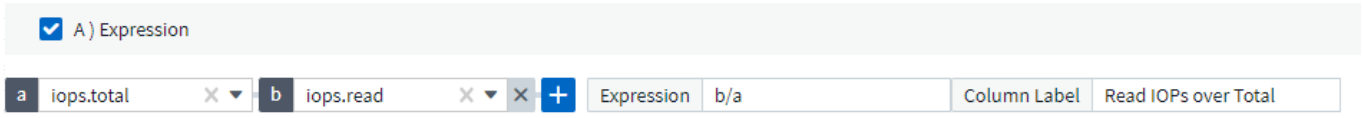
   Le graphique affiche le nombre total d'IOPS sous forme de graphique linéaire et un graphique de superficie illustrant la combinaison d'opérations d'E/S par seconde en lecture et en écriture ci-dessous. La différence entre les deux montre les IOPS qui ne sont pas directement liées aux opérations de lecture ou d'écriture de données. Il s'agit de vos IOPS de système.

10. Cliquez sur **Enregistrer** pour enregistrer le graphique dans votre tableau de bord.

Pour utiliser une variable dans une expression, tapez 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 traitent les expressions un peu différemment. Vous pouvez avoir jusqu'à cinq expressions dans un widget de table unique, chacune étant ajoutée en tant que nouvelle colonne à la table. Chaque expression peut inclure jusqu'à cinq valeurs sur lesquelles effectuer son calcul. Vous pouvez facilement nommer la colonne quelque chose de significatif.



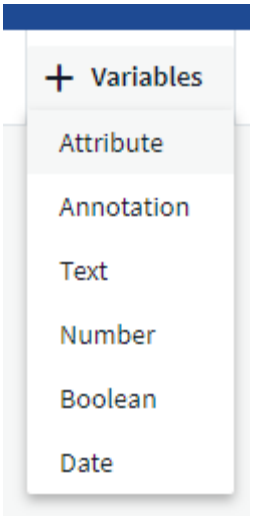
Variables

Les variables vous permettent de modifier simultanément les données affichées dans certains ou tous les widgets d'un tableau de bord. En définissant un ou plusieurs widgets pour utiliser une variable commune, les modifications effectuées à un endroit provoquent la mise à jour automatique des données affichées dans chaque widget.

Types de variables

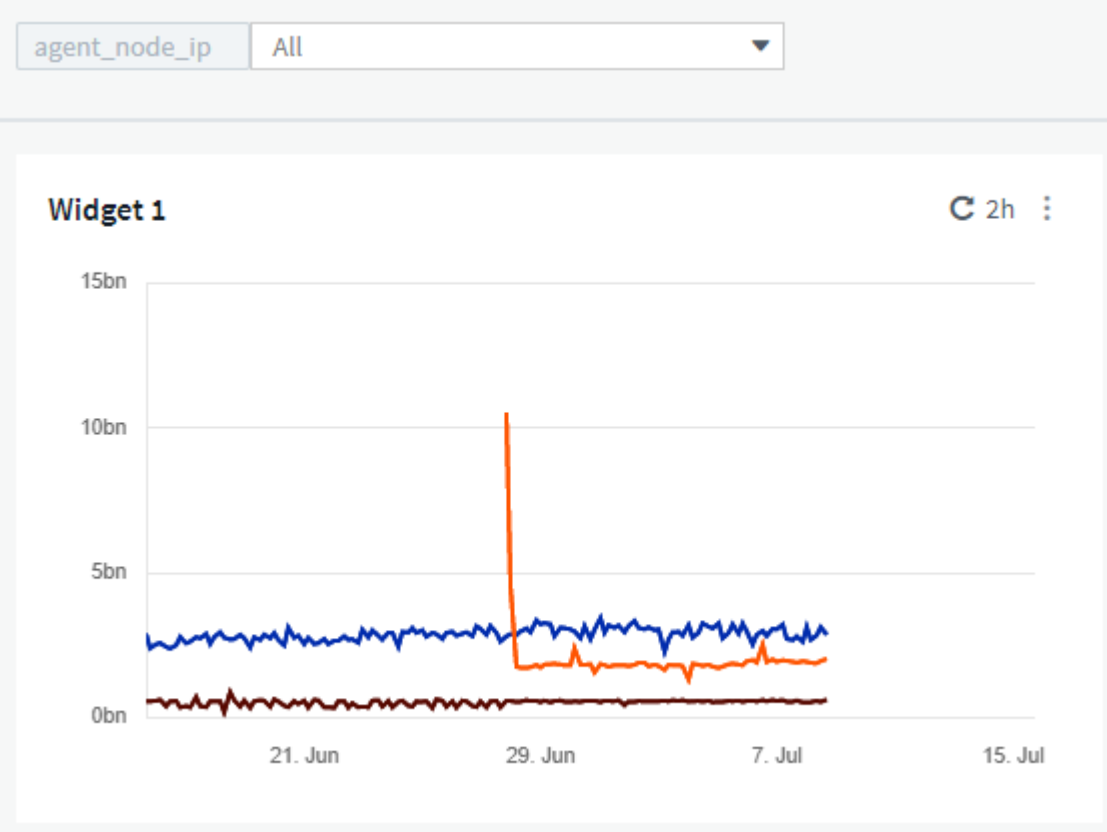
Une variable peut être de l'un des types suivants :

- **Attribut** : utilisez les attributs ou les métriques d'un objet pour filtrer
- **Annotation** : utilisez un pré-défini "Annotation" pour filtrer les données du widget.
- **Texte** : une chaîne alphanumérique.
- **Numérique** : une valeur numérique. Utiliser par lui-même, ou comme valeur « de » ou « à », en fonction de votre champ de widget.
- **Boolean** : utiliser pour les champs avec les valeurs vrai/Faux, Oui/non, etc. Pour la variable booléenne, les choix sont Oui, non, aucun, n'importe.
- **Date** : une valeur de date. Utiliser comme valeur « de » ou « à », en fonction de la configuration de votre widget.

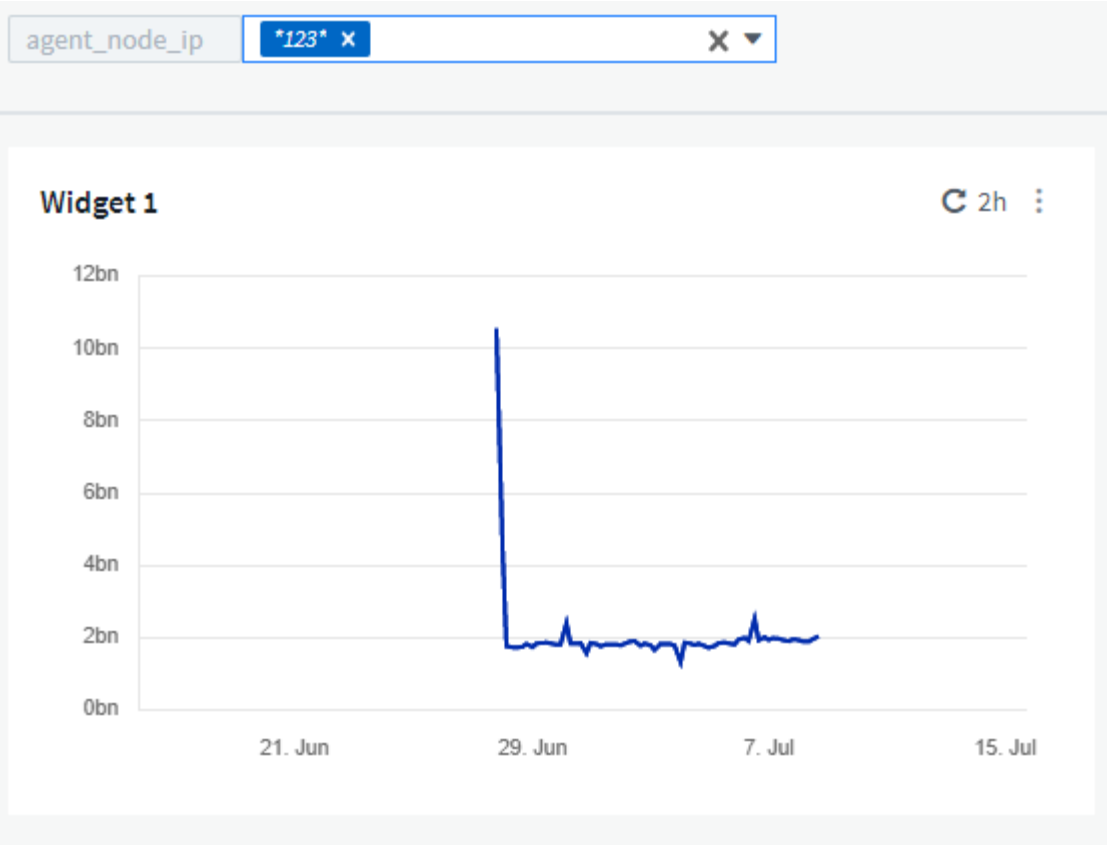


Variables d'attribut

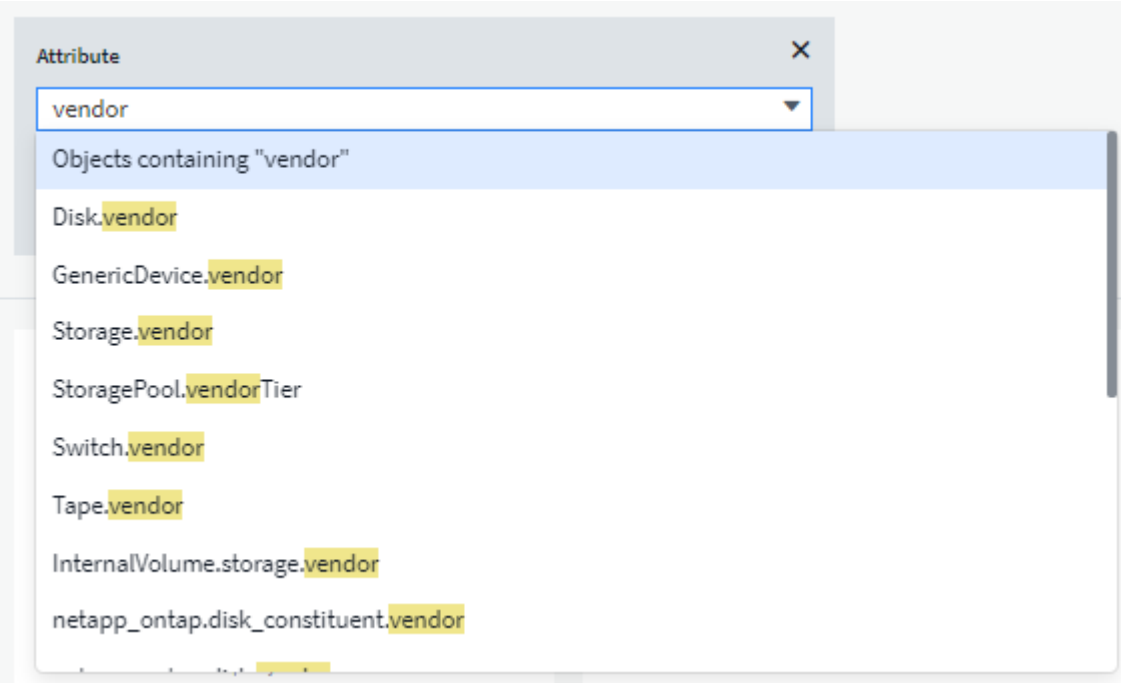
La sélection d'une variable de type d'attribut permet de filtrer les données de widget contenant la ou les valeurs d'attribut spécifiées. L'exemple ci-dessous montre un widget de ligne affichant les tendances de mémoire libre pour les nœuds Agent. Nous avons créé une variable pour les adresses IP de nœud d'agent, actuellement définie pour afficher toutes les adresses IP :



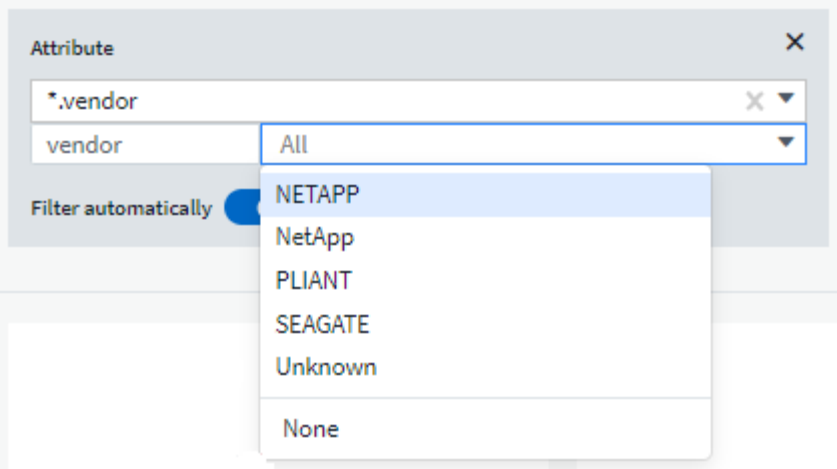
Mais si vous voulez temporairement voir uniquement les nœuds sur des sous-réseaux individuels de votre locataire, vous pouvez définir ou modifier la variable en une ou plusieurs adresses IP de nœud d'agent spécifiques. Ici, nous n'visualise que les nœuds sur le sous-réseau « 123 » :



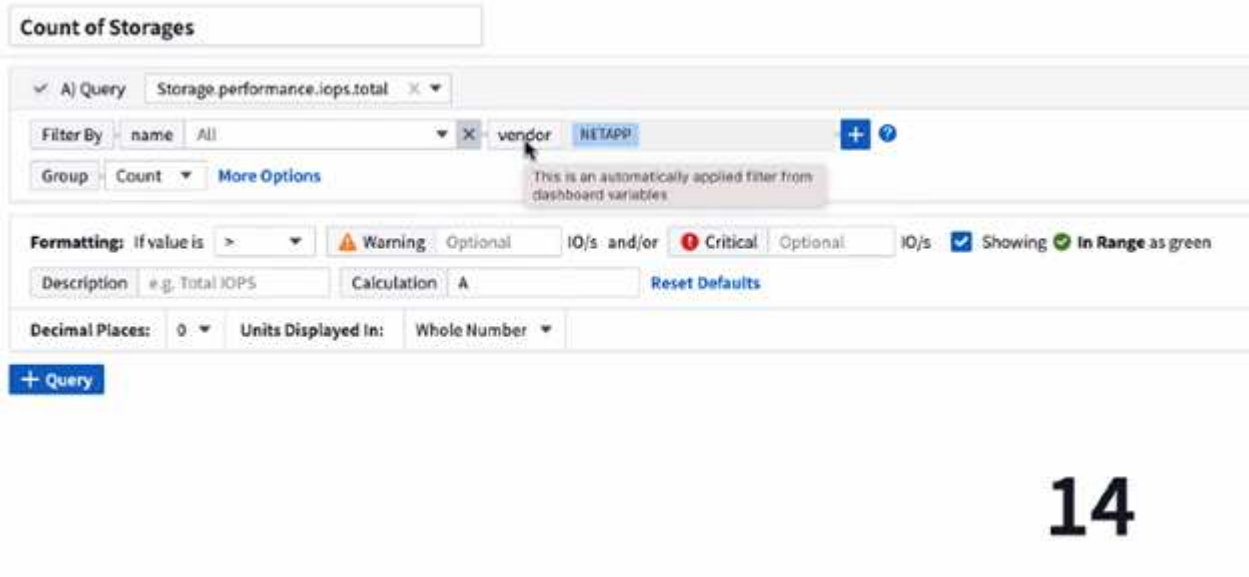
Vous pouvez également définir une variable pour filtrer sur *All* objects avec un attribut particulier quel que soit le type d'objet, par exemple les objets avec un attribut de "vendor", en spécifiant **.vendor* dans le champ variable. Il n'est pas nécessaire de saisir le "*."; Data Infrastructure Insights le fournira si vous sélectionnez l'option générique.



Lorsque vous effectuez la liste déroulante des choix de la valeur variable, les résultats sont filtrés. N'affichez donc que les fournisseurs disponibles en fonction des objets de votre tableau de bord.



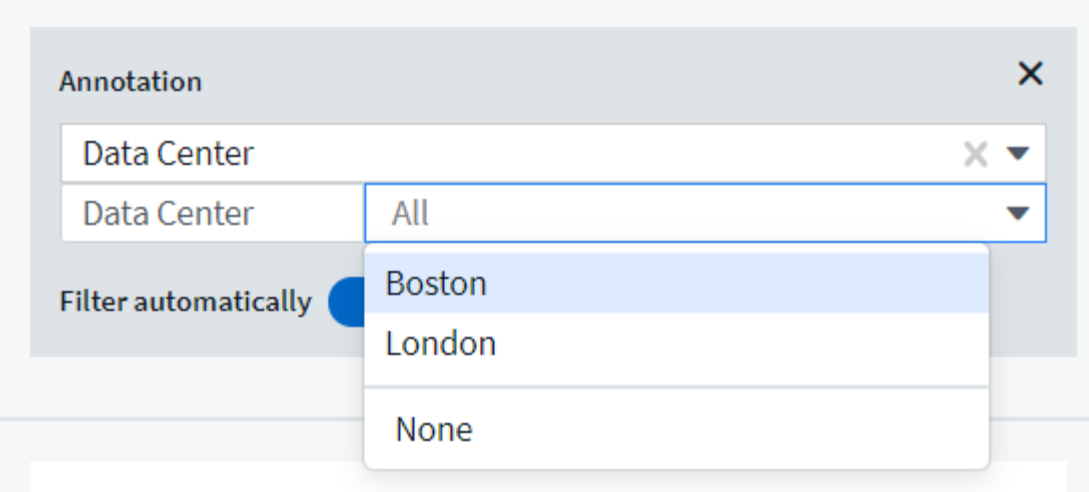
Si vous modifiez un widget sur votre tableau de bord où le filtre d'attribut est pertinent (c'est-à-dire que les objets du widget contiennent un attribut **.vendor*), il vous indique que le filtre d'attribut est automatiquement appliqué.



L'application des variables est aussi simple que la modification des données d'attribut de votre choix.

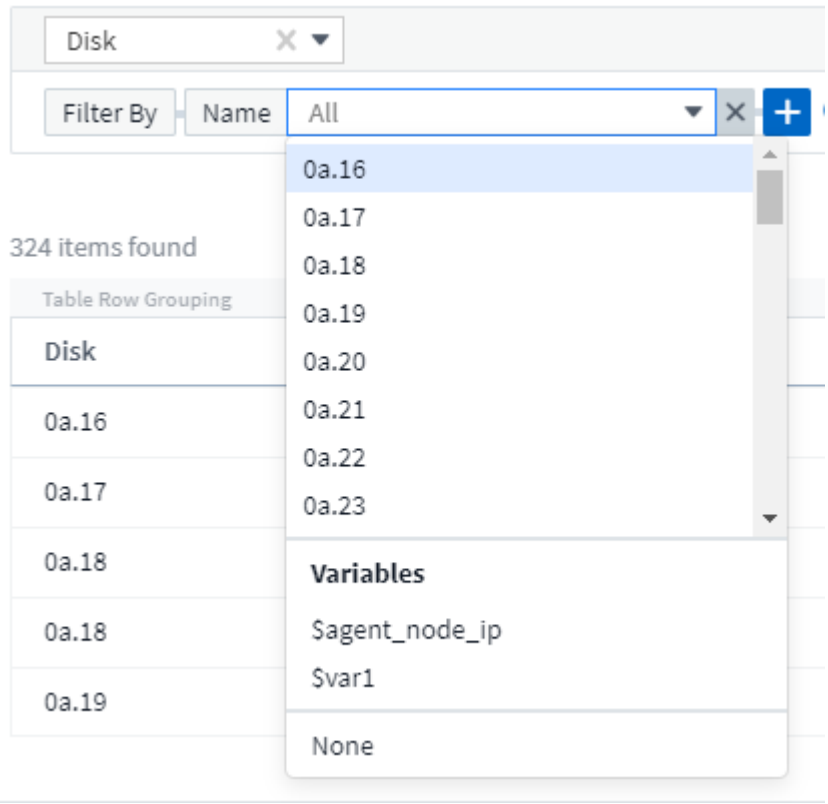
Variables d'annotation

La sélection d'une variable d'annotation permet de filtrer les objets associés à cette annotation, par exemple ceux appartenant au même centre de données.



Texte, nombre, Date ou variable booléenne

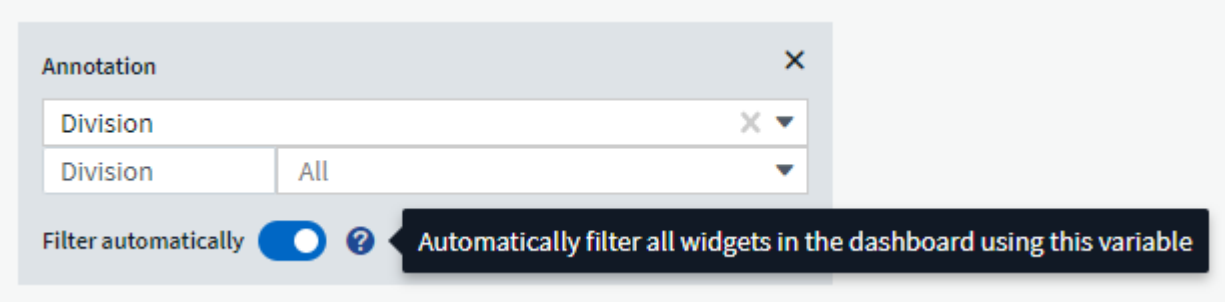
Vous pouvez créer des variables génériques qui ne sont pas associées à un attribut particulier en sélectionnant un type de variable : *Text*, *Number*, *Boolean* ou *Date*. Une fois la variable créée, vous pouvez la sélectionner dans un champ de filtre de widget. Lors de la définition d'un filtre dans 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 dans la section "variables" de la liste déroulante et ont des noms commençant par "$". Le choix d'une variable dans ce filtre vous permettra de rechercher les valeurs que vous entrez dans le champ variable du tableau de bord lui-même. Tous les widgets utilisant cette variable dans un filtre seront mis à jour dynamiquement.



Portée du filtre variable

Lorsque vous ajoutez une variable Annotation ou attribut à votre tableau de bord, la variable peut être

appliquée à *All* widgets du tableau de bord, ce qui signifie que tous les widgets de votre tableau de bord afficheront les résultats filtrés en fonction de la valeur que vous avez définie dans la variable.



Notez que seules les variables attribut et Annotation peuvent être filtrées automatiquement comme ceci. Les variables non-Annotation ou -Attribute ne peuvent pas être filtrées automatiquement. Chaque widget doit être configuré pour utiliser des variables de ces types.

Pour désactiver le filtrage automatique de sorte que la variable s'applique uniquement aux widgets pour lesquels vous l'avez défini spécifiquement, 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 *Filter by*. Avec une variable d'annotation, vous pouvez sélectionner une ou plusieurs valeurs spécifiques ou sélectionner le nom de la variable (indiqué par le « $ ») pour permettre la saisie dans 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 affichent les résultats filtrés.

Le filtrage dans les variables est *Contextual* ; lorsque vous sélectionnez une valeur de filtre ou des valeurs pour une variable, les autres variables de votre page n'affichent que les valeurs pertinentes pour ce filtre. Par exemple, lorsque vous définissez un filtre variable sur un stockage *Model* spécifique, toutes les variables définies pour filtrer pour Storage *Name* n'affichent que les valeurs pertinentes pour ce modèle.

Pour utiliser une variable dans une expression, tapez simplement le nom de la variable dans 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 numérique ou d'attribut dans les expressions.

Le filtrage dans les variables est *Contextual* ; lorsque vous sélectionnez une valeur de filtre ou des valeurs pour une variable, les autres variables de votre page n'affichent que les valeurs pertinentes pour ce filtre. Par exemple, lorsque vous définissez un filtre variable sur un stockage *Model* spécifique, toutes les variables définies pour filtrer pour Storage *Name* n'affichent que les valeurs pertinentes pour ce modèle.

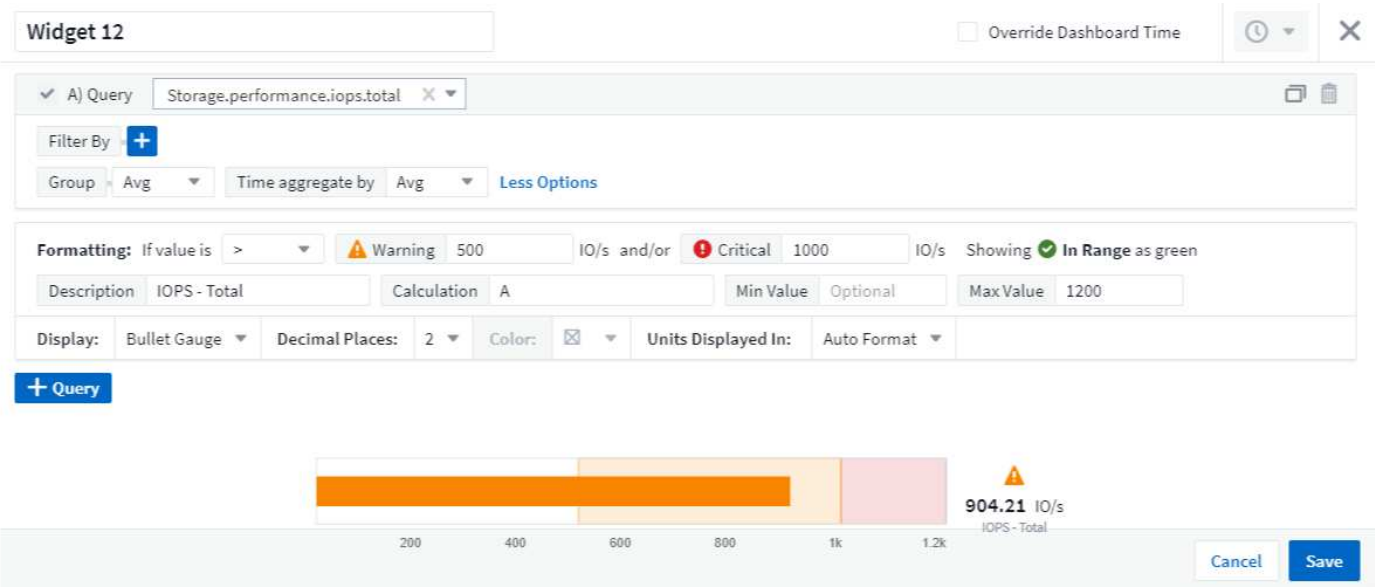
Dénomination des variables

Noms des variables :

- Ne doit inclure que les lettres a-z, les chiffres 0-9, point (.), trait de soulignement (_) et espace ( ).
- Ne peut pas comporter plus de 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.

Formatage des widgets de jauge

Les widgets solide et jauge à puce vous permettent de définir des seuils pour les niveaux *Warning* et/ou *Critical*, fournissant une représentation claire des données que vous spécifiez.

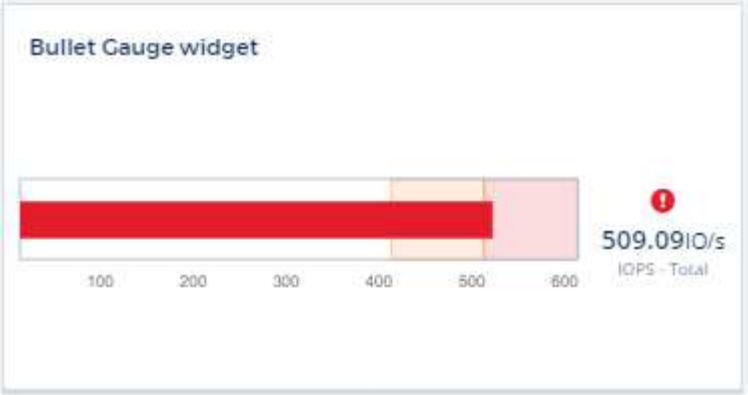


Pour définir le formatage de ces widgets, procédez comme suit :

1. Choisissez si vous souhaitez mettre en surbrillance des valeurs supérieures à (>) ou inférieures à (<) vos seuils. Dans cet exemple, nous allons mettre en surbrillance des valeurs supérieures à (>) les 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 ». Des valeurs supérieures à ce niveau entraînent l'affichage de la jauge en rouge.

Vous pouvez choisir une valeur minimale et maximale pour la jauge. Les valeurs inférieures au minimum n'affichent pas la jauge. Les valeurs supérieures au maximum affichent une jauge complète. Si vous ne choisissez pas les valeurs minimum ou maximum, le widget sélectionne les valeurs min et max optimales en fonction de la valeur du widget.





Formatage du widget à valeur unique

Dans le widget valeur unique, outre le réglage des seuils d'avertissement (orange) et critique (rouge), vous pouvez choisir d'avoir des valeurs « dans la plage » (celles qui se trouvent sous le niveau d'avertissement) affichées avec un arrière-plan vert ou blanc.

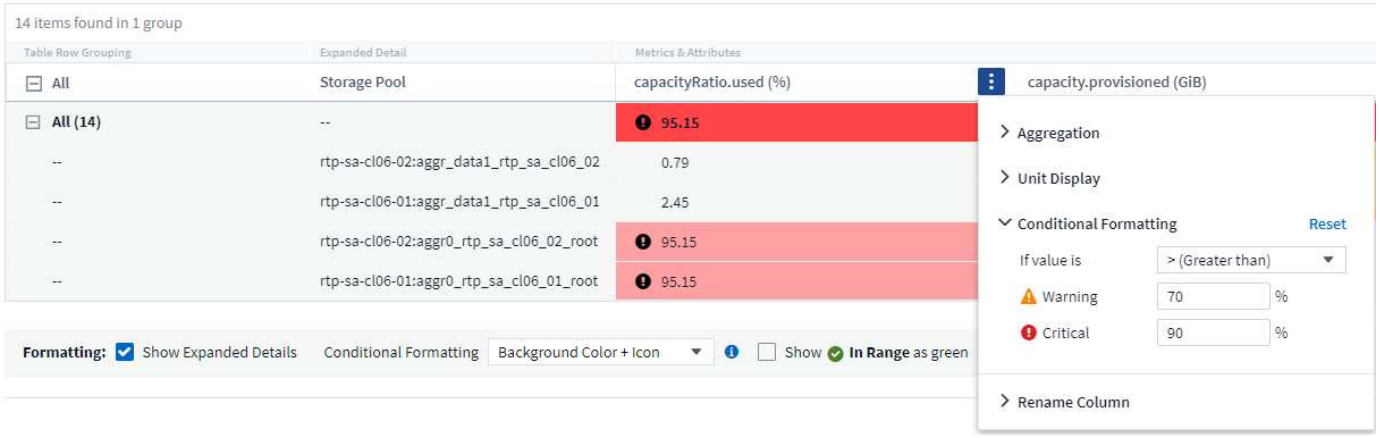


Si vous cliquez sur le lien dans un widget à valeur unique ou un widget de jauge, une page de requête correspondant à la première requête du widget s'affiche.

Formatage des widgets de tableau

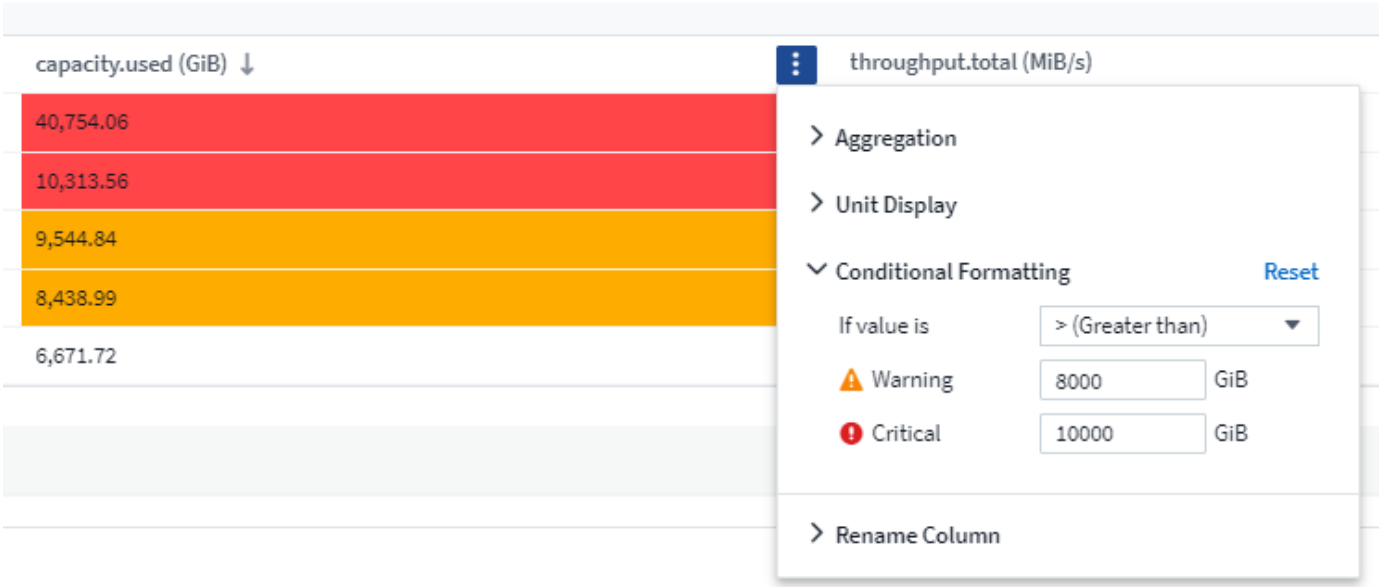
Comme les widgets à valeur unique et jauge, vous pouvez définir un formatage conditionnel dans les widgets de tableau, ce qui vous permet de mettre en évidence des données avec des couleurs et/ou des icônes spéciales.

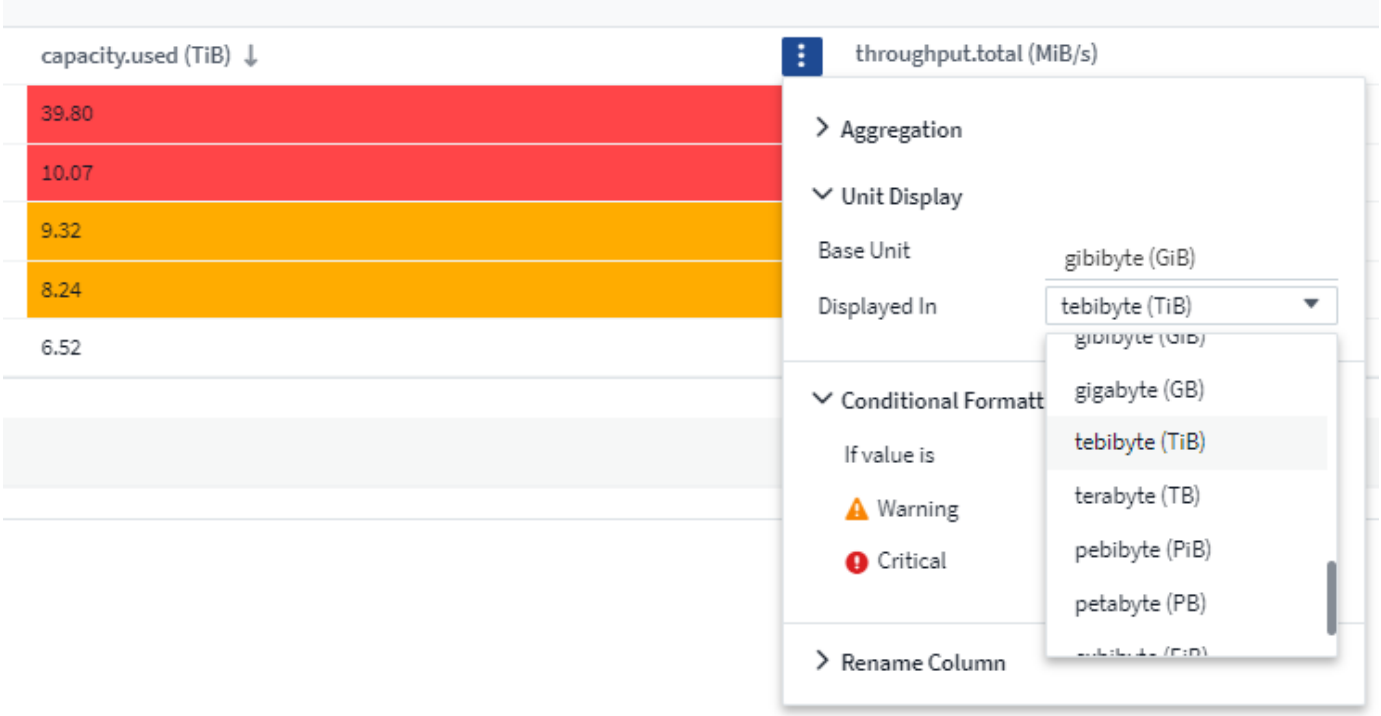
La mise en forme conditionnelle vous permet de définir et de mettre en évidence les seuils de niveau d'avertissement et de niveau critique dans les widgets de tableau, offrant ainsi une visibilité instantanée des valeurs aberrantes et des points de données exceptionnels.



Le formatage conditionnel est défini séparément pour chaque colonne d'une table. Par exemple, vous pouvez choisir un ensemble de seuils pour une colonne de capacité et un autre pour une colonne de débit.

Si vous modifiez l'affichage des unités pour une colonne, le formatage conditionnel reste et reflète la modification des valeurs. Les images ci-dessous montrent le même formatage conditionnel, même si l'unité d'affichage est différente.



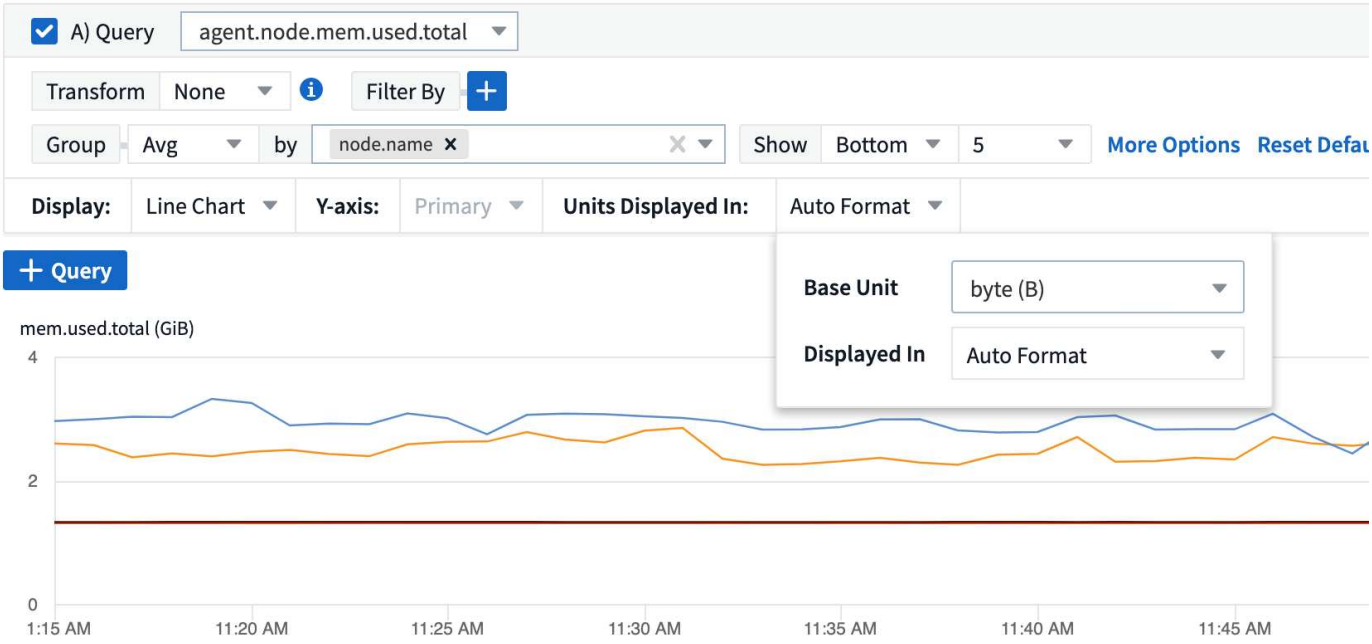


Vous pouvez choisir d'afficher ou non le format de condition en tant que couleur, icônes ou les deux.

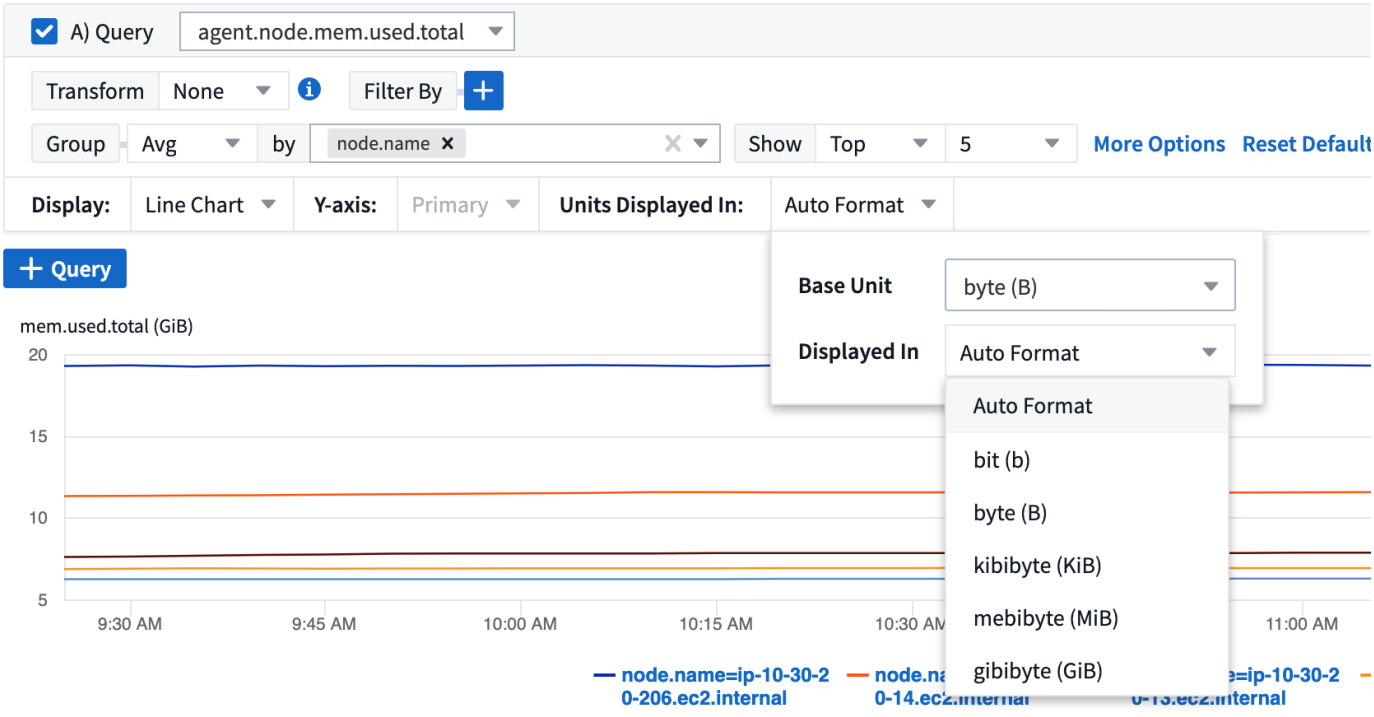
Choix de l'unité pour l'affichage des données

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. Lorsque le format le plus adapté n'est pas connu, vous pouvez définir le format de votre choix.

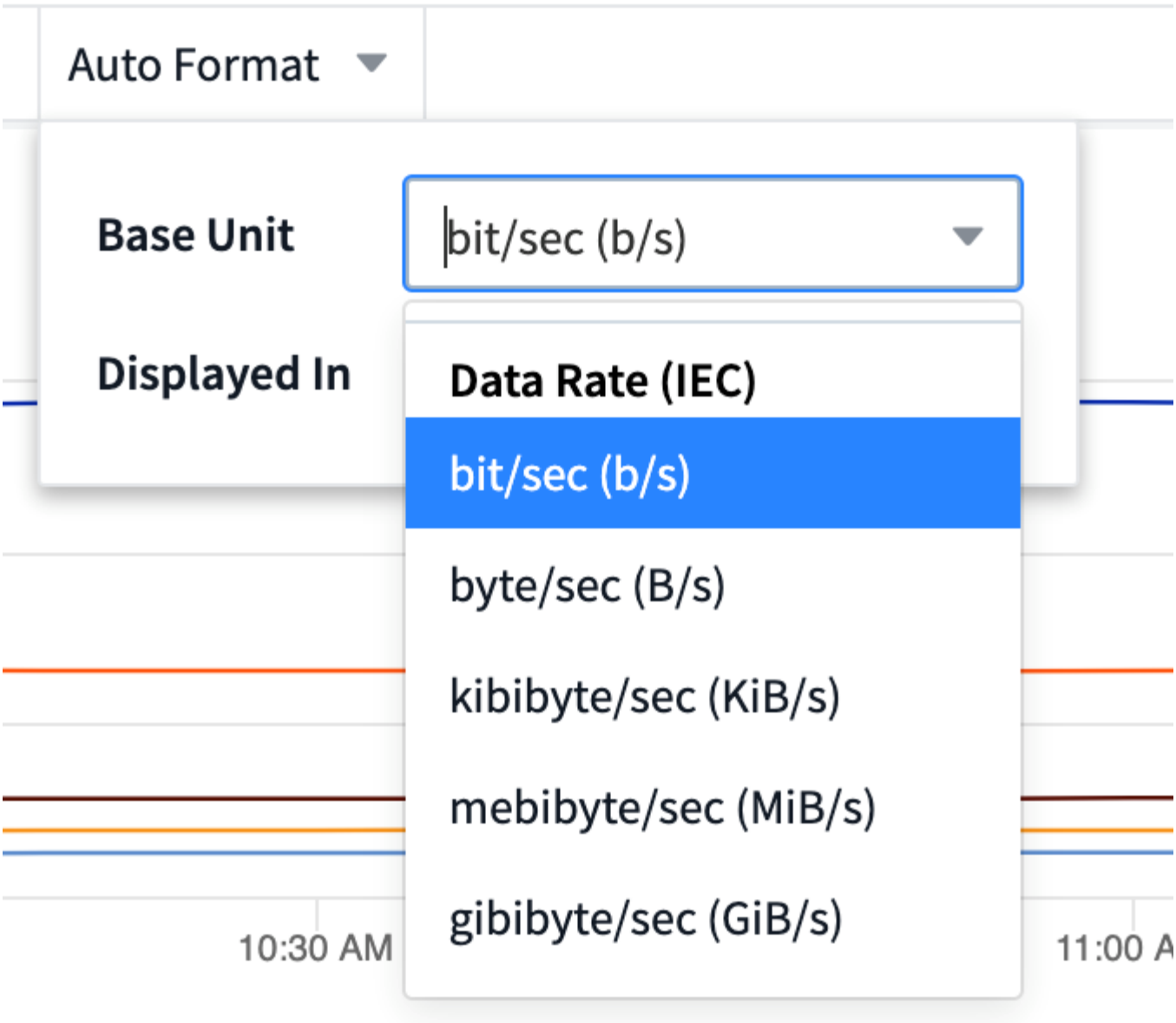
Dans l'exemple de graphique en courbes ci-dessous, les données sélectionnées pour le widget sont connues sous la forme *octets* (l'unité de données CEI de base : voir le tableau ci-dessous), de sorte que l'unité de base est automatiquement sélectionnée sous la forme 'octet (B)'. Toutefois, les valeurs de données sont suffisamment importantes pour être présentées sous forme de gibioctets (Gio). Data Infrastructure Insights formate donc automatiquement les valeurs par défaut sous forme de Gio. L'axe y du graphique affiche « Gio » comme unité d'affichage, et toutes les valeurs sont affichées en termes d'unité.



Si vous souhaitez afficher le graphique dans une autre unité, vous pouvez choisir un autre format d'affichage des valeurs. Comme l'unité de base de cet exemple est *byte*, vous pouvez choisir parmi les formats « octet » pris en charge : bit (b), octet (B), kibyte (Kio), mebibyte (MIB), gibibyte (Gio). L'étiquette et les valeurs de l'axe y changent selon le format choisi.



Dans les cas où l'unité de base n'est pas connue, vous pouvez attribuer une unité à partir de l' "unités disponibles"ou saisir votre propre unité. Une fois l'unité de base affectée, vous pouvez choisir d'afficher les données dans l'un des formats pris en charge appropriés.



Pour effacer vos paramètres et recommencer, cliquez sur **Réinitialiser les paramètres par défaut**.

Un mot sur le format automatique

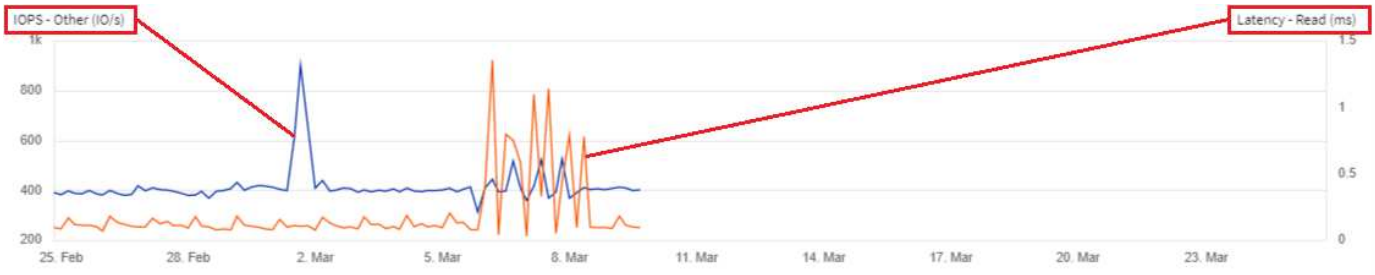
La plupart des mesures sont signalées par des collecteurs de données dans la plus petite unité, par exemple en nombre entier, comme 1,234,567,890 octets. Par défaut, Data Infrastructure Insights formate automatiquement la valeur pour l'affichage le plus lisible. Par exemple, une valeur de données de 1,234,567,890 octets serait formatée automatiquement en 1.23 *Gibioctet*. Vous pouvez choisir de l'afficher dans un autre format, par exemple *mébioctets*. La valeur s'affiche en conséquence.

Data Infrastructure Insights utilise les normes de nommage en anglais américain. Le "milliard" américain équivaut à "mille millions".

Widgets avec plusieurs requêtes

Si vous disposez d'un widget de séries chronologiques (ligne, spline, zone, zone empilée) comportant deux requêtes dans lesquelles les deux sont tracées sur l'axe y principal, l'unité de base n'est pas affichée en haut de l'axe Y. Toutefois, si votre widget a une requête sur l'axe y principal et une requête sur l'axe y secondaire,

les unités de base de chacune sont affichées.



Si votre widget a au moins trois requêtes, les unités de base ne sont pas affichées sur l'axe Y.

Unités disponibles

Le tableau suivant montre toutes les unités disponibles par catégorie.

Catégorie	Unités
Devise	dollar
Données (CEI)	octet binaire kibbyte mebibyte gibibyte tebibyte pebibyte exbibyte
Date(CEI)	bit/sec octet/sec kibyte/sec mebibyte/sec gibibyte/sec tebibyte/sec pebibyte/sec
Données (métriques)	kilo-octet octet octet octet octet octet octet octet octet octet octet téraoctet
Date(métrique)	kilo-octet/s mégaoctet par seconde et gigaoctet par seconde téraoctet/s plusieurs pétaoctets/sec
CEI	bami mebi gibi tebi exbi
Décimale	nombre entier de milliers de milliards de bilions
Pourcentage	pourcentage
Heure	nanoseconde microseconde milliseconde seconde minute heure
Température	celsius fahrenheit
Fréquence	hertz kilohertz mégahertz gigahertz
CPU	nanocores microcœurs millicores cœurs kilocolores megacores gigacores teracores petacores exacores
Débit	Opérations d'E/S par seconde (OPS/s) demandes par seconde (lectures/s) opérations par seconde (OPS/min) en lecture/min en écriture/min (min)

Mode TV et actualisation automatique

Les données des widgets des tableaux de bord et des pages d'accueil des ressources sont automatiquement actualisées selon 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 soit des séries chronologiques (ligne, spline, zone, graphique à surface empilée) ou des séries non temporelles (tous les autres graphiques).

Plage de temps du tableau de bord	Intervalle d'actualisation des séries de temps	Intervalle d'actualisation des séries non horaires
Dernières 15 minutes	10 secondes	1 minute
Dernières 30 minutes	15 secondes	1 minute
Dernières 60 minutes	15 secondes	1 minute
Dernières 2 heures	30 secondes	5 minutes
Dernières 3 heures	30 secondes	5 minutes
Dernières 6 heures	1 minute	5 minutes
Dernières 12 heures	5 minutes	10 minutes
Dernières 24 heures	5 minutes	10 minutes
2 derniers jours	10 minutes	10 minutes
3 derniers jours	15 minutes	15 minutes
7 derniers jours	1 heure	1 heure
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 de temps du tableau de bord personnalisé.

Combiné au **mode TV**, l'actualisation automatique permet d'afficher les données en temps quasi réel sur un tableau de bord ou une page de ressources. Le mode TV offre un affichage sans encombré ; le menu de navigation est masqué, offrant davantage d'espace pour l'affichage de vos données, tout comme le bouton Modifier. Le mode TV ignore les délais d'expiration habituels de Data Infrastructure Insights, laissant l'affichage en direct jusqu'à ce que la session soit fermée manuellement ou automatiquement par les protocoles de sécurité d'autorisation.

Comme NetApp BlueXP a son propre délai de connexion utilisateur de 7 jours, les informations de l'infrastructure de données doivent également se déconnecter avec cet événement. Il vous suffit de vous connecter à nouveau pour que votre tableau de bord continue à s'afficher.

- Pour activer le mode TV, cliquez sur le bouton mode TV.
- Pour désactiver le mode TV, cliquez sur le bouton **Quitter** dans le coin supérieur gauche de l'écran.

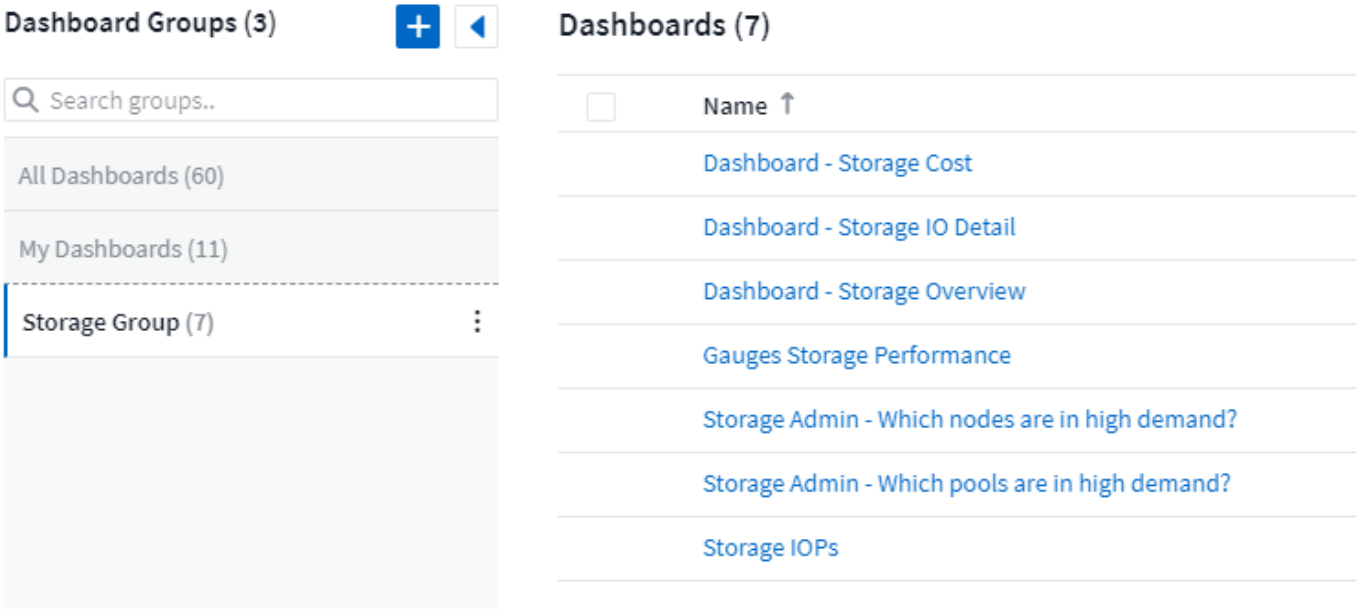
Vous pouvez suspendre temporairement l'actualisation automatique en cliquant sur le bouton Pause dans le coin supérieur droit. En pause, le champ de plage de temps du tableau de bord affiche la plage de temps active des données en pause. Vos données sont toujours en cours d'acquisition et de mise à jour pendant l'actualisation automatique. Cliquez sur le bouton reprendre pour continuer l'actualisation automatique des données.



Groupes de tableaux de bord

Le regroupement vous permet d'afficher et de gérer les tableaux de bord associés. Par exemple, vous pouvez disposer d'un groupe de tableaux de bord dédié au stockage de 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 s'affiche en regard du nom du groupe.

Pour créer un nouveau groupe, cliquez sur le bouton **"+" Créer un nouveau groupe de tableau de bord**. Entrez 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, cliquez sur *Mes tableaux de bord* si vous souhaitez uniquement afficher les tableaux de bord que vous possédez, puis effectuez l'une des opérations suivantes :

- Pour ajouter un tableau de bord unique, 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 cochant la case en regard de chaque tableau de bord, puis cliquez sur le bouton **actions groupées** 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 de tableaux de bord du groupe *All Dashboards* ou *My Dashboards*.

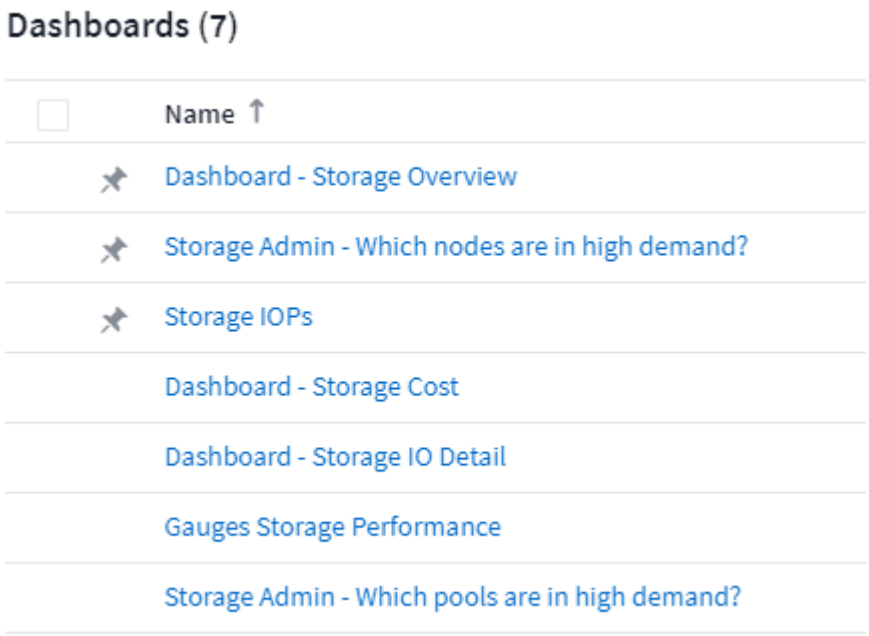
La suppression d'un tableau de bord d'un groupe ne supprime pas le tableau de bord de Data Infrastructure Insights. Pour supprimer complètement un tableau de bord, sélectionnez-le et cliquez sur *Delete*. Ceci le supprime de tous les groupes auxquels il appartenait et il n'est plus disponible pour aucun utilisateur.

Épinglez vos tableaux de bord favoris

Vous pouvez gérer davantage vos tableaux de bord en les épingler en haut de votre liste de bord. Pour épingler un tableau de bord, cliquez simplement sur le bouton de la molette affiché lorsque vous placez le

pointeur de la souris sur un tableau de bord dans n'importe quelle liste.

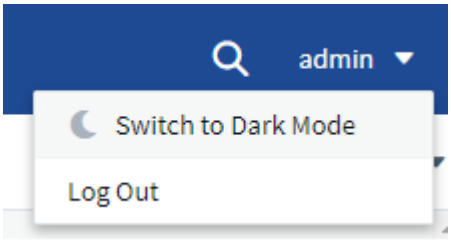
Le PIN/unpin du tableau de bord est une préférence utilisateur individuelle et indépendante du groupe (ou des groupes) auquel appartient le tableau de bord.



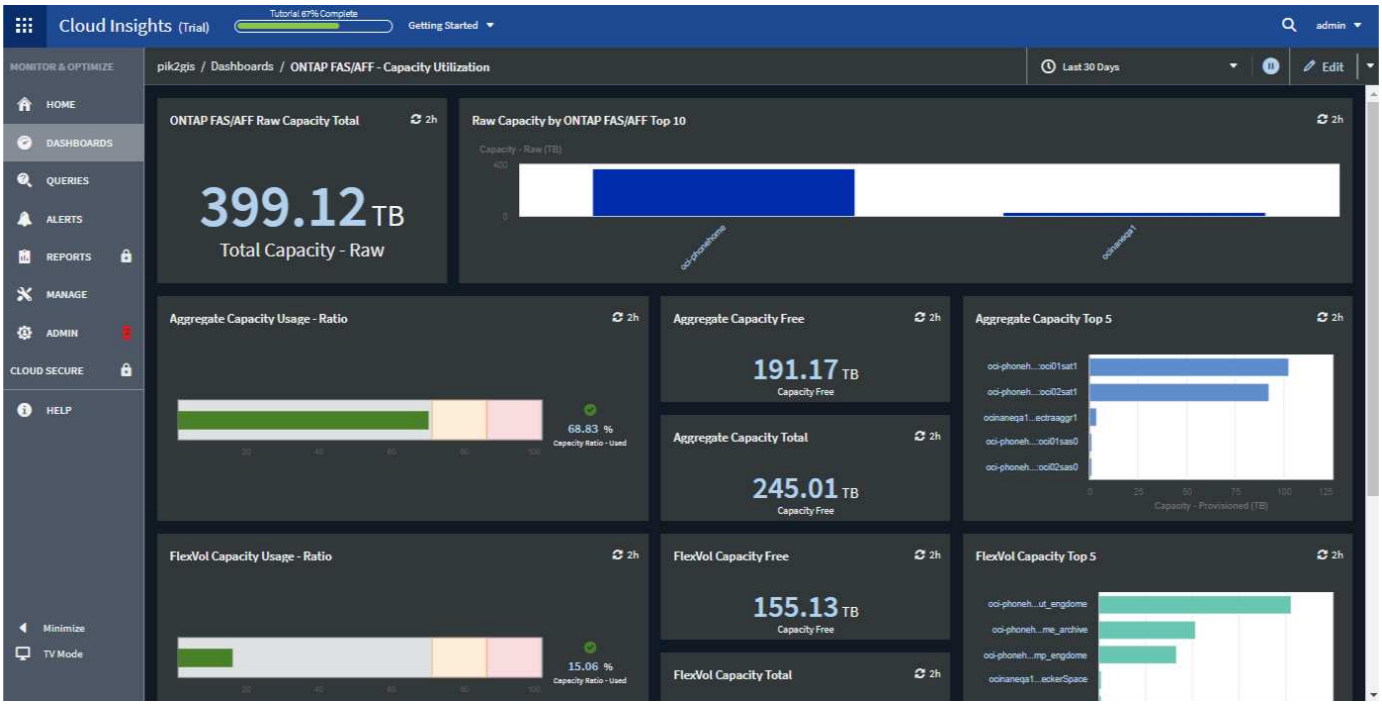
Thème sombre

Vous pouvez choisir d'afficher Data Infrastructure Insights à l'aide d'un thème clair (par défaut), qui affiche la plupart des écrans à l'aide d'un fond clair avec du texte foncé, ou d'un thème sombre qui affiche la plupart des écrans à l'aide d'un fond sombre avec du texte clair.

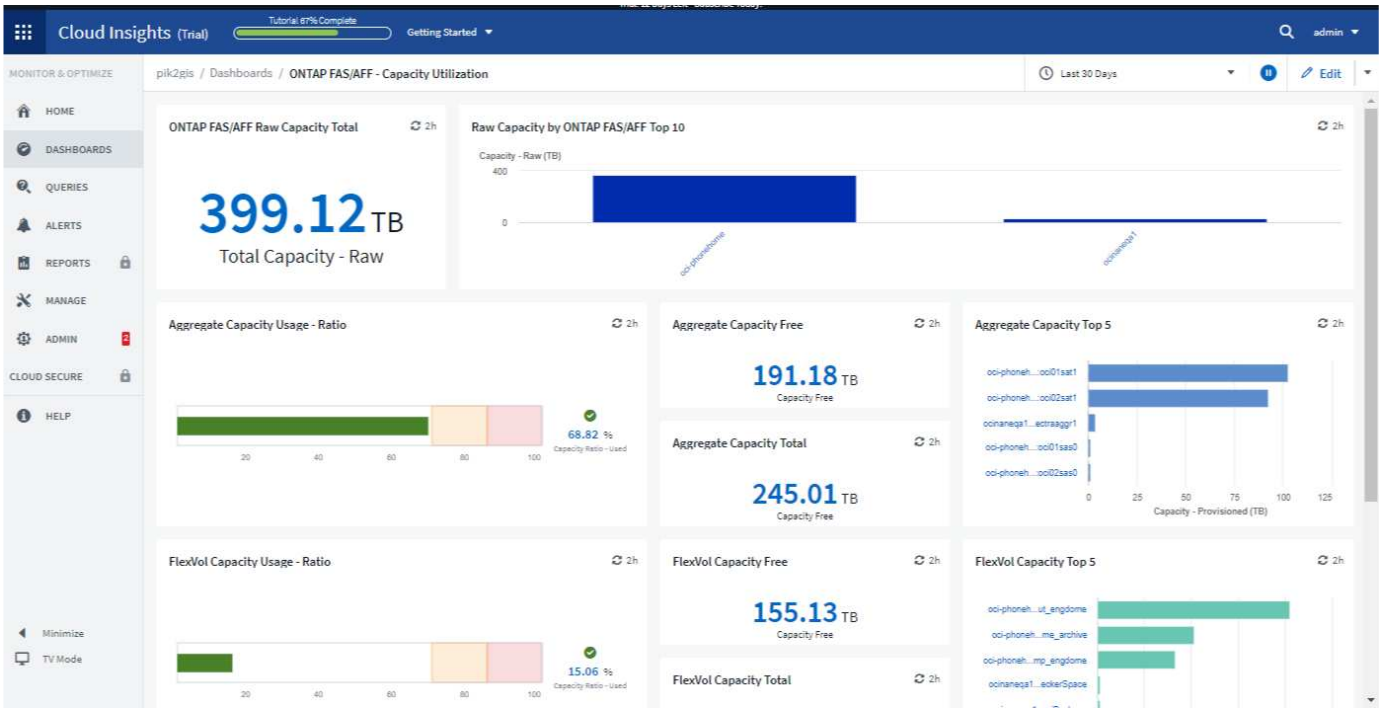
Pour basculer entre les thèmes clairs et sombres, cliquez sur le bouton username dans le coin supérieur droit de l'écran et choisissez le thème souhaité.



Vue Tableau de bord thème sombre :



Vue Tableau de bord thème clair :



Certaines zones d'écran, telles que certaines graphiques de widgets, affichent toujours des arrière-plans clairs, même lorsqu'elles sont visualisées sur un thème sombre.

Interpolation de l'histogramme linéaire

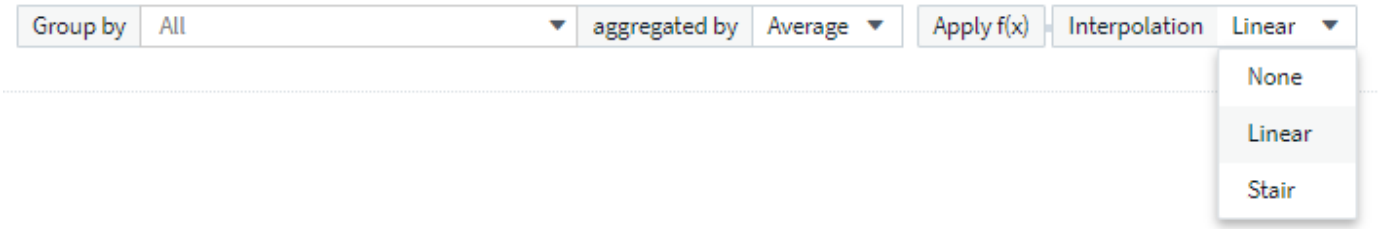
Différents collecteurs de données scruent souvent leurs données à différents intervalles. Par exemple, le collecteur de données A peut interroger toutes les 15 minutes alors que le collecteur de données B interroge toutes les cinq minutes. Lorsqu'un widget de graphique en ligne (également des graphiques de spline, de zone et de zone empilée) rassemble ces données de plusieurs collecteurs de données en une seule ligne (par exemple, lorsque le widget est regroupé par « tous »), Et actualiser la ligne toutes les cinq minutes, les

données du collecteur B peuvent être affichées avec précision alors que les données du collecteur A peuvent avoir des écarts, ce qui affecte l'agrégat jusqu'à ce que le collecteur A interroge à nouveau.

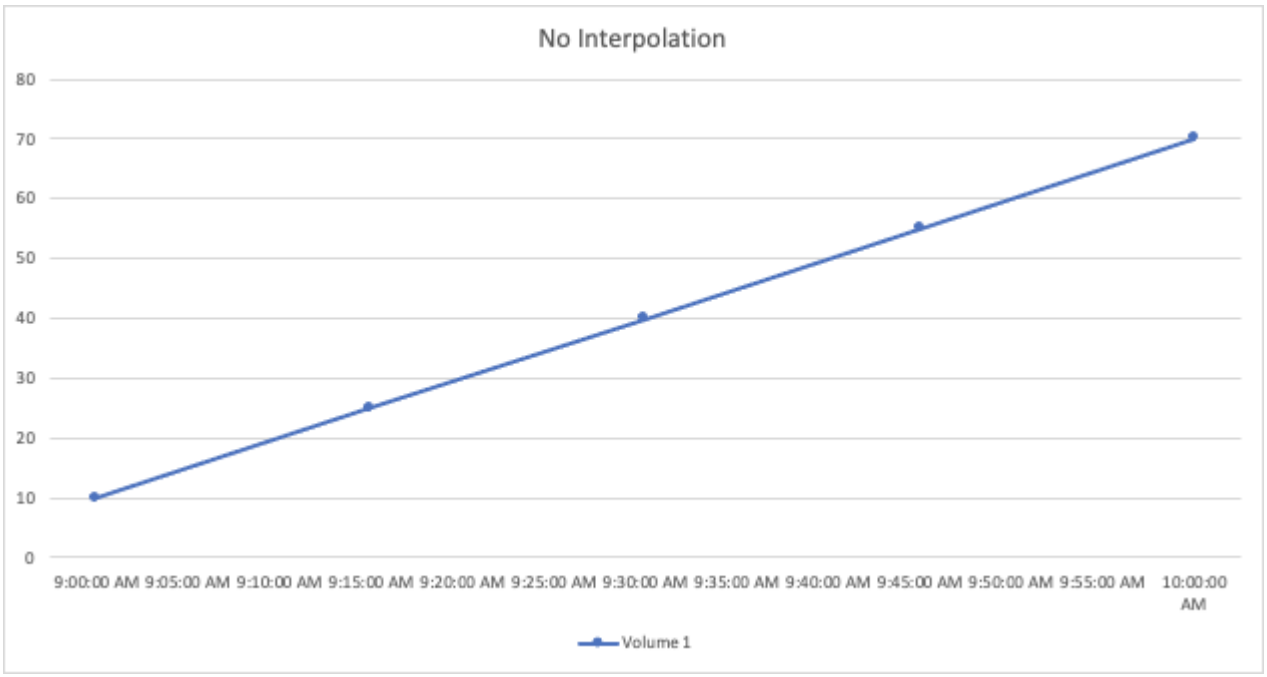
Pour résoudre ce problème, Data Infrastructure Insights interpole les données lors de l'agrégation, en utilisant les points de données environnants pour faire une « meilleure estimation » aux données jusqu'à ce que les collecteurs de données interrogent à nouveau. Vous pouvez toujours afficher les données de chaque objet du collecteur de données individuellement en ajustant le regroupement du widget.

Méthodes d'interpolation

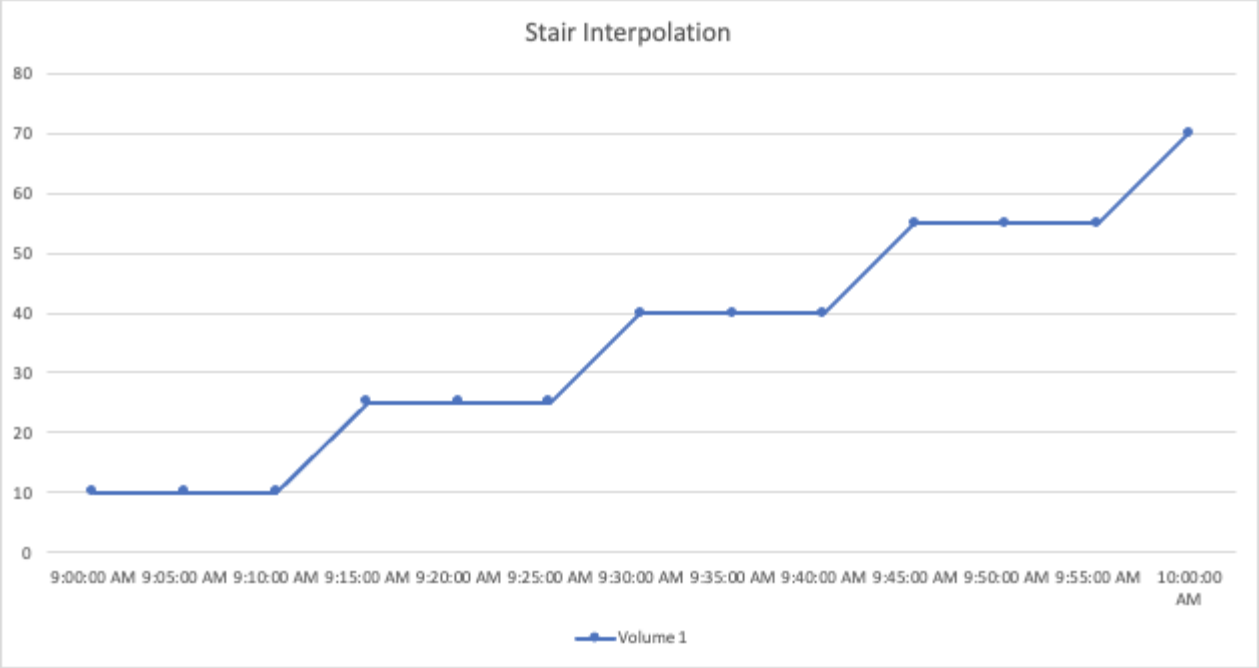
Lors de la création ou de la modification d'un graphique linéaire (ou d'une spline, d'une zone ou d'une zone empilée), vous pouvez définir la méthode d'interpolation sur l'un des trois types. Dans la section « Grouper par », choisissez l'interpolation souhaitée.



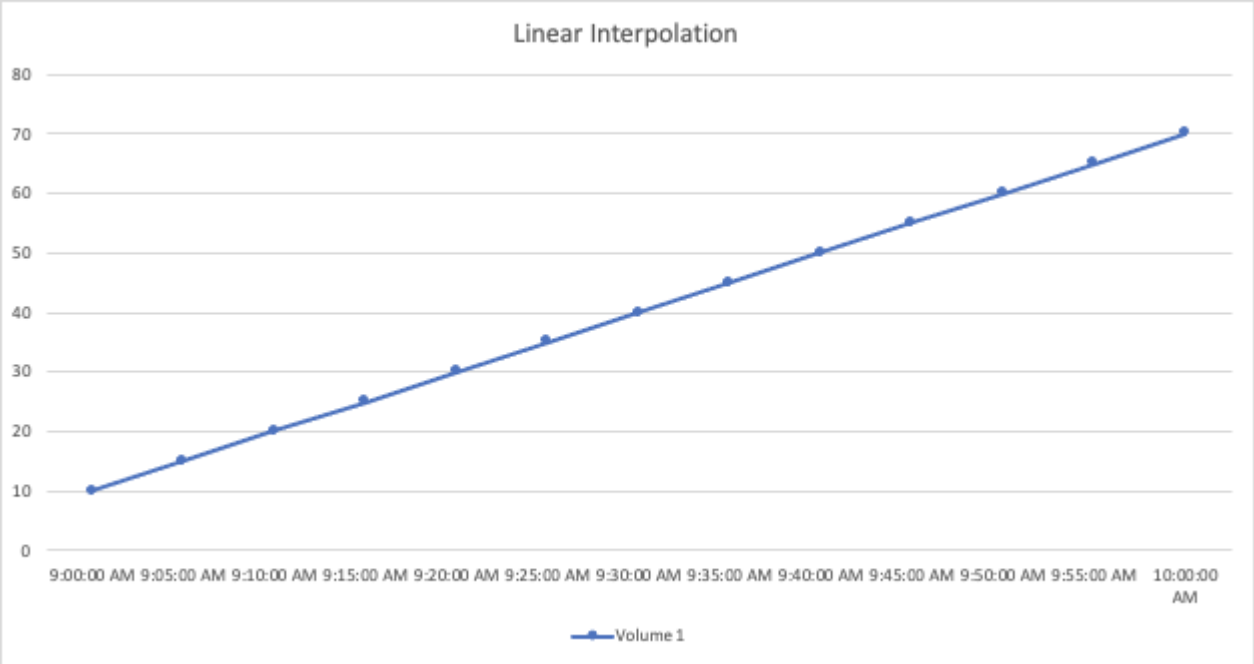
- **Aucun** : ne rien faire, c'est-à-dire ne pas générer de points entre les deux.



- **Escalier** : un point est généré à partir de la valeur du point précédent. Dans une ligne droite, ceci s'affichera comme une disposition type « escalier ».



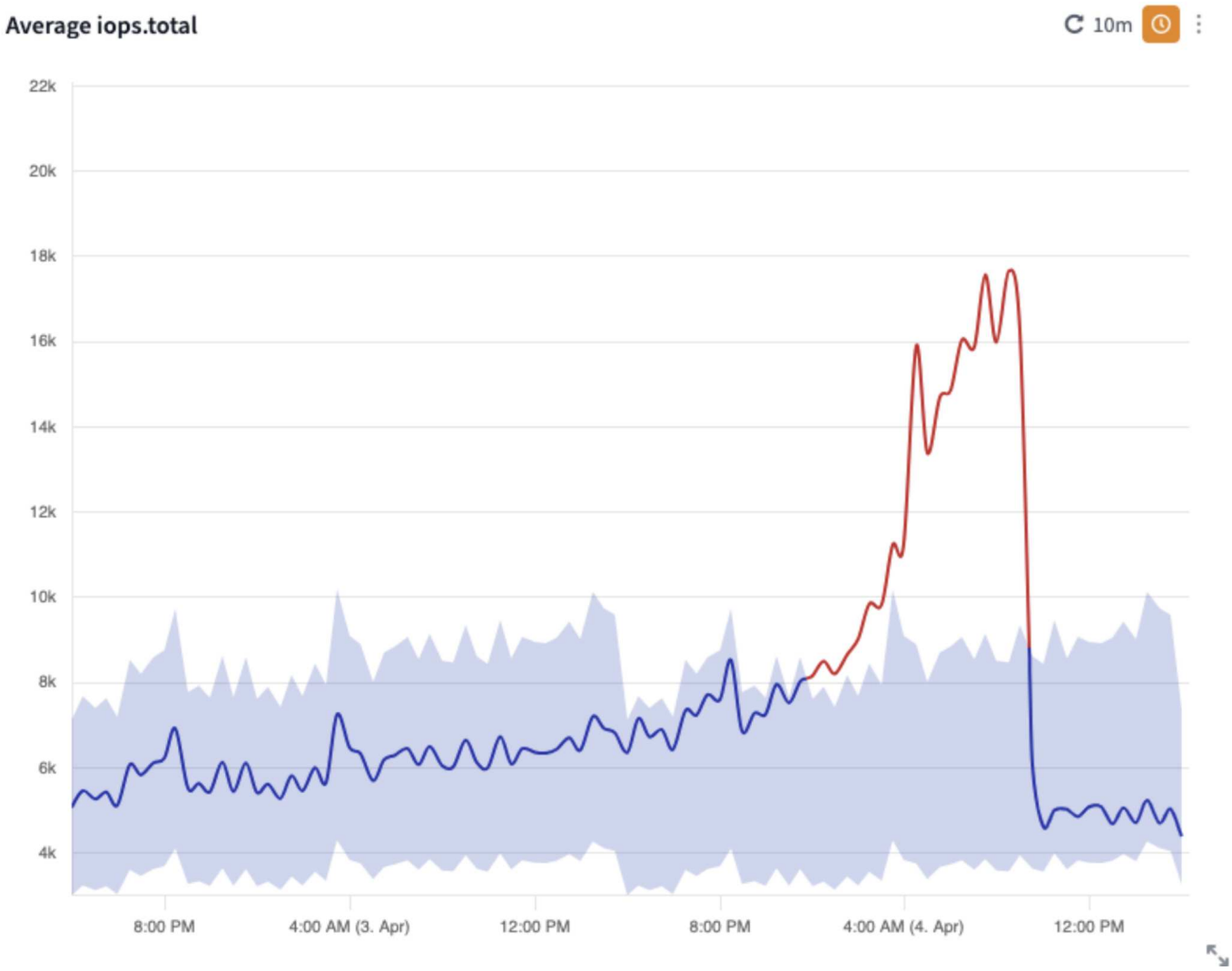
- **Linéaire** : un point est généré comme valeur entre la connexion des deux points. Génère une droite qui ressemble à la ligne reliant les deux points, mais avec des points de données supplémentaires (interpolés).



Limites d'anomalies dans les widgets en ligne

Lors de l'inclusion d'un widget de graphique ligne ou Spline sur un tableau de bord ou une page d'accueil, vous pouvez choisir d'afficher le graphique dans le contexte des **limites attendues** pour les données. Vous pouvez penser à rechercher des anomalies dans les modèles de vos données.

DII utilise les données saisonnières (horaire ou quotidien) pour définir les limites supérieures et inférieures là où il attend que les données tombent à un moment donné. Si les données dépassent ou tombent en dessous des limites attendues, le graphique les met en évidence comme une anomalie.



Pour afficher les limites d'anomalie, modifiez le widget et choisissez *Afficher les limites d'anomalie*. Vous pouvez choisir parmi deux algorithmes de détection :

- **Adaptive Detector** s'adapte rapidement aux changements, ce qui le rend utile pour les examens détaillés.
- **Smooth Detector** minimise le bruit et les faux positifs, filtrant les fluctuations à court terme tout en détectant toujours des décalages importants.

En outre, vous pouvez choisir d'afficher la saisonnalité *horaire* ou *quotidienne*, ainsi que de définir la sensibilité de la détection. *Haute* sensibilité détecte plus de franchissement de limite, *faible* sensibilité détecte moins.



N'oubliez pas que vous ne pouvez afficher que les limites attendues lorsque le graphique est configuré pour afficher une seule ligne. Si vos paramètres ou filtres regrouper par affichent plusieurs lignes ou si vous avez défini plusieurs requêtes pour le widget, l'option d'affichage des limites attendues sera désactivée.

Exemple de tableaux de bord

Exemple de tableau de bord : performances des ordinateurs virtuels

Les opérations IT sont confrontées à de nombreux défis. Les administrateurs doivent en faire plus avec moins, et une visibilité complète sur vos data centers dynamiques est primordiale. Dans cet exemple, nous allons vous montrer comment créer un tableau de bord avec des widgets qui vous fournissent des informations opérationnelles sur les performances des machines virtuelles de votre locataire. En suivant cet exemple et en créant des widgets pour cibler vos propres besoins spécifiques, vous pouvez exemple visualiser les performances de stockage back-end par rapport aux performances des machines virtuelles front-end, ou afficher la latence des machines virtuelles par rapport à la demande d'E/S.

Description de la tâche

Dans cette section, nous allons créer un tableau de bord des performances des ordinateurs virtuels comprenant les éléments suivants :

- Un tableau répertoriant les noms de VM et les données de performances
- Tableau comparant la latence du serveur virtuel à la latence du stockage
- Un graphique illustrant le nombre total d'IOPS en lecture, écriture et lecture pour les machines virtuelles
- Un graphique illustrant le débit maximal pour vos machines virtuelles

Ce n'est qu'un exemple de base. Vous pouvez personnaliser votre tableau de bord pour mettre en évidence et comparer les données de performances de votre choix, afin de cibler vos propres meilleures pratiques opérationnelles.

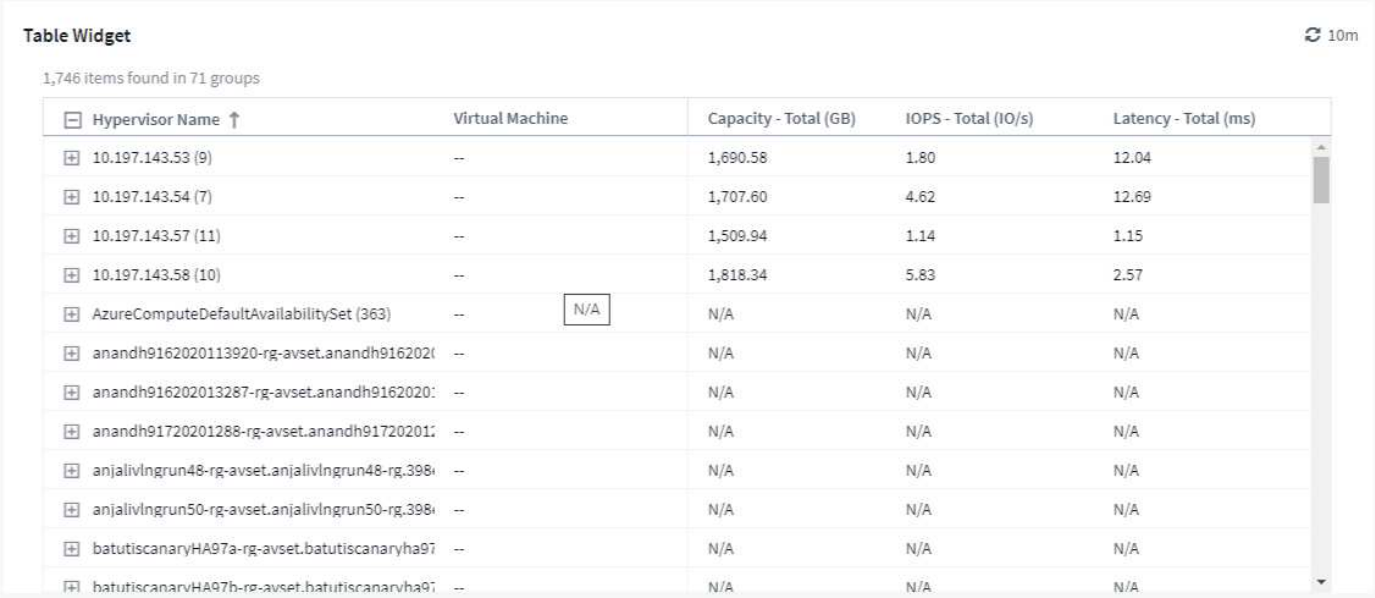
Étapes

1. Connectez-vous à Insight en tant qu'utilisateur avec des autorisations d'administration.
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 « VM Performance by 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 **Edit** pour activer le mode Edit.
6. Cliquez sur l'icône **Add widget** et sélectionnez **Table** pour ajouter un nouveau widget de tableau de bord.

   La boîte de dialogue Modifier le widget s'ouvre. Les données affichées par défaut s'affichent pour tous les stockages de votre locataire.



1. Nous pouvons personnaliser ce widget. Dans le champ Nom en haut, supprimez le widget 1 et entrez le tableau performances de l'ordinateur virtuel.
2. Cliquez sur la liste déroulante Type de ressource et remplacez *Storage* par *Virtual machine*.

   Les données du tableau changent pour afficher toutes les machines virtuelles de votre locataire.

3. Ajoutons quelques colonnes à la table. Cliquez sur l'icône engrenage à droite et sélectionnez *Hypervisor name*, *IOPS - Total* et *latence - Total*. Vous pouvez également essayer de saisir le nom dans la recherche pour afficher rapidement le champ souhaité.

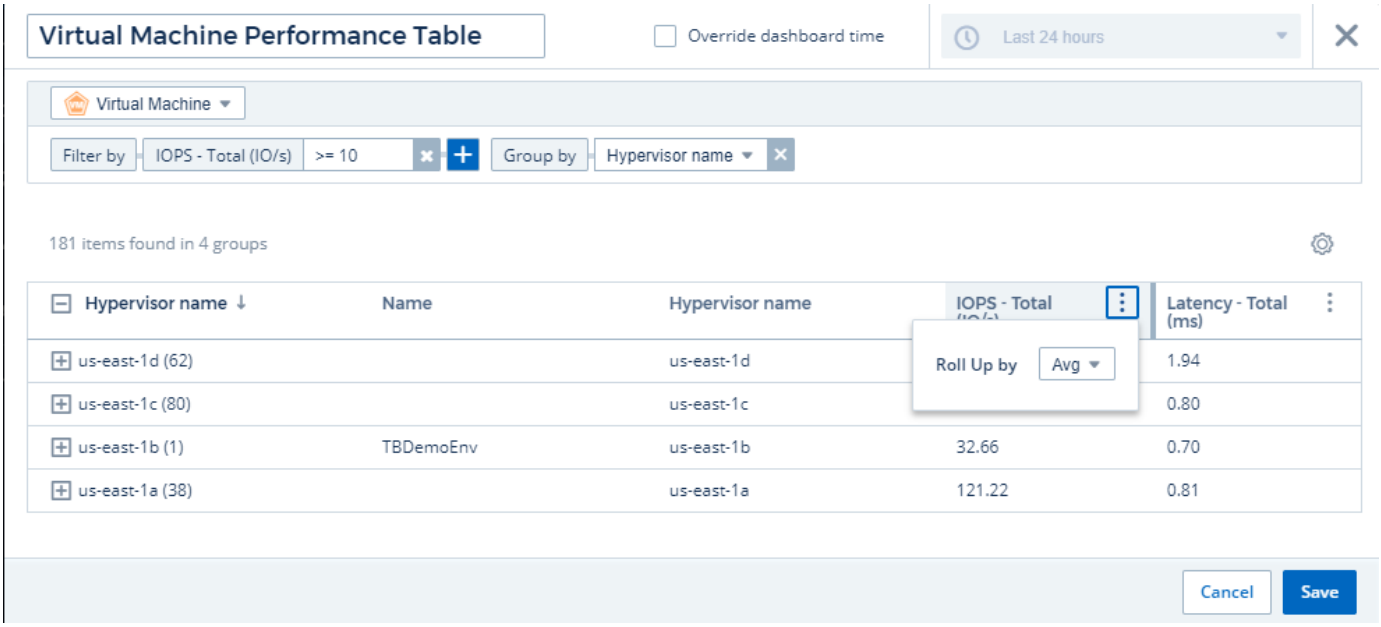
   Ces colonnes sont maintenant affichées dans le tableau. Vous pouvez trier la table en fonction de l'une de ces colonnes. Notez que les colonnes sont affichées dans l'ordre dans lequel elles ont été ajoutées au widget.

4. Dans le cadre de cet exercice, nous exclurons les machines virtuelles qui ne sont pas utilisées activement. Analysons tout autre élément avec moins de 10 000 IOPS totales. Cliquez sur le bouton **[+]** en regard de **Filtrer par** et sélectionnez *IOPS - Total*. Cliquez sur **any** et saisissez "10" dans le champ **de**. Laissez le champ **à** vide. Cliquez sur outrder le champ de filtre ou appuyez sur entrée pour définir le filtre.

   Le tableau montre désormais uniquement les machines virtuelles avec au moins 10 IOPS totales.

5. Nous pouvons réduire davantage la table en regroupant les résultats. Cliquez sur le bouton **[+]** en regard de **Grouper par** et sélectionnez un champ à regrouper par, comme *application* ou *Hypervisor name*. Le regroupement est automatiquement appliqué.

   Les lignes de la table sont désormais regroupées en fonction de vos paramètres. Vous pouvez développer et réduire les groupes selon vos besoins. Les lignes groupées affichent des données cumulées pour chacune des colonnes. Certaines colonnes vous permettent de choisir la méthode de défilement de cette colonne.



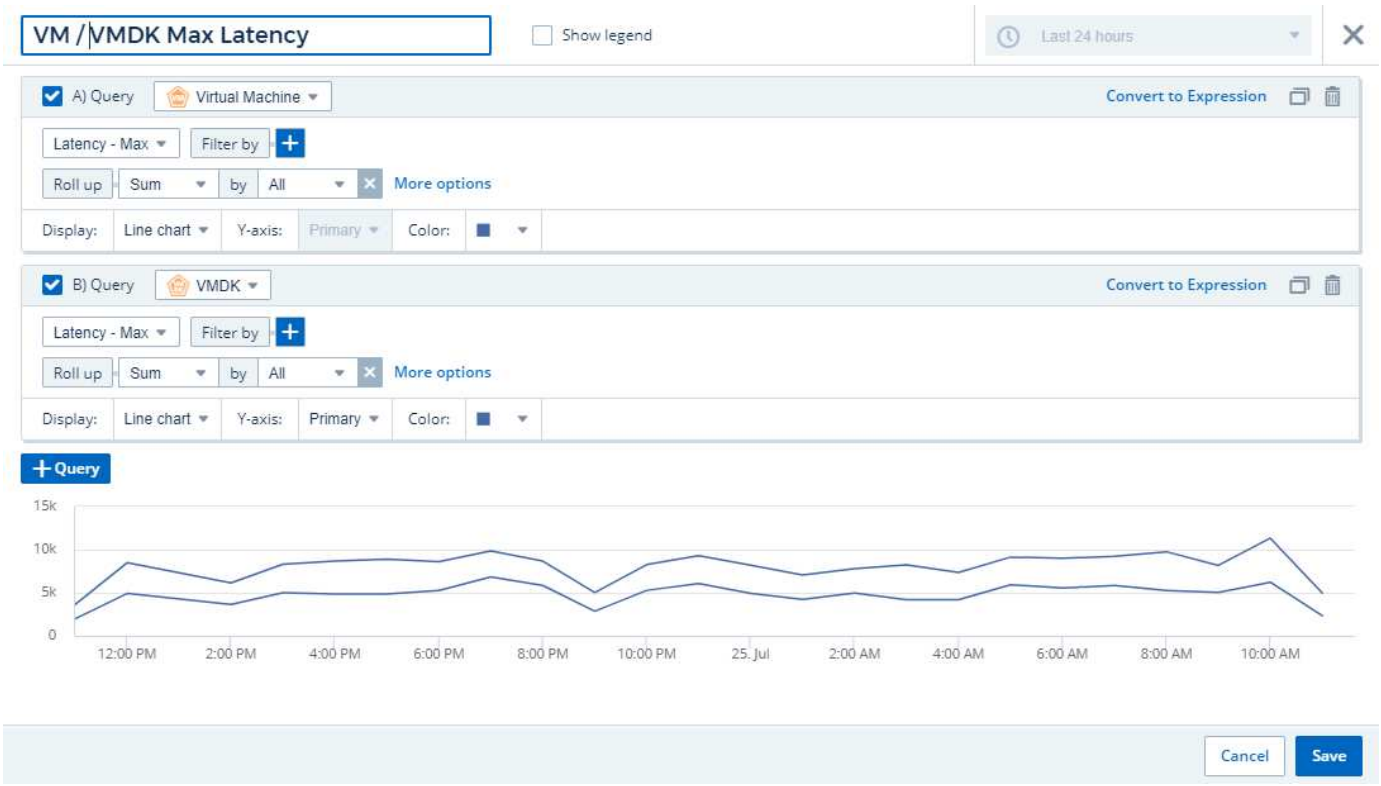
1. Lorsque vous avez personnalisé le widget de tableau à votre convenance, cliquez sur le bouton **[Save]**.

   Le widget de tableau de bord est enregistré dans le tableau de bord.

Vous pouvez redimensionner le widget du tableau de bord en faisant glisser le coin inférieur droit. Rendez le widget plus large pour afficher clairement toutes les colonnes. Cliquez sur **Enregistrer** pour enregistrer le tableau de bord actuel.

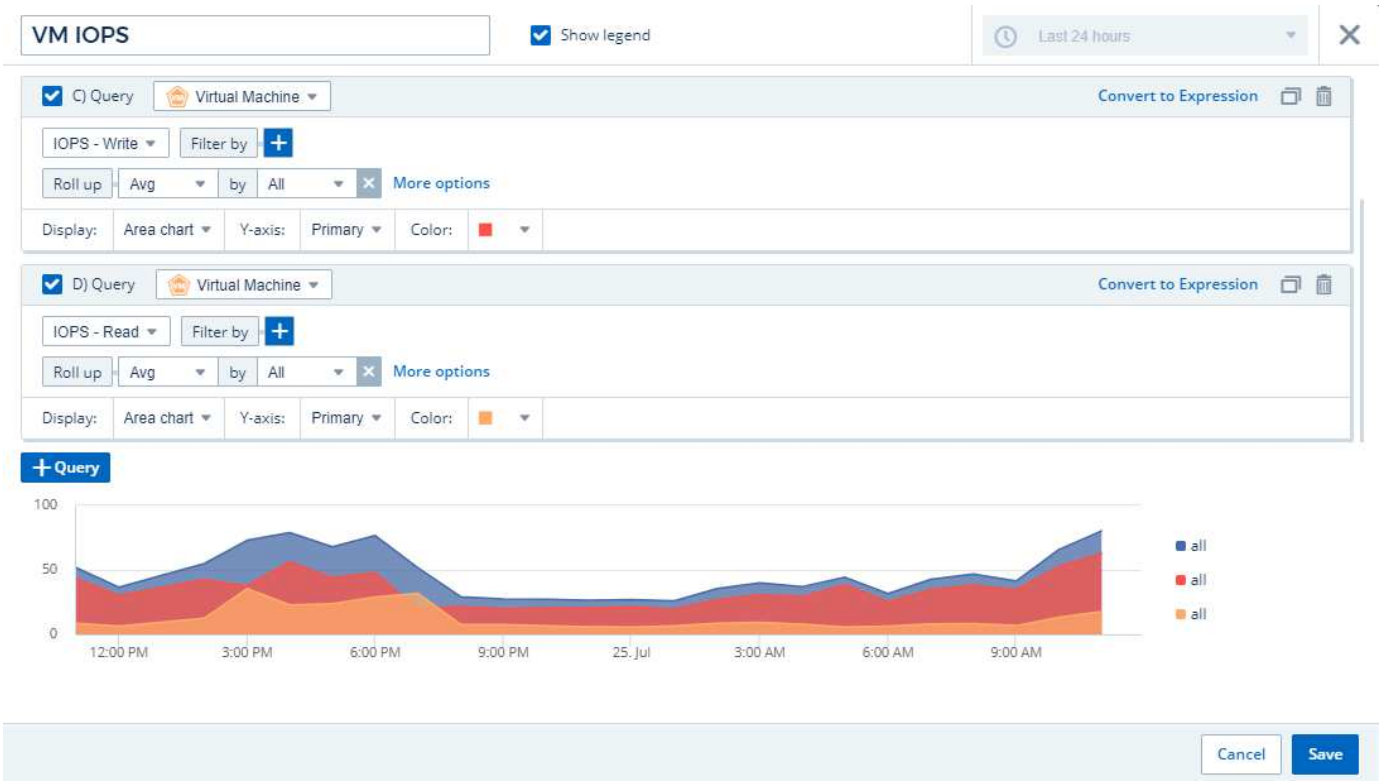
Nous ajouterons ensuite des graphiques pour afficher les performances de nos machines virtuelles. Créons un graphique qui compare la latence des machines virtuelles à la latence des disques VMDK.

1. Si nécessaire, cliquez sur l'icône **Edit** du tableau de bord pour activer le mode Edit.
2. Cliquez sur l'icône **[Add widget]** et sélectionnez *Line Chart* pour ajouter un nouveau widget graphique en ligne au tableau de bord.
3. La boîte de dialogue **Edit widget** s'ouvre. Nommez ce widget « VM/latence maximale VMDK »
4. Sélectionnez **machine virtuelle** et choisissez *latence - Max*. Définissez les filtres que vous souhaitez ou laissez **Filter by** vide. Pour **faire un cumul**, choisissez *sum* par *All*. Afficher ces données sous la forme d'un *Line Chart* et laisser *y-Axis* comme *Primary*.
5. Cliquez sur le bouton **[+Query]** pour ajouter une seconde ligne de données. Pour cette ligne, sélectionnez *VMDK* et *latence - Max*. Définissez les filtres que vous souhaitez ou laissez **Filter by** vide. Pour **faire un cumul**, choisissez *sum* par *All*. Afficher ces données sous la forme d'un *Line Chart* et laisser *y-Axis* comme *Primary*.
6. Cliquez sur **[Save]** pour ajouter ce widget au tableau de bord.



Nous allons ensuite ajouter un graphique illustrant le nombre total d'IOPS, lecture, écriture et lecture de VM dans un seul graphique.

1. Cliquez sur l'icône **[Ajouter widget]** et sélectionnez *Area Chart* pour ajouter un nouveau widget graphique de zone au tableau de bord.
2. La boîte de dialogue Modifier le widget s'ouvre. Nommez ce widget « VM IOPS »
3. Sélectionnez **Virtual machine** et choisissez *IOPS - Total*. Définissez les filtres que vous souhaitez ou laissez **Filtrer par** vide. Pour **cumul**, choisissez *somme* par *tout*. Afficher ces données sous la forme d'un *Area Chart* et laisser *y-Axis* sous la forme *Primary*.
4. Cliquez sur le bouton **[+Query]** pour ajouter une seconde ligne de données. Pour cette ligne, sélectionnez **Virtual machine** et choisissez *IOPS - Read*.
5. Cliquez sur le bouton **[+Query]** pour ajouter une troisième ligne de données. Pour cette ligne, sélectionnez **Virtual machine** et choisissez *IOPS - Write*.
6. Cliquez sur **Afficher la légende** pour afficher une légende pour ce widget sur le tableau de bord.



1. Cliquez sur **[Save]** pour ajouter ce widget au tableau de bord.

Nous allons ensuite ajouter un tableau illustrant le débit des ordinateurs virtuels pour chaque application associée à la machine virtuelle. Nous allons utiliser la fonction d'enroulement pour cela.

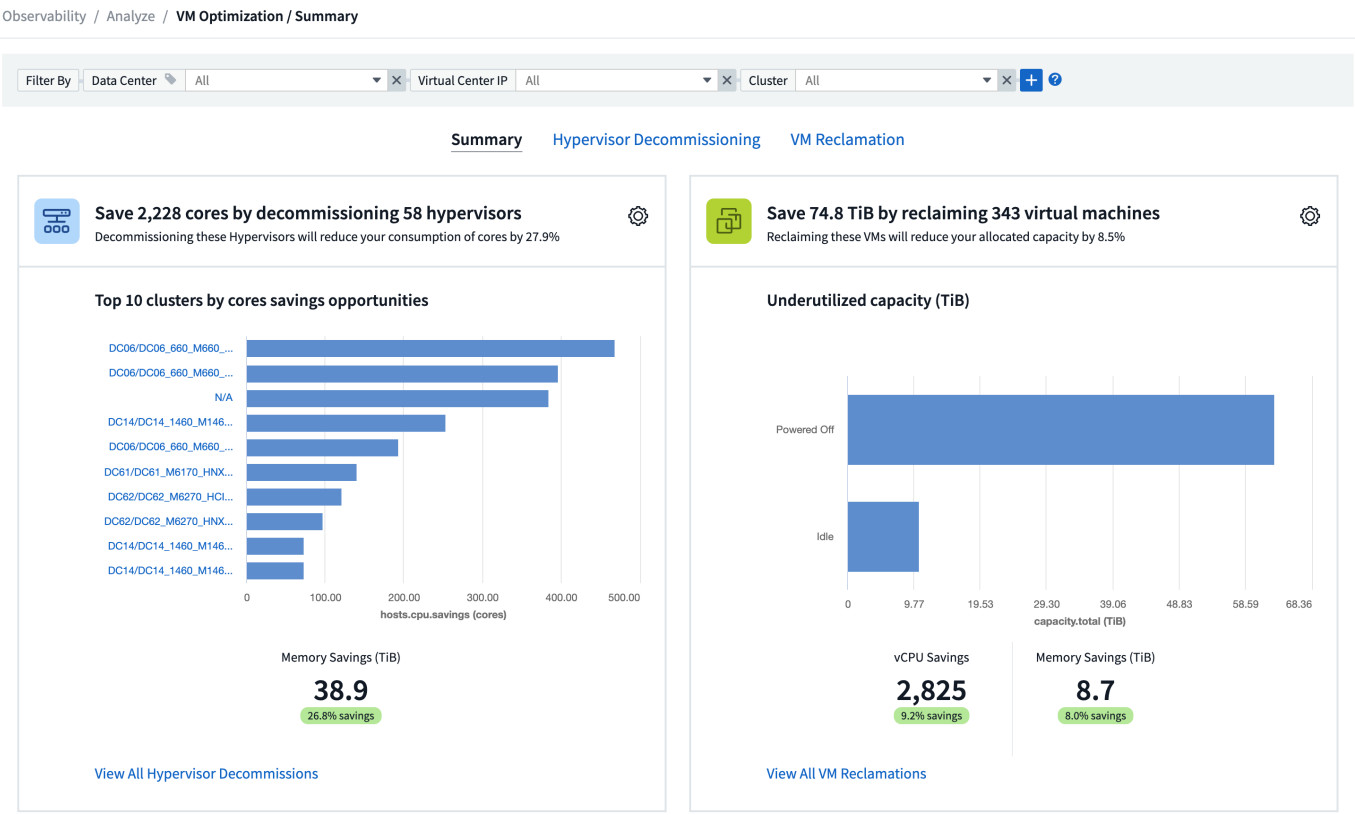
1. Cliquez sur l'icône **[Add widget]** et sélectionnez *Line Chart* pour ajouter un nouveau widget graphique en ligne au tableau de bord.
2. La boîte de dialogue Modifier le widget s'ouvre. Nommez ce widget « VM Throughput by application »
3. Sélectionnez Virtual machine (ordinateur virtuel) et choisissez Throughput - Total. Définissez les filtres que vous souhaitez ou laissez le filtre vide. Pour faire un cumul, choisissez « Max » et sélectionnez par « application » ou « Nom ». Afficher les 10 principales applications. Affichez ces données sous forme de graphique linéaire et laissez l'axe y comme principal.
4. Cliquez sur **[Save]** pour ajouter ce widget au tableau de bord.

Vous pouvez déplacer les 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.

Une fois vos modifications effectuées, assurez-vous que **[Save]** est le tableau de bord.

Votre tableau de bord final des performances VM se présente comme suit :



Meilleures pratiques pour les tableaux de bord et les widgets

Conseils et astuces pour vous aider à tirer le meilleur parti des fonctionnalités puissantes des tableaux de bord et des widgets.

Trouver la mesure appropriée

Data Infrastructure Insights acquiert des compteurs et des metrics à l'aide de noms qui diffèrent parfois du collecteur de données au collecteur de données.

Lorsque vous recherchez la mesure ou le compteur adéquat pour votre widget tableau de bord, gardez à l'esprit que la mesure souhaitée peut être sous un nom différent de celui que vous pensez. Bien que les listes déroulantes de Data Infrastructure Insights soient généralement alphabétiques, il arrive parfois qu'un terme ne s'affiche pas dans la liste à l'endroit où vous pensez qu'il devrait. Par exemple, les termes « capacité brute » et « capacité utilisée » n'apparaissent pas 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 colonne pour trouver ce que vous recherchez. Par exemple, une recherche portant sur « Cap » indique tous les metrics dont le nom contient « capacité », quel que soit l'endroit où ils se trouvent dans la liste. Vous pouvez ensuite facilement sélectionner les mesures souhaitées dans cette liste plus courte.

Voici quelques phrases alternatives que vous pouvez essayer lors de la recherche de mesures :

Quand vous voulez trouver :	Essayez également de rechercher :
CPU	Processeur

Capacité	Capacité utilisée capacité brute provisionnée capacité provisionnée pools de stockage capacité <autre type d'actif> capacité écrite
Vitesse du disque	Vitesse de disque la plus faible du 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 <autre type de ressource> Nom simple Nom de ressource alias de structure
Lecture / écriture	IOPS en attente de lecture partielle - latence de la capacité d'écriture - utilisation du cache de lecture - lecture
Ordinateur virtuel	La machine virtuelle est virtuel

Cette liste n'est pas exhaustive. Voici quelques exemples de termes de recherche possibles uniquement.

Trouver les bonnes ressources

Les ressources que vous pouvez référencer dans les filtres de widget et les recherches varient d'un type d'actif à l'autre.

Dans les tableaux de bord et les pages de ressources, le type de ressource autour duquel vous créez votre widget détermine les autres compteurs de types de ressources pour lesquels vous pouvez filtrer ou ajouter une colonne. Tenez compte des éléments suivants lors de la création de votre widget :

Ce type/compteur d'actifs :	Peut être filtré pour sous ces actifs :
Ordinateur virtuel	VMDK
Datastore(s)	Volume interne VMDK Virtual machine Volume
Hyperviseur	La machine virtuelle est l'hôte de l'hyperviseur
Hôte(s)	Ordinateur virtuel hôte de volume Volume Cluster interne
Structure	Port

Cette liste n'est pas exhaustive.

Meilleure pratique: Si vous filtrez pour 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 tracé de diffusion : connaissance de l'axe

La modification de l'ordre des compteurs dans un widget de tracé de dispersion modifie les axes sur lesquels les données sont affichées.

Description de la tâche

Cet exemple va créer un tracé de dispersion qui vous permettra de voir des VM sous-performants présentant une latence élevée par rapport à un nombre d'opérations d'entrée/sortie par seconde faible.

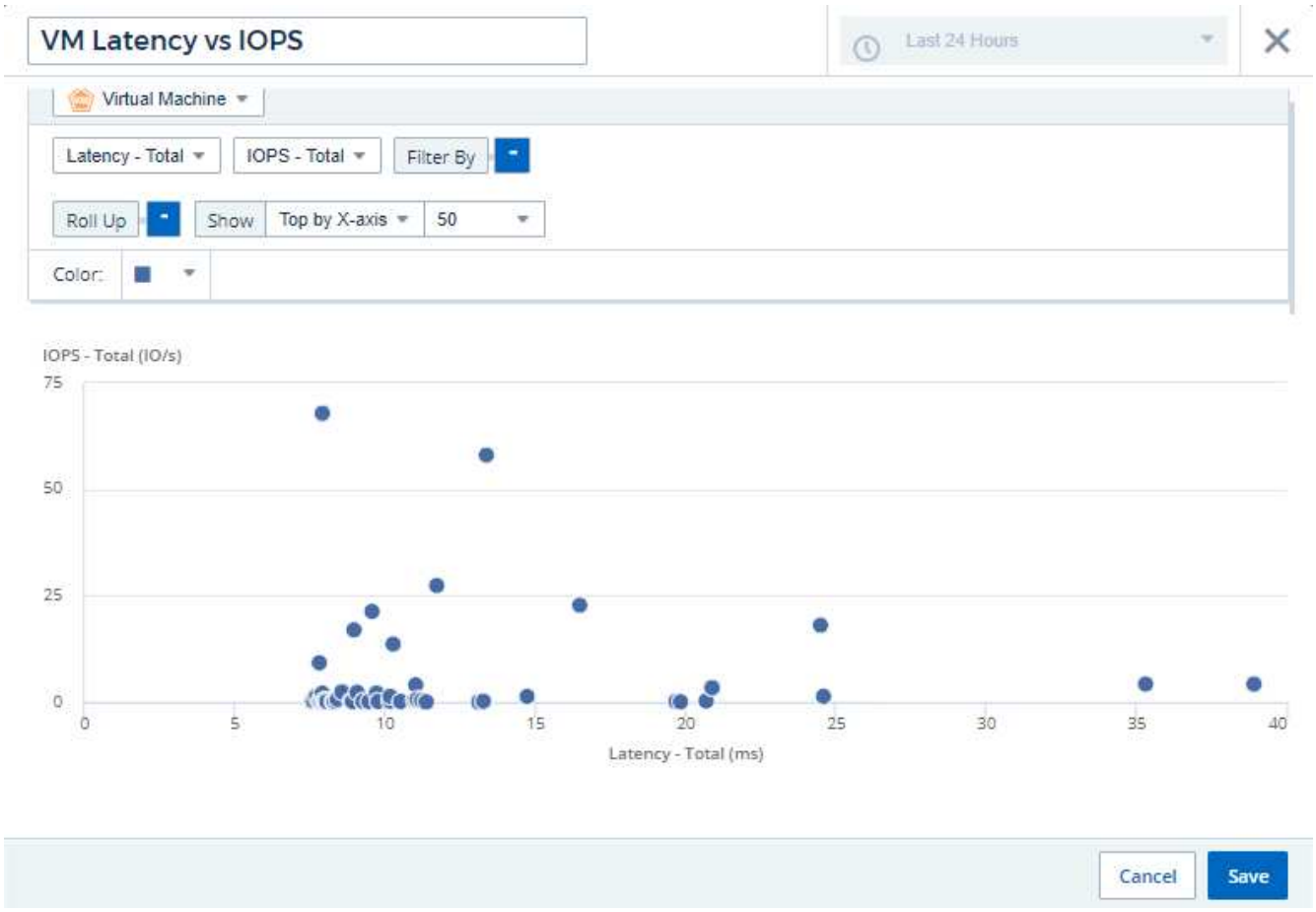
Étapes

1. Créez ou ouvrez un tableau de bord en mode édition et ajoutez un widget graphique graphique graphique * Scatter.
2. Sélectionnez un type d'actif, par exemple *Virtual machine*.
3. Sélectionnez le premier compteur à tracer. Dans cet exemple, sélectionnez *latence - Total*.

   Latence - Total est transcrit le long de l'axe X du graphique.

4. Sélectionnez le second compteur à tracer. Dans cet exemple, sélectionnez *IOPS - Total*.

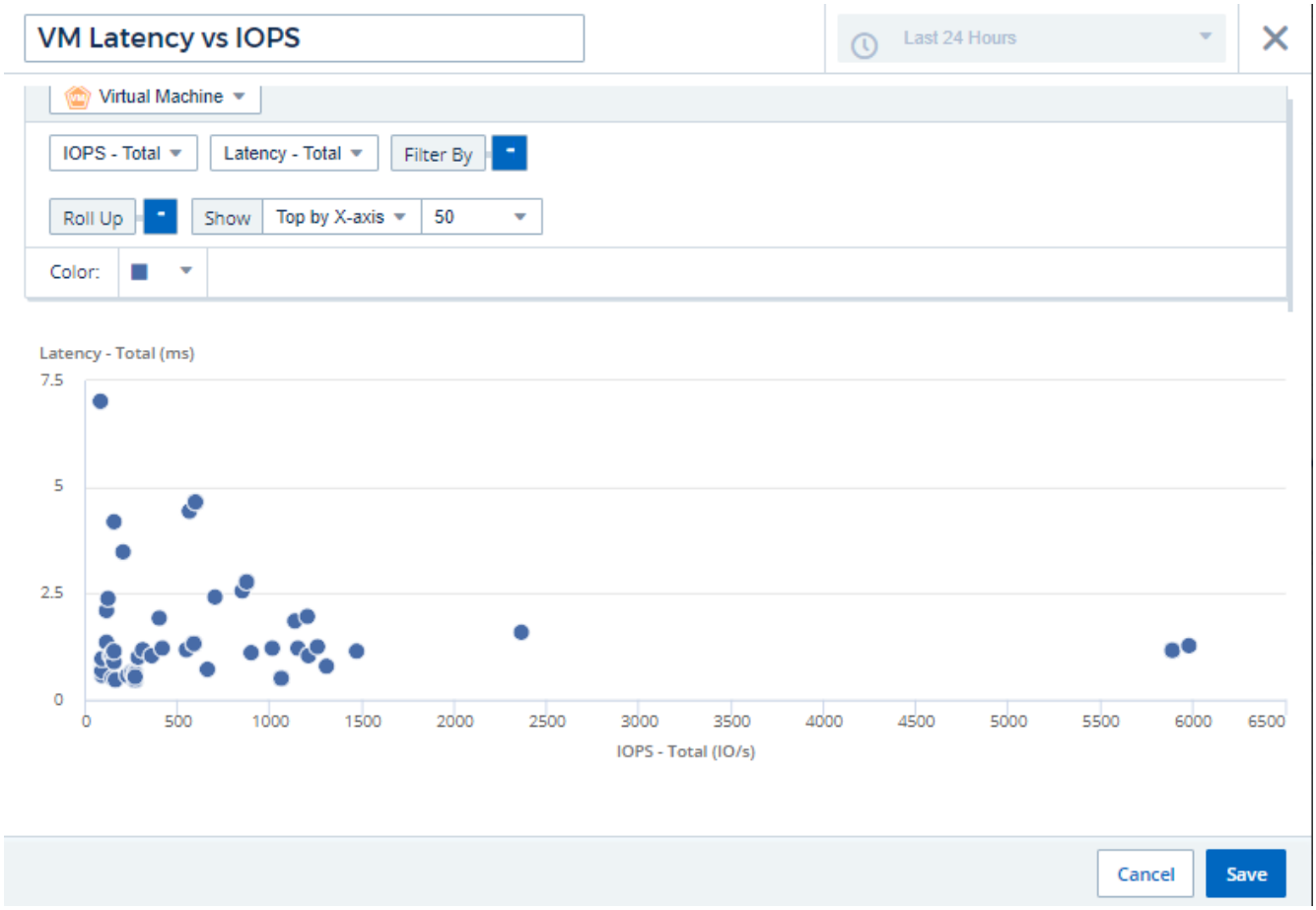
   IOPS - Total est transcrit le long de l'axe y dans le graphique. Les machines virtuelles avec latence plus élevée s'affichent à droite du graphique. Seules les 100 machines virtuelles à latence la plus élevée sont affichées, car le paramètre **Top by X-AXIS** est actuel.



5. Inversez maintenant l'ordre des compteurs en réglant le premier compteur sur *IOPS - Total* et le second sur *latence - Total*.

   Latence- Total est maintenant transcrit le long de l'axe y dans le graphique, et *IOPS - Total* le long de l'axe X. Les machines virtuelles dont les IOPS sont plus élevées s'affichent à droite du tableau.

   Notez que, étant donné que nous n'avons pas modifié le paramètre **Top by X-Axis**, le widget affiche désormais les 100 meilleures machines virtuelles IOPS, car c'est ce qui est actuellement tracé le long de l'axe X.



Vous pouvez choisir d'afficher le N supérieur par axe X, le N supérieur par axe y, le N inférieur par axe X ou le N inférieur par axe Y. Dans notre dernier exemple, le graphique affiche les 100 meilleures machines virtuelles qui présentent le nombre total d'IOPS le plus élevé. Si nous le changerons **Top by y-AXIS**, le graphique affichera à nouveau les 100 meilleures machines virtuelles ayant la latence totale la plus élevée.

Notez que dans un graphique de diagramme de dispersion, vous pouvez cliquer sur un point pour accéder à la page de ressource de cette ressource.

Utilisation des requêtes

Ressources utilisées dans les requêtes

Les requêtes vous permettent de surveiller et de dépanner votre réseau en recherchant les ressources et les mesures de votre locataire à un niveau granulaire basé sur des critères sélectionnés par l'utilisateur (par exemple, les annotations).

Notez que les règles d'annotation, qui attribuent automatiquement des annotations aux ressources, *exigent* une requête.

Vous pouvez interroger les ressources d'inventaire physiques ou virtuelles (et leurs metrics associés) sur votre locataire, ou les metrics fournis avec l'intégration, comme Kubernetes ou ONTAP Advanced Data.

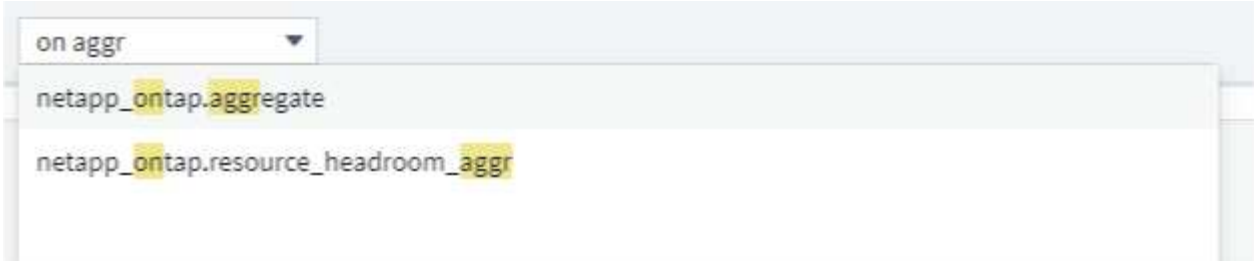
Inventaire des actifs

Les types de ressources suivants peuvent être utilisés dans les requêtes, les widgets de tableau de bord et les pages d'accueil personnalisées des ressources. Les champs et compteurs disponibles pour les filtres, les expressions et l'affichage varient selon les types d'actifs. Toutes les ressources ne peuvent pas être utilisées dans tous les types de widget.

- Client supplémentaire
- Datastore
- Disque
- Structure
- Périphérique générique
- Hôte
- Volume interne
- Session iSCSI
- Portail réseau iSCSI
- Chemin
- Port
- Qtree
- Quota
- Partagez
- Stockage
- Nœud de stockage
- Pool de stockage
- Storage Virtual machine (SVM)
- Commutateur
- Bande
- VMDK
- Ordinateur virtuel
- Volumétrie
- Zone
- Membre de la zone

Métriques d'intégration

Outre les requêtes relatives aux ressources d'inventaire et aux mesures de performances associées, vous pouvez également effectuer des requêtes pour des indicateurs **de données d'intégration**, tels que ceux générés par Kubernetes ou Docker, ou fournis avec les métriques avancées de ONTAP.



Création de requêtes

Les requêtes vous permettent de rechercher les ressources de votre locataire à un niveau granulaire, ce qui vous permet de filtrer les données que vous souhaitez et de trier les résultats selon vos préférences.

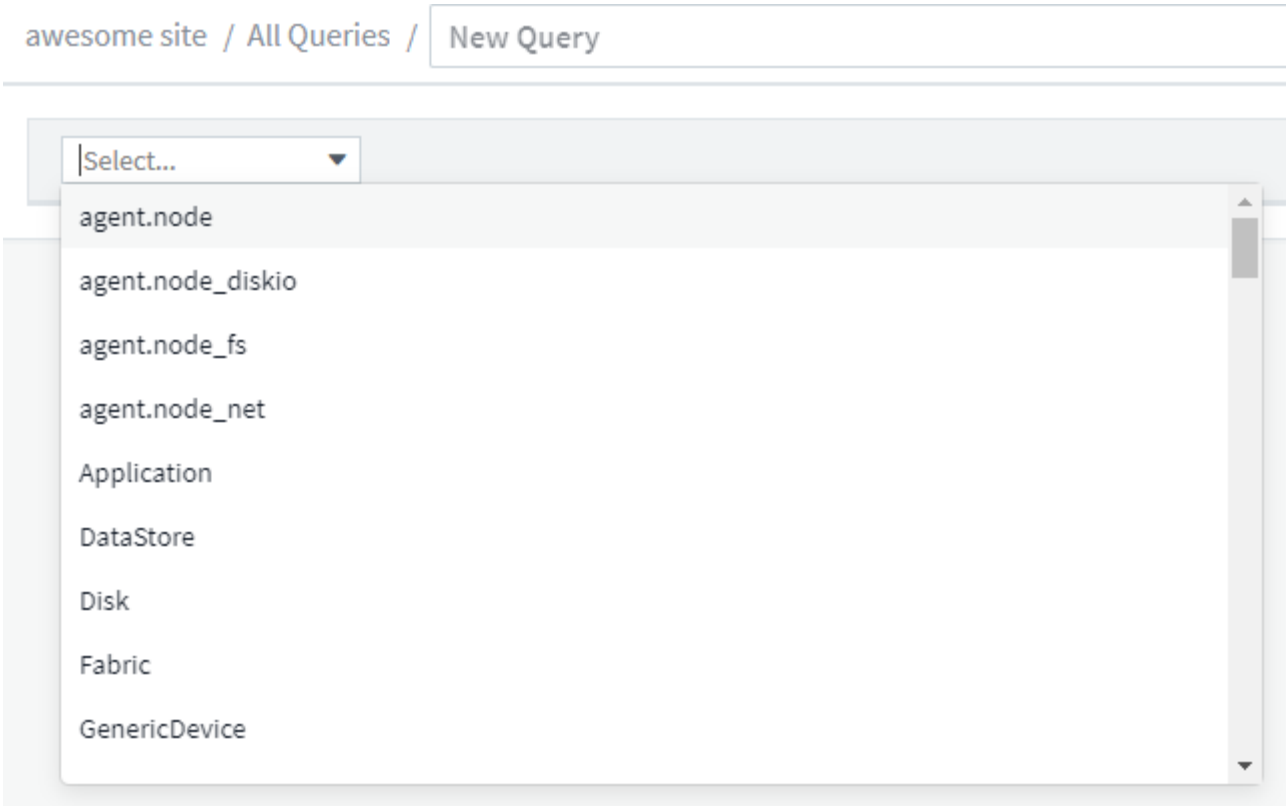
Par exemple, vous pouvez créer une requête pour *volumes*, ajouter un filtre pour trouver des *stockages* particuliers associés aux volumes sélectionnés, ajouter un autre filtre pour trouver une *annotation* particulière, par exemple "Tier 1" dans les stockages sélectionnés, Et enfin, ajoutez un autre filtre pour trouver tous les stockages avec *IOPS - Read (IO/s)* supérieur à 25. Lorsque les résultats sont affichés, vous pouvez trier les colonnes d'informations associées à la requête dans l'ordre croissant ou décroissant.

Remarque : lorsqu'un nouveau collecteur de données est ajouté qui acquiert des ressources ou que des annotations ou des affectations d'application sont effectuées, vous pouvez interroger ces nouveaux actifs, annotations ou applications uniquement après l'indexation des requêtes. L'indexation a lieu à un intervalle planifié régulièrement ou pendant certains événements tels que l'exécution de règles d'annotation.

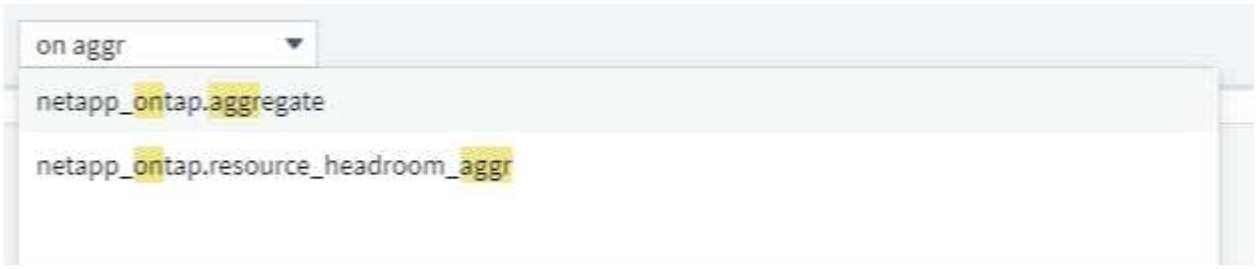
La création d'une requête est très simple :

1. Accédez à **requêtes > *+Nouvelle requête**.
2. Dans la liste 'Sélectionner…', sélectionnez le type d'objet à rechercher. Vous pouvez faire défiler la liste ou commencer à taper pour trouver plus rapidement ce que vous recherchez.

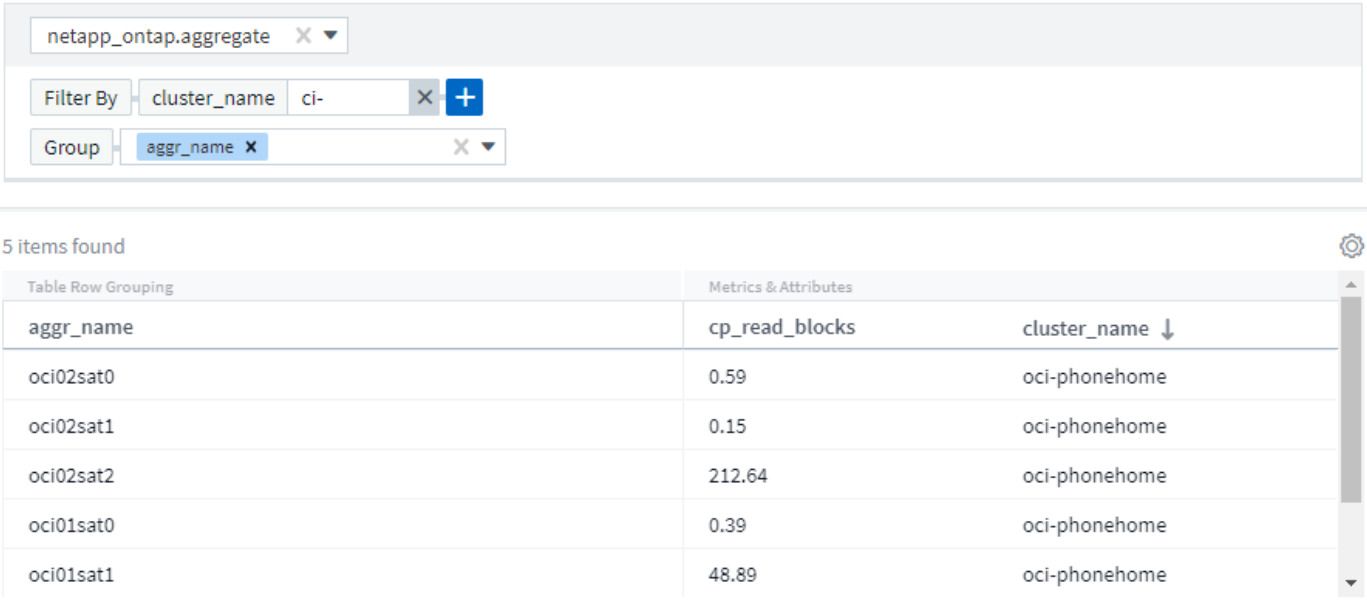
Liste de défilement :



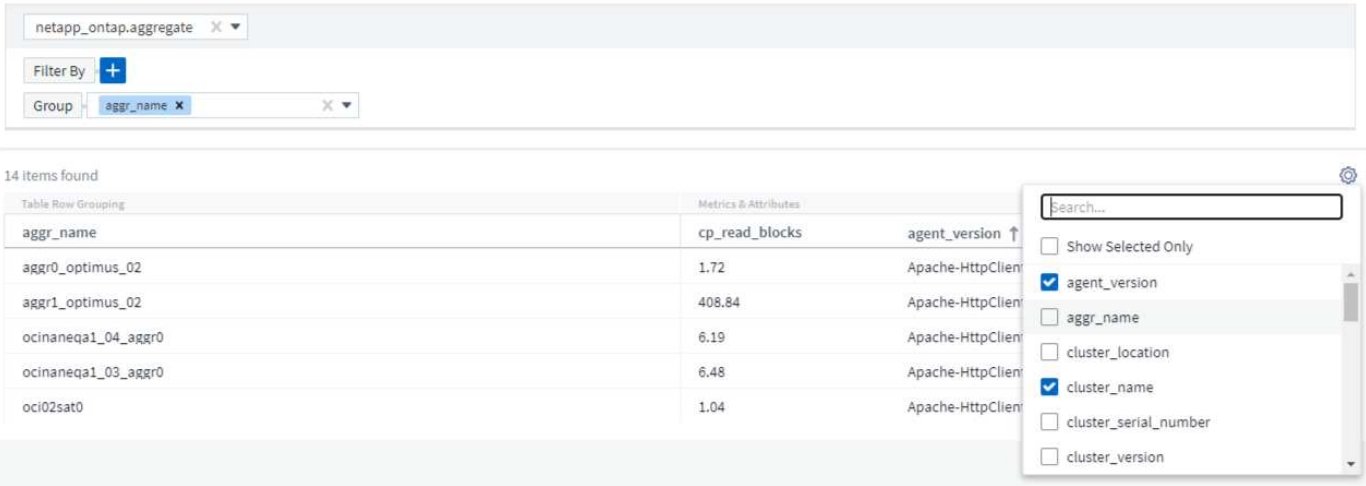
Type à rechercher :



Vous pouvez ajouter des filtres pour affiner davantage votre requête en cliquant sur le bouton **+** dans le champ **Filtrer par**. Grouper les lignes par objet ou attribut. Lorsque vous utilisez 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 engrenage à droite du tableau. Les colonnes disponibles varient en fonction du type de ressource/mesure.



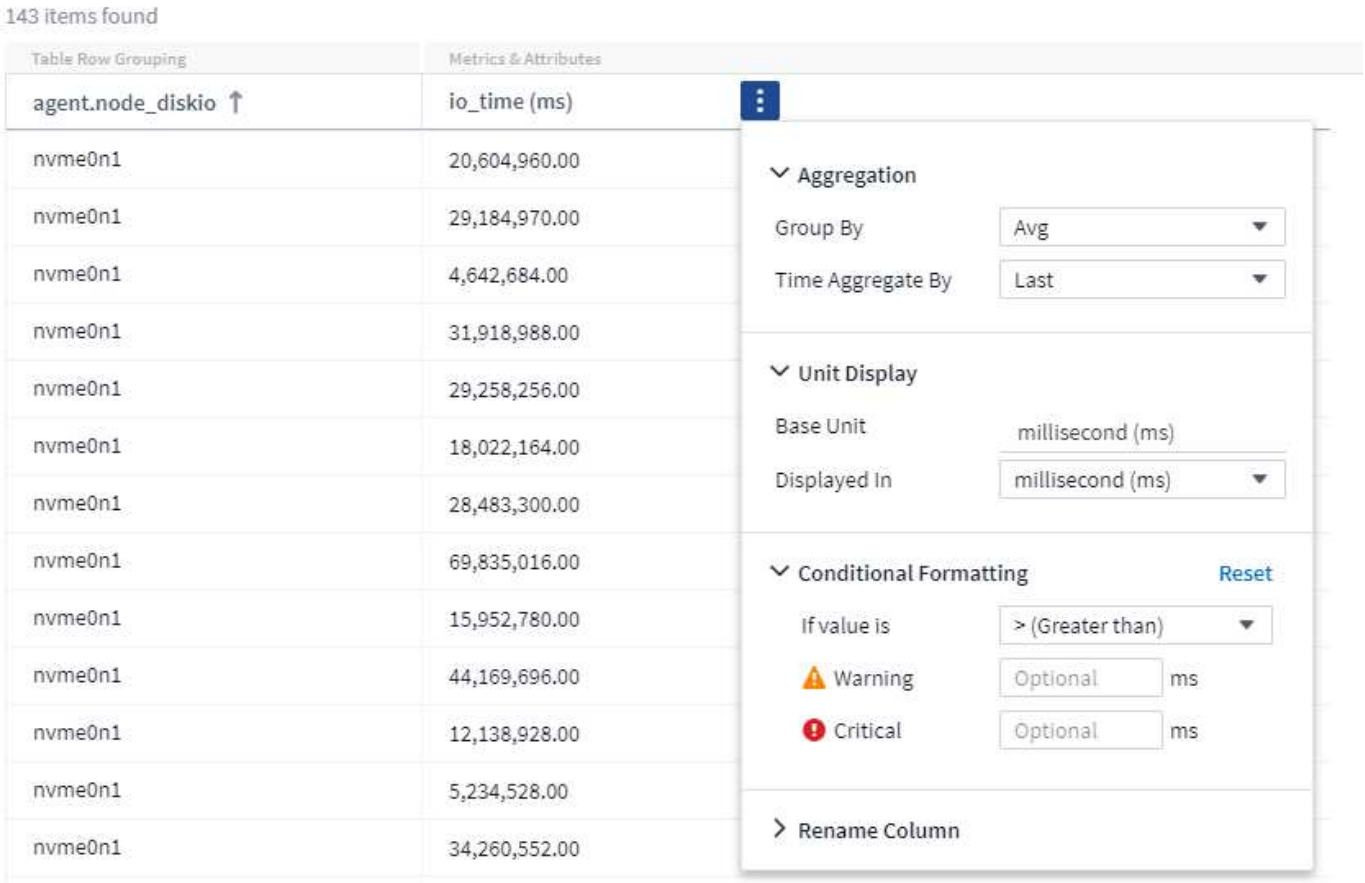
Voyez-le en action

"Explorez et analysez avec des requêtes dans Data Infrastructure Insights (vidéo)"

Choisissez agrégation, unités, 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 et en sélectionnant les unités dans lesquelles ces valeurs sont affichées. Ces options sont disponibles 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 sélectionné affiche la capacité brute et que les valeurs s'affichent en Gio, mais que vous préférez les afficher en Tio, sélectionnez simplement Tio dans la liste déroulante Affichage des unités.

Agrégation

Par le même jeton, si les valeurs affichées sont agrégées à partir des données sous-jacentes sous la forme « moyenne », Mais vous préférez afficher la somme de toutes les valeurs, sélectionnez « somme » dans la liste déroulante *regrouper par* (si vous voulez que des valeurs groupées affichent les sommes) ou dans la liste déroulante *Time Aggregate by* (si vous voulez que les valeurs de ligne affichent des sommes de données sous-jacentes).

Vous pouvez choisir d'agréger des points de données groupés par *AVG, Max, min ou SUM*.

Vous pouvez agréger des données de ligne 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 Avertissement et critique dans la liste des résultats de la requête, ce qui apporte une visibilité instantanée sur les valeurs aberrantes et les points de données exceptionnels.



Le formatage conditionnel est défini séparément pour chaque colonne. Par exemple, vous pouvez choisir un ensemble de seuils pour une colonne de capacité et un autre 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.

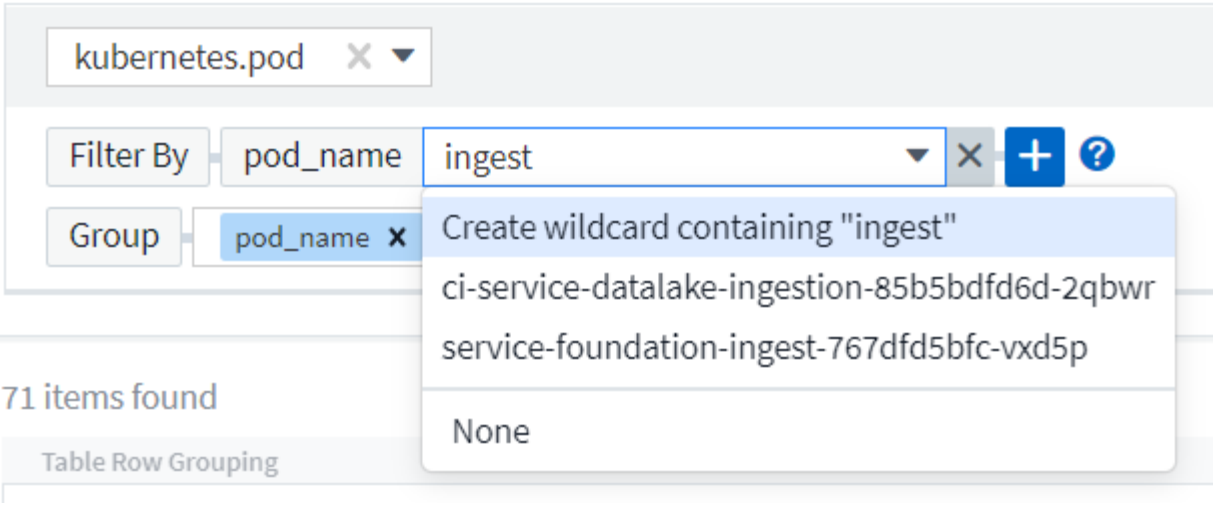
Économisez

Une fois que vous avez configuré votre requête pour afficher les résultats souhaités, vous pouvez cliquer sur le bouton **Enregistrer** pour enregistrer la requête en vue d'une utilisation ultérieure. Donnez-lui un nom unique et significatif.

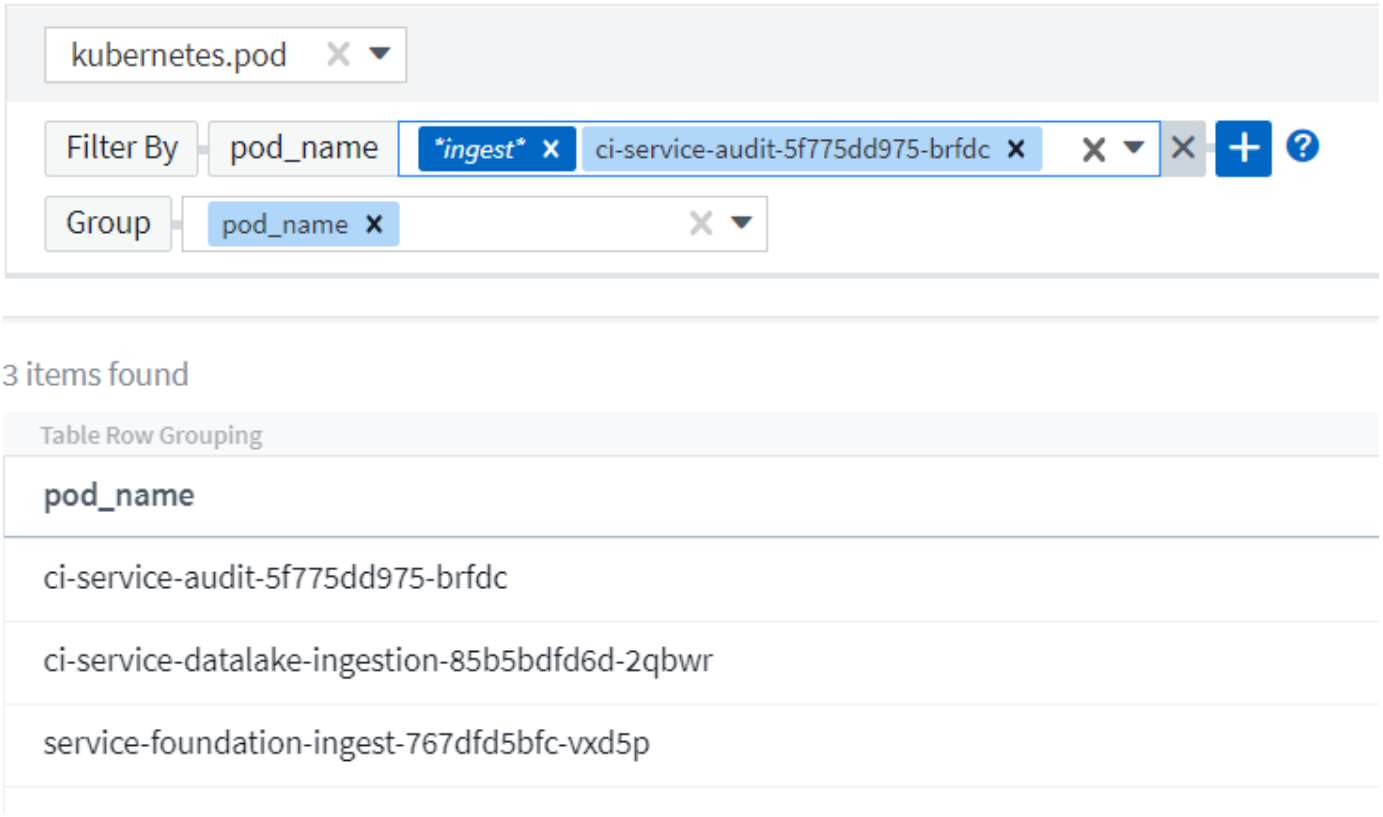
Plus d'informations sur le filtrage

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 taper, vous avez la possibilité de créer un **filtre générique** basé sur le texte en cours. Si vous sélectionnez cette option, tous les résultats correspondant à l'expression de caractère générique seront résélectionnés. Vous pouvez également créer **expressions** à l'aide DE NOT ou OU, ou sélectionner l'option "aucun" pour filtrer les valeurs nulles dans le champ.



Filtres basés sur des caractères génériques ou des expressions (par exemple NON, OU « aucun », etc.) s'affiche en bleu foncé dans le champ du filtre. Les éléments que vous sélectionnez directement dans la liste s'affichent en bleu clair.



Notez que le filtrage des caractères génériques et des expressions fonctionne avec du texte ou des listes, mais pas avec des valeurs numériques, des dates ou des valeurs booléennes.

Raffinage des filtres

Vous pouvez utiliser les éléments suivants pour affiner votre filtre :

Filtre	Ce qu'il fait	Exemple	Résultat

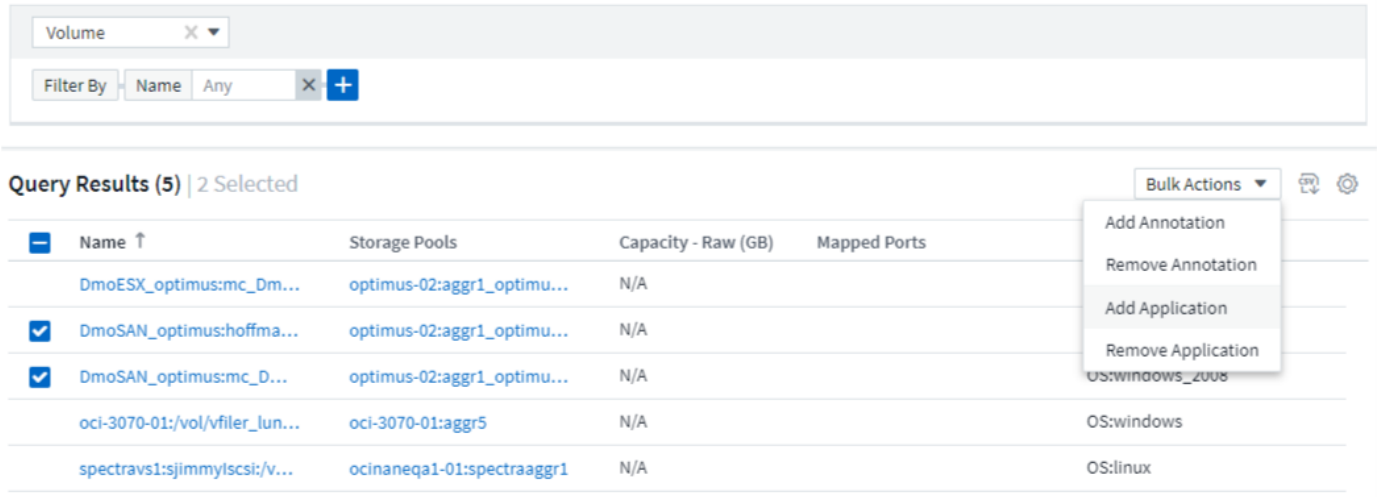
* (Astérisque)	permet de rechercher tout	vol*rhel	renvoie toutes les ressources commençant par « vol » et se terminant par « rhel ».
? (point d'interrogation)	permet de rechercher un nombre spécifique de caractères	BOS-PRD ??-S12	Renvoie BOS-PRD***12*** -S12, BOS-PRD***23***-S12, etc
OU	vous permet de spécifier plusieurs entités	FAS2240 OU CX600 OU FAS3270	Renvoie l'un des modèles FAS2440, CX600 ou FAS3270
PAS	permet d'exclure du texte des résultats de la recherche	PAS EMC*	Elle renvoie tous les éléments qui ne sont pas à l'avant par « EMC ».
Aucun	Recherche les valeurs NULL dans tous les champs	*Aucun*	renvoie les résultats où le champ cible est vide
Pas *	Recherche les valeurs NULL dans les champs *text-only*	Pas *	renvoie les résultats où le champ cible est vide

Si vous placez une chaîne de filtre entre deux guillemets, Insight traite tout entre le premier et le dernier devis comme une correspondance exacte. Tous les caractères spéciaux ou opérateurs situés dans les guillemets seront traités comme des littéraux. Par exemple, le filtrage pour "*" renvoie des résultats qui sont un astérisque littéral ; l'astérisque ne sera pas traité comme un caractère générique dans ce cas. Les opérateurs OU ET NON sont également traités comme des chaînes littérales lorsqu'ils sont entourés de guillemets doubles.

Que dois-je faire maintenant que j'ai des résultats de requête ?

L'interrogation permet d'ajouter des annotations ou d'affecter des applications aux ressources en toute simplicité. Notez que vous pouvez uniquement attribuer des applications ou des annotations à vos ressources d'inventaire (disque, stockage, etc.). Les metrics d'intégration ne peuvent pas prendre en charge les affectations d'annotations ou d'applications.

Pour affecter une annotation ou une application aux ressources résultant de votre requête, sélectionnez la ou les ressources à l'aide de la case à cocher située à gauche du tableau des résultats, puis cliquez sur le bouton **actions groupées** à droite. Choisissez l'action 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 à utiliser. Mais comme vous l'avez vu ci-dessus, les requêtes peuvent être aussi larges ou aussi étroites que vous le souhaitez.

Affichage des requêtes

Vous pouvez afficher vos requêtes pour surveiller vos actifs et modifier la façon dont vos requêtes affichent les données associées à vos ressources.

Étapes

1. Connectez-vous à votre locataire Data Infrastructure Insights.
2. Cliquez sur **requêtes** et sélectionnez **Afficher toutes les requêtes**. Vous pouvez modifier l'affichage des requêtes en effectuant l'une des actions suivantes :
3. Vous pouvez entrer du texte dans la zone de filtre pour rechercher des requêtes spécifiques.
4. Vous pouvez modifier l'ordre de tri des colonnes dans le tableau de requêtes en croissant (flèche vers le haut) ou en descendant (flèche vers le bas) en cliquant sur la flèche dans l'en-tête de colonne.
5. Pour redimensionner une colonne, placez le curseur de la souris sur l'en-tête de la colonne jusqu'à ce qu'une barre bleue s'affiche. 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 colonne et faites-la glisser vers la droite ou vers la gauche.

Lorsque vous faites défiler les résultats de la requête, sachez que les résultats peuvent changer, car Data Infrastructure Insights interroge automatiquement vos collecteurs de données. Cela peut entraîner l'absence de certains éléments ou l'affichage de certains éléments hors de la commande en fonction du mode de tri.

Exportation des résultats de la requête dans un fichier .CSV

Vous pouvez exporter les résultats de n'importe quelle requête dans un fichier .CSV, 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.

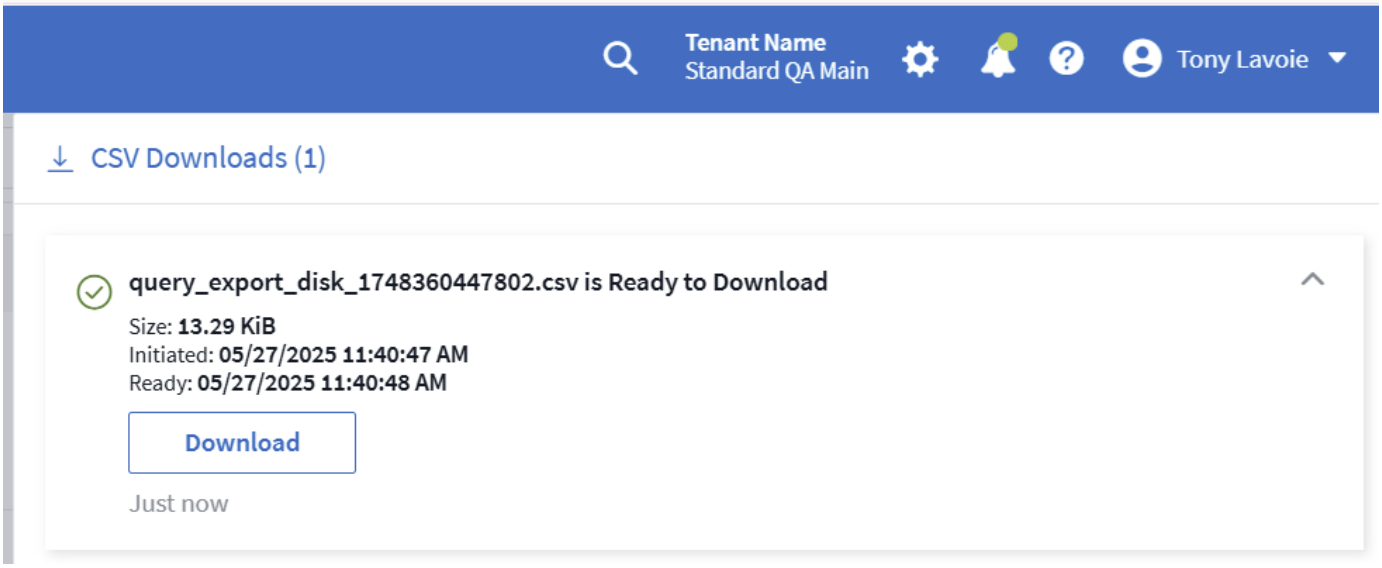
3. Cliquez sur une requête.
4. Cliquez sur pour exporter les résultats de la requête vers un fichier .CSV.

L'exportation au format .CSV est également disponible dans le menu « trois points » des widgets de tableau de bord, ainsi que dans la plupart des tables de pages d'accueil.

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, vous permettant ainsi 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 reflètent le filtrage, les colonnes et les noms de colonne affichés.

Virgules dans les noms d'actifs

Remarque : lorsqu'une virgule apparaît dans le nom d'un bien, l'exportation enferme le nom dans les guillemets, en préservant le nom du bien 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 d'un deux-points suivi de deux autres chiffres), Excel interprète parfois ce nom comme un format d'heure, au lieu du format texte. Cela peut entraîner l'affichage dans Excel de valeurs incorrectes dans ces colonnes. Par exemple, un objet nommé "81:45" s'affichera dans Excel comme "81:45:00".

Pour contourner ce problème, importez le fichier .CSV dans Excel en procédant comme suit :

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 » pour le délimiteur et cliquez sur Suivant.
6. Sélectionnez les colonnes souhaitées et choisissez "texte" pour le format de données de la colonne.
7. Cliquez sur Terminer.

   Vos objets doivent s'afficher dans Excel au format approprié.

Modification ou suppression d'une requête

Vous pouvez modifier les critères qui sont associés à une requête lorsque vous voulez modifier les critères de recherche des ressources que vous interrogez.

Modification d'une requête

Étapes

1. Cliquez sur **Explorer** et sélectionnez **toutes les requêtes 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 mesure ou un attribut dans la liste.

Lorsque 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 la liste déroulante en regard du bouton **Enregistrer** et sélectionnez **Enregistrer sous** pour enregistrer la requête sous un autre nom. Cette opération n'écrase pas la requête d'origine.
- Cliquez sur la liste déroulante en regard du bouton **Enregistrer** et sélectionnez **Renommer** pour modifier le nom de la requête que vous avez utilisée initialement. Ceci écrase la requête d'origine.
- Cliquez sur la liste déroulante en regard du bouton **Enregistrer** et sélectionnez **Ignorer 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**.

Attribution ou suppression de plusieurs applications à des ressources ou à des applications multiples

Vous pouvez affecter plusieurs "en termes de latence"applications à des ressources ou en supprimer en utilisant une requête au lieu de devoir les affecter ou les supprimer manuellement.

Vous pouvez utiliser ces étapes pour ajouter ou supprimer de "annotations"la même manière.

Avant de commencer

Vous devez avoir déjà créé une requête qui trouve toutes les ressources à modifier.

Étapes

1. Cliquez sur **Explorer** et sélectionnez **requêtes métriques**.

   La page requêtes s'affiche.

2. Cliquez sur le nom de la requête qui trouve les ressources.

   La liste des actifs associés à la requête s'affiche.

3. Sélectionnez les ressources souhaitées dans la liste ou cliquez sur la case supérieure pour tout sélectionner.

   La liste déroulante actions groupées 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, mais vous ne pouvez sélectionner qu'une seule application pour un volume ou un partage.

6. Cliquez sur **Enregistrer**.
7. Pour supprimer une application affectée 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 la ressource dérivées d'une autre ressource. Par exemple, les volumes héritent des applications des hôtes. Lorsque de nouvelles applications sont attribuées à un volume, la nouvelle application est prioritaire sur l'application dérivée.

Après avoir cliqué sur *Save* sur un ajout en bloc ou sur *Remove* sur une action de suppression en bloc, Data Infrastructure Insights vous informe que l'action prendra un certain temps. Vous pouvez ignorer ce message ; l'action se poursuit en arrière-plan.

Pour les environnements disposant d'un grand nombre de ressources associées, l'héritage des affectations d'applications peut prendre plusieurs minutes. Veuillez laisser plus de temps à l'héritage si vous disposez de nombreux biens connexes.

Copie des valeurs de table

Vous pouvez copier des valeurs dans les tableaux dans le presse-papiers pour les utiliser dans les zones de recherche ou dans d'autres applications.

Description de la tâche

Vous pouvez utiliser deux méthodes pour copier des valeurs des tableaux ou des résultats de requête dans le presse-papiers.

Étapes

1. Méthode 1 : mettez en surbrillance le texte souhaité à l'aide de la souris, copiez-le et collez-le dans des champs de recherche ou dans d'autres applications.
2. Méthode 2 : pour les champs à valeur unique, placez le pointeur de la souris sur le champ et cliquez sur l'icône du presse-papiers qui s'affiche. La valeur est copiée dans le presse-papiers pour être utilisée dans les champs de recherche ou dans d'autres applications.

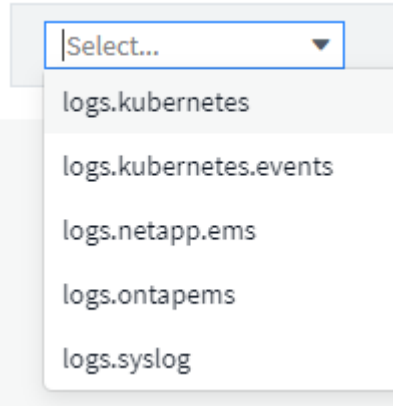
   Notez que seules les valeurs qui sont des liens vers des ressources peuvent être copiées à l'aide de cette méthode. Seuls les champs contenant des valeurs uniques (c'est-à-dire des non-listes) possèdent l'icône de copie.

Explorateur de journaux

Data Infrastructure Insights Log Explorer est un outil puissant d'interrogation des journaux système. En plus de vous aider dans les enquêtes, vous pouvez également enregistrer une requête de journal dans un moniteur afin de 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.

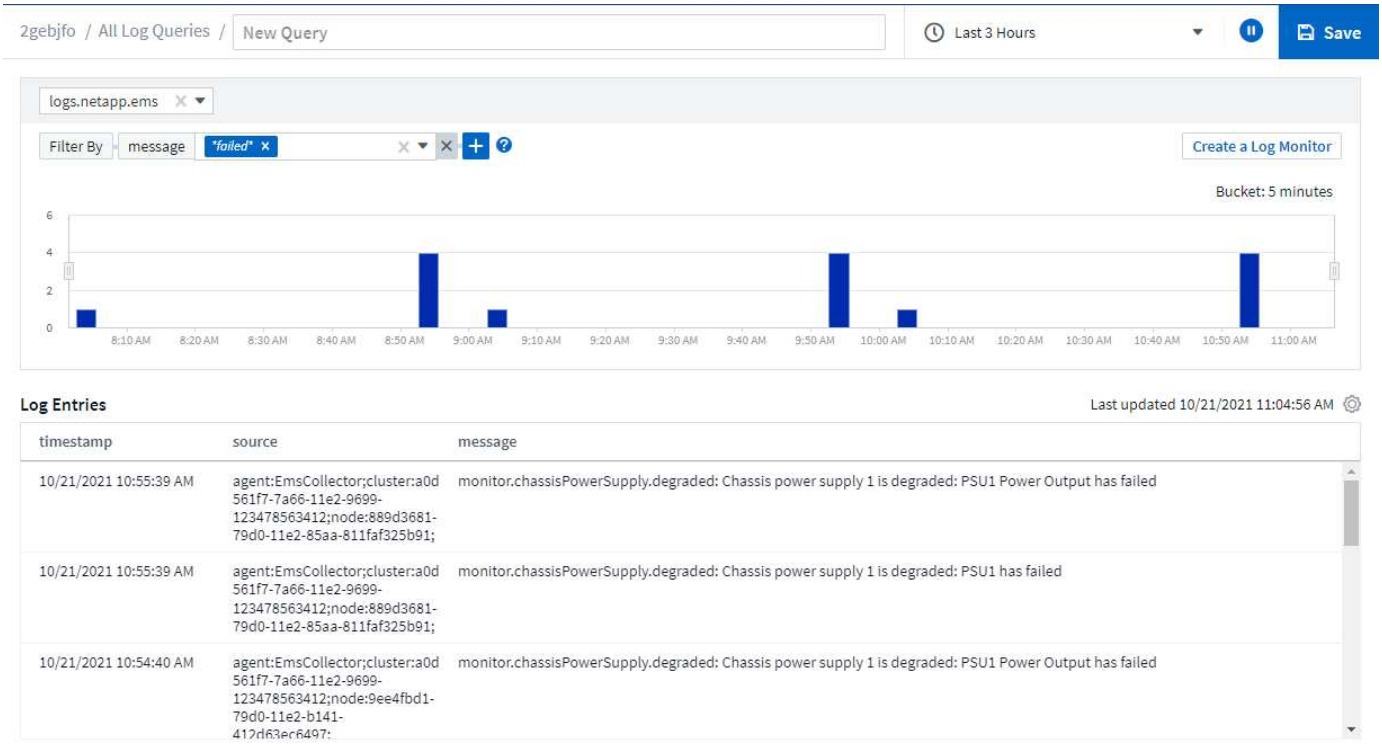


Les types de journaux disponibles pour les requêtes peuvent varier en fonction de votre environnement. D'autres types de journaux peuvent être ajoutés au fil du temps.

Vous pouvez définir des filtres pour affiner davantage les résultats de la requête. Par exemple, pour rechercher tous les messages de journal affichant une défaillance, 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 invite à créer une recherche générique contenant la chaîne au fur et à mesure de la saisie.

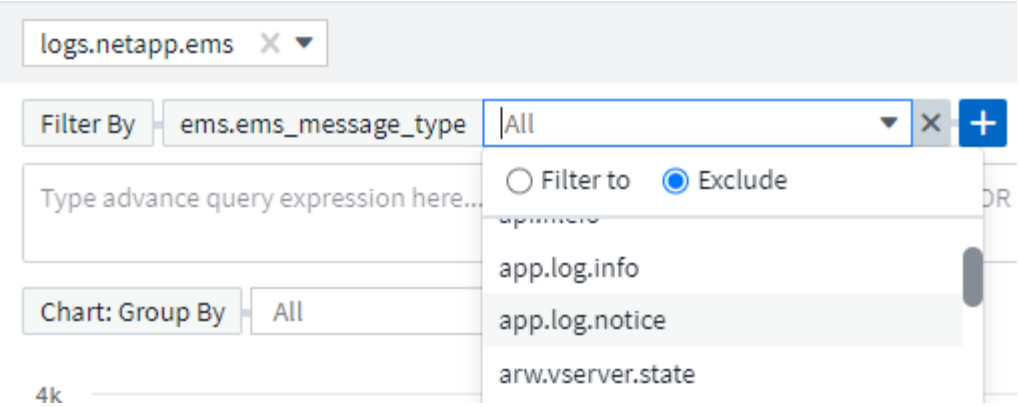
Les résultats s'affichent dans un graphique indiquant le nombre d'instances de journal pour chaque période affichée. Sous le graphique se trouvent les entrées du journal temindividus. Le graphique et les entrées se réactualisent automatiquement en fonction de la plage horaire sélectionnée.



Filtrage

Inclure / exclure

Lorsque vous filtrez les journaux, vous pouvez choisir d'inclure **les chaînes que vous tapez (c'est-à-dire "Filtrer vers") ou *les exclure**. Les chaînes exclues sont affichées dans le filtre terminé sous la forme « NOT <string> ».



Filtres basés sur des caractères génériques ou des expressions (par exemple NON, OU « aucun », etc.) s'affiche en bleu foncé dans le champ du filtre. Les éléments que vous sélectionnez directement dans la liste s'affichent en bleu clair.

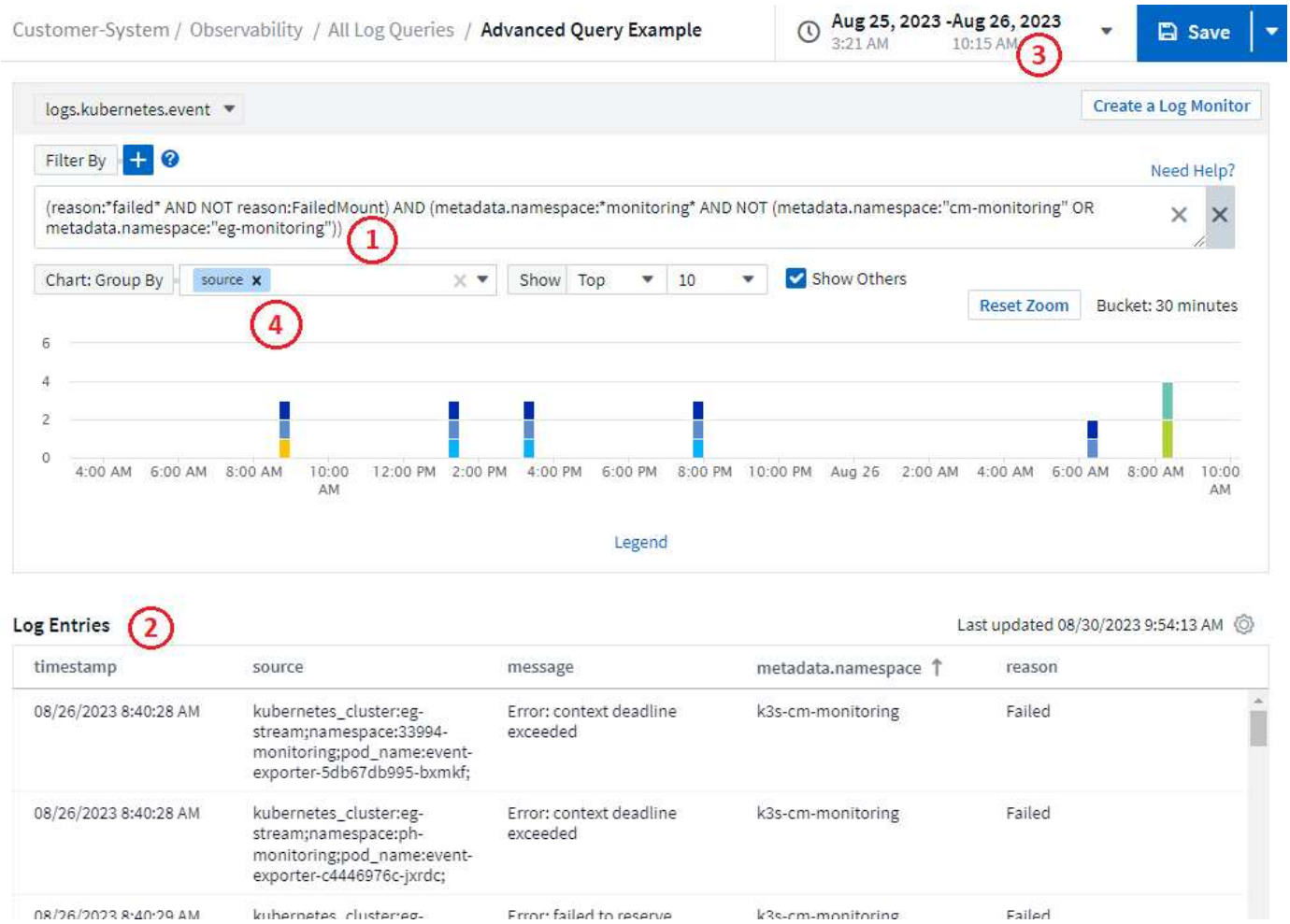
A tout moment, vous pouvez cliquer sur *Créer un moniteur de journal* pour créer un nouveau moniteur basé sur le filtre actuel.

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 taper, vous avez la possibilité de créer un **filtre générique** basé sur le texte en cours. Si vous sélectionnez cette option, tous les résultats correspondant à l'expression de caractère générique seront résélectionnés. Vous pouvez également créer des expressions à l'aide de NOT, AND, or ou, ou vous pouvez sélectionner l'option « aucun » pour filtrer les valeurs nulles.

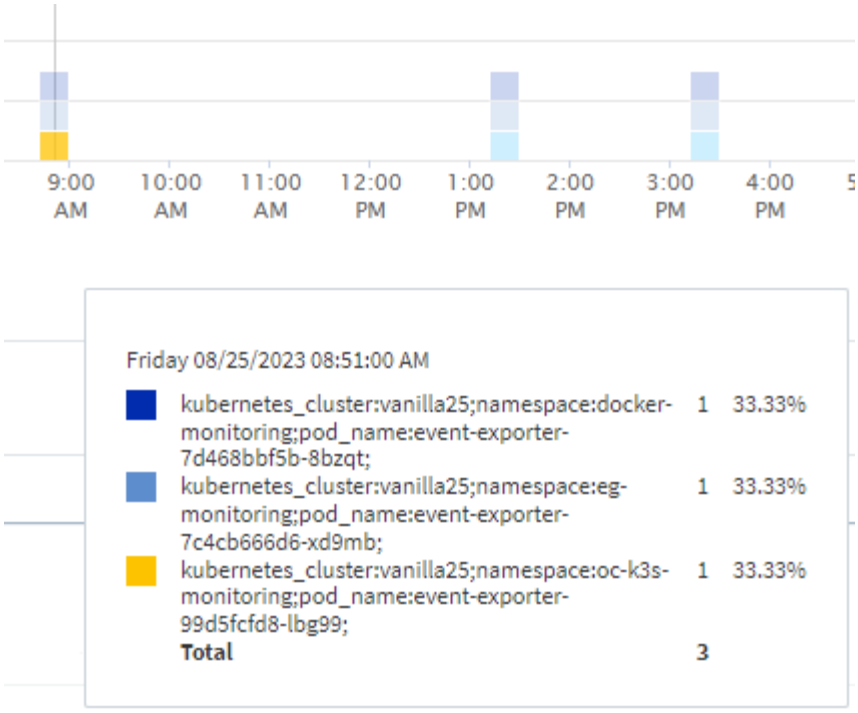
Assurez-vous d'enregistrer votre requête tôt et souvent lorsque vous créez votre filtrage. Advanced Querying est une entrée de chaîne de "forme libre", et des erreurs d'analyse peuvent se produire au fur et à mesure que vous construisez.

Jetez un coup d'œil à cette image d'écran affichant les résultats filtrés pour une requête avancée du journal *logs.kubernetes.event*. Il y a beaucoup de choses dans cette page, qui est expliquée ci-dessous l'image:



1. Cette chaîne de requête avancée filtre les éléments suivants :
   - Filtrer les entrées de journal avec un *motif* qui inclut le mot "échec", mais pas n'importe quoi avec la raison spécifique de "FailedMount".
   - Incluez toutes les entrées qui incluent également un *metadata.namespace* incluant le mot "monitoring", mais excluez les espaces de noms spécifiques de "cm-monitoring" ou "EG-monitoring".

     Notez que, dans le cas ci-dessus, étant donné que "cm-monitoring" et "EG-monitoring" contiennent un tiret ("-"), les chaînes doivent être incluses entre guillemets ou 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 les valeurs « Filtrer par » ET le filtre de requête avancée, sont affichés dans la liste des résultats. La liste peut être triée par colonnes affichées. Pour afficher des colonnes supplémentaires, sélectionner l'icône « vitesse ».
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 de temps actuelle de Data Infrastructure Insights.
4. Les résultats du graphique ont été regroupés par le champ *source*. Le graphique présente les résultats dans chaque colonne, regroupés en couleurs. Passez le curseur sur une colonne du graphique pour afficher des détails sur les entrées spécifiques.



Raffinage des filtres

Vous pouvez utiliser les éléments suivants pour affiner votre filtre :

Filtre	Ce qu'il fait
* (Astérisque)	permet de rechercher tout
? (point d'interrogation)	permet de rechercher un nombre spécifique de caractères
OU	vous permet de spécifier plusieurs entités
PAS	permet d'exclure du texte des résultats de la recherche
Aucun	Recherche les valeurs NULL dans tous les champs
Pas *	Recherche les valeurs NULL dans les champs *text-only*

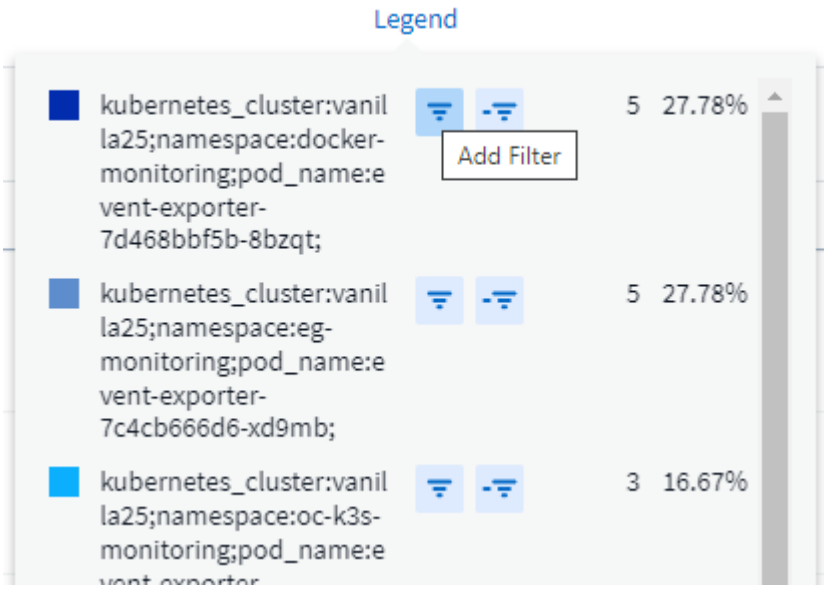
Si vous placez une chaîne de filtre entre deux guillemets, Insight traite tout entre le premier et le dernier devis comme une correspondance exacte. Tous les caractères spéciaux ou opérateurs situés dans les guillemets seront traités comme des littéraux. Par exemple, le filtrage pour "*" renvoie des résultats qui sont un astérisque littéral ; l'astérisque ne sera pas traité comme un caractère générique dans ce cas. Les opérateurs OU ET NON sont également traités comme des chaînes littérales lorsqu'ils sont entourés de guillemets doubles.

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 tableau a aussi quelques surprises. Pour chaque résultat (basé sur le filtre actuel) affiché dans la légende, vous avez la possibilité d'afficher uniquement les résultats pour cette ligne (Ajouter un filtre) ou d'afficher les résultats AUTRES QUE pour cette ligne (Ajouter un filtre d'exclusion). Le graphique et la liste

des entrées du journal sont mis à jour pour afficher les résultats en fonction de votre sélection. Pour supprimer ce filtre, ouvrez de nouveau la légende et sélectionnez [X] pour effacer le filtre de légende.

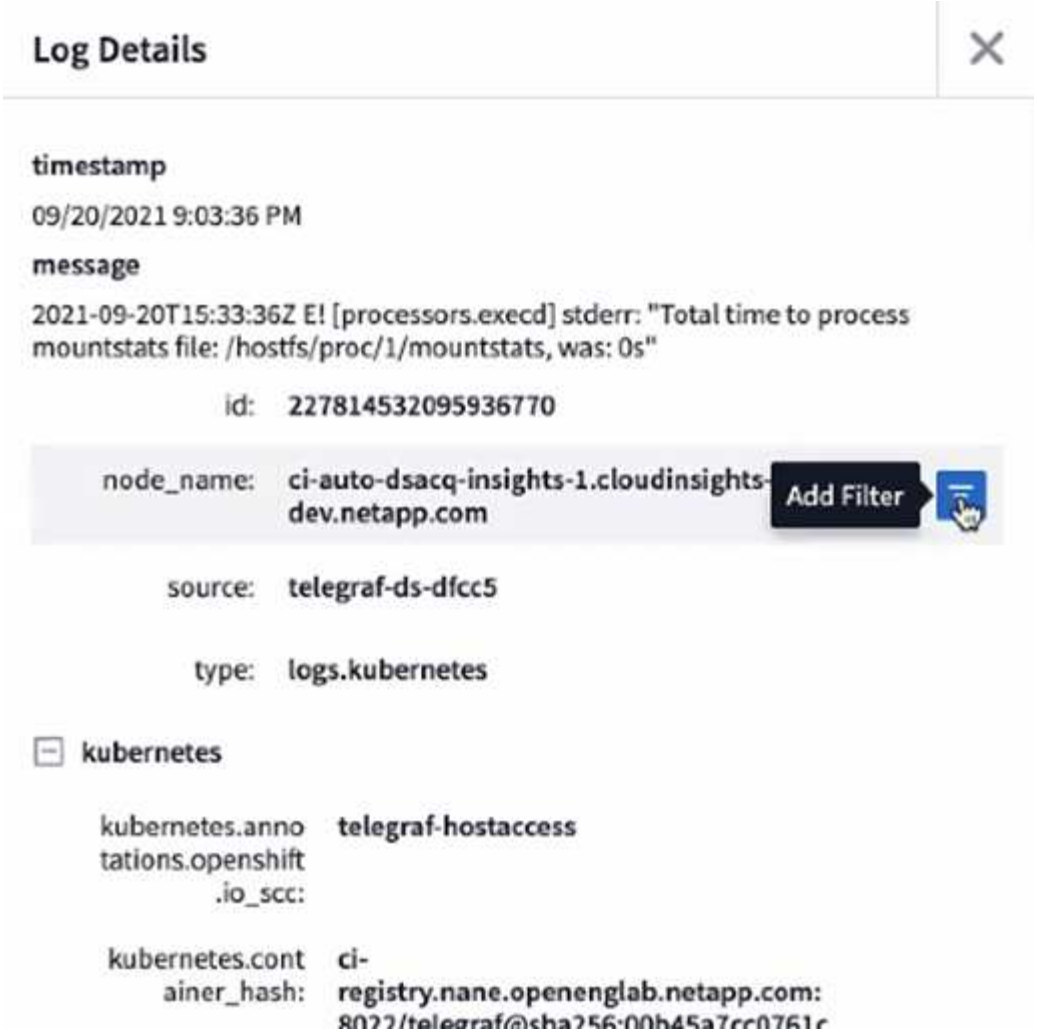


Détails du journal

Si vous cliquez n'importe où dans une entrée de journal de la liste, un volet de détails s'ouvre pour cette entrée. Ici, vous pouvez explorer d'autres informations sur cet événement.

Cliquez sur « Ajouter un filtre » pour ajouter le champ sélectionné au filtre actuel. La liste des entrées de journal sera mise à jour en fonction du nouveau filtre.

Notez que certains champs ne peuvent pas être ajoutés en tant que filtres ; dans ce cas, l'icône *Ajouter un filtre* n'est pas disponible.



Dépannage

Vous trouverez ici des suggestions de dépannage des problèmes liés aux requêtes de journal.

Problème:	Essayez ceci:
Je ne vois pas les messages "debug" dans ma requête de journal	La messagerie du journal de débogage n'est pas collectée. Pour capturer les messages que vous souhaitez, définissez la gravité du message en question sur *informationnel, erreur, alerte, urgence,* ou *avis*.

Identification des périphériques inactifs

L'identification des ressources dont vous disposez et de qui les utilise est essentielle pour « dimensionner correctement » et libérer l'infrastructure inutilisée. Vous pouvez facilement réaffecter ou désaffecter les ressources sous-utilisées et éviter ainsi les achats inutiles.

Procédez comme suit pour identifier les ressources inactives.

Étapes

- Naviguez jusqu'à **observabilité > Explorer → +Nouvelle requête métrique**.
- Sélectionnez *Storage* dans la liste déroulante.
- Cliquez sur l'engrenage et ajoutez *isActive* comme colonne.

  Les lignes affichant une vérification sont actives. "X" indique les périphériques inactifs.

Pour supprimer des périphériques inactifs, sélectionnez simplement les périphériques à supprimer et, dans la liste déroulante **actions groupées**, sélectionnez *Supprimer les périphériques inactifs*.

Visibilité

Visibilité

Grâce aux informations exploitables, vous pouvez examiner différentes choses, comme l'utilisation des ressources et leur incidence sur d'autres ressources ou des analyses complètes.

Plusieurs informations sont disponibles. Naviguez jusqu'à **tableaux de bord > Insights** pour commencer à plonger dans. Vous pouvez afficher les informations actives (les informations qui se produisent actuellement) dans l'onglet principal ou les informations inactives dans l'onglet *informations inactives*. Les informations inactives sont celles qui étaient précédemment actives, mais qui n'ont plus lieu.

Types d'Insight

Ressources partagées sous contrainte

Les charges de travail à fort impact peuvent réduire les performances d'autres workloads d'une ressource partagée. La ressource partagée est alors contrainte. Les informations sur l'infrastructure de données fournissent des outils qui vous aident à étudier la saturation des ressources et l'impact sur votre locataire. "En savoir plus"

Espaces de noms Kubernetes manque d'espace

L'espace de noms Kubernetes épuisé dans l'espace Insight vous offre une vue d'ensemble des workloads de 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"

Récupération du stockage à froid ONTAP

L'outil *Reclaim ONTAP Cold Storage* Insight fournit des données sur la capacité à froid, les économies potentielles en termes de coûts/d'énergie et les actions recommandées pour les volumes des systèmes ONTAP. "En savoir plus"



Il s'agit d'une fonction *Preview* qui peut changer au fil du temps à mesure que des améliorations sont apportées. "En savoir plus >>" A propos des fonctionnalités de prévisualisation de Data Infrastructure Insights.

Perspectives : partage de ressources sous stress

Les charges de travail à fort impact peuvent réduire les performances d'autres workloads

d’une ressource partagée. La ressource partagée est alors contrainte. Les informations sur l’infrastructure de données fournissent des outils qui vous aident à étudier la saturation des ressources et l’impact sur votre locataire.

Terminologie

Lorsqu’on parle de l’impact sur la charge de travail ou les ressources, les définitions suivantes sont utiles.

Une charge de travail **exigeante** est une charge de travail actuellement identifiée comme ayant un impact sur les autres ressources du pool de stockage partagé. Ces charges de travail sont exécutées sur des IOPS supérieures (par exemple), ce qui réduit les IOPS dans les charges de travail affectées. Les charges de travail exigeantes sont parfois appelées des charges de travail exigeantes_.

Une * charge de travail * affectée est une charge de travail affectée par une charge de travail élevée dans le pool de stockage partagé. Ces charges de travail rencontrent un nombre réduit d’IOPS et/ou une latence plus élevée en raison des charges de travail exigeantes.

Notez que si Data Infrastructure Insights n’a pas détecté la charge de travail de calcul la plus importante, le volume ou le volume interne lui-même sera reconnu comme la charge de travail. Cela s’applique aux workloads exigeants et impactés.

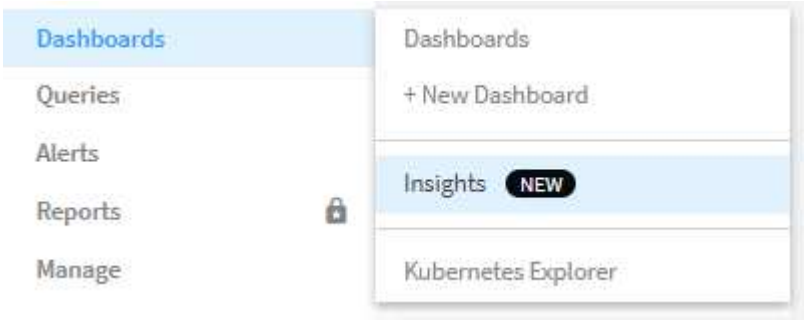
La saturation des ressources partagées est le rapport entre les IOPS impactantes et *baseline*.

Baseline est défini comme le point de données maximum rapporté pour chaque charge de travail dans l’heure précédant immédiatement la saturation détectée.

Un **conflit** ou **saturation** survient lorsque les IOPS sont déterminées à affecter d’autres ressources ou charges de travail dans le pool de stockage partagé.

Et des workloads exigeants

Pour commencer à examiner les charges de travail exigeantes et affectées dans vos ressources partagées, cliquez sur **tableaux de bord > Insights** et sélectionnez **Ressources partagées sous stress** Insight.



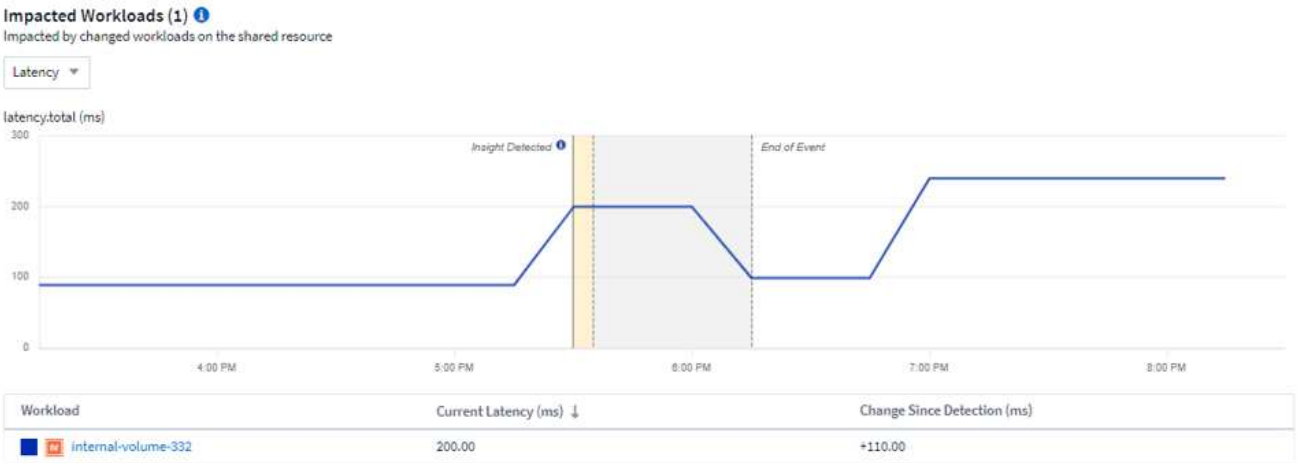
Data Infrastructure Insights affiche la liste des charges de travail pour lesquelles une saturation a été détectée. Notez que Data Infrastructure Insights affiche les charges de travail où au moins une ressource *exigeante* **ou** *ressource affectée* a été détectée.

Cliquez sur une charge de travail pour afficher la page de détails correspondante. Le graphique du haut indique l’activité sur la ressource partagée (par exemple, un pool de stockage) sur laquelle se produit la contention/saturation.



Voici deux graphiques illustrant les *charges de travail* exigeantes_ et les charges de travail *affectées* par les charges de travail exigeantes.





Le tableau ci-dessous répertorie les charges de travail et/ou les ressources qui affectent ou sont affectées par les conflits. Un clic sur une ressource (par exemple, une VM) ouvre une page détaillée pour cette ressource. Un clic sur une charge de travail ouvre une page de requête qui affiche les modules concernés. Notez que si le lien ouvre une requête vide, cela peut être dû au fait que le pod affecté ne fait plus partie du conflit actif. Vous pouvez modifier la plage de temps de la requête pour afficher la liste des pods dans une plage de temps plus ou plus ciblée.

Que dois-je faire pour résoudre la saturation ?

Vous pouvez prendre plusieurs mesures pour réduire ou éliminer le risque de saturation de votre locataire.

Elles sont présentées en développant le lien **+Afficher les recommandations** sur la page. Voici quelques choses que vous pouvez essayer.

- Grands consommateurs d'IOPS

  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 les coûts inutiles ou les contentions supplémentaires.

- Implémentation d'une règle de qualité de service (QoS

  L'implémentation d'une politique de QoS par charge de travail pour garantir qu'un nombre suffisant de ressources disponibles permettra de réduire la saturation sur le pool de stockage. Il s'agit d'une solution à long terme.

- Ajoutez des ressources supplémentaires

  Si la ressource partagée (par exemple, Storage Pool) a atteint le point de saturation IOPS, l'ajout de disques plus ou plus rapides au pool garantit que suffisamment de ressources disponibles pour réduire la saturation.

Enfin, vous pouvez cliquer sur le lien **Copier Insight** pour copier l'url de la page dans le presse-papiers, afin de partager plus facilement avec vos collègues.

Indications : espaces de noms Kubernetes manque d'espace

Manquer d'espace sur votre locataire n'est jamais une bonne situation. Les informations sur l'infrastructure de données vous aident à prévoir le temps nécessaire avant que les volumes persistants de Kubernetes ne soient pleins.

La *Kubernetes Namespaces étant hors d'Space* Insight, vous disposez d'une vue détaillée des workloads sur vos espaces de noms Kubernetes qui risquent d'être à court d'espace, avec une estimation du nombre de jours restants avant que chaque volume persistant ne soit plein.

Vous pouvez visualiser cette présentation en accédant à **tableaux de bord > Insights**.

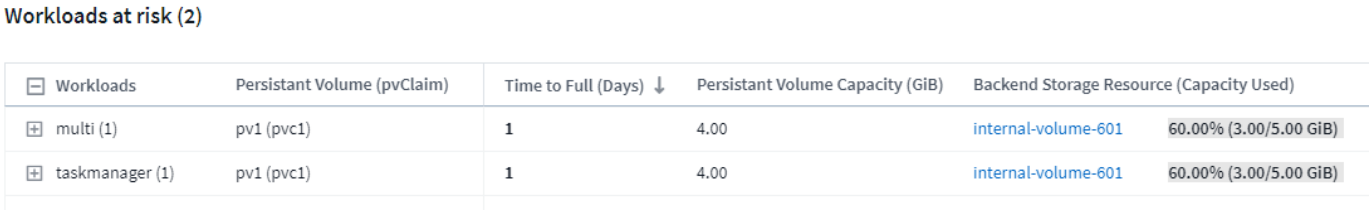
Kubernetes Namespaces Running Out of Space (3)

Description	Estimated Days to Full	Workloads at Risk	Detected ↓
1 workload at risk on es	35	1	2 days ago
1 workload at risk on manager	24	1	2 days ago
2 workloads at risk on cloudinsights	1	2	2 days ago

Cliquez sur une charge de travail pour ouvrir une page détaillée de la conférence Insight. Sur cette page, un graphique répertoriant les tendances de capacité de charge de travail s'affiche, ainsi qu'un tableau répertoriant les éléments suivants :

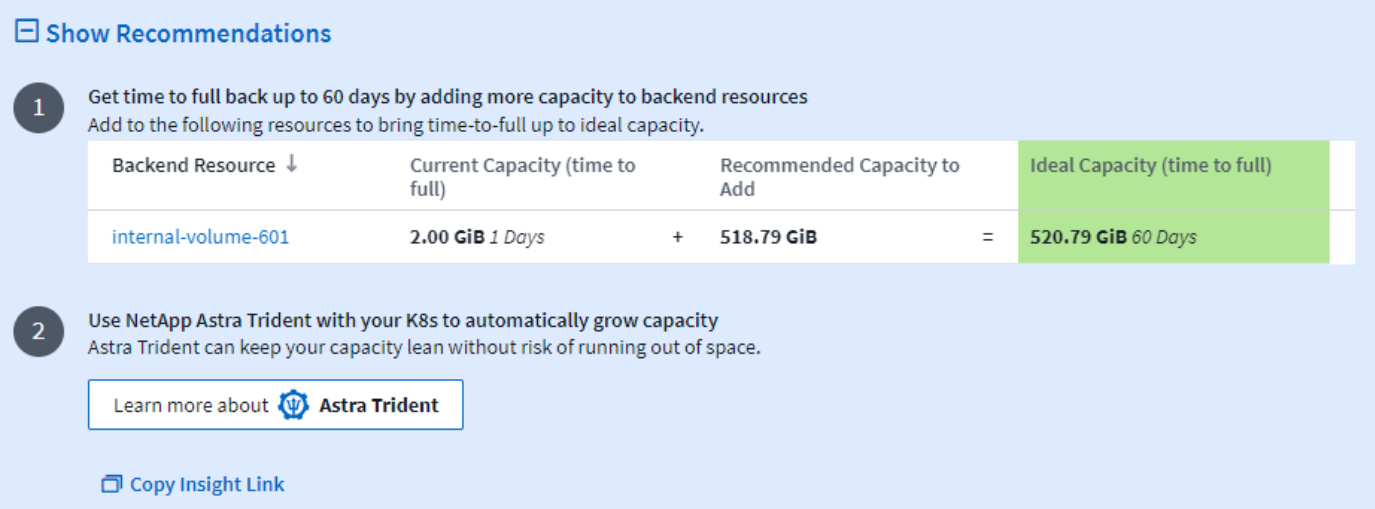
- Nom de la charge de travail
- Volume persistant affecté

- Temps avant plein prévu en jours
- Capacité de volume persistant
- Ressource de stockage interne affectée, la capacité actuelle étant utilisée à partir de la capacité totale. En cliquant sur ce lien, vous accédez à la page d'accueil détaillée du volume principal.



Que faire si l'espace est insuffisant ?

Sur la page Insight, cliquez sur **+Afficher les recommandations** pour voir les solutions possibles. En cas de manque d'espace, l'option la plus simple consiste à ajouter toujours plus de capacité, et Data Infrastructure Insights vous montre la capacité optimale à ajouter pour accélérer le temps de traitement d'une prévision cible de 60 jours. D'autres recommandations sont également présentées.



C'est également ici que vous pouvez copier un lien pratique vers cette présentation, ajouter une page à vos signets ou partager facilement avec votre équipe.

Informations : récupération du stockage à froid ONTAP

L'outil *Reclaim ONTAP Cold Storage* Insight fournit des données sur la capacité à froid, les économies potentielles en termes de coûts/d'énergie et les actions recommandées pour les volumes des systèmes ONTAP.

Pour en savoir plus, accédez à **tableaux de bord > Insights** et découvrez l'analyse *Reclaim ONTAP Cold Storage* Insight. Notez que cette Insight répertorie uniquement les stockages affectés si Data Infrastructure Insights a détecté un stockage à froid. Sinon, un message « tout effacer » s'affiche.

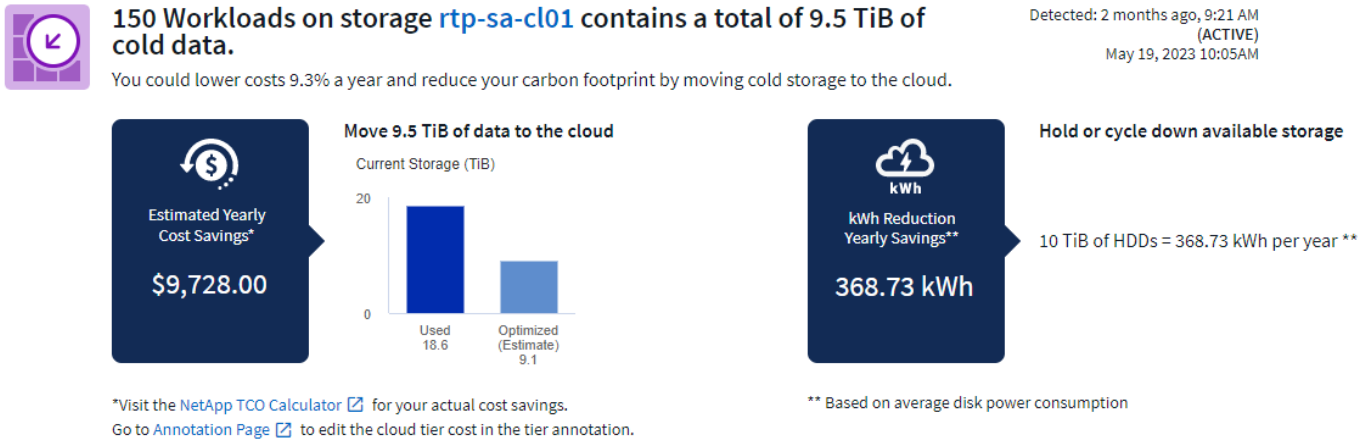
N'oubliez pas que les données inactives de moins de 30 jours ne sont pas affichées.

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 fournit une indication rapide de la quantité de données détectées en tant que « inactives » et du stockage sur lequel résident les données. Le tableau indique également le nombre de charges de travail avec des données inactives.

Si vous sélectionnez un Insight dans la liste, une page contenant plus de détails s'ouvre. Vous y trouverez notamment des recommandations pour transférer des données vers le cloud ou arrêter des disques non isés, ainsi qu'une estimation des coûts et des économies d'énergie que vous pourriez réaliser grâce à l'implémentation de ces recommandations. La page fournit même un lien pratique vers "Calculateur de TCO de NetApp" afin que vous puissiez expérimenter avec les nombres.



Recommandations

Sur la page Insight, développez les **recommandations** pour explorer les options suivantes :

- Déplacez les workloads non utilisés (zombies) vers un Tier de stockage moins coûteux (HDD).

  En utilisant l'indicateur zombie, le stockage à froid et le nombre de jours, trouvez la quantité de données la plus froide et la plus importante, puis déplacez la charge de travail vers un niveau de stockage moins coûteux (par exemple, un pool de stockage utilisant du stockage sur disque dur). Une charge de travail est considérée comme un « zombie » lorsque le système IS n'a reçu aucune demande d'E/S significative pendant au moins 30 jours.

- Supprimez 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.

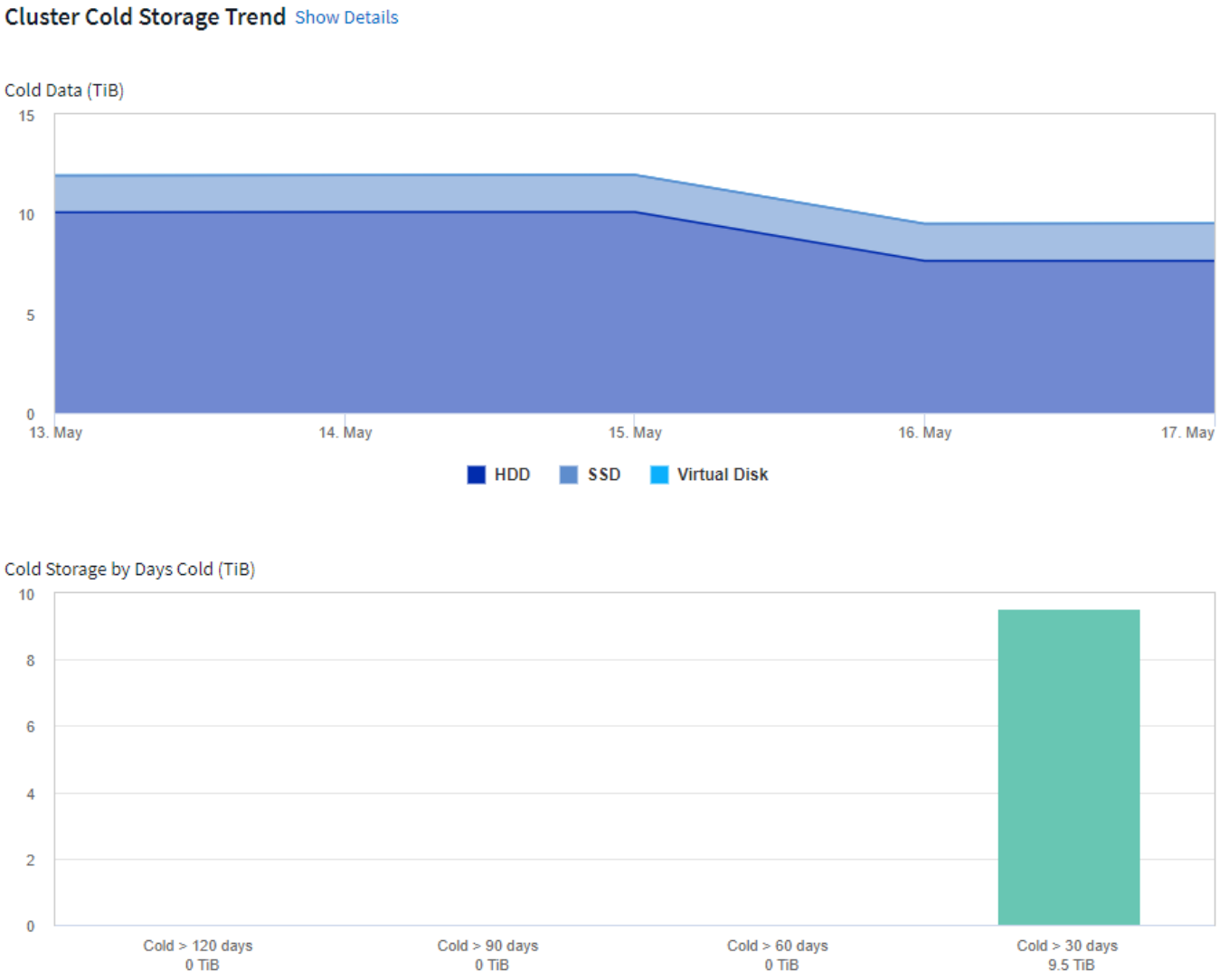
- Prenons l'exemple de la solution NetApp Fabric Pool

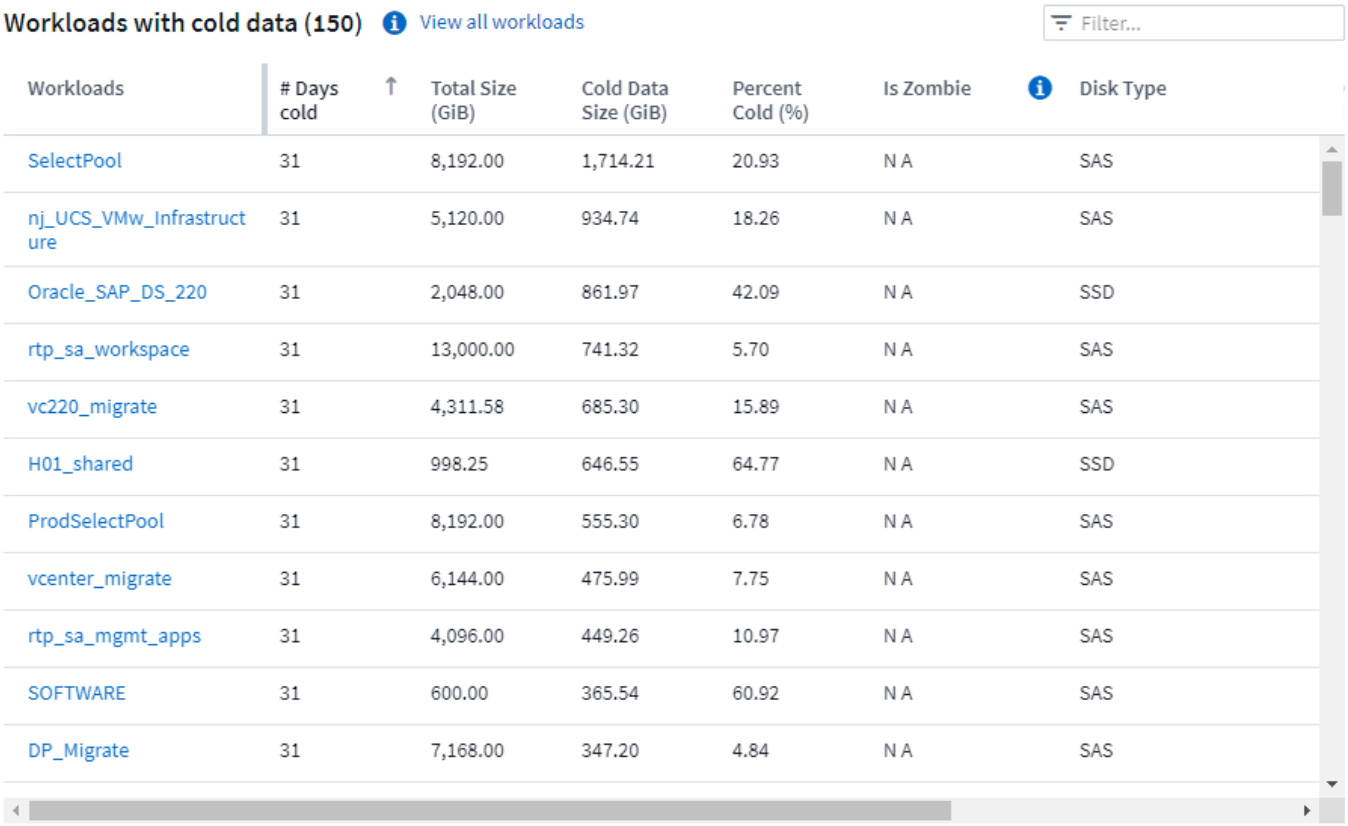
  NetApp "Solution FabricPool"transfère automatiquement les données inactives vers un stockage cloud à faible coût, ce qui augmente l'efficacité de votre Tier de performance tout en assurant la protection des

données à distance.

Visualiser et explorer

Les graphiques et le tableau fournissent des informations supplémentaires sur les tendances et vous permettent d'explorer chaque charge de travail.





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

Surveille et alerte

Alertes avec les moniteurs

Vous créez des moniteurs pour définir des seuils qui déclenchent des alertes pour vous informer des problèmes liés aux ressources de votre réseau. Par exemple, vous pouvez créer un moniteur pour signaler la latence d'écriture *node* pour n'importe lequel d'une multitude de protocoles.

Les moniteurs et alertes sont disponibles dans toutes les éditions Data Infrastructure Insights. Cependant, l'édition Basic est soumise aux conditions suivantes : * vous ne pouvez avoir jusqu'à cinq moniteurs personnalisés actifs à la fois. Tous les moniteurs au-delà de cinq seront créés ou déplacés à l'état *Pause*. * Les moniteurs de metrics VMDK, Virtual machine, Host et DataStore ne sont pas pris en charge. Si des moniteurs ont été créés pour ces mesures, ils seront mis en pause et ne peuvent pas être repris lors de la rétrogradation vers l'édition de base.

Les moniteurs vous permettent de définir des seuils sur les metrics générés par des objets d'infrastructure tels que le stockage, les serveurs virtuels, EC2 et les ports, ainsi que pour les données « intégration », telles que celles collectées pour Kubernetes, les metrics avancés ONTAP et les plug-ins Telegraf. Ces *mesures* permettent de vous alerter lorsque les seuils de niveau d'avertissement ou de niveau critique sont croisés.

Vous pouvez également créer des moniteurs pour déclencher des alertes de niveau avertissement, critique ou informationnel lorsque les *événements log* spécifiés sont détectés.

Les informations d'infrastructure de données fournissent également un certain nombre

d'informations"Moniteurs définis par le système", en fonction de votre environnement.

Meilleures pratiques en matière 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 d'entrer n'importe quelle adresse e-mail valide en tant que destinataire des alertes. Si vous travaillez dans un environnement sécurisé, soyez particulièrement attentif à la personne qui reçoit la notification ou a accès à l'alerte.

Moniteur de mesures ou de journaux ?

1. Dans le menu informations sur l'infrastructure de données, cliquez sur **alertes > gérer les moniteurs**

   La page de liste moniteurs s'affiche et affiche les moniteurs actuellement configurés.

2. Pour modifier un moniteur existant, cliquez sur son nom dans la liste.
3. Pour ajouter un moniteur, cliquez sur **+ moniteur**.



   Lorsque vous ajoutez un nouveau moniteur, vous êtes invité à créer un moniteur métrique ou un moniteur de journal.

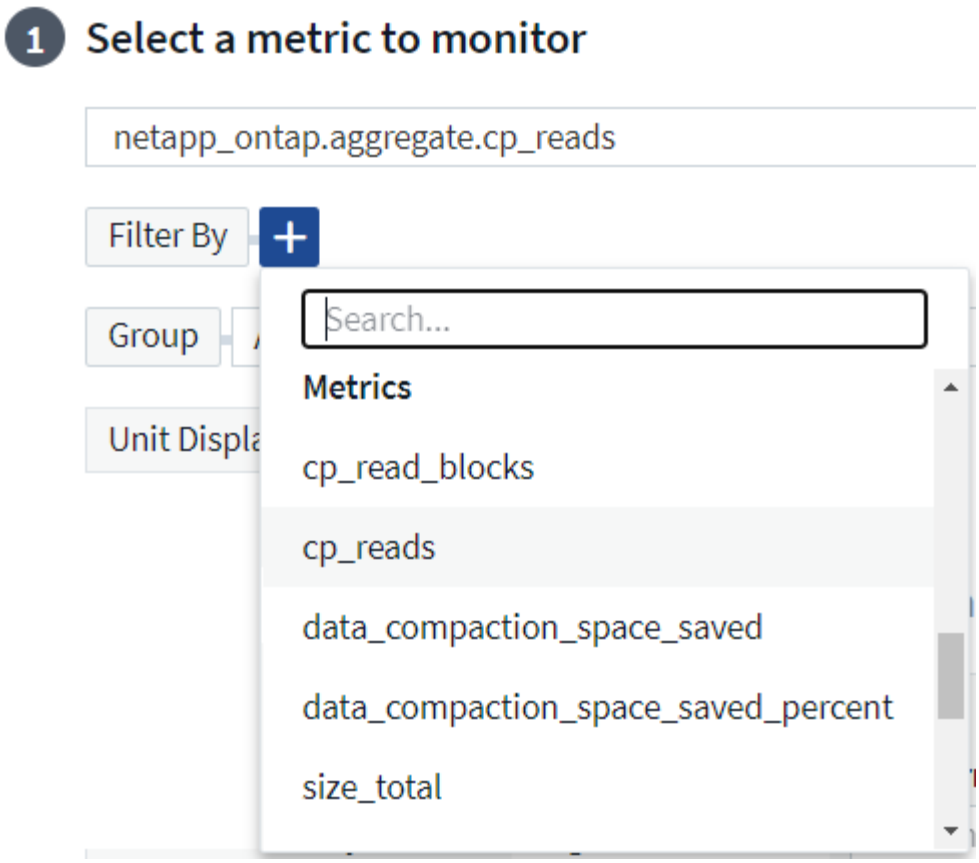
   - *Metric* surveille l'alerte sur les déclencheurs liés à l'infrastructure ou aux performances
   - *Log* surveille l'alerte sur l'activité liée au journal

   Après avoir sélectionné 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 mesure à surveiller.

Vous pouvez définir des filtres pour réduire les attributs d'objet ou les mesures à surveiller.



Lors de l'utilisation des données d'intégration (Kubernetes, ONTAP Advanced Data, etc.), le filtrage des mesures supprime les points de données individuels/non inégalés 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 peuvent potentiellement supprimer l'objet entier du graphique.

Pour créer un moniteur multicondition (par exemple, IOPS > X et latence > y), définissez la première condition comme un seuil et la deuxième condition comme un filtre.

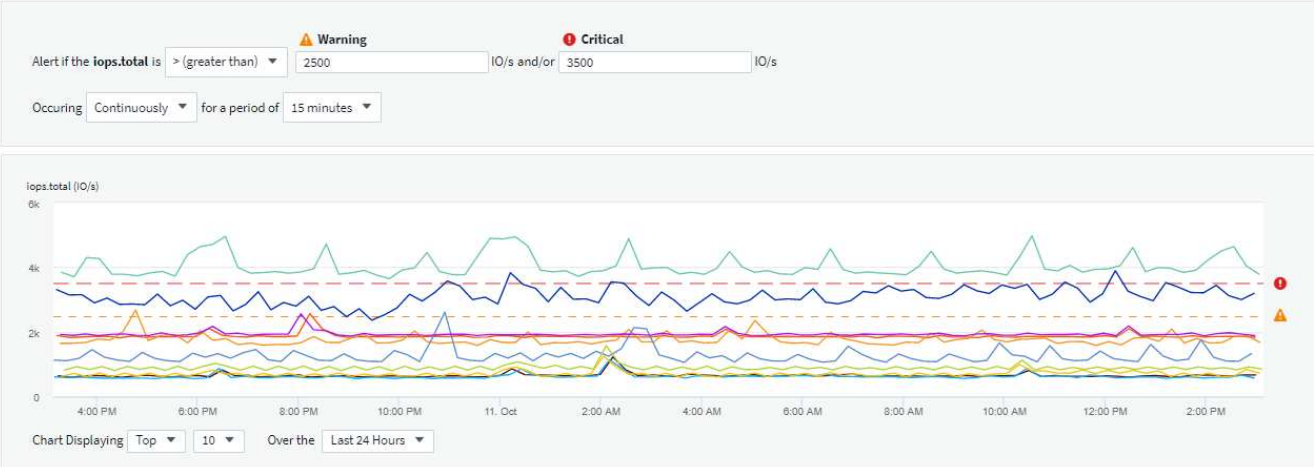
Définissez les conditions du moniteur.

1. Après avoir choisi l'objet et la mesure à surveiller, définissez les seuils de niveau d'avertissement et/ou critique.
2. Pour le niveau *Warning*, entrez 200 pour notre exemple. La ligne en pointillés indiquant ce niveau d'avertissement s'affiche dans le graphique exemple.
3. Pour le niveau *critique*, entrez 400. La ligne en pointillés indiquant ce niveau critique s'affiche dans le graphique exemple.

   Le graphique affiche les données historiques. Les lignes d'avertissement et de niveau critique sur le graphique sont une représentation visuelle du moniteur, ce qui vous permet de voir facilement quand le moniteur peut déclencher une alerte dans chaque cas.

4. Pour l'intervalle d'occurrence, choisissez *permanent* pour une période de *15 minutes*.

   Vous pouvez choisir de déclencher une alerte au moment où un seuil est atteint ou d'attendre que le seuil ait été atteint pendant un certain temps. Dans notre exemple, nous ne voulons pas être alerté chaque fois que le nombre total d'IOPS est supérieur au niveau Avertissement ou critique, mais uniquement lorsqu'un objet surveillé dépasse en permanence l'un de ces niveaux pendant au moins 15 minutes.



Définir le comportement de résolution d'alerte

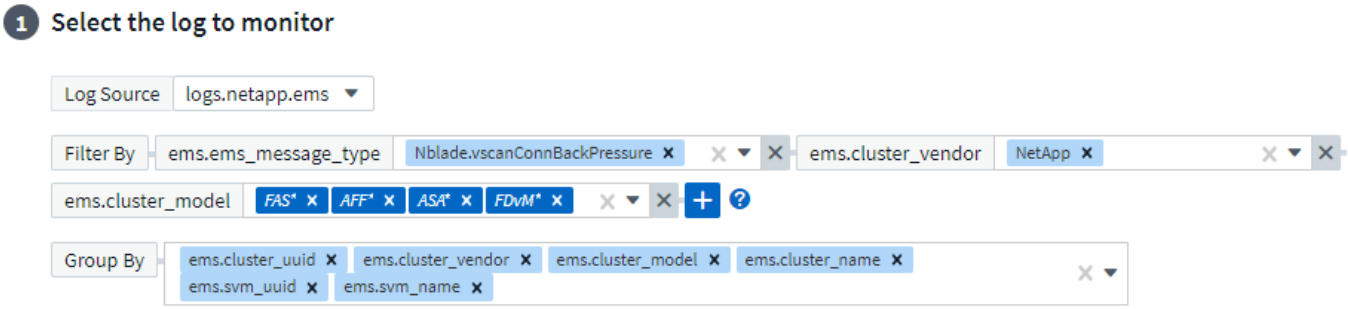
Vous pouvez choisir comment une alerte de surveillance des mesures est résolue. Deux options s'offrent à vous :

- Résoudre le problème lorsque la mesure revient à la plage acceptable.
- Résoudre lorsque la mesure se trouve dans la plage acceptable pendant une durée spécifiée, de 1 minute à 7 jours.

Surveillance des journaux

Lors de la création d'un moniteur **Log Monitor**, 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 de surveillance du journal ne peut pas être vide.



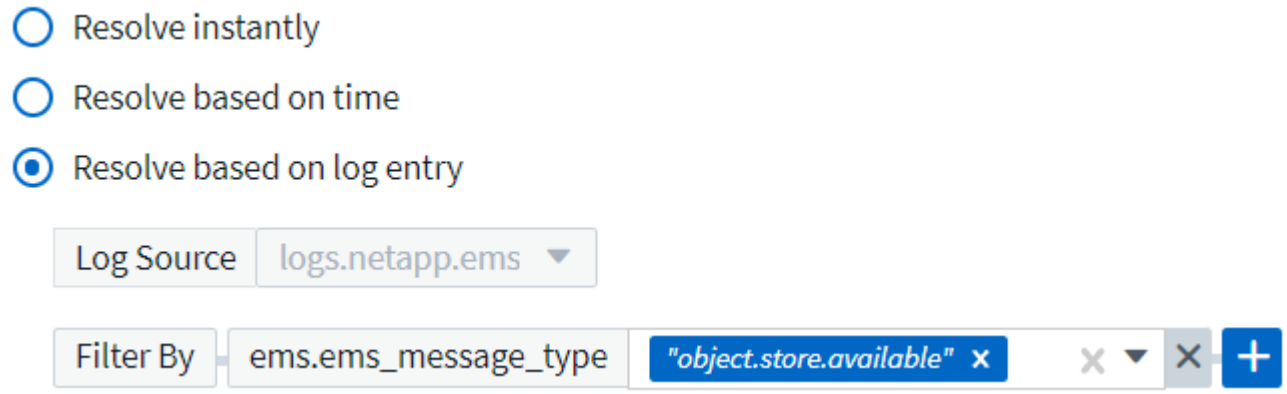
Définir le comportement de l'alerte

Vous pouvez créer le moniteur pour qu'il vous alerte avec un niveau de gravité de *critique*, *Avertissement* ou *information*, lorsque les conditions définies ci-dessus se produisent une fois (c'est-à-dire immédiatement), ou attendre que les conditions se produisent 2 fois ou plus.

Définir le comportement de résolution d'alerte

Vous pouvez choisir la façon dont une alerte de surveillance de journal est résolue. Trois choix sont proposés :

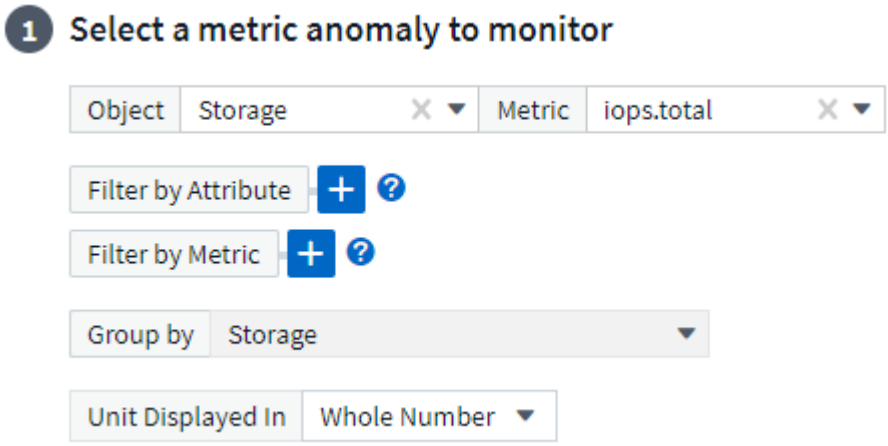
- **Résoudre instantanément**: L'alerte est immédiatement résolue sans action supplémentaire
- **Résoudre en fonction de l'heure** : l'alerte est résolue une fois l'heure spécifiée écoulée
- **Résoudre en fonction de l'entrée de journal** : l'alerte est résolue lorsqu'une activité de journal ultérieure s'est produite. Par exemple, lorsqu'un objet est enregistré comme « disponible ».



Moniteur de détection des anomalies

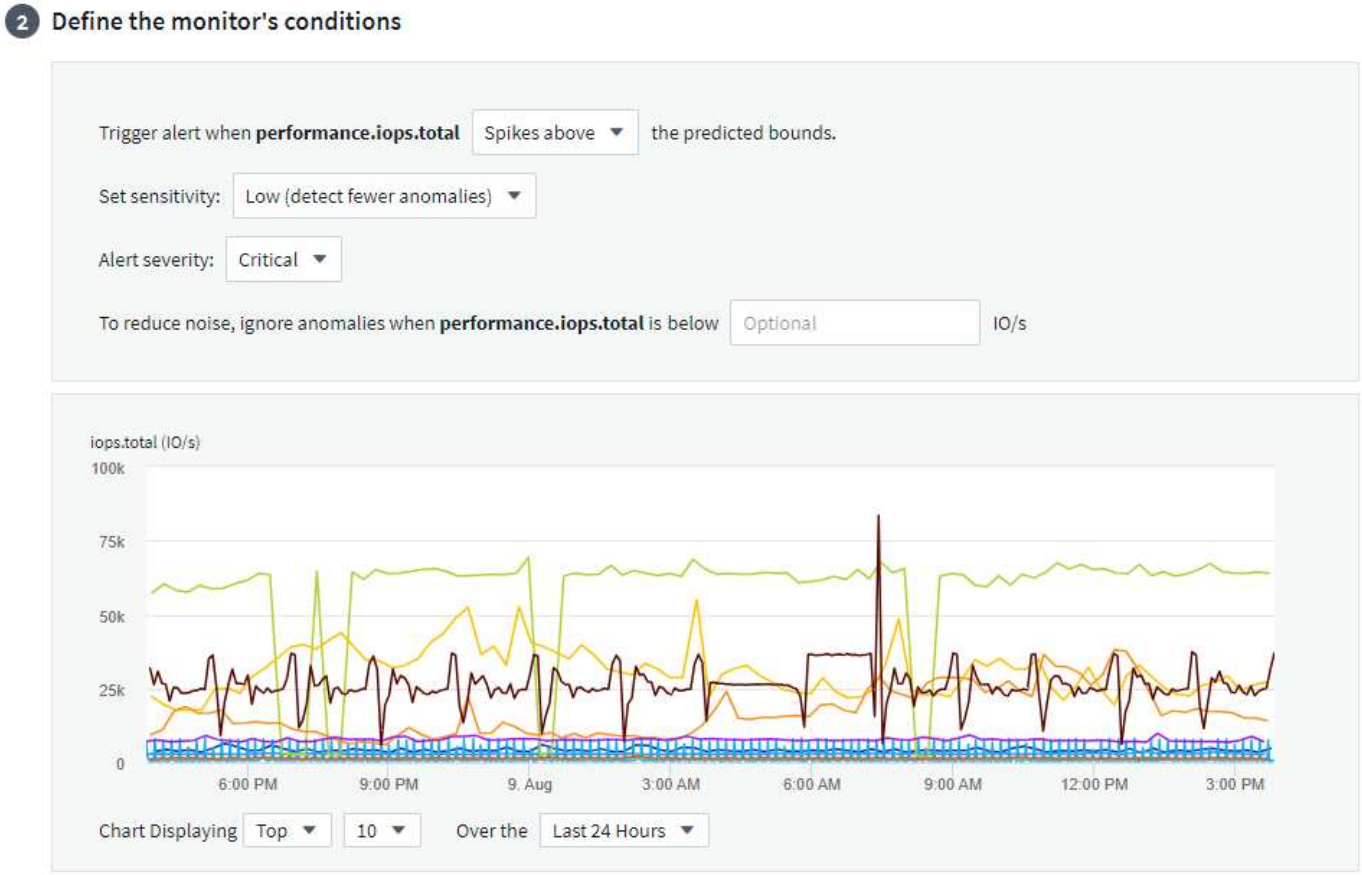
1. Dans la liste déroulante, recherchez et choisissez un type d'objet et une mesure à surveiller.

Vous pouvez définir des filtres pour réduire les attributs d'objet ou les mesures à surveiller.



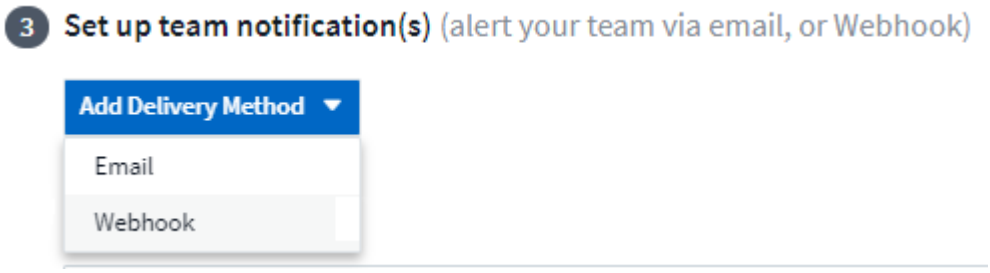
Définissez les conditions du moniteur.

1. Après avoir choisi l'objet et la mesure à surveiller, vous pouvez définir les conditions dans lesquelles une anomalie est détectée.
   - Choisissez de détecter une anomalie lorsque la métrique choisie **pointe au-dessus** des limites prévues, **chute en dessous** de ces limites, ou **pointe au-dessus ou chute en dessous** des limites.
   - Régler la **sensibilité** de la détection. **Faible** (moins d'anomalies sont détectées), **moyenne** ou **élevée** (plus d'anomalies sont détectées).
   - Définissez les alertes sur Wither **Warning** ou **Critical**.
   - Si vous le souhaitez, vous pouvez choisir de réduire le bruit, en ignorant les anomalies lorsque la mesure choisie est inférieure à un seuil que vous avez défini.



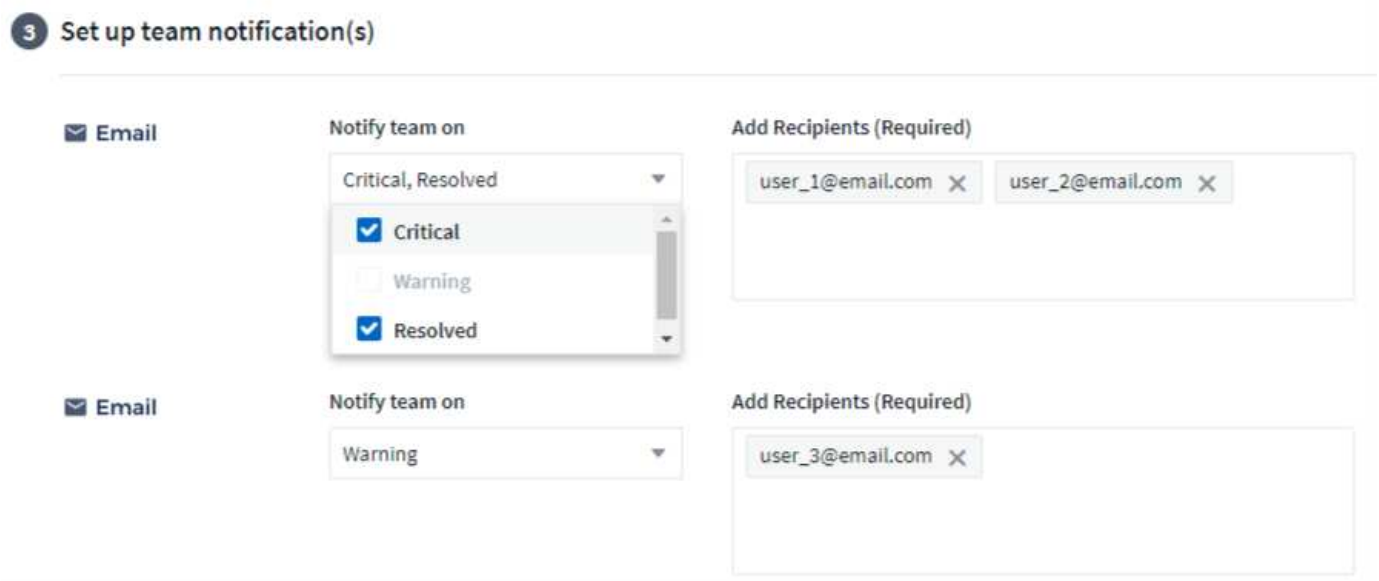
Sélectionnez le type de notification et les destinataires

Dans la section *configurer les notifications d'équipe*, vous pouvez choisir d'alerter votre équipe par e-mail ou via Webhook.



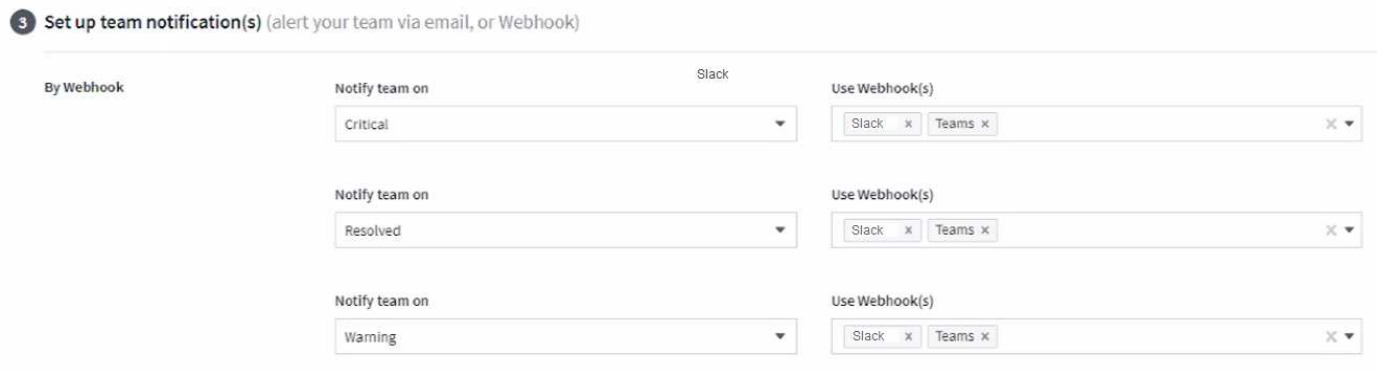
Alertes par e-mail:

Spécifiez les destinataires de l'e-mail pour les notifications d'alerte. Si vous le souhaitez, vous pouvez choisir différents destinataires pour les alertes d'avertissement ou critiques.



Alertes via Webhook:

Spécifiez le ou les webhook(s) pour les notifications d'alerte. Si vous le souhaitez, vous pouvez choisir différents crochets pour les alertes d'avertissement ou critiques.



Les notifications ONTAP Data Collector prévalent sur toute notification Monitor spécifique pertinente au cluster/Data Collector. La liste des destinataires que vous définissez pour le Data Collector lui-même recevra les alertes du Data Collector. Si aucune alerte de collecte de données n'est active, des alertes générées par le moniteur seront envoyées à des destinataires de moniteur spécifiques.

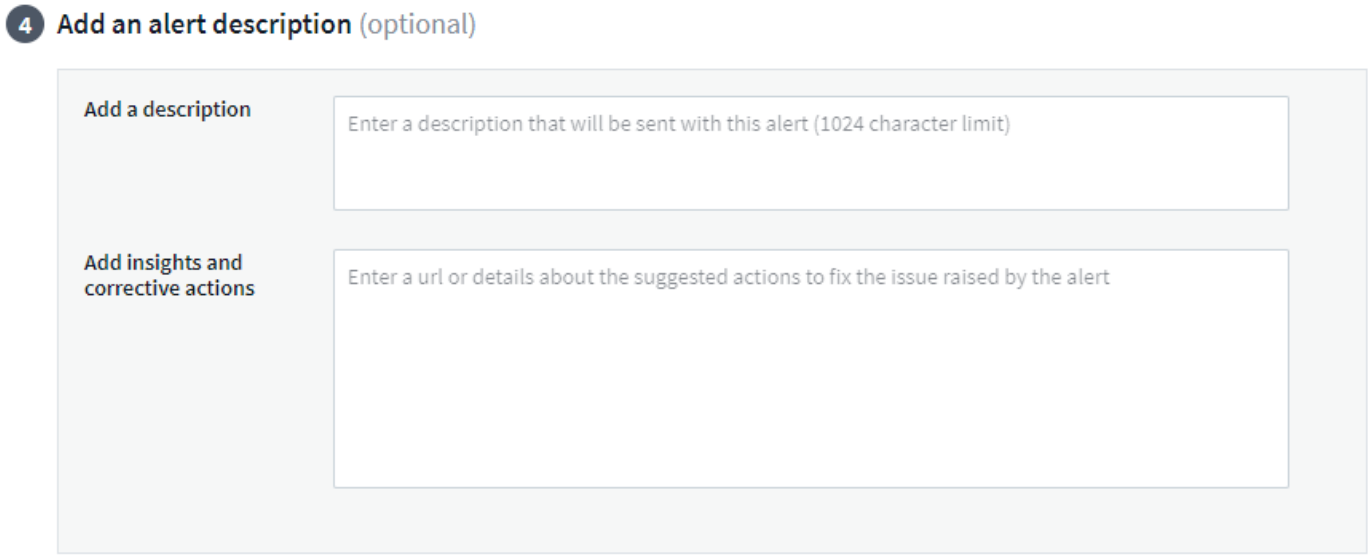
Définition d'actions correctives ou d'informations supplémentaires

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 comporter jusqu'à 1024 caractères et sera envoyée avec l'alerte. Le champ d'action corrective peut contenir jusqu'à 67,000 caractères et sera affiché dans la section récapitulative de la page d'accueil de l'alerte.

Dans ces champs, vous pouvez fournir des notes, des liens ou des étapes à suivre pour corriger ou résoudre l'alerte.

Vous pouvez ajouter n'importe quel attribut d'objet (par exemple, nom du 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 comme : « latence élevée pour le volume : *%%relatedObject.volume.name%%*,

stockage : *%%relatedObject.storage.name%%*".



Enregistrez votre moniteur

1. Si vous le souhaitez, vous pouvez ajouter une description du moniteur.
2. Donnez un nom significatif au moniteur et cliquez sur **Enregistrer**.

   Votre nouveau moniteur est ajouté à la liste des moniteurs actifs.

Liste des moniteurs

La page Monitor répertorie les moniteurs actuellement configurés, avec les informations suivantes :

- Nom du moniteur
- État
- Objet/mesure surveillé
- Conditions du moniteur

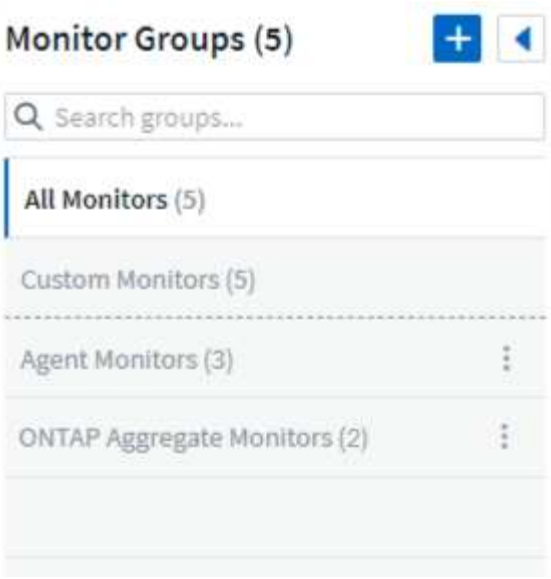
Vous pouvez choisir de suspendre temporairement la surveillance d'un type d'objet en cliquant sur le menu à droite du moniteur et en sélectionnant **Pause**. Lorsque vous êtes prêt à reprendre la surveillance, cliquez sur **reprendre**.

Vous pouvez copier un moniteur en sélectionnant **Dupliquer** dans le menu. Vous pouvez ensuite modifier le nouveau moniteur et modifier l'objet/la mesure, le filtre, les conditions, les destinataires de l'e-mail, 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 avoir un groupe de moniteurs dédié au stockage de votre locataire ou des moniteurs pertinents pour une liste de destinataires donnée.



Les groupes de moniteurs suivants sont affichés. Le nombre de moniteurs contenus dans un groupe s'affiche en regard du nom du groupe.

- **Tous les moniteurs** répertorie tous les moniteurs.
- **Moniteurs personnalisés** répertorie tous les moniteurs créés par l'utilisateur.
- **Les moniteurs suspendus** répertorieront tous les moniteurs système qui ont été suspendus par Data Infrastructure Insights.
- Les informations sur l'infrastructure de données afficheront également un certain nombre de **groupes de surveillance du 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 mis en pause, repris, supprimés ou déplacés vers un autre groupe. Les moniteurs définis par le système peuvent être mis en pause et repris, mais ne peuvent pas être supprimés ni déplacés.

Moniteurs suspendus

Ce groupe s'affiche uniquement 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 des moniteurs suspendus lorsque le problème à l'origine de la suspension est résolu.

Moniteurs définis par le système

Ces groupes affichent 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, volumes, etc.) ou pour les charges de travail (moniteurs de journaux), ou pour d'autres groupes. NetApp évalue en permanence les besoins des clients et les fonctionnalités des produits et les met à jour ou ajoute aux contrôles système et aux groupes 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 pouvez souhaiter créer un groupe pour tous vos moniteurs de stockage.

Pour créer un nouveau groupe de moniteurs personnalisé, cliquez sur le bouton **"+" Créer un nouveau groupe de moniteurs**. Entrez 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*.



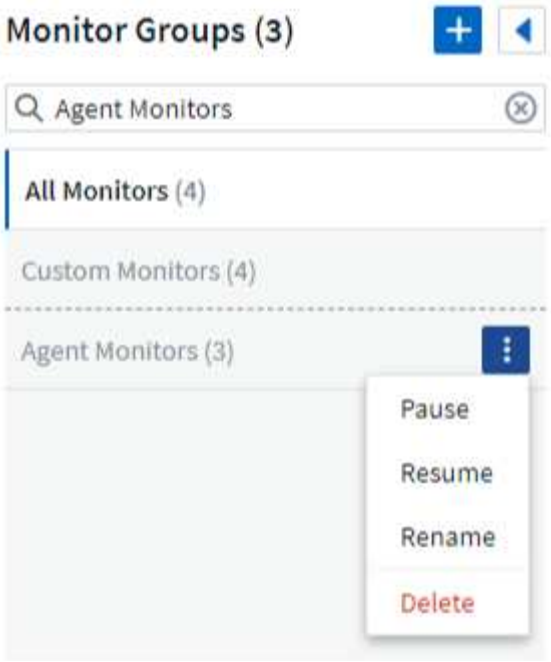
Supprimer les moniteurs en cliquant sur un groupe et en sélectionnant *Supprimer du groupe* dans le menu. Vous ne pouvez pas supprimer de moniteurs du groupe *tous les moniteurs* ou *moniteurs personnalisés*. Pour supprimer un moniteur de ces groupes, vous devez le supprimer lui-même.

> La suppression d'un moniteur d'un groupe ne supprime pas le moniteur de Data Infrastructure Insights. Pour supprimer complètement un moniteur, sélectionnez-le et cliquez sur *Delete*. Ceci le supprime également du groupe auquel il appartenait et n'est plus disponible pour aucun utilisateur.

Vous pouvez également déplacer un moniteur vers un autre groupe de la même manière, en sélectionnant *Move to Group*.

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

Les informations d'infrastructure de données comprennent un certain nombre de contrôles définis par le système pour les metrics 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 changent.

Consultez la "Moniteurs définis par le système" page pour obtenir la description des moniteurs inclus dans Data Infrastructure Insights.

Plus d'informations

- "Affichage et rejet des alertes"

Affichage et gestion des alertes à partir des moniteurs

Data Infrastructure Insights affiche des alertes en cas "seuils surveillés"de dépassement.

Les fonctions de surveillance et d'alerte 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 des 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

- **Déclenché Time** : heure à laquelle le moniteur concerné a déclenché l'alerte
- **Gravité actuelle** (onglet alertes actives) : gravité actuelle de l'alerte active
- **Gravité supérieure** (onglet alertes résolues); gravité maximale de l'alerte avant sa résolution
- **Moniteur** : moniteur configuré pour déclencher l'alerte
- **Déclenché le** : objet sur lequel le seuil surveillé a été dépassé
- **État** : état d'alerte actuel, *New* ou *In Process*
- **État actif** : *actif* ou *résolu*
- **Condition** : condition de seuil qui a déclenché l'alerte
- **Métrique** : la mesure 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 situé à droite de l'alerte et en choisissant l'une des options suivantes :

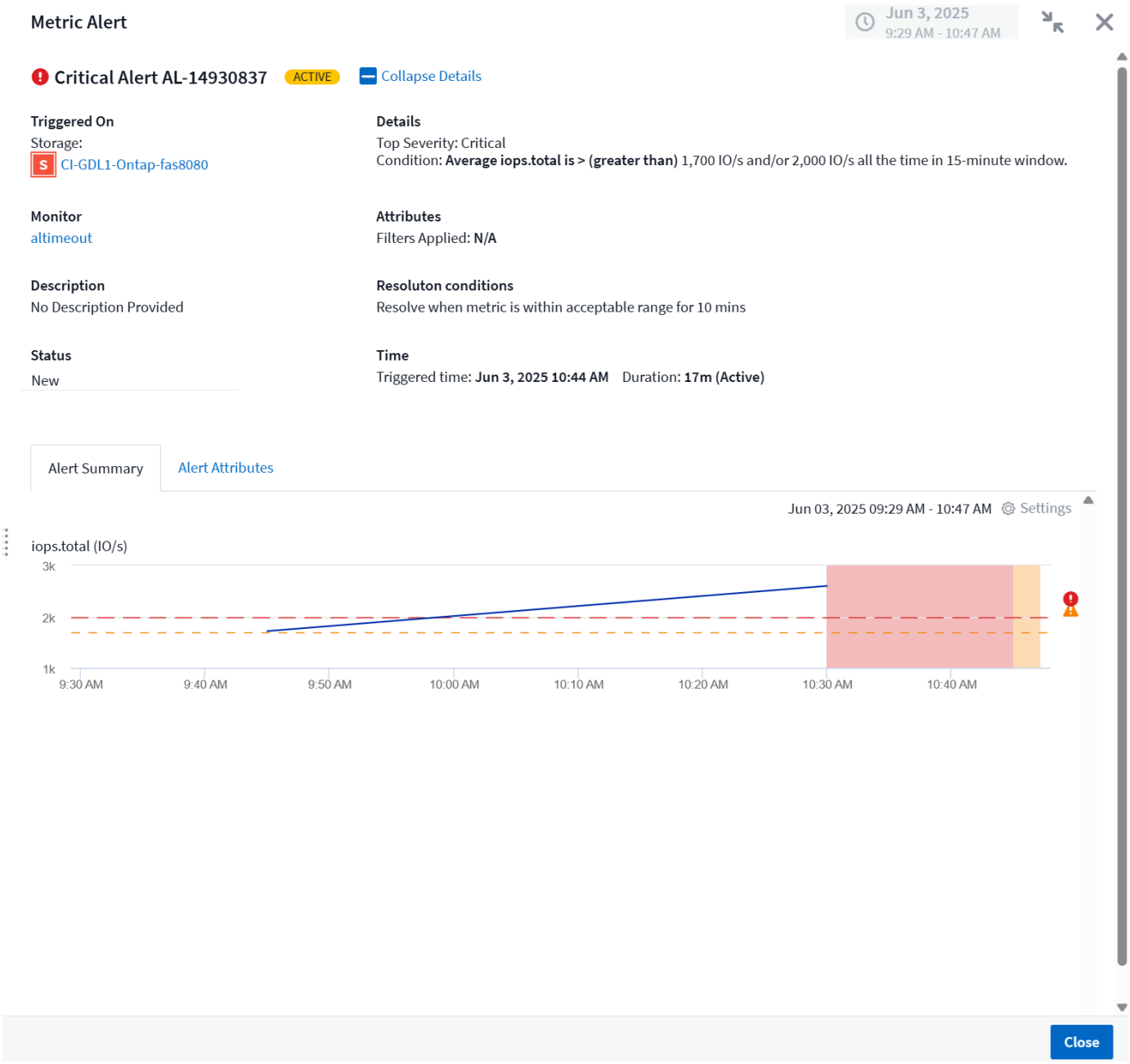
- **En cours** pour indiquer que l'alerte est en cours d'enquête ou doit être maintenue ouverte
- **Rejeter** pour supprimer l'alerte de la liste des alertes actives.

Vous pouvez gérer plusieurs alertes en cochant la case à gauche de chaque alerte et en cliquant sur *Modifier le statut des alertes sélectionnées*.

Cliquez sur un ID d'alerte pour ouvrir la page Détails de l'alerte.

Panneau de détails des alertes

Sélectionnez une ligne d'alerte pour ouvrir son panneau de détails. Ce panneau fournit des informations supplémentaires sur l'alerte, notamment un résumé, une vue expert affichant des graphiques relatifs aux données de l'objet, les actifs associés et les commentaires saisis par les enquêteurs.



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 :

- la prochaine donnée à arriver
- un minuteur à tirer lorsqu'il n'y a pas de point de données et que vous avez attendu assez longtemps

Comme c'est le cas avec une arrivée de données lente, ou pas d'arrivée de données, le mécanisme de temporisation doit prendre le relais car le taux d'arrivée des données est insuffisant pour déclencher des alertes en « temps réel ». La question se pose donc généralement comme « combien de temps puis-je attendre avant de fermer la fenêtre d'analyse et d'examiner ce que j'ai ? ». Si vous attendez trop longtemps, vous ne générez pas les alertes assez rapidement pour être utile.

Si vous disposez d'un moniteur avec une fenêtre de 30 minutes qui indique qu'une condition est violée par le

dernier point de données avant une perte de données à long terme, Une alerte est générée car le moniteur n'a reçu aucune autre information à utiliser pour confirmer la récupération de la mesure ou noter que la condition persiste.

Alertes « actives en permanence »

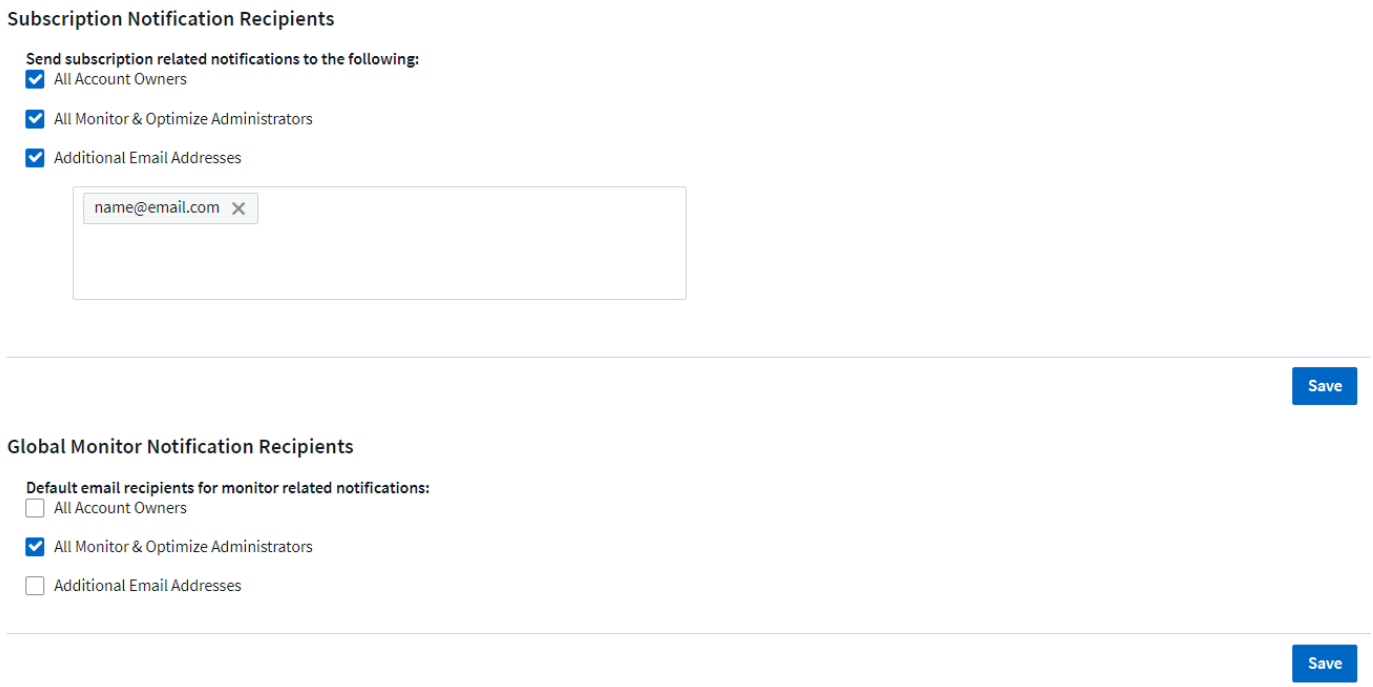
Il est possible de configurer un moniteur de façon à ce que la condition existe toujours * sur l'objet surveillé—par exemple, IOPS > 1 ou latence > 0. Ils sont souvent créés sous forme de moniteurs « test » puis oubliés. Ces moniteurs créent des alertes qui restent ouvertes en permanence sur les objets constitutifs, ce qui peut entraîner des problèmes de stabilité et de contrainte du système au fil du temps.

Pour éviter cela, Data Infrastructure Insights fermera automatiquement toute alerte « active en permanence » au bout de 7 jours. Notez que les conditions sous-jacentes du moniteur peuvent (probablement) continuer à exister, ce qui provoque l'émission d'une nouvelle alerte presque immédiatement, mais cette fermeture d'alertes « toujours actives » réduit une partie de la contrainte système qui peut autrement se produire.

Configuration des notifications par e-mail

Vous pouvez configurer une liste d'e-mails pour les notifications relatives à un abonnement, ainsi qu'une liste globale de destinataires pour la notification des violations de seuil de la stratégie de performances.

Pour configurer les paramètres du destinataire de la notification, accédez à la page **Admin > Notifications** et sélectionnez l'onglet *Email*.



Destinataires de la notification d'abonnement

Pour configurer des destinataires pour les notifications d'événements liés à un abonnement, accédez à la section « destinataires de la notification d'abonnement ». Vous pouvez choisir d'envoyer des notifications par e-mail pour les événements liés à un abonnement à l'un ou l'ensemble des destinataires suivants :

- Tous les propriétaires de compte

- Tous les administrateurs *Monitor & Optimize*
- Adresses e-mail supplémentaires que vous spécifiez

Voici des exemples de types de notifications pouvant être envoyées et d'actions utilisateur que vous pouvez effectuer.

Notification:	Action de l'utilisateur:
La version d'essai ou l'abonnement a été mis à jour	Consultez les détails de l'abonnement sur la "Abonnement"page
L'abonnement expirera dans 90 jours. L'abonnement expirera dans 30 jours	Aucune action requise si le renouvellement automatique est activé. Contactez le service commercial NetApp pour renouveler l'abonnement
L'essai se termine dans 2 jours	Renouveler l'essai à partir de la "Abonnement"page. Vous pouvez renouveler une version d'évaluation une seule fois. Contactez le service commercial de NetApp pour souscrire un abonnement
La période d'essai ou l'abonnement a expiré le compte cessera de collecter les données dans 48 heures. Le compte sera supprimé après 48 heures	Contactez le service commercial de NetApp pour souscrire un abonnement

Pour vous assurer que vos destinataires reçoivent des notifications de Data Infrastructure Insights, ajoutez les adresses e-mail suivantes à n'importe quelle liste « Autoriser » :

- accounts@service.cloudinsights.netapp.com
- DoNotReply@cloudinsights.netapp.com

Liste globale des destinataires des alertes

Les notifications par e-mail d'alertes sont envoyées à la liste des destinataires de l'alerte pour chaque action de l'alerte. Vous pouvez choisir d'envoyer des notifications d'alerte à une liste de destinataires globale.

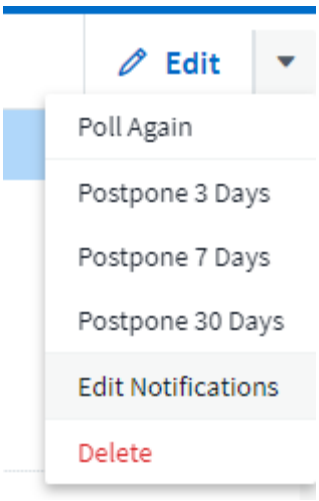
Pour configurer les destinataires d'alertes globales, sélectionnez les destinataires souhaités dans la section **destinataires de notification du moniteur global**.

Vous pouvez toujours remplacer la liste globale des destinataires d'un moniteur individuel lors de la création ou de la modification du moniteur.

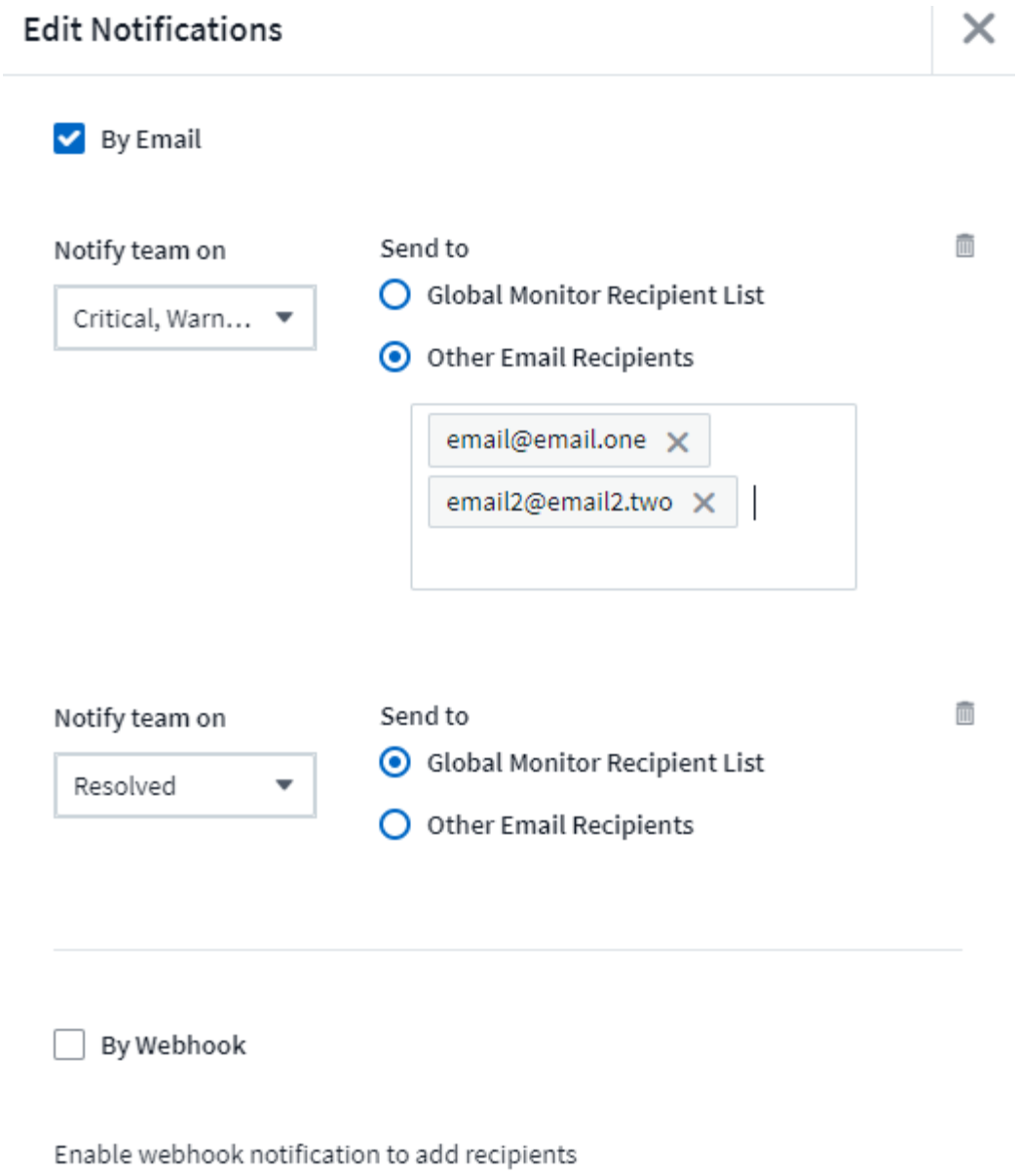
Les notifications ONTAP Data Collector prévalent sur toute notification Monitor spécifique pertinente au cluster/Data Collector. La liste des destinataires que vous définissez pour le Data Collector lui-même recevra les alertes du Data Collector. Si aucune alerte de collecte de données n'est active, des 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 le menu déroulant situé en haut à droite de la page d'accueil stockage.



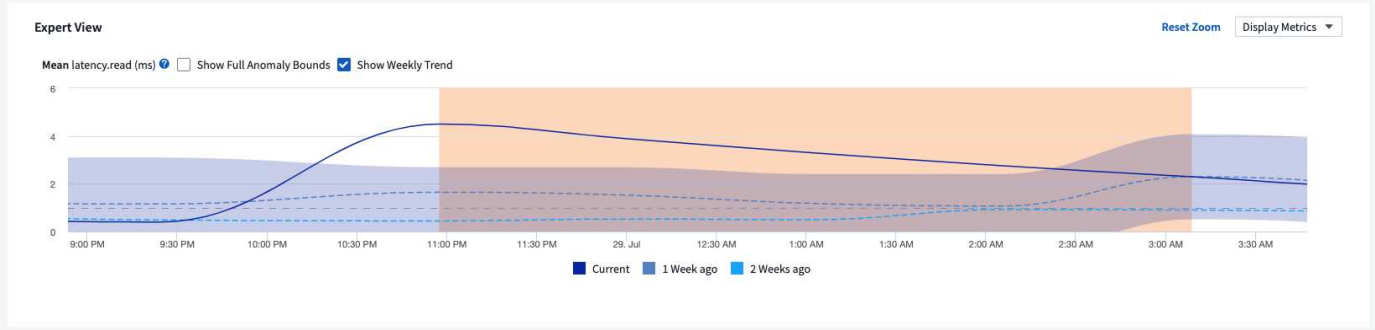
À partir de là, vous pouvez définir des notifications pour les alertes critiques, d'avertissement, d'information et/ou résolues. Chaque scénario peut avertir la liste des destinataires globaux ou les autres destinataires que vous choisissez.



Moniteurs de détection d'anomalies

La détection des anomalies fournit des informations sur les changements inattendus dans les modèles de données de votre locataire. Une anomalie se produit lorsque le comportement d'un objet change, par exemple, si un objet subit un certain niveau de latence le mercredi, mais que la latence dépasse ce niveau le mercredi suivant, ce pic est considéré comme une anomalie. Les informations sur l'infrastructure de données permettent de créer des moniteurs qui envoient des alertes en cas d'anomalies de ce type.

La détection des anomalies convient aux metrics objet qui présentent un modèle prévisible et récurrent. Lorsque ces metrics d'objet dépassent ou dépassent les niveaux attendus, Data Infrastructure Insights peut générer une alerte pour une investigation rapide.



Qu’est-ce que la détection des anomalies ?

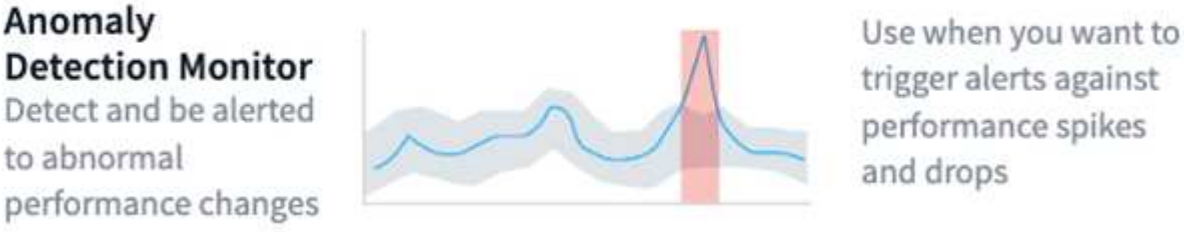
Une anomalie se produit lorsque la valeur moyenne d’une mesure est un certain nombre d’écarts-types par rapport à la moyenne pondérée de cette mesure pour les semaines précédentes, avec des semaines récentes ayant plus de poids que les semaines précédentes. Les informations sur l’infrastructure de données permettent de surveiller les données et d’émettre des alertes en cas de détection d’anomalies. Vous avez le choix de définir les niveaux de « sensibilité » de détection. Par exemple, une sensibilité plus élevée serait lorsque la valeur moyenne est moins d’écarts standard par rapport à la moyenne, ce qui entraînerait la génération d’alertes supplémentaires. Inversement, une sensibilité plus faible = des écarts plus standard par rapport à la moyenne = moins d’alertes.

La surveillance de la détection des anomalies diffère de la surveillance du seuil.

- **La surveillance basée sur le seuil** 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 plage normale).



- **La surveillance de la détection d’anomalie** utilise des algorithmes d’apprentissage automatique pour identifier les valeurs aberrantes qui dévient de la norme, car lorsque la définition de « normal » n’est pas claire.



Quand aurais-je besoin de la détection des anomalies ?

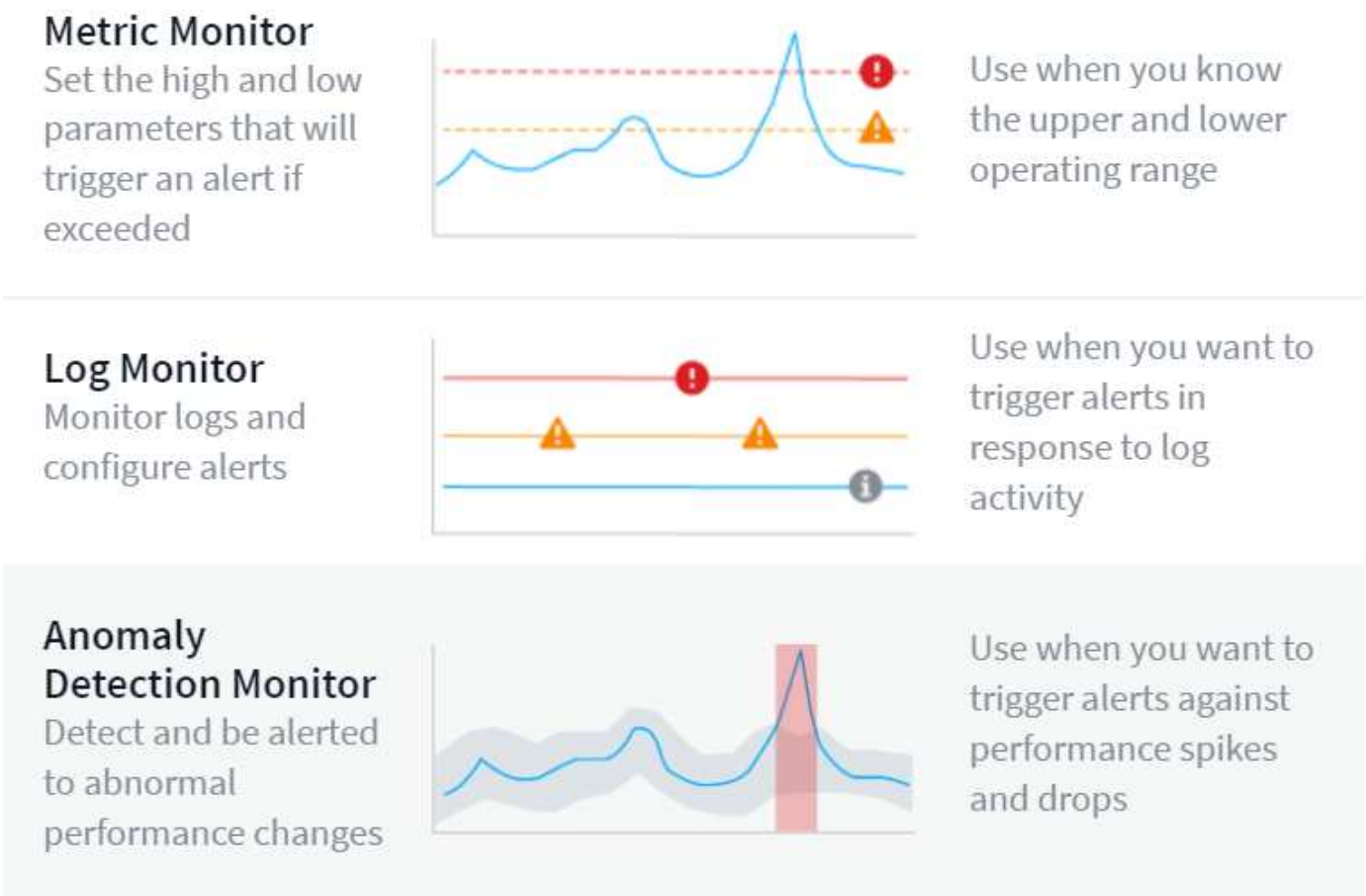
La surveillance de la détection des anomalies peut fournir des alertes utiles dans de nombreuses situations,

notamment :

- Lorsque la définition de *normal* n'est pas claire. Par exemple, les taux d'erreur SAN peuvent varier en fonction du port. Les alertes d'une erreur sont bruyantes et inutiles, mais une augmentation soudaine ou importante peut indiquer un problème à grande échelle.
- Là où il y a des changements dans le temps. Charges de travail soumises à des variations saisonnières (c'est-à-dire occupées ou peu actives à certains moments). Cela peut inclure des périodes de silence inattendues qui peuvent indiquer un blocage par lots.
- Vous ne pouvez pas travailler avec de grandes quantités de données pour définir et ajuster manuellement des seuils. Par exemple, un locataire qui compte un grand nombre d'hôtes et/ou de volumes avec des charges de travail variables. Si chacun d'entre eux présente différents SLA, il est donc important de comprendre ceux qui dépassent la norme.

Création d'un moniteur de détection des anomalies

Pour signaler des anomalies, créez un moniteur en accédant à **observabilité > alertes > +Monitor**. Sélectionnez *surveillance de détection d'anomalie* comme type de moniteur.

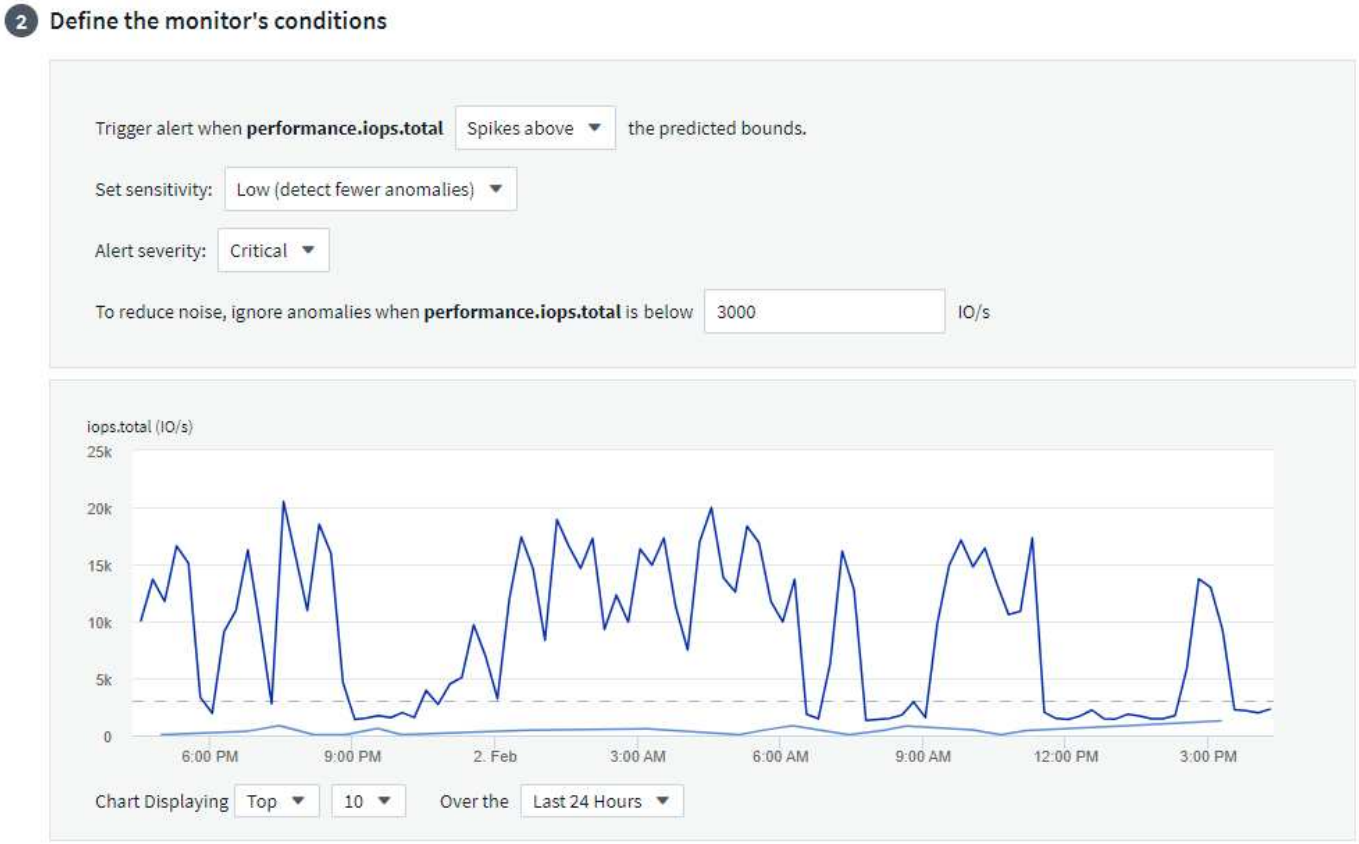


Choisissez l'objet et la mesure à surveiller. Vous pouvez définir des filtres et des groupes comme pour d'autres types de moniteurs.

Définissez ensuite les conditions du moniteur.

- Déclencher une alerte lorsque la mesure sélectionnée est *surportée* les limites prévues, *chute en dessous* ces limites, ou les deux.

- Réglez la sensibilité sur *moyenne*, *faible* (moins d'anomalies détectées) ou *élevée* (plus d'anomalies détectées).
- Déterminez si le niveau d'alerte est *critique* ou *Avertissement*.
- Vous pouvez également définir une valeur au-dessous de laquelle les anomalies sont *ignorées*. Cela peut contribuer à réduire le bruit. Cette valeur s'affiche sous la forme d'une ligne pointillée sur le graphique échantillon.



Enfin, vous pouvez configurer une méthode de livraison pour les alertes (e-mail, webhook, ou les deux), fournir au moniteur une description facultative ou des actions correctives, et ajouter le moniteur à un groupe personnalisé, si vous le souhaitez.

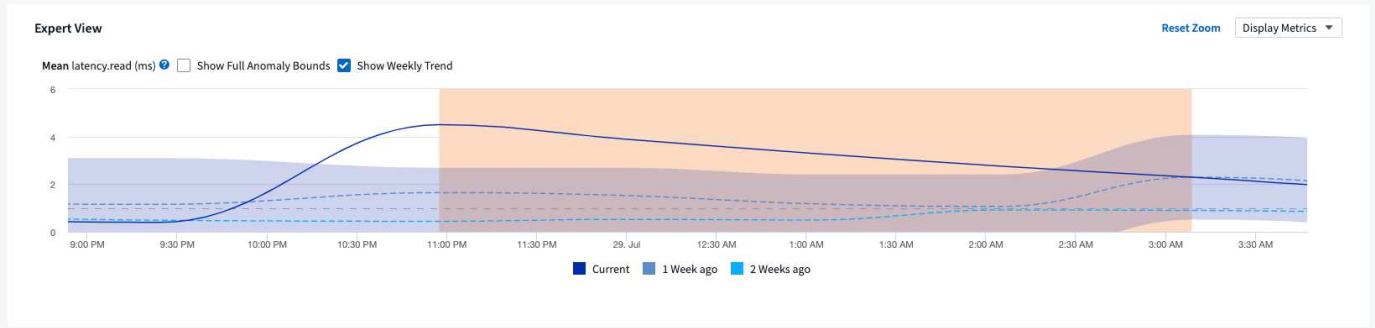
Enregistrez le moniteur avec un nom significatif, et vous avez terminé.

Lors de sa création, le moniteur analyse les données de la semaine précédente afin d'établir une base initiale. La détection des anomalies est plus précise au fil du temps et l'historique s'en trouve accru.

> Lors de la création d'un moniteur, DII analyse les données de la semaine précédente pour détecter les pics ou les baisses significatifs ; ces données sont considérées comme des anomalies. Durant la première semaine suivant la création du moniteur (phase d'apprentissage), il est possible que les alertes présentent un risque de bruit accru. Pour atténuer ce bruit, seules les pics ou les baisses de plus de 30 minutes sont considérées 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.

Affichage des anomalies

Sur une page d'accueil d'alerte, les alertes déclenchées lorsque des anomalies sont détectées affichent une bande mise en surbrillance dans le graphique, à partir du moment où la mesure a surpassé les limites prévues jusqu'au moment où elle est replacée à l'intérieur de ces limites.



Lorsque vous affichez un graphique d'anomalies sur une page d'accueil d'alerte, vous pouvez choisir les options suivantes :

- Tendance hebdomadaire : comparez les valeurs à la même heure, le jour même des semaines précédentes, pour un maximum de 5 semaines précédentes.
- Limites d'anomalie complètes : par défaut, le graphique se concentre sur la valeur de la mesure pour vous permettre de mieux analyser le comportement de la mesure. Sélectionnez cette option pour afficher les limites d'anomalie complètes (valeur maximale, etc.)

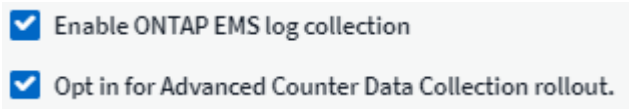
Vous pouvez également afficher les objets qui ont contribué à l'anomalie en les sélectionnant dans la vue experte de la page d'accueil. Le graphique affiche le comportement des objets sélectionnés.



Moniteurs système

Les informations d'infrastructure de données comprennent un certain nombre de contrôles définis par le système pour les metrics 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 changent.

Par défaut, de nombreux moniteurs système sont en état *pause*. Vous pouvez activer un moniteur système en sélectionnant l'option *Resume* pour le moniteur. Assurez-vous que *la collecte avancée de données de compteur* et *l'activation de la collecte de journaux EMS ONTAP* sont activées dans le collecteur de données. Ces options se trouvent dans le Data Collector ONTAP sous *Configuration avancée*:



sommaire :[]

Description du moniteur

Les moniteurs définis par le système comprennent des mesures et des conditions prédéfinies, ainsi que des descriptions par défaut et des actions correctives, qui ne peuvent pas être modifiées. Vous pouvez *CAN* modifier la liste des destinataires de notification pour les moniteurs définis par le système. Pour afficher les mesures, 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 ni supprimés.

Les moniteurs définis par le système suivants sont disponibles dans les groupes indiqués.

- **ONTAP Infrastructure** comprend des moniteurs pour les problèmes liés à l'infrastructure dans les clusters ONTAP.
- **Exemples de charge de travail ONTAP** comprend des moniteurs pour les problèmes liés à la charge de travail.
- Les moniteurs des deux groupes sont par défaut à l'état *Pause*.

Voici les moniteurs système actuellement inclus dans Data Infrastructure Insights :

Moniteurs métriques

Nom du moniteur	Gravité	Description du moniteur	Action corrective

Taux d’utilisation des ports Fibre Channel élevé	PRIMORDIAL	Les ports Fibre Channel Protocol sont utilisés pour recevoir et transférer le trafic SAN entre le système hôte du client et les LUN ONTAP. Si l’utilisation du port est élevée, Ensuite, il deviendra un goulot d’étranglement et aura une incidence sur les performances des charges de travail sensibles du protocole Fibre Channel.…Une alerte d’avertissement indique que des actions planifiées doivent être prises pour équilibrer le trafic réseau.…Une alerte critique indique que l’interruption du service est imminente et que des mesures d’urgence doivent être prises pour équilibrer le réseau trafic pour assurer la continuité des services.	Si le seuil critique est atteint, prenez en compte les mesures immédiates pour limiter les interruptions de service : 1. Déplacez les charges de travail vers un autre port FCP le plus utilisé. 2. Limitez le trafic de certaines LUN uniquement au travail essentiel, via des règles de QoS dans ONTAP ou une configuration côté hôte pour alléger l’utilisation des ports FCP.… Si le seuil d’avertissement est dépassé, prévoyez d’effectuer les actions suivantes : 1. Configurez davantage de ports FCP pour gérer le trafic de données afin que l’utilisation des ports soit répartie entre plusieurs ports. 2. Déplacez les charges de travail vers un autre port FCP le plus utilisé. 3. Limitez le trafic de certaines LUN uniquement à un travail essentiel, via des règles de QoS dans ONTAP ou une configuration côté hôte pour alléger l’utilisation des ports FCP.

Latence élevée de la LUN	PRIMORDIAL	Les LUN sont des objets qui servent le trafic d'E/S souvent pilotés par les applications sensibles aux performances telles que les bases de données. Des latences de LUN élevées signifient que les applications elles-mêmes pourraient souffrir et être incapables d'accomplir leurs tâches. Une alerte d'avertissement indique que des actions planifiées doivent être prises pour déplacer la LUN vers le nœud ou l'agrégat approprié. Une alerte critique indique que l'interruption du service est imminente et que des mesures d'urgence doivent être prises assurer la continuité des services Voici les latences attendues pour le type de support : SSD jusqu'à 1-2 millisecondes, SAS jusqu'à 8-10 millisecondes et disques durs SATA de 17-20 milliseconde	Si le seuil critique est dépassé, envisagez les actions suivantes pour minimiser l'interruption de service : si la LUN ou son volume dispose d'une politique de QoS associée, évaluez ses limites de seuil et validez si elles provoquent le plafrement de la charge de travail de la LUN.… Si le seuil d'avertissement est dépassé, prévoyez d'effectuer les actions suivantes : 1. Si l'agrégat connaît également un taux d'utilisation élevé, déplacez le LUN vers un autre agrégat. 2. Si l'utilisation du nœud est également élevée, déplacez-le vers un autre nœud ou réduisez la charge de travail totale du nœud. 3. Si une règle de QoS est associée à la LUN ou à son volume, évaluez ses limites de seuil et vérifiez s'ils provoquent le plafissement de la charge de travail de la LUN.

Optimisation de l'utilisation des ports réseau élevée	PRIMORDIAL	Les ports réseau permettent de recevoir et de transférer le trafic protocole NFS, CIFS et iSCSI entre les systèmes hôtes du client et les volumes ONTAP. Si l'utilisation du port est élevée, cela devient un goulot d'étranglement et affecte à terme les performances de NFS, Les charges de travail CIFS et iSCSI… Une alerte d'avertissement indique que des actions planifiées doivent être entreprises pour équilibrer le trafic réseau.…Une alerte critique indique que l'interruption du service est imminente et que des mesures d'urgence doivent être prises pour équilibrer le trafic réseau afin d'assurer la continuité du service.	Si le seuil critique est atteint, prenez en compte les actions immédiates suivantes pour limiter les interruptions de service : 1. Limiter le trafic de certains volumes uniquement à un travail essentiel, soit via les stratégies de QoS dans ONTAP, soit l'analyse côté hôte pour diminuer l'utilisation des ports réseau. 2. Configurez un ou plusieurs volumes pour utiliser un autre port réseau utilisé inférieur.… Si le seuil d'avertissement est dépassé, prenez en compte les actions immédiates suivantes : 1. Configurez davantage de ports réseau pour gérer le trafic de données afin que l'utilisation des ports soit répartie entre plusieurs ports. 2. Configurez un ou plusieurs volumes pour qu'ils utilisent un autre port réseau moins utilisé.

Latence élevée du namespace NVMe	PRIMORDIAL	Les espaces de noms NVMe sont des objets qui servent le trafic d'E/S piloté par des applications sensibles aux performances, telles que les bases de données. Une latence élevée pour les espaces de noms NVMe signifie que les applications elles-mêmes sont susceptibles de subir des problèmes et qu'elles ne peuvent pas accomplir leurs tâches. Une alerte d'avertissement indique que des actions planifiées doivent être entreprises pour déplacer la LUN vers le nœud ou l'agrégat approprié. Une alerte critique indique que l'interruption du service est imminente et que des mesures d'urgence doivent être prises pour assurer la continuité des services.	Si le seuil critique est dépassé, prenez des mesures immédiates pour minimiser l'interruption des services : si une règle de QoS est attribuée à l'espace de noms NVMe ou à son volume, évaluez ses seuils au cas où ils seraient à l'origine de la restriction de la charge de travail de l'espace de noms NVMe.… Si le seuil d'avertissement est dépassé, prenez les mesures suivantes : 1. Si l'agrégat connaît également un taux d'utilisation élevé, déplacez le LUN vers un autre agrégat. 2. Si l'utilisation du nœud est également élevée, déplacez-le vers un autre nœud ou réduisez la charge de travail totale du nœud. 3. Si une politique de QoS est attribuée au namespace NVMe ou à son volume, évaluez ses seuils limites si celui-ci est à l'origine de la restriction de la charge de travail de l'espace de noms NVMe.

Capacité qtree saturée	PRIMORDIAL	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 quotas pour limiter la quantité de données stockées dans l'arborescence dans la capacité du volume.…Une alerte d'avertissement indique que l'action planifiée doit être prise pour augmenter l'espace.…Une alerte critique indique que l'interruption du service est imminente et imminente des mesures d'urgence doivent être prises pour libérer de l'espace afin d'assurer la continuité du service.	Si le seuil critique est atteint, prenez en compte les mesures immédiates pour limiter les interruptions de service : 1. Augmenter l'espace du qtree afin de faire face 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 suivantes : 1. Augmenter l'espace du qtree afin de faire face à la croissance. 2. Supprimez les données indésirables pour libérer de l'espace.

Limite matérielle de capacité qtree	PRIMORDIAL	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, utilisé pour stocker les données afin de contrôler la croissance des données utilisateur dans le volume et de ne pas dépasser sa capacité totale.…Un qtree maintient un quota de capacité de stockage souple qui permet à l'utilisateur d'être averti de manière proactive avant d'atteindre le total quota de capacité limité dans le qtree et incapable de stocker des données plus. La surveillance de la quantité de données stockées dans un qtree permet à l'utilisateur de recevoir un service de données sans interruption.	Si le seuil critique est atteint, prenez en compte les actions immédiates suivantes pour limiter les interruptions de service : 1. Augmenter le quota d'espace de l'arbre afin de s'adapter à la croissance 2. Demandez à l'utilisateur de supprimer des 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 les données afin de contrôler la croissance des données utilisateur dans le volume et de ne pas dépasser sa capacité totale.…Un qtree maintient un quota de capacité de stockage souple qui permet à l'utilisateur d'être averti de manière proactive avant d'atteindre le limite de quota de capacité totale dans le qtree, impossible de stocker des données plus. La surveillance de la quantité de données stockées dans un qtree permet à l'utilisateur de recevoir un service de données sans interruption.	Si le seuil d'avertissement est dépassé, prenez en compte les actions immédiates suivantes : 1. Augmenter le quota d'espace de l'arbre 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	PRIMORDIAL	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 de nombre de fichiers qu'elle peut contenir pour maintenir une taille de système de fichiers gérable au sein du volume.…Un qtree conserve un quota de nombre de fichiers au-delà duquel les nouveaux fichiers de l'arborescence sont refusés. La surveillance du nombre de fichiers dans un qtree permet à l'utilisateur de recevoir un service de données sans interruption.	Si le seuil critique est atteint, prenez en compte les mesures immédiates pour limiter les interruptions de service : 1. Augmenter 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 d'un nombre de fichiers qu'il peut contenir afin de maintenir une taille de système de fichiers gérable au sein du volume.…Un qtree conserve un quota de numéro de fichier logiciel afin de fournir une alerte à l'utilisateur de manière proactive avant d'atteindre la limite de fichiers dans le qtree et impossible de stocker des fichiers supplémentaires. La surveillance du nombre de fichiers dans un qtree permet à l'utilisateur de recevoir un service de données sans interruption.	Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures suivantes : 1. Augmenter le quota de nombre de fichiers pour le qtree. 2. Supprimez les fichiers indésirables du système de fichiers qtree.

Espace de réserve Snapshot plein	PRIMORDIAL	La capacité de stockage d'un volume est nécessaire pour stocker les données des applications et des clients. Une partie de cet espace, appelée espace réservé pour les instantanés, est utilisée pour stocker des instantanés qui permettent de protéger les données localement. Plus les données stockées dans le volume ONTAP sont récentes, plus la capacité Snapshot est élevée et moins la capacité de stockage des copies Snapshot est disponible pour les données mises à jour ou nouvelles. Si la capacité des données snapshot d'un volume atteint l'espace total de réserve snapshot, il se peut que le client ne puisse pas stocker de nouvelles données snapshot et qu'il ne puisse pas réduire le niveau de protection des données du volume. La surveillance du volume utilisé permet la continuité des services de données.	Si le seuil critique est atteint, prenez en compte les mesures immédiates pour limiter les interruptions de service : 1. Configurez les instantanés pour utiliser l'espace de données dans le volume lorsque la réserve Snapshot est pleine. 2. Supprimez quelques anciens snapshots indésirables pour libérer de l'espace.… Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures suivantes : 1. Augmentez l'espace de réserve Snapshot au sein du volume pour faire face à la croissance. 2. Configurez les instantanés pour utiliser l'espace de données dans le volume lorsque la réserve Snapshot est pleine.

Limite de capacité de stockage	PRIMORDIAL	Lorsqu'un pool de stockage (agrégat) est en cours de remplissage, les opérations d'E/S ralentissent et finissent par entraîner un incident lors d'une panne du stockage. Une alerte d'avertissement indique que l'action planifiée doit être prise prochainement pour restaurer un espace disponible minimal. Une alerte critique indique que l'interruption des services est imminente et que des mesures d'urgence doivent être prises pour libérer de l'espace afin d'assurer la continuité des services.	Si le seuil critique est atteint, prendre immédiatement en compte les actions suivantes pour minimiser les interruptions de service : 1. Supprimez des snapshots sur des volumes non critiques. 2. Supprimez des volumes ou des LUN qui ne sont pas des workloads essentiels et qui peuvent être restaurés à partir de copies de stockage…… si le seuil d'avertissement est dépassé, planifiez les actions immédiates suivantes : 1. Déplacement d'un ou plusieurs volumes vers un autre emplacement de stockage 2. Ajoutez de la capacité de stockage. 3. Modifiez les paramètres d'efficacité du stockage ou transférez les données inactives vers le stockage cloud.

Limite de performances du stockage	PRIMORDIAL	Lorsqu'un système de stockage atteint ses limites de performances, les opérations sont lentes, la latence augmente et les charges de travail et les applications peuvent tomber en panne. ONTAP évalue l'utilisation du pool de stockage pour les charges de travail et estime le pourcentage de performance consommé. Une alerte d'avertissement indique que des actions planifiées doivent être effectuées pour réduire la charge du pool de stockage afin de garantir que les pics de charge de travail du pool de stockage seront suffisants.…Une alerte critique indique que cela ces problèmes de performances sont imminents et des mesures d'urgence doivent être prises pour réduire la charge des pools de stockage afin d'assurer la continuité des services.	Si le seuil critique est atteint, prenez en compte les actions immédiates suivantes pour limiter les interruptions de service : 1. Suspendre les tâches planifiées telles que les snapshots ou la réplication SnapMirror. 2. Charges de travail inactives non essentielles.… Si le seuil d'avertissement est dépassé, effectuez immédiatement les actions suivantes : 1. Déplacez une ou plusieurs charges de travail vers un autre emplacement de stockage. 2. Ajout de nœuds de stockage (AFF) ou de tiroirs disques (FAS) et redistribution des charges de travail 3. Modifiez les caractéristiques des charges de travail (taille de bloc, mise en cache des applications).

Limite matérielle de capacité de quota utilisateur	PRIMORDIAL	ONTAP reconnaît les utilisateurs des systèmes Unix ou Windows qui sont autorisés à accéder aux volumes, aux fichiers ou aux 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 politique utilisateur ou 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 capacité utilisée dans le volume est juste avant d'atteindre le quota de capacité totale. Le contrôle de la quantité de données stockées dans un quota utilisateur ou groupe garantit que l'utilisateur reçoit un service de données ininterrompu.	Si le seuil critique est atteint, prenez en compte les actions immédiates suivantes pour limiter les interruptions de service : 1. Augmenter l'espace du quota de l'utilisateur ou du groupe pour faire face à la croissance. 2. Demandez à l'utilisateur ou au groupe de supprimer les données indésirables pour libérer de l'espace.

Quota utilisateur - limite logicielle de capacité	AVERTISSEMENT	ONTAP reconnaît l'utilisateur des systèmes Unix ou Windows qui sont autorisés à accéder aux volumes, aux fichiers ou aux 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 utilisateur ou groupe limite l'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 capacité utilisée dans le volume atteint le quota de capacité totale. Le contrôle de la quantité de données stockées dans un quota utilisateur ou groupe garantit que l'utilisateur reçoit un service de données ininterrompu.	Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures suivantes : 1. Augmenter l'espace du quota de l'utilisateur ou du groupe pour faire face à la croissance. 2. Supprimez les données indésirables pour libérer de l'espace.

Capacité du volume saturée	PRIMORDIAL	La capacité de stockage d'un volume est nécessaire pour stocker les données des applications et des clients. Plus le volume ONTAP est stocké, plus la disponibilité du stockage des données futures est faible. Si la capacité de stockage de données d'un volume atteint la capacité de stockage totale, cela peut conduire le client à ne pas pouvoir stocker les données en raison d'une capacité de stockage insuffisante. La surveillance du volume utilisé permet d'assurer la continuité des services de données.	Si le seuil critique est atteint, prenez en compte les actions immédiates suivantes pour limiter les interruptions de service : 1. Augmentation de l'espace du volume pour suivre la croissance. 2. Supprimez les données indésirables pour libérer de l'espace. 3. Si les copies snapshot occupent plus d'espace que la réserve d'instantanés, supprimez les anciens snapshots ou activez l'instantané de volume.…si le seuil d'avertissement est dépassé, prévoyez d'effectuer les actions immédiates suivantes : 1. Augmentation de l'espace du volume pour suivre la croissance 2. Si les copies snapshot occupent plus d'espace que la réserve de snapshots, supprimez les anciens snapshots ou activez la suppression automatique de l'instantané de volume.……

Limite des inodes de volume	PRIMORDIAL	Les volumes qui stockent des fichiers utilisent des nœuds d'index (inode) pour stocker les métadonnées de fichiers. Lorsqu'un volume épuise son allocation d'inode, Aucun autre fichier ne peut y être ajouté.…Une alerte d'avertissement indique que des actions planifiées doivent être prises pour augmenter le nombre d'inodes disponibles.…Une alerte critique indique que la limite de fichier est imminente et que des mesures d'urgence doivent être prises pour libérer des inodes afin d'assurer la continuité du service.	Si le seuil critique est atteint, prenez en compte les actions immédiates suivantes pour limiter 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 pour prendre en charge de grands systèmes de fichiers.… Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures 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 pour la prise en charge de systèmes de fichiers volumineux

Latence de volume élevée	PRIMORDIAL	Les volumes sont des objets qui servent le trafic d'E/S souvent pilotés par les applications sensibles aux performances, telles que les applications DevOps, les répertoires locaux et les bases de données. Une latence élevée signifie que les applications elles-mêmes risquent de subir des conséquences et d'être dans l'impossibilité d'accomplir leurs tâches. Pour maintenir des performances prévisibles au niveau des applications, il est essentiel de contrôler les latences des volumes. Les latences suivantes sont attendues pour le type de support : SSD jusqu'à 1-2 millisecondes ; SAS jusqu'à 8-10 millisecondes et disques durs SATA 17-20 millisecondes.	Si le seuil critique est dépassé, envisagez de suivre des actions immédiates pour minimiser l'interruption de service : si une politique de QoS est attribuée au volume, évaluez ses seuils limites au cas où ils provoquent l'étranglement de la charge de travail du volume.… Si le seuil d'avertissement est dépassé, prenez en compte les actions immédiates suivantes : 1. Si l'agrégat connaît également un taux d'utilisation élevé, déplacez le volume vers un autre agrégat. 2. Si une politique de QoS est attribuée au volume, évaluez ses seuils limités si celui-ci ralentit la charge de travail du volume. 3. Si l'utilisation du nœud est également élevée, déplacez-le vers un autre nœud ou réduisez la charge de travail totale du nœud.
Nom du moniteur	Gravité	Description du moniteur	Action corrective

Latence élevée du nœud	AVERTISSEMENT / CRITIQUE	La latence du nœud a atteint les niveaux où elle peut affecter les performances des applications du nœud. Une latence de nœud moindre garantit la prévisibilité des performances des applications. Les latences attendues pour le type de support sont : SSD jusqu'à 1-2 millisecondes ; SAS jusqu'à 8-10 millisecondes et disques durs SATA 17-20 millisecondes.	Si un seuil critique est atteint, des mesures immédiates doivent être prises pour limiter les interruptions de service : 1. Suspension des tâches planifiées, des snapshots ou de la réplication SnapMirror 2. Réduisez les besoins des workloads à priorité faible grâce aux limites de qualité de service 3. Désactiver les charges de travail non essentielles considère les 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 les besoins des workloads à priorité faible grâce aux limites de qualité de service 3. Ajout de nœuds de stockage (AFF) ou de tiroirs disques (FAS) et redistribution des charges de travail 4. Modifier les caractéristiques des charges de travail (taille de bloc, mise en cache des applications, etc.)

Limite de performance du nœud	AVERTISSEMENT / CRITIQUE	L'utilisation des performances du nœud a atteint les niveaux où elle peut affecter les performances des E/S et des applications prises en charge par le nœud. Des nœuds peu performants garantissent la prévisibilité des performances des applications.	Des mesures immédiates doivent être prises pour minimiser les interruptions de service si un seuil critique est atteint : 1. Suspension des tâches planifiées, des snapshots ou de la réplication SnapMirror 2. Réduisez les besoins des workloads à priorité faible grâce aux limites de qualité de service 3. Inactiver les charges de travail non essentielles tenez compte des 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 les besoins des workloads à priorité faible grâce aux limites de qualité de service 3. Ajout de nœuds de stockage (AFF) ou de tiroirs disques (FAS) et redistribution des charges de travail 4. Modifier les caractéristiques des charges de travail (taille de bloc, mise en cache des applications, etc.)

Latence élevée des machines virtuelles de stockage	AVERTISSEMENT / CRITIQUE	La latence des VM de stockage a atteint les niveaux où elle peut affecter les performances des applications sur la VM de stockage. La faible latence des machines virtuelles de stockage garantit la prévisibilité des performances des applications. Les latences attendues pour le type de support sont : SSD jusqu'à 1-2 millisecondes ; SAS jusqu'à 8-10 millisecondes et disques durs SATA 17-20 millisecondes.	Si le seuil critique est atteint, évaluez immédiatement les limites de seuil des volumes de la machine virtuelle de stockage auxquels une règle de qualité de service est attribuée, afin de vérifier s'il est en cause, les charges de travail des volumes seront immédiatement mises en œuvre en cas de dépassement du seuil d'avertissement : 1. Si l'agrégat connaît également une exploitation 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 règle de qualité de service assignée, évaluez les limites du seuil s'ils provoquent l'étranglement des charges de travail de volume 3. Si l'utilisation du nœud est élevée, déplacez certains volumes de la machine virtuelle de stockage vers un autre nœud ou réduisez l'ensemble de la charge de travail du nœud
Limite stricte des fichiers de quota utilisateur	PRIMORDIAL	Le nombre de fichiers créés au sein du volume a atteint la limite critique et aucun fichier supplémentaire ne peut être créé. La surveillance du nombre de fichiers stockés permet à l'utilisateur de recevoir un service de données sans interruption.	Des actions immédiates sont requises pour minimiser les interruptions de service si le seuil critique est atteint.…envisager de prendre les actions 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 logicielle des fichiers de quota utilisateur	AVERTISSEMENT	Le nombre de fichiers créés au sein du volume a atteint la limite seuil du quota et se situe à proximité 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.	Prenez en compte les actions immédiates si le seuil d'avertissement est dépassé : 1. Augmenter le quota de nombre de fichiers pour le quota d'utilisateur spécifique 2. Supprimez les fichiers indésirables pour réduire la pression sur le quota de fichiers pour l'utilisateur spécifique

Taux de Miss. Du cache du volume	AVERTISSEMENT / CRITIQUE	Volume cache Miss ratio est le pourcentage de demandes de lecture des applications client renvoyées du disque au lieu d'être renvoyées à partir du cache. Cela signifie que le volume a atteint le seuil défini.	Si un seuil critique est atteint, des mesures immédiates doivent être prises pour limiter les interruptions de service : 1. Déplacez certaines charges de travail depuis le nœud du volume pour réduire la charge d'E/S 2. Si ce n'est pas déjà le cas sur le nœud du volume, augmentez le cache WAFL en achetant et en ajoutant un module Flash cache 3. Lorsque le seuil d'avertissement est dépassé, réduisez les besoins en charges de travail moins prioritaires sur le même nœud via les limites de QoS. Déplacez certaines charges de travail depuis le nœud du volume pour réduire la charge d'E/S 2. Si ce n'est pas déjà le cas sur le nœud du volume, augmentez le cache WAFL en achetant et en ajoutant un module Flash cache 3. Réduisez les besoins en charges de travail prioritaires sur le même nœud via la limitation de la qualité de service 4. Modifier les caractéristiques des charges de travail (taille de bloc, mise en cache des applications, etc.)

Surallocation du quota de qtree volume	AVERTISSEMENT / CRITIQUE	Volume qtree quota overcommit spécifie le pourcentage auquel un volume est considéré comme surallouant par les quotas qtree. Le seuil défini pour le quota qtree est atteint pour le volume. La surveillance du surengagement de quota qtree du volume permet à l'utilisateur de recevoir un service de données sans interruption.	Si un seuil critique est atteint, des mesures immédiates doivent être prises pour limiter les interruptions de service : 1. Augmenter l'espace du volume 2. Supprimez les données non souhaitées lorsque le seuil d'avertissement est atteint, puis envisagez d'augmenter l'espace du volume.

Haut de la page

Moniteurs de journaux

Nom du moniteur	Gravité	Description	Action corrective
Identifiants AWS non initialisés	INFO	Cet événement se produit lorsqu'un module tente d'accéder aux identifiants basés sur les rôles Amazon Web Services (AWS) et de gestion des identités et des accès à partir du thread d'informations d'identification cloud avant leur initialisation.	Attendez que le thread des informations d'identification du cloud, ainsi que le système, aient terminé l'initialisation.

Cloud Tier inaccessible	PRIMORDIAL	Un nœud de stockage ne peut pas se connecter à l'API de 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 fonctionnelle 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 nœud de destination LIF intercluster… Assurez-vous ce qui suit :…la configuration de votre magasin d'objets n'a pas changé.…les informations de connexion et de connectivité sont Toujours valide… 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 d'assainissement ou est entré dans le centre de maintenance.	Aucune.

Composant FlexGroup complet	PRIMORDIAL	Un composant d'un volume FlexGroup est saturé, 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 dans le composant ne peut être modifié. Par conséquent, des erreurs aléatoires liées au manque d'espace peuvent s'afficher lorsque vous tentez d'effectuer des opérations d'écriture sur le volume FlexGroup.	Il est recommandé d'ajouter de la capacité au volume FlexGroup à l'aide de la commande « volume modify -Files +X »….alternativement, supprimez des fichiers du volume FlexGroup. Toutefois, il est difficile de déterminer quels fichiers ont été débarqués sur le composant.
FlexGroup Constituent presque plein	AVERTISSEMENT	Un composant d'un volume FlexGroup est quasiment à court d'espace, ce qui peut entraîner une interruption potentielle du service. Vous pouvez créer et développer des fichiers. Cependant, si le composant est à court d'espace, il se peut que vous ne puissiez pas ajouter ou modifier les fichiers du composant.	Il est recommandé d'ajouter de la capacité au volume FlexGroup à l'aide de la commande « volume modify -Files +X »….alternativement, supprimez des fichiers du volume FlexGroup. Toutefois, il est difficile de déterminer quels fichiers ont été débarqués sur le composant.
FlexGroup Constituent quasiment hors des inodes	AVERTISSEMENT	Un composant d'un volume FlexGroup se trouve quasiment en dehors des inodes, à l'origine d'une interruption potentielle du service. Le composant reçoit des demandes de création moins élevées que la moyenne. Cela peut avoir un impact sur les performances globales du volume FlexGroup, car les demandes sont acheminées à des composants avec davantage d'inodes.	Il est recommandé d'ajouter de la capacité au volume FlexGroup à l'aide de la commande « volume modify -Files +X »….alternativement, supprimez des fichiers du volume FlexGroup. Toutefois, il est difficile de déterminer quels fichiers ont été débarqués sur le composant.

FlexGroup Constituent à partir d'inodes	PRIMORDIAL	Un composant d'un volume FlexGroup a des inodes, à un risque de perturbation potentielle du service. Vous ne pouvez pas créer de nouveaux fichiers sur ce composant. Cela peut conduire à une distribution du contenu globalement iméquilibrée sur l'ensemble du volume FlexGroup.	Il est recommandé d'ajouter de la capacité au volume FlexGroup à l'aide de la commande « volume modify -Files +X »….alternativement, supprimez des fichiers du volume FlexGroup. Toutefois, il est difficile de déterminer quels fichiers ont été débarqués sur le composant.
LUN hors ligne	INFO	Cet événement se produit lorsqu'une LUN est mise hors ligne manuellement.	Remettre la LUN en ligne.
Echec du ventilateur de l'unité principale	AVERTISSEMENT	Un ou plusieurs ventilateurs de l'unité principale sont défectueux. 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 en état d'avertissement.	Remplacer les ventilateurs indiqués pour éviter toute surchauffe.

Batterie NVRAM faible	AVERTISSEMENT	La capacité de la batterie NVRAM est extrêmement faible. Une perte de données peut se produire si la batterie devient hors tension.…votre système génère et transmet un message AutoSupport ou d'appel en cas d'incident au support technique NetApp et aux destinations configurées si elle est configurée pour le faire. La transmission réussie d'un message AutoSupport améliore considérablement la détermination et la résolution des problèmes.	Effectuez les actions correctives suivantes :…visualisez l'état actuel de la batterie, sa capacité et son état de charge à l'aide de la commande « System node Environment Sensors ».…si la batterie a été remplacée récemment ou si le système n'était pas opérationnel pendant une période prolongée, Surveillez la batterie pour vérifier qu'elle se charge correctement.…contactez le support technique de 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 une fois par semaine pour vous rappeler de configurer le processeur de service. Le processeur de service est un dispositif physique intégré à votre système pour fournir des fonctions d'accès à distance et de gestion à distance. Vous devez configurer le processeur de service pour qu'il utilise toutes ses fonctionnalités.	Effectuez les actions correctives suivantes :…configurez le SP à l'aide de la commande « system service-processor network modify ».…facultativement, Obtenir l'adresse MAC du processeur de service à l'aide de la commande « system service-processor network show ».…Vérifiez la configuration du réseau du processeur de service à l'aide de la commande « system service-processor network show ».…Vérifiez que le processeur de service peut envoyer un e-mail AutoSupport à l'aide de la commande « system service-processor AutoSupport Invoke ». REMARQUE : les hôtes de messagerie et les destinataires AutoSupport doivent être configurés dans ONTAP avant d'exécuter cette commande.

Processeur de service hors ligne	PRIMORDIAL	Le processeur de service ne reçoit plus de signaux émis par le processeur de service, même si toutes les actions de restauration du processeur de service ont été effectuées. ONTAP ONTAP ne peut pas surveiller l'état du matériel sans le SP.… le système s'arrêtera pour éviter des dommages matériels et des pertes de données. Configurez une alerte de panique pour être immédiatement avertie en cas de mise hors ligne du processeur de service.	Mettez le système hors tension puis sous tension en exécutant les actions suivantes :…retirez le contrôleur du châssis.…remettez le contrôleur sous tension.…si le problème persiste, remplacez le module de contrôleur.
Défaillance des ventilateurs du tiroir	PRIMORDIAL	Le module de ventilateur ou de ventilateur de refroidissement indiqué du shelf est défectueux. Les disques du tiroir peuvent ne pas recevoir suffisamment d'air de refroidissement, ce qui peut entraîner une panne du disque.	Effectuez les actions correctives suivantes :…Vérifiez que le module de ventilateur est bien en place et bien fixé. REMARQUE : le ventilateur est intégré au module d'alimentation dans certains tiroirs disques.… si le problème persiste, remplacez le module de ventilation.… 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	PRIMORDIAL	Un ou plusieurs ventilateurs de l'unité principale sont défectueux, ce qui interrompt le fonctionnement du système. Cela peut entraîner une perte potentielle de données.	Remplacez les ventilateurs défectueux.

Disques non assignés	INFO	Le système contient des disques non attribués. La capacité est alors gaspillée et votre système peut disposer de erreurs de configuration ou de modifications partielles de la configuration.	Effectuez les actions correctives suivantes :…déterminez quels disques sont non affectés en utilisant la commande « disk show -n »….affectez les disques à un système à l'aide de la commande « disk assigned ».
Serveur antivirus occupé	AVERTISSEMENT	Le serveur antivirus est trop occupé pour accepter toute nouvelle demande de scan.	Si ce message se produit fréquemment, assurez-vous qu'il y a suffisamment de serveurs antivirus pour gérer la charge d'analyse antivirus générée par la SVM.
Informations d'identification AWS pour le rôle IAM expirées	PRIMORDIAL	Cloud volumes ONTAP est devenu inaccessible. Les identifiants basés sur les rôles de gestion des identités et des accès ont expiré. Les identifiants sont acquis auprès du serveur de métadonnées Amazon Web Services (AWS) via le rôle IAM et signent des demandes d'API à Amazon simple Storage Service (Amazon S3).	Procédez comme suit :…Connectez-vous à la console de gestion EC2 AWS.…accédez à la page instances.…recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son intégrité.…Vérifiez que le rôle IAM AWS associé à l'instance est valide et a reçu les privilèges appropriés à l'instance.
Informations d'identification AWS pour le rôle IAM introuvables	PRIMORDIAL	Le thread d'identification cloud ne peut pas acquérir les identifiants basés sur les rôles Amazon Web Services (AWS) Identity and Access Management (IAM) à partir du serveur de métadonnées AWS. Ces identifiants sont utilisés pour signer des demandes d'API vers Amazon simple Storage Service (Amazon S3). Cloud volumes ONTAP est devenu inaccessible.…	Procédez comme suit :…Connectez-vous à la console de gestion EC2 AWS.…accédez à la page instances.…recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son intégrité.…Vérifiez que le rôle IAM AWS associé à l'instance est valide et a reçu les privilèges appropriés à l'instance.

Informations d'identification AWS pour le rôle IAM non valides	PRIMORDIAL	Les identifiants basés sur les rôles de gestion des identités et des accès ne sont pas valides. Les identifiants sont acquis auprès du serveur de métadonnées Amazon Web Services (AWS) via le rôle IAM et signent des demandes d'API à Amazon simple Storage Service (Amazon S3). Cloud volumes ONTAP est devenu inaccessible.	Procédez comme suit :…Connectez-vous à la console de gestion EC2 AWS.…accédez à la page instances.…recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son intégrité.…Vérifiez que le rôle IAM AWS associé à l'instance est valide et a reçu les privilèges appropriés à l'instance.
Rôle IAM AWS introuvable	PRIMORDIAL	Le thread des rôles de gestion des identités et des accès ne peut pas trouver de rôle IAM Amazon Web Services (AWS) sur le serveur de métadonnées AWS. Le rôle IAM est requis pour acquérir des identifiants basés sur des rôles afin de signer les demandes d'API vers Amazon simple Storage Service (Amazon S3). Cloud volumes ONTAP est devenu inaccessible.…	Procédez comme suit :…Connectez-vous à la console de gestion EC2 AWS.…accédez à la page instances.…recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son état.…Vérifiez que le rôle IAM AWS associé à l'instance est valide.
Rôle IAM AWS non valide	PRIMORDIAL	Le rôle de gestion des identités et des accès Amazon Web Services (AWS) sur le serveur de métadonnées AWS n'est pas valide. Cloud Volume ONTAP est devenu inaccessible.…	Procédez comme suit :…Connectez-vous à la console de gestion EC2 AWS.…accédez à la page instances.…recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son intégrité.…Vérifiez que le rôle IAM AWS associé à l'instance est valide et a reçu les privilèges appropriés à l'instance.

Échec de la connexion au serveur de métadonnées AWS	PRIMORDIAL	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). Il convient de établir une communication pour acquérir les identifiants basés sur les rôles AWS IAM nécessaires à la signature des demandes d'API à Amazon simple Storage Service (Amazon S3). Cloud volumes ONTAP est devenu inaccessible.…	Procédez comme suit :…Connectez-vous à la console de gestion EC2 AWS.…accédez à la page instances.…recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son état de santé.…
Limite d'utilisation de l'espace FabricPool presque atteinte	AVERTISSEMENT	L'utilisation de l'espace FabricPool total dans le cluster des magasins d'objets auprès de fournisseurs sous licence en termes de capacité a presque atteint la limite autorisée.	Exécutez les actions correctives suivantes :…Vérifiez le pourcentage de la capacité sous licence utilisée par chaque Tier de stockage FabricPool à l'aide de la commande « Storage Aggregate Object-store show-space ».…supprimez les copies Snapshot de volumes grâce à la règle de hiérarchisation « snapshot » ou « sauvegarde » à l'aide de la commande « volume snapshot delete » pour libérer de l'espace.…installez une nouvelle licence sur le cluster, vous pouvez augmenter la capacité sous licence.

Limite d’utilisation de l’espace FabricPool atteinte	PRIMORDIAL	L’utilisation totale de l’espace FabricPool sur l’ensemble du cluster des magasins d’objets auprès de fournisseurs sous licence en fonction de la capacité a atteint la limite de licence.	Exécutez les actions correctives suivantes :…Vérifiez le pourcentage de la capacité sous licence utilisée par chaque Tier de stockage FabricPool à l’aide de la commande « Storage Aggregate Object-store show-space »….supprimez les copies Snapshot de volumes grâce à la règle de hiérarchisation « snapshot » ou « sauvegarde » à l’aide de la commande « volume snapshot delete » pour libérer de l’espace….installez une nouvelle licence sur le cluster, vous pouvez augmenter la capacité sous licence.

Échec du rétablissement de l'agrégat	PRIMORDIAL	Cet événement a lieu pendant la migration d'un agrégat dans le cadre d'un rétablissement de basculement du stockage (SFO), lorsque le nœud de destination ne peut pas atteindre les magasins d'objets.	Effectuer les actions correctives suivantes :…Vérifiez que votre LIF intercluster est en ligne et fonctionnelle 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 nœud de destination LIF intercluster. …Vérifiez que la configuration de votre magasin d'objets n'a pas changé et que les informations de connexion et de connectivité sont toujours précises à l'aide de la commande « Aggregate Object-store config show »….alternativement, Vous pouvez ignorer l'erreur en spécifiant false pour le paramètre « exiger-Partner-waiting » de la commande giveback.…contactez le support technique de NetApp pour plus d'informations ou d'aide.

Interconnexion HAUTE DISPONIBILITÉ en panne	AVERTISSEMENT	L'interconnexion haute disponibilité est en panne. Le risque d'interruption de service lorsque le basculement n'est pas disponible.	Les actions correctives dépendent du nombre et du type de liaisons d'interconnexion haute disponibilité prises en charge par la plateforme, ainsi que de la raison pour laquelle l'interconnexion est en panne. …Si les liaisons sont en panne :…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 petits SFP (Form-factor plugables), 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 à l'aide de la commande "ic link on". …Si un poste n'est pas connecté, désactivez et réactivez les liens l'un après l'autre à l'aide des commandes « ic link off » et « ic link on ».…contactez le support technique de 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 terminez toutes celles qui ne fonctionnent pas correctement.…redémarrez le client.…Vérifiez si le problème est causé par une nouvelle application ou une application existante :… si l'application est nouvelle, définissez un seuil plus élevé pour le client en utilisant la commande "cifs option modify -max-ouvre -même-fichier-par -arborescence". Dans certains cas, les clients fonctionnent comme prévu, mais nécessitent un seuil plus élevé. Vous devez disposer d'un privilège avancé 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. Pour plus d'informations ou pour obtenir de l'aide, contactez le support technique NetApp.

Nombre max. D’heures d’ouverture par fichier 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 la fermeture de 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 ne pas fonctionner correctement en raison de l’exécution de l’application.…Reboot le client.…Vérifiez si le problème est causé par une nouvelle application ou une application existante :…si l’application est nouvelle, définissez un seuil plus élevé pour le client en utilisant la commande "option cifs modify -max-iouverture -même-fichier-par -arborescence". Dans certains cas, les clients fonctionnent comme prévu, mais nécessitent un seuil plus élevé. Vous devez disposer d’un privilège avancé 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. Pour plus d’informations ou pour obtenir de l’aide, contactez le support technique NetApp.

Conflit de nom NetBIOS	PRIMORDIAL	Le service de noms NetBIOS a reçu une réponse négative à une demande d'enregistrement de nom provenant d'un ordinateur distant. Ceci est généralement causé par un conflit dans le nom NetBIOS ou un alias. Par conséquent, les clients ne peuvent pas accéder aux données ou se connecter au nœud qui transmet les données approprié dans le cluster.	Effectuez l'une des actions correctives suivantes :…en cas de conflit dans le nom NetBIOS ou dans un alias, Effectuer l'une des opérations suivantes :…Supprimer l'alias NetBIOS en double en utilisant la commande « vserver cifs delete -alias -vserver vserver vserver »….Renommer un alias NetBIOS en supprimant le nom dupliqué et en ajoutant un alias avec un nouveau nom en utilisant la commande « vserver cifs create -alias -vserver ». …En l'absence d'alias configurés et en présence d'un conflit dans le nom NetBIOS, renommez le serveur CIFS en utilisant les commandes « vserver cifs delete -vserver 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 l'ordinateur distant.
Pool de magasins NFSv4 épuisé	PRIMORDIAL	Un pool de magasins 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 de lecture enregistré	PRIMORDIAL	L'antivirus Connector a notifié à ONTAP qu'il ne possède pas de moteur d'analyse enregistré. Cela peut entraîner une indisponibilité des données si l'option « Scan-mandatory » est activée.	Effectuez les actions correctives suivantes :…Assurez-vous que le logiciel du moteur de scan installé sur le serveur antivirus est compatible avec ONTAP.…Assurez-vous que le logiciel du moteur de scan est en cours d'exécution et configuré pour se connecter au connecteur antivirus sur la boucle locale.
Aucune connexion Vscan	PRIMORDIAL	ONTAP n'a pas de connexion Vscan pour les demandes de scan antivirus. Cela peut entraîner une indisponibilité des données si l'option « Scan-mandatory » est activée.	Assurez-vous que le pool de scanner est correctement configuré et que les serveurs antivirus sont actifs et connectés à ONTAP.
Espace de volume racine du nœud faible	PRIMORDIAL	Le système a détecté que le volume racine est dangereusement faible sur l'espace. Le nœud n'est pas entièrement opérationnel. Les LIF de données peuvent avoir basculé sur le cluster car l'accès NFS et CIFS est limité sur le nœud. La capacité administrative est limitée aux procédures de restauration locale pour que le nœud vide l'espace sur le volume racine.	Effectuez les actions correctives suivantes :…effacez 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 développant la capacité du volume racine.…redémarrez le contrôleur.…contactez le support technique NetApp pour obtenir plus d'informations ou d'assistance.
Partage Admin inexistant	PRIMORDIAL	Problème Vscan : un client a tenté de se connecter à un partage ONTAP_ADMIN$ inexistant.	S'assurer que le Vscan est activé pour l'ID SVM mentionné. L'activation du Vscan sur un SVM entraîne la création automatique du partage ONTAP_ADMIN$ pour la SVM.

Espace de nom NVMe insuffisant	PRIMORDIAL	Un namespace NVMe a été mis hors ligne pour cause d'une défaillance d'écriture provoquée par le manque d'espace.	Ajoutez de l'espace au volume, puis mettez le namespace NVMe en ligne en utilisant la commande « vserver nvme namespace modify ».
Délai de grâce NVMe-of actif	AVERTISSEMENT	Cet événement se produit tous les jours lorsque le protocole NVMe over Fabrics (NVMe-of) est en cours d'utilisation et que la période de grâce de la licence est active. La fonctionnalité NVMe-of requiert une licence après l'expiration de la période de grâce de la licence. La fonctionnalité NVMe-of est désactivée lorsque la période de grâce des licences est terminée.	Contactez votre ingénieur commercial pour obtenir une licence NVMe-of et l'ajouter au cluster, ou supprimer toutes les instances de la configuration NVMe-of du cluster.
Délai de grâce NVMe-of expiré	AVERTISSEMENT	La période de grâce de la licence NVMe-of (NVMe over Fabrics) est terminée et la fonctionnalité NVMe-of est désactivée.	Contactez votre ingénieur commercial pour obtenir une licence NVMe-of et l'ajouter au cluster.
Début du délai de grâce NVMe-of	AVERTISSEMENT	La configuration NVMe-of (NVMe over Fabrics) a été détectée lors de la mise à niveau du logiciel ONTAP 9.5. La fonctionnalité NVMe-of requiert une licence après l'expiration de la période de grâce de la licence.	Contactez votre ingénieur commercial pour obtenir une licence NVMe-of et l'ajouter au cluster.
L'hôte de magasin d'objets ne peut pas être résolu	PRIMORDIAL	Le nom d'hôte du serveur de stockage d'objets ne peut pas être résolu en adresse IP. Le client de magasin d'objets ne peut pas communiquer avec le serveur de 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 Object Store en panne	PRIMORDIAL	Le client Object-Store ne peut pas trouver une LIF opérationnelle qui communique avec le serveur de magasin d'objets. Le nœud n'autorise pas le trafic client de magasin d'objets tant que le LIF intercluster n'est pas opérationnel. Par conséquent, les données peuvent être inaccessibles.	Effectuer les actions correctives suivantes :…Vérifiez le statut de LIF intercluster en utilisant la commande « network interface show -role intercluster ».…Vérifiez que le LIF intercluster est configuré correctement et opérationnel.…si une LIF intercluster n'est pas configurée, ajoutez-la en utilisant la commande « network interface create -role intercluster ».
Incohérence de signature de magasin d'objets	PRIMORDIAL	La signature de demande envoyée au serveur de stockage 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 configurée correctement. Si elle est correctement configurée, contactez le support technique NetApp pour obtenir de l'aide.

Délai D’attente DU RÉADR	PRIMORDIAL	Une opération DE fichier DE REMADDIR a dépassé le délai d’exécution autorisé dans WAFL. Ceci peut être dû à des répertoires très grands ou épars. Une action corrective est recommandée.	Effectuez les actions correctives suivantes :…recherchez les informations spécifiques aux répertoires récents qui ont eu DES opérations DE fichier DE RÉADDIR expirant en utilisant la commande suivante 'diag' Privilege nodeshell CLI: WAFL readdir avis show.…Vérifiez si les répertoires sont indiqués comme sparse ou non:… si un répertoire est indiqué comme sparse, il est recommandé de copier le contenu du répertoire dans un nouveau répertoire pour supprimer l’sparseness du fichier de répertoire. …Si un répertoire n’est pas indiqué comme étant sparse 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.

Le transfert de l'agrégat a échoué	PRIMORDIAL	Cet événement a lieu pendant le transfert d'un agrégat, si le nœud de destination ne peut pas atteindre les magasins d'objets.	Effectuer les actions correctives suivantes :…Vérifiez que votre LIF intercluster est en ligne et fonctionnelle 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 nœud de destination LIF intercluster. …Vérifiez que la configuration de votre magasin d'objets n'a pas changé et que les informations de connexion et de connectivité sont toujours précises à l'aide de la commande « Aggregate Object-store config show ».…vous pouvez également ignorer l'erreur en utilisant le paramètre « override-destination-chvérifié » de la commande de transfert.…Contactez le support technique de NetApp pour plus d'informations ou d'assistance.
Échec de la copie en double	PRIMORDIAL	Une opération VSS (Volume Shadow Copy Service), un service de sauvegarde et de restauration Microsoft Server, a échoué.	Vérifiez ce qui suit à l'aide des informations fournies dans le message d'événement :…la configuration de copie en double est-elle activée?…les licences appropriées sont-elles installées? …Sur quels partages l'opération de copie en double est-elle effectuée?…le nom du partage est-il correct?…le chemin du partage existe-t-il?…Quels sont les États du jeu de copies en double et de ses copies en double ?

Échec des blocs d'alimentation du commutateur de stockage	AVERTISSEMENT	Il manque une alimentation dans le commutateur du cluster. La redondance est réduite, le risque de panne lié à d'autres pannes de courant.	Effectuez les actions correctives suivantes :…Assurez-vous que l'alimentation secteur, qui alimente le commutateur du cluster, est sous tension.…assurez-vous que le cordon d'alimentation est connecté à l'alimentation.…contactez le support technique NetApp si le problème persiste.
Authentification CIFS trop nombreuses	AVERTISSEMENT	De nombreuses négociations d'authentification ont eu lieu simultanément. Il y a 256 nouvelles demandes de session incomplètes de ce client.	Étudier les raisons pour lesquelles le client a créé au moins 256 nouvelles demandes de connexion. Vous devrez peut-être contacter le fournisseur du client ou de l'application pour déterminer la raison de l'erreur.
Accès utilisateur non autorisé au partage Admin	AVERTISSEMENT	Un client a tenté de se connecter au partage Privileged ONTAP_ADMIN$, même si l'utilisateur connecté n'est pas un utilisateur autorisé.	Effectuer les actions correctives suivantes :…Assurez-vous que le nom d'utilisateur et l'adresse IP mentionnés sont configurés dans l'un des pools de scanner Vscan actifs.…Vérifiez la configuration du pool de scanner actuellement active 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 causer 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.	Vérifier le journal du serveur Vscan signalé dans l'événement « syslog » pour voir s'il peut nettoyer, mettre en quarantaine ou supprimer le fichier infecté. S'il n'a pas pu le faire, un administrateur système peut avoir à supprimer manuellement le fichier.
Volume hors ligne	INFO	Ce message indique qu'un volume est mis hors ligne.	Remettre le volume en ligne.
Volume restreint	INFO	Cet événement indique qu'un volume flexible est réduit.	Remettre le volume en ligne.
L'arrêt de la VM de stockage a réussi	INFO	Ce message se produit lorsqu'une opération « arrêt vServer » réussit.	Utiliser la commande « vserver start » pour démarrer l'accès aux données sur une machine virtuelle de stockage.
Problème au niveau des nœuds	AVERTISSEMENT	Cet événement est émis en cas de panique	Contactez l'assistance client NetApp.

Haut de la page

Moniteurs de journal anti-ransomware

Nom du moniteur	Gravité	Description	Action corrective
Surveillance anti-ransomware des VM de stockage désactivée	AVERTISSEMENT	La surveillance anti-ransomware pour la machine virtuelle de stockage est désactivée. Activation d'une protection contre les ransomwares pour protéger la VM de stockage	Aucune
Surveillance anti-ransomware des machines virtuelles de stockage activée (mode de formation)	INFO	La surveillance anti-ransomware de la machine virtuelle de stockage est activée en mode d'apprentissage.	Aucune

Surveillance anti-ransomwares du volume activée	INFO	La surveillance anti-ransomwares du volume est activée.	Aucune
Surveillance anti-ransomware du volume désactivée	AVERTISSEMENT	La surveillance anti-ransomware du volume est désactivée. Activation d'anti-ransomwares pour protéger le volume	Aucune
Surveillance anti-ransomware des volumes activée (mode apprentissage)	INFO	La surveillance anti-ransomwares du volume est activée en mode d'apprentissage.	Aucune
Mise en pause de la surveillance anti-ransomware des volumes (mode apprentissage)	AVERTISSEMENT	La surveillance anti-ransomware du volume est suspendue en mode d'apprentissage.	Aucune
Mise en pause de la surveillance anti-ransomware du volume	AVERTISSEMENT	La surveillance anti-ransomware du volume est suspendue.	Aucune
Surveillance anti-ransomwares du volume désactivation	AVERTISSEMENT	La surveillance anti-ransomwares du volume est désactivée.	Aucune
Activité de ransomware détectée	PRIMORDIAL	Pour protéger les données contre le ransomware détecté, une copie Snapshot peut être utilisée pour restaurer les données d'origine. Votre système génère et transmet un message AutoSupport ou d'appel en cas d'incident au support technique NetApp, ainsi qu'à toute destination configurée. Le message AutoSupport améliore l'identification et la résolution des problèmes.	Reportez-vous au « NOM DU DOCUMENT FINAL » pour prendre des mesures correctives concernant l'activité de ransomware.

Haut de la page

FSX pour moniteurs ONTAP NetApp

Nom du moniteur	Seuils	Description du moniteur	Action corrective

La capacité du volume FSX est pleine	Avertissement @ > 85 %…critique @ > 95 %	La capacité de stockage d'un volume est nécessaire pour stocker les données des applications et des clients. Plus le volume ONTAP est stocké, plus la disponibilité du stockage des données futures est faible. Si la capacité de stockage de données d'un volume atteint la capacité de stockage totale, cela peut conduire le client à ne pas pouvoir stocker les données en raison d'une capacité de stockage insuffisante. La surveillance du volume utilisé permet d'assurer la continuité des services de données.	Des actions immédiates sont requises pour minimiser les interruptions de service si le seuil critique est atteint :…1. Envisagez de supprimer les données qui ne sont plus nécessaires pour libérer de l'espace
Volume FSX latence élevée	Avertissement @ > 1000 µs…critique @ > 2000 µs	Les volumes sont des objets qui servent le trafic d'E/S souvent pilotées par des applications sensibles aux performances, notamment les applications DevOps, les répertoires locaux et les bases de données. Une latence élevée signifie que les applications elles-mêmes risquent de subir des conséquences et d'être dans l'impossibilité d'accomplir leurs tâches. Pour maintenir des performances prévisibles au niveau des applications, il est essentiel de contrôler les latences des volumes.	Des actions immédiates sont requises pour minimiser les interruptions de service si le seuil critique est atteint :…1. Si une règle de QoS lui est attribuée, évaluez ses seuils de limite au cas où la charge de travail du volume serait mise au ralenti…… planifier de prendre les actions suivantes rapidement si le seuil d'avertissement est dépassé :…1. Si une règle de QoS lui est attribuée, évaluez ses seuils de limite au cas où la charge de travail du volume serait mise au ralenti.…2. Si l'utilisation du nœud est également élevée, déplacez-le vers un autre nœud ou réduisez la charge de travail totale du nœud.

Limite des inodes de volume FSX	Avertissement @ > 85 %…critique @ > 95 %	Les volumes qui stockent des fichiers utilisent des nœuds d'index (inode) pour stocker les métadonnées de fichiers. Lorsqu'un volume épuise son allocation d'inode, aucun autre fichier ne peut lui être ajouté. Une alerte d'avertissement indique que l'action planifiée doit être prise pour augmenter le nombre d'inodes disponibles. Une alerte critique indique que la limite d'épuisement des fichiers est imminente et que des mesures d'urgence doivent être prises pour libérer les inodes afin d'assurer la continuité des services	Des actions immédiates sont requises pour minimiser les interruptions de service si le seuil critique est atteint :…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 les actions suivantes rapidement 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
Surallocation du quota qtree volume FSX	Avertissement @ > 95 %…critique @ > 100 %	Volume qtree quota overcommit spécifie le pourcentage auquel un volume est considéré comme surallouant par les quotas qtree. Le seuil défini pour le quota qtree est atteint pour le volume. La surveillance du surengagement de quota qtree du volume permet à l'utilisateur de recevoir un service de données sans interruption.	Si un seuil critique est atteint, des mesures immédiates doivent être prises pour limiter les interruptions de service : 1. Supprimez les données indésirables… lorsque le seuil d'avertissement est atteint, envisagez d'augmenter l'espace du volume.

Espace de réserve Snapshot FSX saturé	Avertissement @ > 90 %…critique @ > 95 %	La capacité de stockage d'un volume est nécessaire pour stocker les données des applications et des clients. Une partie de cet espace, appelée espace réservé pour les instantanés, est utilisée pour stocker des instantanés qui permettent de protéger les données localement. Plus les données stockées dans le volume ONTAP sont récentes, plus la capacité Snapshot est élevée et moins la capacité de stockage Snapshot sera disponible pour les données à venir (nouvelles ou mises à jour). Si la capacité des données snapshot d'un volume atteint l'espace total de réserve snapshot, il se peut que le client ne puisse pas stocker de nouvelles données snapshot et qu'il ne puisse pas réduire le niveau de protection des données du volume. La surveillance du volume utilisé permet la continuité des services de données.	Des actions immédiates sont requises pour minimiser les interruptions de service si le seuil critique est atteint :…1. Envisagez de configurer les instantanés pour utiliser l'espace de données dans le volume lorsque la réserve de snapshot est pleine… 2. Pensez à supprimer des instantanés plus anciens qui pourraient ne plus être nécessaires pour libérer de l'espace…… planifier pour prendre les actions suivantes bientôt si le seuil d'avertissement est dépassé:…1. Envisagez d'augmenter l'espace de réserve snapshot au sein du volume pour répondre à la croissance…2. Envisagez de configurer des instantanés pour utiliser l'espace de données dans le volume lorsque la réserve Snapshot est pleine

Taux de Miss. Du cache du volume FSX	Avertissement @ > 95 %…critique @ > 100 %	Volume cache Miss ratio est le pourcentage de demandes de lecture des applications client renvoyées du disque au lieu d'être renvoyées à partir du cache. Cela signifie que le volume a atteint le seuil défini.	Si un seuil critique est atteint, des mesures immédiates doivent être prises pour limiter les interruptions de service : 1. Déplacez certaines charges de travail depuis le nœud du volume pour réduire la charge d'E/S 2. Réduisez la demande de charges de travail moins prioritaires sur le même nœud via des limites de QoS… prenez des mesures immédiates en cas de dépassement du seuil d'avertissement : 1. Déplacez certaines charges de travail depuis le nœud du volume pour réduire la charge d'E/S 2. Réduisez les besoins en charges de travail prioritaires sur le même nœud via la limitation de la qualité de service 3. Modifier les caractéristiques des charges de travail (taille de bloc, mise en cache des applications, etc.)

Haut de la page

Contrôleurs K8s

Nom du moniteur	Description	Actions correctives	Gravité/seuil

Latence élevée du volume persistant	Avec des latences de volume persistantes élevées, les applications elles-mêmes risquent d'être affectées et ne peuvent pas accomplir leurs tâches. La surveillance de la latence des volumes persistants est essentielle pour maintenir la cohérence des performances des applications. Les latences suivantes sont attendues pour le type de support : SSD jusqu'à 1-2 millisecondes ; SAS jusqu'à 8-10 millisecondes et disques durs SATA 17-20 millisecondes.	**Actions immédiates** si le seuil critique est dépassé, prenez en compte les actions immédiates pour minimiser l'interruption de service : si une stratégie de QoS est attribuée au volume, évaluez ses seuils limites au cas où la charge de travail du volume serait limitée. **Actions à faire bientôt** si le seuil d'avertissement est dépassé, planifiez les actions immédiates suivantes : 1. Si l'utilisation du pool de stockage est également élevée, déplacez le volume vers un autre pool de stockage. 2. Si une politique de QoS est attribuée au volume, évaluez ses seuils limités si celui-ci ralentit la charge de travail du volume. 3. Si le taux d'utilisation du contrôleur est également élevé, 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 de la mémoire du cluster élevée	La saturation de la mémoire allouable du cluster est élevée. La saturation du CPU 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 K8s.	Ajouter des nœuds. Corrigez tous les nœuds non planifiés. Pods de taille adéquate pour libérer de la mémoire sur les nœuds.	Avertissement @ > 80 % critique @ > 90 %
Échec de la connexion DU POD	Cette alerte se produit en cas d'échec d'une pièce jointe à un volume avec POD.		Avertissement

Taux de retransmission élevé	Taux de retransmission TCP élevé	Vérifier l'encombrement du réseau : identifiez les charges de travail qui consomment beaucoup de bande passante réseau. Vérifiez si le taux d'utilisation du processeur du Pod est élevé. Vérifiez les performances du réseau matériel.	Avertissement @ > 10 % critique @ > 25 %
Capacité élevée du système de fichiers nœud	Capacité élevée du système de fichiers nœud	- Augmenter la taille des disques de nœud pour s'assurer qu'il y a suffisamment de place pour les fichiers d'application. - Diminuer l'utilisation du fichier d'application.	Avertissement @ > 80 % critique @ > 90 %
Charge de travail instabilité du réseau élevée	Puissance TCP élevée (variations de temps de réponse/latence élevées)	Vérifiez la présence d'une congestion du réseau. Identifiez les charges de travail qui consomment beaucoup de bande passante réseau. Vérifiez si le taux d'utilisation du processeur du Pod est élevé. Vérifiez les performances du réseau matériel	Avertissement à > 30 ms critique à > 50 ms.

Débit de volume persistant	Les seuils EN MBIT/S sur les volumes persistants peuvent être utilisés pour alerter l'administrateur lorsque les volumes persistants dépassent les attentes de performance prédéfinies, ce qui peut affecter d'autres volumes persistants. L'activation de ce moniteur génère des alertes adaptées au profil de débit type des volumes persistants sur les disques SSD. Ce contrôle couvre tous les volumes persistants de votre locataire. Les valeurs de seuil critique et d'avertissement peuvent être ajustées en fonction de vos objectifs de surveillance en dupliquant ce moniteur et en définissant des seuils appropriés à votre classe de stockage. Un moniteur dupliqué peut être davantage ciblé sur un sous-ensemble de volumes persistants de votre locataire.	**Actions immédiates** si le seuil critique est dépassé, prévoir des actions immédiates pour réduire au minimum la perturbation du service : 1. Introduire DES limites DE QoS EN MBIT/S pour le volume. 2. Examinez l'application qui génère le workload sur le volume pour détecter d'éventuelles anomalies. **Actions à faire bientôt** si le seuil d'avertissement est dépassé, prévoir de prendre les mesures suivantes immédiatement : 1. Introduire DES limites DE QoS EN MBIT/S pour le volume. 2. Examinez l'application qui génère le workload sur le volume pour détecter d'éventuelles anomalies.	Avertissement @ > 10,000 Mo/s critique @ > 15,000 Mo/s.
Conteneur à risque de tuer le MOO	Les limites de mémoire du conteneur sont trop basses. Le conteneur risque d'être expulsé (mémoire saturée).	Augmentez les limites de la mémoire du conteneur.	Avertissement @ > 95 %
Charge de travail réduite	La charge de travail ne comporte pas de pods sains.		Critique @ < 1
Échec de liaison de la demande de volume persistant	Cette alerte se produit en cas d'échec de liaison sur un volume persistant.		Avertissement
Resourcequota Mem limites sur le point de dépasser	Les limites de mémoire pour l'espace de noms vont dépasser Resourcequota		Avertissement @ > 80 % critique @ > 90 %
Resourcequota Mem requêtes sur le point de dépasser	Les demandes de mémoire pour l'espace de noms vont dépasser Resourcequota		Avertissement @ > 80 % critique @ > 90 %

La création du nœud a échoué	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 configuration.	Primordial
Échec de la récupération du volume persistant	La récupération automatique du volume a échoué.		Avertissement @ > 0 B.
Restriction du processeur du conteneur	Les limites de l'UC du conteneur sont trop basses. Les processus de conteneur sont ralentis.	Augmentez les limites du processeur du conteneur.	Avertissement @ > 95 % critique @ > 98 %
Échec de la suppression de Service Load Balancer			Avertissement
IOPS de volume persistant	Les seuils d'IOPS pour les volumes persistants peuvent être utilisés pour alerter l'administrateur lorsque les volumes persistants dépassent les attentes de performance prédéfinies. L'activation de ce moniteur génère des alertes appropriées pour le profil IOPS type des volumes de persistance. Ce contrôle couvre tous les volumes persistants de votre locataire. Les valeurs de seuil critique et d'avertissement 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, prévoir des actions immédiates pour minimiser la perturbation du service : 1. Introduire des limites d'IOPS liées à la QoS pour le volume. 2. Examinez l'application qui génère le workload sur le volume pour détecter d'éventuelles anomalies. **Actions à faire bientôt** si le seuil d'avertissement est dépassé, planifiez les actions immédiates suivantes : 1. Introduire des limites d'IOPS liées à la QoS pour le volume. 2. Examinez l'application qui génère le workload sur le volume pour détecter d'éventuelles anomalies.	Avertissement @ > 20,000 E/S critiques @ > 25,000 E/S.
Échec de la mise à jour de Service Load Balancer			Avertissement
Échec du montage DU POD	Cette alerte survient lorsqu'un montage est en panne sur un POD.		Avertissement

Nœud pression PID	Les identificateurs de processus disponibles sur le nœud (Linux) sont tombés en dessous d'un seuil d'exclusion.	Recherchez et corrigez les pods qui génèrent de nombreux processus et qui ne disposent plus des 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 d'image pod	Kubernetes n'a pas pu extraire l'image du conteneur du pod.	- Assurez-vous que l'image du pod est correctement orthographiée dans la configuration du pod. - Vérifiez que la balise 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'arrivez pas aux limites de taux imposées par les fournisseurs de registres publics.	Avertissement
Tâche en cours d'exécution trop longue	Le travail est en cours d'exécution trop longtemps		Avertissement @ > 1 h critique @ > 5 h
Mémoire de nœud élevée	L'utilisation de la mémoire des nœuds est élevée	Ajouter des nœuds. Corrigez tous les nœuds non planifiés. Pods de taille adéquate pour libérer de la mémoire sur les nœuds.	Avertissement @ > 85 % critique @ > 90 %
Resourcequota CPU limites sur le point de dépasser	Les limites de CPU pour l'espace de noms vont dépasser Resourcequota		Avertissement @ > 80 % critique @ > 90 %
Boucle de collision du pod	Le pod s'est écrasé et a tenté de redémarrer plusieurs fois.		Critique @ > 3
CPU du nœud haut	L'utilisation du processeur du nœud est élevée.	Ajouter des nœuds. Corrigez tous les nœuds non planifiés. Pods de taille appropriée pour libérer le processeur sur les nœuds.	Avertissement @ > 80 % critique @ > 90 %

Temps de réponse de latence du réseau de la charge de travail élevé	Temps de latence TCP RTT (aller-retour) élevé	Vérifier la congestion du réseau ▒ identifier les charges de travail qui consomment beaucoup de bande passante du réseau. Vérifiez si le taux d'utilisation du processeur du Pod est élevé. Vérifiez les performances du réseau matériel.	Avertissement à > 150 ms critique à > 300 ms.
Echec du travail	La tâche ne s'est pas terminée correctement en raison d'une panne ou d'un redémarrage du nœud, d'un épuisement de la ressource, d'un délai d'attente de la tâche ou d'un échec de la planification du pod.	Recherchez les causes d'échec dans les journaux d'événements Kubernetes.	Avertissement @ > 1
Volume persistant plein en quelques jours	L'espace d'un volume persistant sera insuffisant dans quelques jours	-Augmentez la taille du volume pour vous assurer qu'il y a suffisamment d'espace pour les fichiers d'application. -Réduire la quantité de données stockées dans les applications.	Avertissement @ < 8 jours critique @ < 3 jours
Pression de mémoire du nœud	La mémoire du nœud est insuffisante. La mémoire disponible a atteint le seuil d'exclusion.	Ajouter des nœuds. Corrigez tous les nœuds non planifiés. Pods de taille adéquate 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, de mémoire et de disque. Vérifiez la connectivité réseau des nœuds. Recherchez les causes d'échec dans les journaux d'événements Kubernetes.	Critique @ < 1
Capacité élevée du volume persistant	La capacité utilisée par le back-end du volume persistant est élevée.	- Augmenter la taille du volume pour s'assurer qu'il y a suffisamment d'espace pour les fichiers d'application. - Réduire la quantité de données stockées dans les applications.	Avertissement @ > 80 % critique @ > 90 %

La création de Service Load Balancer a échoué	Échec de la création de Service Load Balancer		Primordial
Incompatibilité du réplica de la charge de travail	Certains modules ne sont actuellement pas disponibles pour un déploiement ou un jeu de démonstration.		Avertissement @ > 1
Resourcequota demandes CPU sur le point de dépasser	Les demandes de processeur pour l'espace de noms vont dépasser Resourcequota		Avertissement @ > 80 % critique @ > 90 %
Taux de retransmission élevé	Taux de retransmission TCP élevé	Vérifier l'encombrement du réseau : identifiez les charges de travail qui consomment beaucoup de bande passante réseau. Vérifiez si le taux d'utilisation du processeur du Pod est élevé. Vérifiez les performances du réseau matériel.	Avertissement @ > 10 % critique @ > 25 %
Pression du disque du nœud	L'espace disque disponible et les inodes sur le système de fichiers racine du nœud ou sur le système de fichiers image ont satisfait un seuil d'exclusion.	- Augmenter la taille des disques de nœud pour s'assurer qu'il y a suffisamment de place pour les fichiers d'application. - Diminuer l'utilisation du fichier d'application.	Critique @ > 0
Saturation élevée de l'UC du cluster	La saturation CPU pouvant être localisée par le cluster est élevée. La saturation des processeurs du cluster est calculée comme la somme de l'utilisation des processeurs divisée par la somme des CPU allouables sur tous les nœuds K8s.	Ajouter des nœuds. Corrigez tous les nœuds non planifiés. Pods de taille appropriée pour libérer le processeur sur les nœuds.	Avertissement @ > 80 % critique @ > 90 %

Haut de la page

Changer les moniteurs de journal

Nom du moniteur	Gravité	Description du moniteur
Volume interne détecté	Informatif	Ce message s'affiche lorsqu'un volume interne est détecté.

Volume interne modifié	Informatif	Ce message s'affiche lorsqu'un volume interne est modifié.
Nœud de stockage détecté	Informatif	Ce message s'affiche lorsqu'un nœud de stockage est détecté.
Nœud de stockage supprimé	Informatif	Ce message apparaît lorsqu'un nœud de stockage est supprimé.
Pool de stockage détecté	Informatif	Ce message s'affiche lorsqu'un pool de stockage est découvert.
Storage Virtual machine découvert	Informatif	Ce message s'affiche lorsqu'un Storage Virtual machine est détecté.
Machine virtuelle de stockage modifiée	Informatif	Ce message apparaît lorsqu'un Storage Virtual machine est modifié.

Haut de la page

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 régulièrement dans le cadre des mises à niveau pour introduire de nouvelles fonctionnalités. Cela se produit une fois par mois ou moins dans un environnement standard. Une alerte d'avertissement indiquant qu'une unité d'acquisition a été arrêtée doit être suivie peu après par une résolution indiquant que l'unité d'acquisition nouvellement redémarrée a terminé un enregistrement avec Data Infrastructure Insights. En général, ce cycle de fermeture à enregistrement prend de 5 à 15 minutes.	Si l'alerte survient fréquemment ou dure plus de 15 minutes, vérifiez le fonctionnement du système hébergeant l'unité d'acquisition, le réseau et tout proxy connectant l'UA à Internet.
Echec du collecteur	Le sondage d'un collecteur de données a rencontré une défaillance inattendue.	Pour en savoir plus sur la situation, consultez la page relative au collecteur de données dans Data Infrastructure Insights.

Avertissement du collecteur	Cette alerte peut généralement survenir en raison d'une configuration erronée du collecteur de données ou du système cible. Revoir les configurations pour éviter les alertes futures. Cela peut également être dû à la récupération de données moins complètes où le collecteur de données a rassemblé toutes les données qu'il pourrait. Cela peut se produire lorsque des situations changent pendant la collecte de données (par exemple, une machine virtuelle présente au début de la collecte de données est supprimée lors de la collecte et avant la capture de ces données).	Vérifier la configuration du collecteur de données ou du système cible. Notez que le moniteur pour l'avertissement du collecteur peut envoyer plus d'alertes que d'autres types de moniteur. Il est donc recommandé de ne définir aucun destinataire d'alerte à moins que vous ne soyez en mesure de résoudre les problèmes.

Haut de la page

Moniteurs de sécurité

Nom du moniteur	Seuil	Description du moniteur	Action corrective
Transport AutoSupport HTTPS désactivé	Avertissement @ < 1	AutoSupport prend en charge les protocoles de transport HTTPS, HTTP et SMTP. En raison des nature sensibles des messages AutoSupport, NetApp recommande fortement d'utiliser HTTPS comme protocole de transport par défaut pour l'envoi des 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
Chiffrement de cluster non sécurisé pour SSH	Avertissement @ < 1	Indique que SSH utilise des chiffrements non sécurisés, par exemple les chiffrements commençant par *cbc.	Pour supprimer le chiffrement CBC, exécutez la commande ONTAP suivante :…Security ssh remove -vserver <admin vserver> -chiffrements 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 qui accèdent 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 pour un cluster, exécutez la commande ONTAP suivante :…Security login banner modify -vserver <admin svm> -message « Access restreint to Authorized Users autorisés »
Communication entre les pairs de cluster non chiffrée	Avertissement @ < 1	Lors de la réplication de données pour la reprise sur incident, la mise en cache ou la sauvegarde, vous devez protéger ces données lors du transport sur le réseau entre un cluster ONTAP et un autre. Le chiffrement doit être configuré sur les clusters source et de destination.	Pour activer le cryptage sur des relations entre clusters qui ont été créées avant ONTAP 9.6, le cluster source et le cluster de destination doivent être mis à niveau vers la version 9.6. Utilisez ensuite la commande « cluster peer modify » afin de modifier les pairs de cluster source et de destination et utiliser le cryptage de peering de cluster.…consultez le guide NetApp sur le renforcement de la sécurité pour ONTAP 9 pour en savoir plus.
Utilisateur Admin local par défaut activé	Avertissement @ > 0	NetApp recommande de verrouiller (désactiver) tous les comptes administrateur utilisateur (intégrés) inutiles à l'aide de 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 les modèles 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 Advanced Privilege :…Security config modify -interface SSL -is-fips -Enabled true

Transfert de journal non crypté	Avertissement @ < 1	Le délestage des données des syslog est nécessaire pour limiter l'impact d'une faille à un seul système ou une seule solution. Par conséquent, NetApp recommande de décharger des informations syslog en toute sécurité vers un emplacement de stockage ou de conservation sécurisé.	Une fois qu'une destination de transfert de journaux est créée, son protocole ne peut pas être modifié. Pour passer à un protocole crypté, supprimez et recréez la destination du transfert du journal à l'aide de la commande ONTAP suivante :…cluster log-forwarding create -destination <destination ip> -protocole TCP chiffré
Mot de passe MD5 hachée	Avertissement @ > 0	NetApp recommande fortement d'utiliser la fonction de hachage SHA-512 plus sécurisée pour les mots de passe des comptes utilisateur ONTAP. Les comptes utilisant la fonction de hachage MD5 moins sécurisée doivent migrer vers la fonction de hachage SHA-512.	NetApp recommande fortement aux utilisateurs de migrer vers la solution SHA-512 plus sécurisée en leur laissant changer de mot de passe… pour verrouiller des 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 ne dispose d'aucun serveur NTP configuré. 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 serveur ntp create -Server <nom d'hôte du serveur ntp ou adresse ip>
Le nombre de serveurs NTP est faible	Avertissement @ < 3	Indique que le cluster comporte 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 serveur ntp create -Server <nom d'hôte du serveur ntp ou adresse ip>

Shell distant activé	Avertissement @ > 0	Le shell distant 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 sécuriser l'accès à distance.	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 VM de stockage désactivé	Avertissement @ < 1	Indique que la journalisation d'audit est désactivée pour SVM.	Pour configurer le journal d'audit d'un vserver, exécutez la commande ONTAP suivante :…vserver audit enable -vserver <svm>
Chiffrement non sécurisé des machines virtuelles de stockage pour SSH	Avertissement @ < 1	Indique que SSH utilise des chiffrements non sécurisés, par exemple les chiffrements commençant par *cbc.	Pour supprimer le chiffrement CBC, exécutez la commande ONTAP suivante :…Security ssh remove -vserver <vserver> -chiffrements aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
Bannière connexion VM de stockage désactivée	Avertissement @ < 1	Indique que la bannière de connexion est désactivée pour les utilisateurs qui accèdent 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 pour un cluster, exécutez la commande ONTAP suivante :…Security login banner modify -vserver <svm> -message « Access restreint to Authorized Users autorisés »
Protocole Telnet activé	Avertissement @ > 0	Telnet n'est pas une méthode sécurisée pour établir l'accès par ligne de commande à la solution ONTAP. Pour sécuriser l'accès à distance, Telnet doit être désactivé.	NetApp recommande un accès sécurisé à distance (SSH). Pour désactiver Telnet sur un cluster, exécutez la commande ONTAP suivante en mode Advanced Privilege :…Security Protocol modify -application telnet -Enabled false

Haut de la page

Moniteurs de protection des données

Nom du moniteur	Seuils	Description du moniteur	Action corrective
Espace insuffisant pour la copie Snapshot de la LUN	(Filtre contient_lun = Oui) Avertissement @ > 95 %…critique @ > 100 %	La capacité de stockage d'un volume est nécessaire pour stocker les données des applications et des clients. Une partie de cet espace, appelée espace réservé pour les instantanés, est utilisée pour stocker des instantanés qui permettent de protéger les données localement. Plus les données stockées dans le volume ONTAP sont récentes, plus la capacité Snapshot est élevée et moins la capacité de stockage Snapshot sera disponible pour les données à venir (nouvelles ou mises à jour). Si la capacité des données snapshot d'un volume atteint l'espace total de réserve snapshot, il se peut que le client ne puisse pas stocker de nouvelles données snapshot et qu'il réduit le niveau de protection des données des LUN du volume. La surveillance du volume utilisé permet la continuité des services de données.	**Actions immédiates** si le seuil critique est dépassé, prenez en considération des mesures immédiates pour minimiser les interruptions de service : 1. Configurez les instantanés pour utiliser l'espace de données dans le volume lorsque la réserve Snapshot est pleine. 2. Supprimez quelques anciens snapshots indésirables pour libérer de l'espace. **Actions à faire bientôt** si le seuil d'avertissement est dépassé, prévoir de prendre les mesures suivantes immédiatement : 1. Augmentez l'espace de réserve Snapshot au sein du volume pour faire face à la croissance. 2. Configurez les instantanés pour utiliser l'espace de données dans le volume lorsque la réserve Snapshot est pleine.

Décalage de la relation SnapMirror	Avertissement @ > 150 %…critique @ > 300 %	Le décalage de la relation SnapMirror est la différence entre l'horodatage de l'instantané et l'heure sur le système de destination. Le décalage_temps_pourcentage correspond au rapport entre le temps de décalage et l'intervalle de planification de la règle SnapMirror. Si le temps de décalage est égal à l'intervalle de planification, le décalage_temps_percent sera de 100 %. Si la politique SnapMirror n'a pas de planification, lag_time_percent ne sera pas calculé.	Surveiller 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 »

Haut de la page

Contrôleurs de Cloud volumes (CVO)

Nom du moniteur	Gravité de l'EC	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 d'assainissement ou est entré dans le centre de maintenance.	Aucune

Échec de la reprise de CVO du pool de stockage	PRIMORDIAL	Cet événement a lieu pendant la migration d'un agrégat dans le cadre d'un rétablissement de basculement du stockage (SFO), lorsque le nœud de destination ne peut pas atteindre les magasins d'objets.	Effectuer les actions correctives suivantes : vérifier que votre LIF intercluster est en ligne et fonctionnelle via la commande « network interface show ». Vérifier la connectivité réseau au serveur de magasin d'objets à l'aide de la commande « ping » sur le nœud de destination LIF intercluster. Vérifiez que la configuration de votre magasin d'objets n'a pas changé et que les informations de connexion et de connectivité sont toujours précises à l'aide de la commande « agrégat Object-store config show ». Vous pouvez également annuler l'erreur en spécifiant false pour le paramètre « exiger-Partner-waiting » de la commande giveback. Pour plus d'informations ou pour obtenir de l'aide, contactez le support technique NetApp.

Panne de l’interconnexion haute disponibilité de CVO	AVERTISSEMENT	L’interconnexion haute disponibilité est en panne. Le risque d’interruption de service lorsque le basculement n’est pas disponible.	Les actions correctives dépendent du nombre et du type de liaisons d’interconnexion haute disponibilité prises en charge par la plateforme, ainsi que de la raison pour laquelle l’interconnexion est en panne. Si les liaisons sont arrêtées : vérifiez que les deux contrôleurs de la paire haute disponibilité sont opérationnels. Pour les liaisons externes, assurez-vous que les câbles d’interconnexion sont correctement connectés et que les SFP (Small form-factor pluggables), 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 liens à l’aide de 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.

Sessions CVO max par utilisateur dépassées	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 exécutées sur le client et arrêtez toutes 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 à l'aide de la commande « cifs option modify -max -iouverture-same-file-per -Tree ». Dans certains cas, les clients fonctionnent comme prévu, mais nécessitent un seuil plus élevé. Vous devez disposer d'un privilège avancé 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. Pour plus d'informations ou pour obtenir de l'aide, contactez le support technique NetApp.

Conflit de nom NetBIOS CVO	PRIMORDIAL	Le service de noms NetBIOS a reçu une réponse négative à une demande d'enregistrement de nom provenant d'un ordinateur distant. Ceci est généralement causé par un conflit dans le nom NetBIOS ou un alias. Par conséquent, les clients ne peuvent pas accéder aux données ou se connecter au nœud qui transmet les données approprié dans le cluster.	Effectuer l'une des actions correctives suivantes : en cas de conflit dans le nom NetBIOS ou avec un alias, effectuer l'une des actions suivantes : supprimer l'alias NetBIOS en double à l'aide de la commande « vserver cifs delete -alias -vserver vserver vserver vserver vserver vserver ». Renommez un alias NetBIOS en supprimant le nom dupliqué et en ajoutant un alias avec un nouveau nom à l'aide de la commande « vserver cifs create -alias -vserver ». Si aucun alias n'est configuré et qu'il existe un conflit dans le nom NetBIOS, renommez le serveur CIFS en utilisant les commandes « vserver cifs delete -vserver 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 l'ordinateur distant.
CVO pour le pool de magasins NFSv4 épuisé	PRIMORDIAL	Un pool de magasins NFSv4 a été épuisé.	Si le serveur NFS ne répond pas pendant plus de 10 minutes après cet événement, contactez le support technique NetApp.
Incident de nœud CVO	AVERTISSEMENT	Cet événement est émis en cas de panique	Contactez l'assistance client NetApp.

Espace de volume racine du nœud CVO faible	PRIMORDIAL	Le système a détecté que le volume racine est dangereusement faible sur l'espace. Le nœud n'est pas entièrement opérationnel. Les LIF de données peuvent avoir basculé sur le cluster car l'accès NFS et CIFS est limité sur le nœud. La capacité administrative est limitée aux procédures de restauration locale pour que le nœud vide l'espace sur le volume racine.	Effectuez les actions correctives suivantes : supprimez 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 étendant la capacité du volume racine. Redémarre le contrôleur. Pour plus d'informations ou pour obtenir de l'aide, contactez le support technique NetApp.
CVO n'a pas de partage d'administration	PRIMORDIAL	Problème Vscan : un client a tenté de se connecter à un partage ONTAP_ADMIN$ inexistant.	S'assurer que le Vscan est activé pour l'ID SVM mentionné. L'activation du Vscan sur un SVM entraîne la création automatique du partage ONTAP_ADMIN$ pour la SVM.
L'hôte du magasin d'objets CVO ne peut pas être résolu	PRIMORDIAL	Le nom d'hôte du serveur de stockage d'objets ne peut pas être résolu en adresse IP. Le client de magasin d'objets ne peut pas communiquer avec le serveur de 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 arrêté	PRIMORDIAL	Le client Object-Store ne peut pas trouver une LIF opérationnelle qui communique avec le serveur de magasin d'objets. Le nœud n'autorise pas le trafic client de magasin d'objets tant que le LIF intercluster n'est pas opérationnel. Par conséquent, les données peuvent être inaccessibles.	Effectuer les actions correctives suivantes : vérifier le statut du LIF intercluster en utilisant la commande « network interface show -role intercluster ». Vérifier que le LIF intercluster est correctement configuré et opérationnel. Si un LIF intercluster n'est pas configuré, ajoutez-le en utilisant la commande « network interface create -role intercluster ».

Discordance de la signature du magasin d'objets CVO	PRIMORDIAL	La signature de demande envoyée au serveur de stockage 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 configurée correctement. Si elle est correctement configurée, contactez le support technique NetApp pour obtenir de l'aide.
QoS de CVO pour surveiller la mémoire insuffisante	PRIMORDIAL	La mémoire dynamique du sous-système QoS a atteint sa limite pour le matériel de la plate-forme actuelle. Certaines fonctionnalités de QoS peuvent fonctionner à une capacité limitée.	Supprimez des charges de travail ou des flux actifs pour libérer de la mémoire. Utilisez la commande "statistics show -object workload -Counter OPS" pour déterminer les charges de travail actives. Les workloads actifs montrent des opérations non nulles. Utilisez ensuite plusieurs fois la commande « workload delete <nom_charge de travail> » pour supprimer des charges de travail spécifiques. Vous pouvez également utiliser la commande « stream delete -workload <nom de charge de travail> * » pour supprimer les flux associés de la charge de travail active.

CVO - temporisation	PRIMORDIAL	Une opération DE fichier DE REMADDIR a dépassé le délai d'exécution autorisé dans WAFL. Ceci peut être dû à des répertoires très grands ou épars. Une action corrective est recommandée.	Effectuez les actions correctives suivantes : recherchez les informations spécifiques aux répertoires récents qui ont eu UNE NOUVELLE ADDIR opérations sur les fichiers expire à l'aide de la commande 'diag' privilege nodeshell CLI: WAFL remaddir notice show. Vérifiez si les répertoires sont indiqués comme sparse ou non : si un répertoire est indiqué comme sparse, il est recommandé de copier le contenu du répertoire dans un nouveau répertoire pour supprimer l'sparseness du fichier de répertoire. Si un répertoire n'est pas indiqué comme étant sparse et que le répertoire est grand, il est recommandé de réduire la taille du fichier de répertoire en réduisant le nombre d'entrées de fichier dans le répertoire.

Échec du transfert de CVO du pool de stockage	PRIMORDIAL	Cet événement a lieu pendant le transfert d'un agrégat, si le nœud de destination ne peut pas atteindre les magasins d'objets.	Effectuer les actions correctives suivantes : vérifier que votre LIF intercluster est en ligne et fonctionnelle via la commande « network interface show ». Vérifier la connectivité réseau au serveur de magasin d'objets à l'aide de la commande « ping » sur le nœud de destination LIF intercluster. Vérifiez que la configuration de votre magasin d'objets n'a pas changé et que les informations de connexion et de connectivité sont toujours précises à l'aide de la commande « agrégat Object-store config show ». Vous pouvez également annuler l'erreur en utilisant le paramètre "override-destination-chèques" de la commande de déplacement. Pour plus d'informations ou pour obtenir de l'aide, contactez le support technique NetApp.
Échec de la copie Shadow CVO	PRIMORDIAL	Une opération VSS (Volume Shadow Copy Service), un service de sauvegarde et de restauration Microsoft Server, a échoué.	Vérifiez les éléments suivants à l'aide des informations fournies dans le message d'événement : la configuration de la copie en double est-elle activée ? Les licences appropriées sont-elles installées ? Sur quels partages l'opération de copie en double est-elle effectuée ? Le nom du partage est-il correct ? Le chemin du partage existe-t-il ? Quels sont les États du jeu de clichés instantanés et de ses clichés instantanés ?

L’arrêt de la VM de CVO Storage a réussi	INFO	Ce message se produit lorsqu’une opération « arrêt vServer » réussit.	Utiliser la commande « vserver start » pour démarrer l’accès aux données sur une machine virtuelle de stockage.
CVO trop nombreuses authentification CIFS	AVERTISSEMENT	De nombreuses négociations d’authentification ont eu lieu simultanément. Il y a 256 nouvelles demandes de session incomplètes de ce client.	Étudier les raisons pour lesquelles le client a créé au moins 256 nouvelles demandes de connexion. Vous devrez peut-être contacter le fournisseur du client ou de l’application pour déterminer la raison de l’erreur.
Disques non affectés par CVO	INFO	Le système contient des disques non attribués. La capacité est alors gaspillée et votre système peut disposer de erreurs de configuration ou de modifications partielles de la configuration.	Effectuez les actions correctives suivantes : identifiez les disques non affectés à l’aide de la commande « disque show -n ». Assigner les disques à un système en utilisant la commande « Disk assignez ».
Accès utilisateur non autorisé de CVO au partage Admin	AVERTISSEMENT	Un client a tenté de se connecter au partage Privileged ONTAP_ADMIN$, même si l’utilisateur connecté n’est pas un utilisateur autorisé.	Effectuer les actions correctives suivantes : assurez-vous que le nom d’utilisateur et l’adresse IP mentionnés sont configurés dans l’un des pools de scanner Vscan actifs. Vérifier la configuration du scanner pool qui est 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 entraîner 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.	Vérifier le journal du serveur Vscan signalé dans l'événement « syslog » pour voir s'il peut nettoyer, mettre en quarantaine ou supprimer le fichier infecté. S'il n'a pas pu le faire, un administrateur système peut avoir à supprimer manuellement le fichier.
Volume CVO hors ligne	INFO	Ce message indique qu'un volume est mis hors ligne.	Remettre le volume en ligne.
Volume CVO restreint	INFO	Cet événement indique qu'un volume flexible est réduit.	Remettre le volume en ligne.

Haut de la page

SnapMirror pour les moniteurs de journaux de l'utilitaire de continuité de l'activité (SMBC)

Nom du moniteur	Gravité	Description du moniteur	Action corrective
ONTAP Mediator ajouté	INFO	Ce message s'affiche lorsque le médiateur ONTAP est correctement ajouté à un cluster.	Aucune
ONTAP Mediator non accessible	PRIMORDIAL	Ce message s'affiche lorsque le médiateur ONTAP est reconverti ou que le progiciel du médiateur n'est plus installé sur le serveur du médiateur. Le basculement de SnapMirror n'est donc pas possible.	Supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror médiateur remove ». Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande SnapMirror médiateur add.
Mediator ONTAP supprimé	INFO	Ce message s'affiche lorsque le médiateur ONTAP a été supprimé avec succès d'un cluster.	Aucune

ONTAP Médiateur inaccessible	AVERTISSEMENT	Ce message apparaît lorsque le médiateur ONTAP est inaccessible sur un cluster. Le basculement de SnapMirror n'est donc pas possible.	Vérifiez la connectivité réseau du médiateur ONTAP à l'aide des commandes "ping réseau" et "traceroute réseau". Si le problème persiste, supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror médiateur remove ». Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande SnapMirror médiateur add.
Certificat CA SMBC expiré	PRIMORDIAL	Ce message s'affiche lorsque le certificat de l'autorité de certification du médiateur ONTAP (CA) a expiré. Par conséquent, toute autre communication avec le médiateur ONTAP ne sera pas possible.	Supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror médiateur remove ». Mettez à jour un nouveau certificat d'autorité de certification sur le serveur du médiateur ONTAP. Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande SnapMirror médiateur add.
Expiration du certificat de l'AC SMBC	AVERTISSEMENT	Ce message survient lorsque le certificat de l'autorité de certification du médiateur (CA) de ONTAP expire 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 médiateur remove ». Mettez à jour un nouveau certificat d'autorité de certification sur le serveur du médiateur ONTAP. Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande SnapMirror médiateur add.

Certificat client SMBC expiré	PRIMORDIAL	Ce message s'affiche lorsque le certificat client du médiateur ONTAP a expiré. Par conséquent, toute autre communication avec le médiateur ONTAP ne sera pas possible.	Supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror médiateur remove ». Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande SnapMirror médiateur add.
Expiration du certificat client SMBC	AVERTISSEMENT	Ce message s'affiche lorsque le certificat du client du médiateur ONTAP 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 médiateur remove ». Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande SnapMirror médiateur add.
Relation SMBC hors synchronisation Remarque : L'UM n'a pas cette relation	PRIMORDIAL	Ce message survient lorsqu'une relation SnapMirror pour la continuité de l'activité (SMBC) passe du statut « In-sync » à « Out-of-sync ». La protection des données RPO=0 sera interrompue.	Vérifiez la connexion réseau entre les volumes source et de destination. Surveillez l'état de la relation SMBC à l'aide de la commande « snapmirror show » sur la destination et en utilisant la commande « snapmirror list-destinations » sur la source. La resynchronisation automatique essaiera de ramener la relation à l'état « in-sync ». Si la resynchronisation échoue, vérifiez que tous les nœuds du cluster se trouvent au quorum et sont en bon état.

Certificat de serveur SMBC expiré	PRIMORDIAL	Ce message s'affiche lorsque le certificat du serveur du médiateur ONTAP a expiré. Par conséquent, toute autre communication avec le médiateur ONTAP ne sera pas possible.	Supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror médiateur remove ». Mettez 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 médiateur add.
Expiration du certificat du serveur SMBC	AVERTISSEMENT	Ce message s'affiche lorsque le certificat du serveur du médiateur ONTAP 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 médiateur remove ». Mettez 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 médiateur add.

Haut de la page

Moniteurs d'alimentation, de fréquence cardiaque et divers systèmes supplémentaires

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Alimentation du tiroir disque détectée	INFORMATIF	Ce message survient lors de l'ajout d'une unité d'alimentation au tiroir disque.	AUCUNE
Blocs d'alimentation des tiroirs disques supprimés	INFORMATIF	Ce message survient lorsqu'une unité d'alimentation est retirée du tiroir disque.	AUCUNE
MetroCluster basculement automatique non planifié désactivé	PRIMORDIAL	Ce message survient lorsque la fonctionnalité de basculement automatique non planifié est désactivée.	Exécutez la commande « MetroCluster modify -node -name <nodename> -Automatic-switchover -onfailure true » pour chaque nœud du cluster afin d'activer le basculement automatique.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Pont de stockage MetroCluster inaccessible	PRIMORDIAL	Le pont de stockage est inaccessible sur le réseau de gestion	1) si le pont est surveillé par SNMP, vérifier que le LIF de node management fonctionne à l'aide de la commande « network interface show ». Vérifiez que le pont est actif à l'aide de la commande « ping réseau ». 2) si le pont est surveillé en bande, vérifiez le câblage de la structure du pont, puis vérifiez que le pont est sous tension.
Température du pont MetroCluster anormale - inférieure à la valeur critique	PRIMORDIAL	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) vérifier que le pont fonctionne dans des conditions de température recommandées.
Température du pont MetroCluster anormale - supérieure à critique	PRIMORDIAL	Le capteur sur le pont Fibre Channel signale une température supérieure au seuil critique.	1) vérifier l'état de fonctionnement du capteur de température du châssis sur le pont de stockage à l'aide de la commande « Storage Bridge show -Cooly ». 2) Vérifiez que le pont de stockage fonctionne dans des conditions de température recommandées.
Agrégat MetroCluster restant derrière	AVERTISSEMENT	L'agrégat a été laissé derrière lors du rétablissement.	1) Vérifiez l'état de l'agrégat à l'aide de la commande « aggr show ». 2) si l'agrégat est en ligne, retournez-le à son propriétaire initial en utilisant la commande « MetroCluster rétablissement ».

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Tous les liens entre les partenaires MetroCluster sont en panne	PRIMORDIAL	Les adaptateurs d'interconnexion RDMA et les LIF intercluster ont des connexions rompues au cluster de peering ou le cluster de peering est en panne.	1) s'assurer que les LIFs intercluster sont opérationnels. Réparer les LIFs intercluster si elles sont en panne. 2) Vérifiez que le cluster peering est opérationnel en utilisant la commande « cluster peer ping ». Reportez-vous au Guide de reprise sur incident de MetroCluster si le cluster de peering est arrêté. 3) pour la structure MetroCluster, vérifiez que les liens ISL de la structure back-end sont opérationnels. Corrigez les liens ISL de la structure back-end s'ils ne sont pas affectés. 4) pour les configurations MetroCluster sans structure, vérifier que le câblage est correct entre les adaptateurs d'interconnexion RDMA. Reconfigurez le câblage si les liaisons sont en panne.
Les partenaires MetroCluster ne sont pas accessibles sur le réseau de peering	PRIMORDIAL	La connectivité au cluster homologue est interrompue.	1) Assurez-vous que le port est connecté au réseau/commutateur approprié. 2) s'assurer que le LIF intercluster est connecté au cluster peering. 3) Assurez-vous que le cluster peering est opérationnel en utilisant la commande « cluster peer ping ». Reportez-vous au Guide de reprise sur incident de MetroCluster si le cluster de peering est hors service.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
MetroCluster inter basculer toutes les liaisons vers le bas	PRIMORDIAL	Toutes les liaisons ISL (Inter-Switch Link) du commutateur de stockage sont en panne.	1) réparer les liens ISL de la structure interne sur le commutateur de stockage. 2) Assurez-vous que le commutateur partenaire est opérationnel et que ses liens ISL sont opérationnels. 3) s'assurer que l'équipement intermédiaire, tel que les appareils xWDM, est opérationnel.
Liaison SAS du nœud MetroCluster vers la pile de stockage	AVERTISSEMENT	L'adaptateur SAS ou son câble connecté peut être défectueux.	1. Vérifiez que l'adaptateur SAS est en ligne et en cours d'exécution. 2. Vérifiez que le câble physique est correctement branché et qu'il fonctionne, puis remplacez-le si nécessaire. 3. Si l'adaptateur SAS est connecté aux tiroirs disques, vérifiez que les modules d'E/S et les disques sont correctement installés.
Initiateurs MetroClusterFC en panne	PRIMORDIAL	L'adaptateur FC initiateur est en panne.	1. Vérifiez que la liaison initiateur FC n'a pas été altérée. 2. Vérifiez le statut opérationnel de l'adaptateur FC initiator en utilisant la commande « system node run -node local -command Storage show adapter ».
Panne de la liaison de l'interconnexion FC-VI	PRIMORDIAL	La liaison physique du port FC-VI est hors ligne.	1. Assurez-vous que la liaison FC-VI n'a pas été altérée. 2. Vérifiez que l'état physique de l'adaptateur FC-VI est « actif » à l'aide de la commande « MetroCluster Interconnect adapter show ». 3. Si la configuration inclut des commutateurs de structure, assurez-vous qu'ils sont correctement câblés et configurés.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Les disques de secours MetroCluster se sont laissés derrière	AVERTISSEMENT	Le disque de spare a été laissé au retard lors du rétablissement.	Si le disque n'est pas en panne, retournez-le à son propriétaire initial en utilisant la commande « MetroCluster rétablissement ».
Port de la passerelle de stockage MetroCluster arrêté	PRIMORDIAL	Le port du Bridge de stockage est hors ligne.	1) Vérifiez le statut opérationnel des ports sur le pont de stockage à l'aide de la commande « Storage Bridge show -ports ». 2) Vérifiez la connectivité logique et physique au port.
Panne des ventilateurs du commutateur de stockage MetroCluster	PRIMORDIAL	Le ventilateur du commutateur de stockage est défectueux.	1) s'assurer que les ventilateurs du commutateur fonctionnent correctement à l'aide de la commande « Storage Switch show -Coolant ». 2) s'assurer que les FRU de ventilateur sont correctement insérées et opérationnelles.
Commutateur de stockage MetroCluster inaccessible	PRIMORDIAL	Le commutateur de stockage est inaccessible sur le réseau de gestion.	1) Assurez-vous que la LIF node management est active à l'aide de la commande « network interface show ». 2) s'assurer que l'interrupteur est actif à l'aide de la commande "ping réseau". 3) Assurez-vous que le commutateur est accessible via SNMP en vérifiant ses paramètres SNMP après avoir ouvert une session sur le commutateur.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Échec des blocs d'alimentation du commutateur MetroCluster	PRIMORDIAL	Une unité d'alimentation sur le commutateur de stockage n'est pas opérationnelle.	1) Vérifiez les détails d'erreur à l'aide de la commande « Storage Switch show -error -switch -name <swtich name> ». 2) identifier l'unité d'alimentation défectueuse à l'aide de 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	PRIMORDIAL	Le capteur du commutateur Fibre Channel est défectueux.	1) vérifier l'état de fonctionnement des capteurs de température sur le commutateur de stockage à l'aide de la commande « Storage Switch show -Coolant ». 2) vérifier que le contacteur fonctionne dans des conditions de température recommandées.
Température du commutateur MetroCluster anormale	PRIMORDIAL	Le capteur de température sur le commutateur Fibre Channel a signalé une température anormale.	1) vérifier l'état de fonctionnement des capteurs de température sur le commutateur de stockage à l'aide de la commande « Storage Switch show -Coolant ». 2) vérifier que le contacteur fonctionne dans des conditions de température recommandées.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Absence de signal de détection du processeur de service	INFORMATIF	Ce message apparaît lorsque ONTAP ne reçoit pas de signal de « pulsation » attendu du processeur de service. En plus de ce message, les fichiers journaux du SP sont envoyés pour débogage. ONTAP réinitialise le processeur de service pour tenter de restaurer la communication. Le processeur de service est indisponible pendant deux minutes maximum lorsqu'il redémarre.	Contactez le support technique NetApp.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Signal de détection du processeur de service arrêté	AVERTISSEMENT	Ce message survient lorsque ONTAP ne reçoit plus les pulsations de l'ensemble du processeur de service. Selon la conception matérielle, le système peut continuer à transmettre des données ou décider de s'arrêter afin d'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 concernant les dispositifs en panne, les erreurs de démarrage ou les erreurs D'autotest de mise sous tension (POST) d'Open Firmware (OFW). Si votre système est configuré pour ce faire, il génère et transmet un message AutoSupport (ou « appel en cas d'incident ») au support technique NetApp et aux destinations configurées. La transmission réussie d'un message AutoSupport améliore considérablement la détermination et la résolution des problèmes.	Si le système s'est arrêté, essayez de mettre hors tension puis sous tension le système : retirez le contrôleur du châssis, poussez-le de nouveau, puis mettez le système sous tension. Si le problème persiste après la mise hors/sous tension ou pour tout autre condition susceptible de justifier votre intervention, contactez le support technique NetApp.

Haut de la page

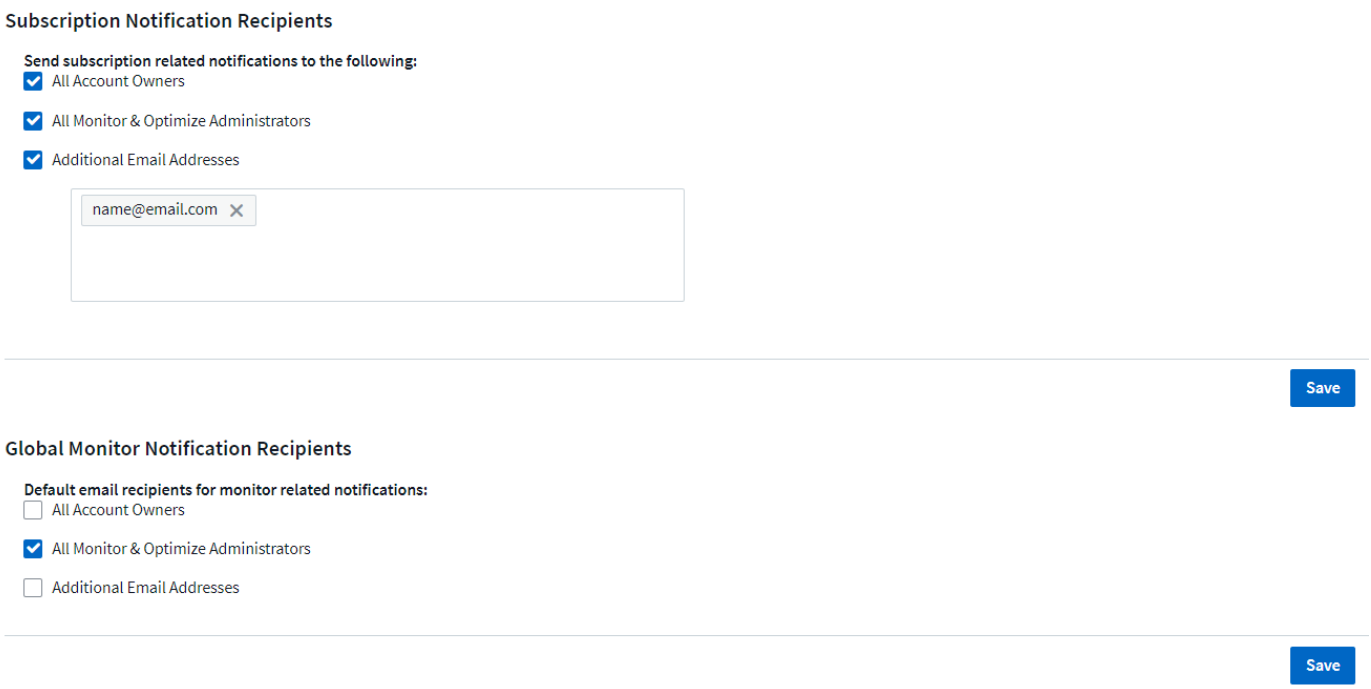
Plus d'informations

- "Affichage et rejet des alertes"

Configuration des notifications par e-mail

Vous pouvez configurer une liste d'e-mails pour les notifications relatives à un abonnement, ainsi qu'une liste globale de destinataires pour la notification des violations de seuil de la stratégie de performances.

Pour configurer les paramètres du destinataire de la notification, accédez à la page **Admin > Notifications** et sélectionnez l'onglet *Email*.



Destinataires de la notification d'abonnement

Pour configurer des destinataires pour les notifications d'événements liés à un abonnement, accédez à la section « destinataires de la notification d'abonnement ». Vous pouvez choisir d'envoyer des notifications par e-mail pour les événements liés à un abonnement à l'un ou l'ensemble des destinataires suivants :

- Tous les propriétaires de compte
- Tous les administrateurs *Monitor & Optimize*
- Adresses e-mail supplémentaires que vous spécifiez

Voici des exemples de types de notifications pouvant être envoyées et d'actions utilisateur que vous pouvez effectuer.

Notification:	Action de l'utilisateur:
La version d'essai ou l'abonnement a été mis à jour	Consultez les détails de l'abonnement sur la "Abonnement"page
L'abonnement expirera dans 90 jours. L'abonnement expirera dans 30 jours	Aucune action requise si le renouvellement automatique est activé. Contactez le service commercial NetApp pour renouveler l'abonnement
L'essai se termine dans 2 jours	Renouveler l'essai à partir de la "Abonnement"page. Vous pouvez renouveler une version d'évaluation une seule fois. Contactez le service commercial de NetApp pour souscrire un abonnement
La période d'essai ou l'abonnement a expiré le compte cessera de collecter les données dans 48 heures. Le compte sera supprimé après 48 heures	Contactez le service commercial de NetApp pour souscrire un abonnement

Pour vous assurer que vos destinataires reçoivent des notifications de Data Infrastructure Insights, ajoutez les adresses e-mail suivantes à n'importe quelle liste « Autoriser » :

- accounts@service.cloudinsights.netapp.com
- DoNotReply@cloudinsights.netapp.com

Liste globale des destinataires des alertes

Les notifications par e-mail d'alertes sont envoyées à la liste des destinataires de l'alerte pour chaque action de l'alerte. Vous pouvez choisir d'envoyer des notifications d'alerte à une liste de destinataires globale.

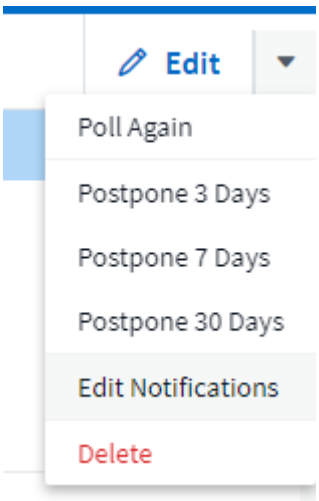
Pour configurer les destinataires d'alertes globales, sélectionnez les destinataires souhaités dans la section **destinataires de notification du moniteur global**.

Vous pouvez toujours remplacer la liste globale des destinataires d'un moniteur individuel lors de la création ou de la modification du moniteur.

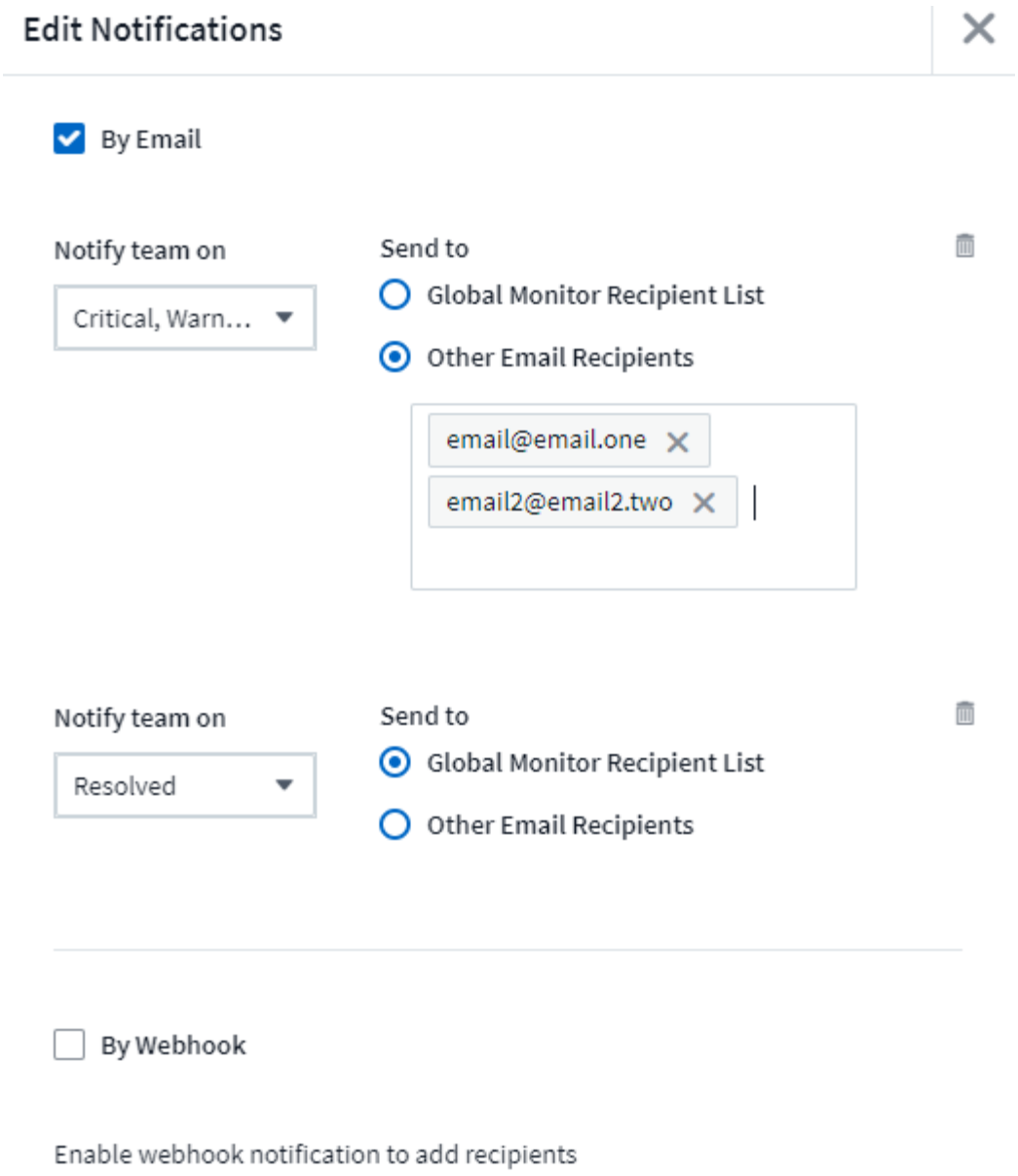
Les notifications ONTAP Data Collector prévalent sur toute notification Monitor spécifique pertinente au cluster/Data Collector. La liste des destinataires que vous définissez pour le Data Collector lui-même recevra les alertes du Data Collector. Si aucune alerte de collecte de données n'est active, des 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 le menu déroulant situé en haut à droite de la page d'accueil stockage.



À partir de là, vous pouvez définir des notifications pour les alertes critiques, d'avertissement, d'information et/ou résolues. Chaque scénario peut avertir la liste des destinataires globaux ou les autres destinataires que vous choisissez.



Notifications de Webhook

Notification à l'aide de Webpatères

Les Webpatères permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal Web personnalisé.

De nombreuses applications commerciales prennent en charge les crochets en tant qu'interface d'entrée standard, par exemple : Slack, PagerDuty, Teams et discorde tous les crochets de support. En prenant en charge un canal webhook générique et personnalisable, Data Infrastructure Insights peut prendre en charge un grand nombre de ces canaux de livraison. Des informations sur les webpatères sont disponibles sur ces sites Web d'application. Par exemple, Slack fournit "ce guide utile".

Vous pouvez créer plusieurs canaux de webhook, chaque canal ciblé pour un usage différent, des applications distinctes, des destinataires différents, etc

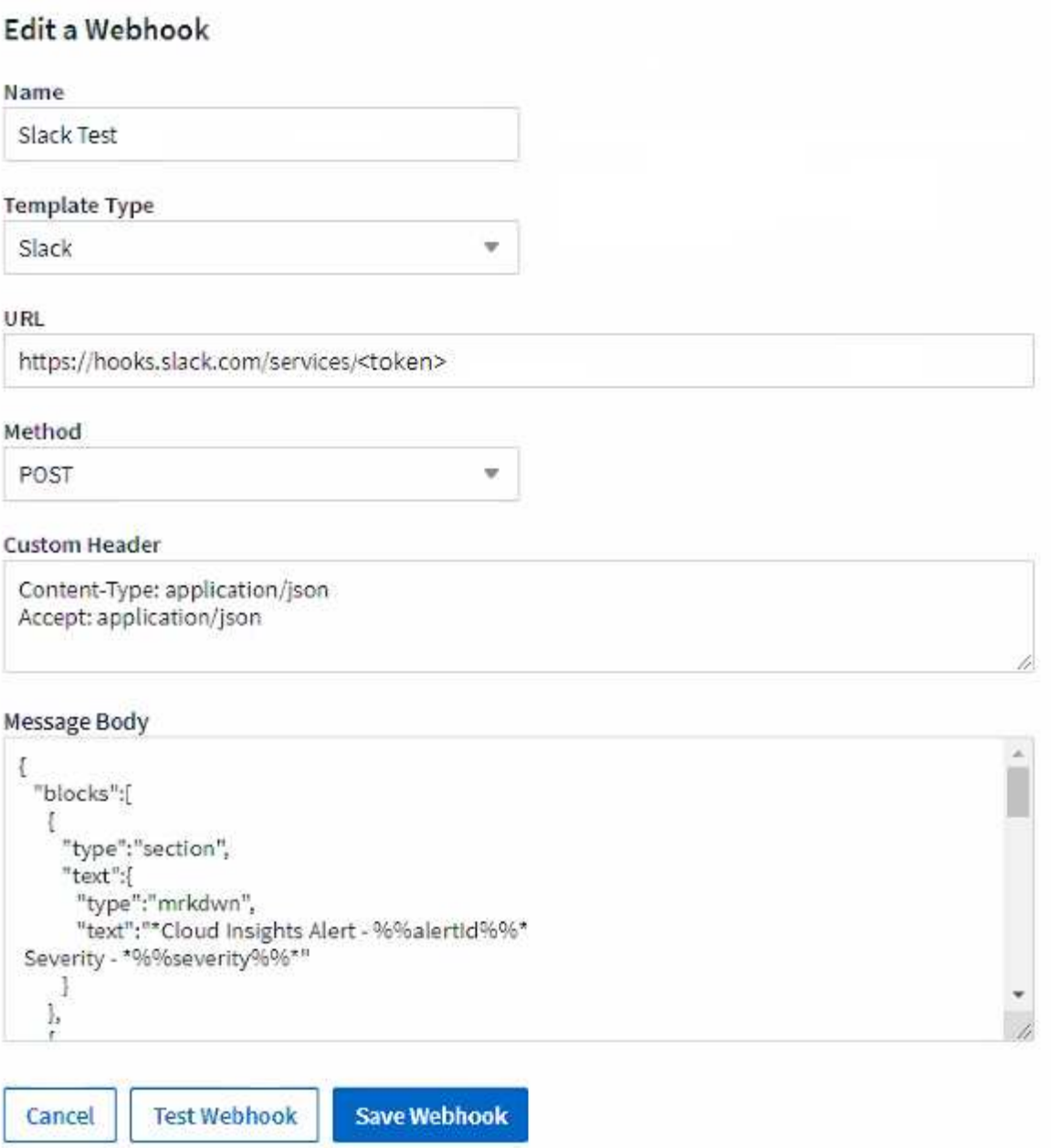
L'instance de canal de webhook comprend les éléments suivants :

Nom	Nom unique
URL	URL cible Webhook, y compris le préfixe *http://* ou *https://* et les paramètres d'url
Méthode	GET, POST : la valeur par défaut EST POST
En-tête personnalisé	Spécifiez ici 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 mousqueton
Paramètres et secrets personnalisés	Des paramètres et des secrets personnalisés vous permettent d'ajouter des paramètres uniques et des éléments sécurisés tels que des mots de passe

Création d'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 crochet Web configuré pour Slack :



Saisissez les informations appropriées pour chacun des champs, puis cliquez sur Save lorsque vous avez terminé.

Vous pouvez également cliquer sur le bouton « Tester Webhook » pour tester la connexion. Notez que le « corps du message » (sans substitutions) est envoyé à l'URL définie selon la méthode sélectionnée.

Les webhooks Data Infrastructure Insights comprennent un certain nombre de paramètres par défaut. En outre, 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 : quels sont-ils et comment les utiliser ?

Les paramètres d'alerte sont des valeurs dynamiques remplies 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, nom de stockage) comme 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 : « High Latency for Volume: *%%relatedObject.volume.name%%*, Storage: *%%relatedObject.storage.name%%*".

Notez que dans cette section, les substitutions sont *non* effectuées lorsque vous cliquez sur le bouton « Tester le Webhook » ; le bouton envoie une charge utile indiquant les substitutions de _ %_ mais ne les remplace pas par des données.

Paramètres et secrets personnalisés

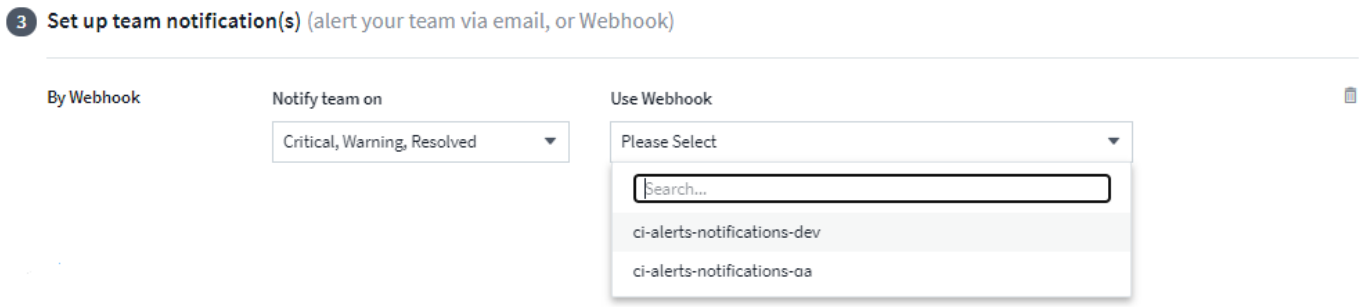
Dans cette section, vous pouvez ajouter des paramètres et/ou des secrets personnalisés. Pour des raisons de sécurité, si un secret est défini, seul le créateur de webhook peut modifier ce canal de webhook. Il est en lecture seule pour les autres. Vous pouvez utiliser les secrets d'URL/en-têtes sous la forme *%<secret_name>%*.

Page de liste Webhooks

Sur la page de liste Webhooks, sont affichés le Nom, créé par, créé le, État, sécurisé, et les champs dernier rapport.

Choix de notification Webhook dans un moniteur

Pour choisir la notification webhook dans un "superviser", accédez à **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 crochet souhaité.



Exemples de Webhook :

Webhooks pour "Mou" Webhooks pour "Service de PagerDuty" Webhooks pour "Équipes""Déroulez"

Exemple de cordon de discorde avec Webhook

Les Webpatères permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal Web personnalisé. Cette page fournit un exemple de configuration des crochets pour le discorde.

> Cette page fait référence aux instructions de tiers, qui peuvent faire l'objet de modifications. Reportez-vous au "Documentation de discorde" pour obtenir les informations les plus récentes.

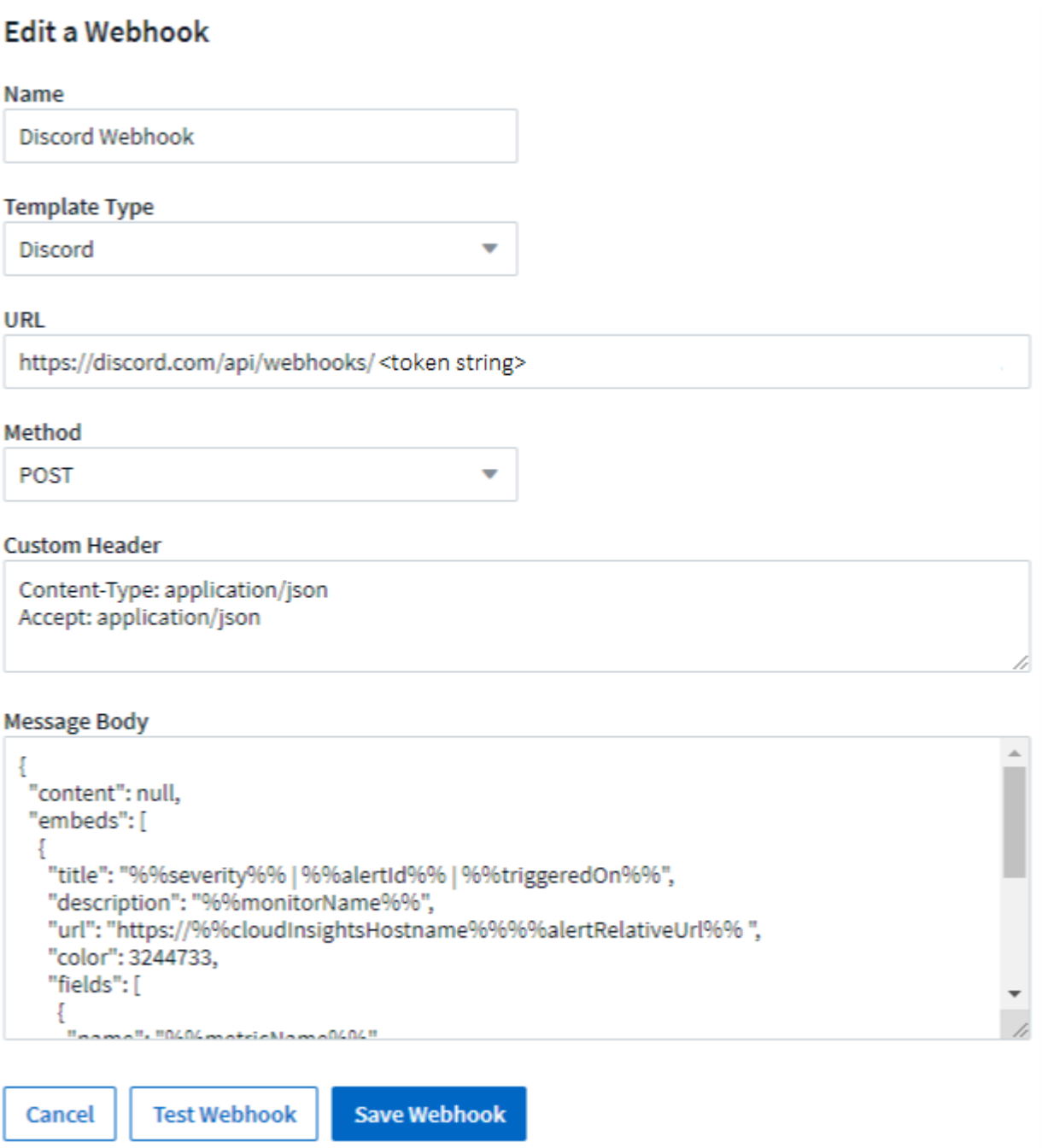
Configuration de la discorde :

- Dans Discordon, sélectionnez le serveur, sous canaux de texte, sélectionnez Modifier le canal (icône d'engrenage)
- Sélectionnez **intégrations > Afficher Webpatères** et cliquez sur **Nouveau Webhook**

- Copiez l'URL du Webhook. Vous devez coller cette information dans la configuration du webhook Data Infrastructure Insights.

Créer le 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 mousqueton.
2. Donnez au webhook un nom significatif, tel que « discorde ».
3. Dans la liste déroulante *Template Type*, sélectionnez **discorde**.
4. Collez l'URL ci-dessus dans le champ *URL*.

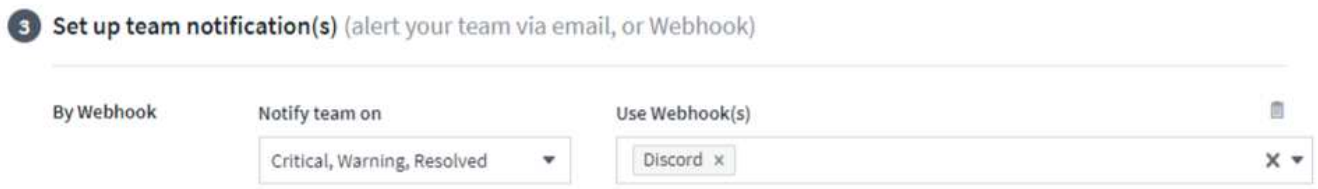


Pour tester le webhook, remplacez temporairement la valeur de l'url dans le corps du message par une URL valide (telle que *https://NetApp.com*), puis cliquez sur le bouton *Test Webhook*. Une fois le test terminé, veillez à remettre le corps du message en place.

Notifications via Webhook

Pour signaler des événements via Webhook, accédez à **alertes > moniteurs** dans Data Infrastructure Insights et cliquez sur **+Monitor** pour créer un nouveau "superviser".

- Sélectionnez une mesure et définissez les conditions du moniteur.
- Sous _configurer la ou les notifications d'équipe, choisissez la méthode de livraison **Webhook**.
- Choisissez le crochet pour le « cordon » pour les événements souhaités (critique, Avertissement, résolu)



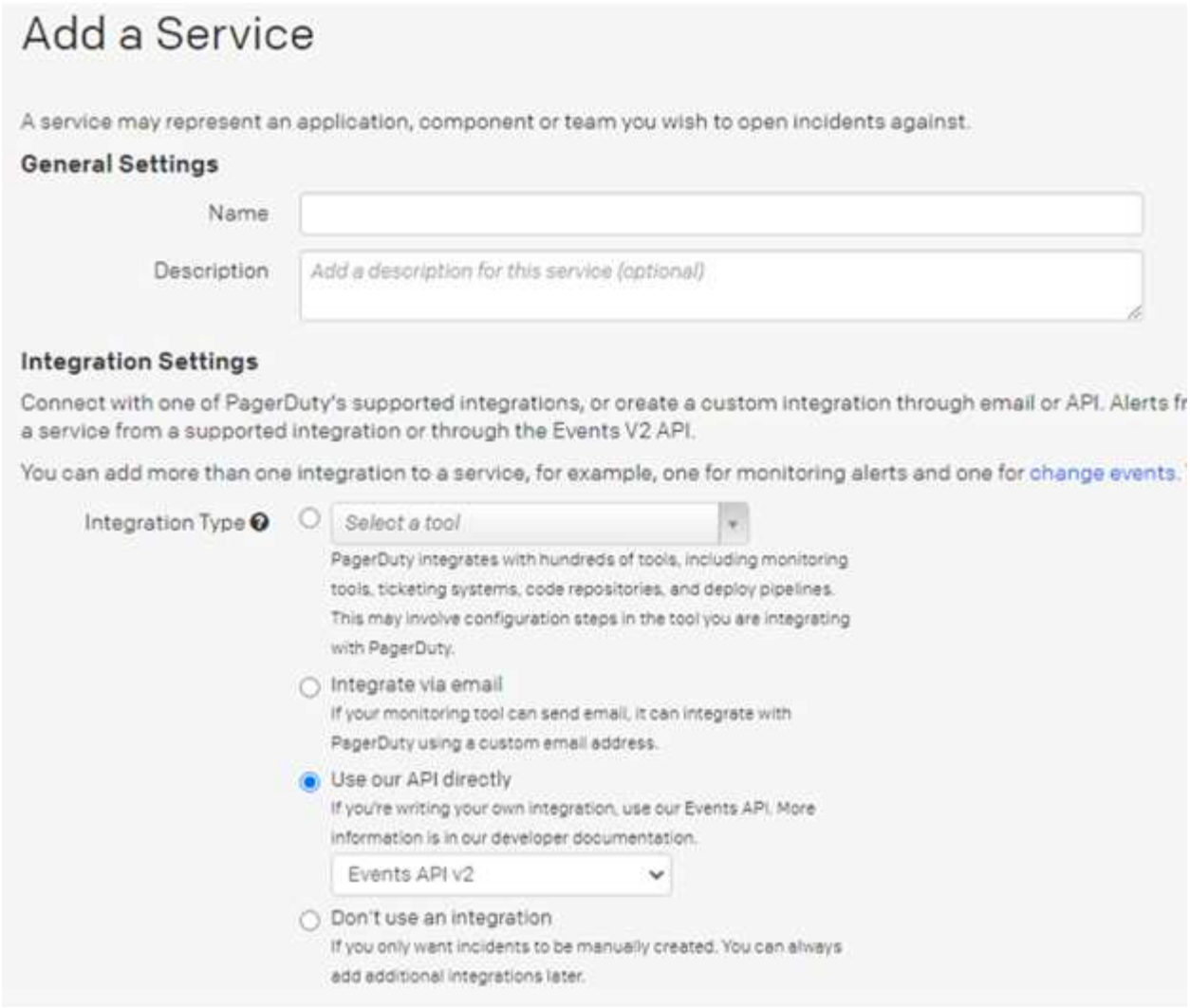
Exemple de Webhook pour PagerDuty

Les Webpatères permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal Web personnalisé. Cette page fournit un exemple de configuration des crochets pour PagerDuty.

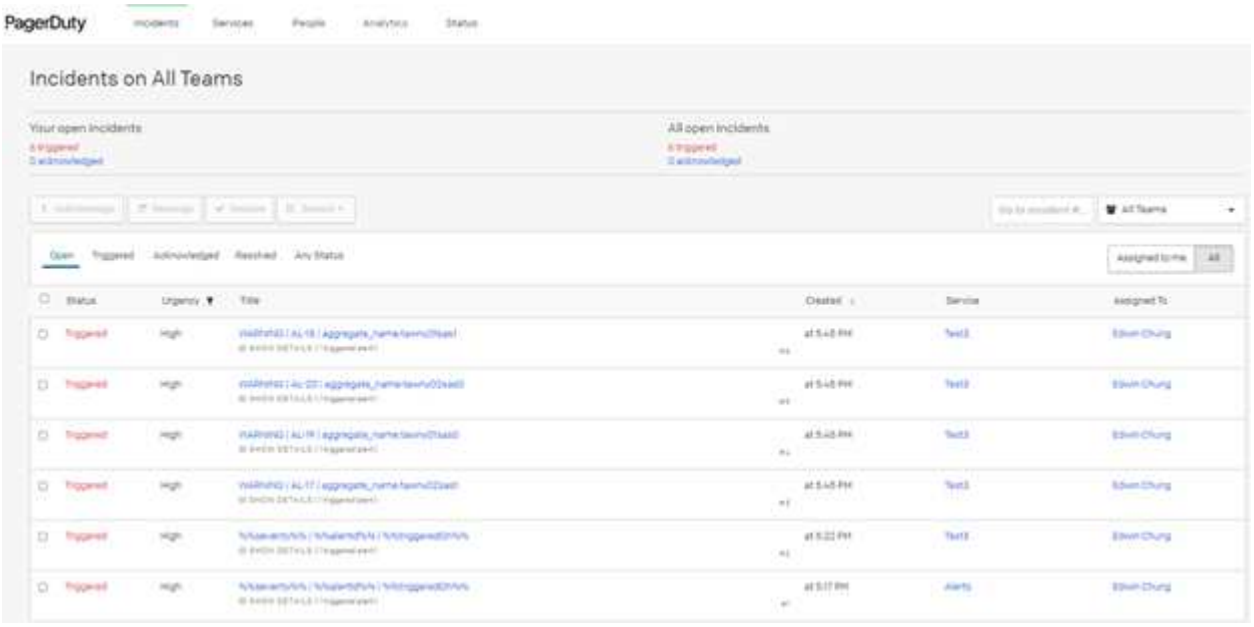
Cette page fait référence aux instructions de tiers, qui peuvent faire l'objet de modifications. Reportez-vous au "Documentation PagerDuty" pour obtenir les informations les plus récentes.

Configuration de la fonction PagerDuty :

1. Dans PagerDuty, accédez à **Services > répertoire de services** et cliquez sur le lien **+Nouveau Service** button
2. Entrez un *Nom* et sélectionnez *utiliser notre API directement*. Cliquez sur *Add Service*.

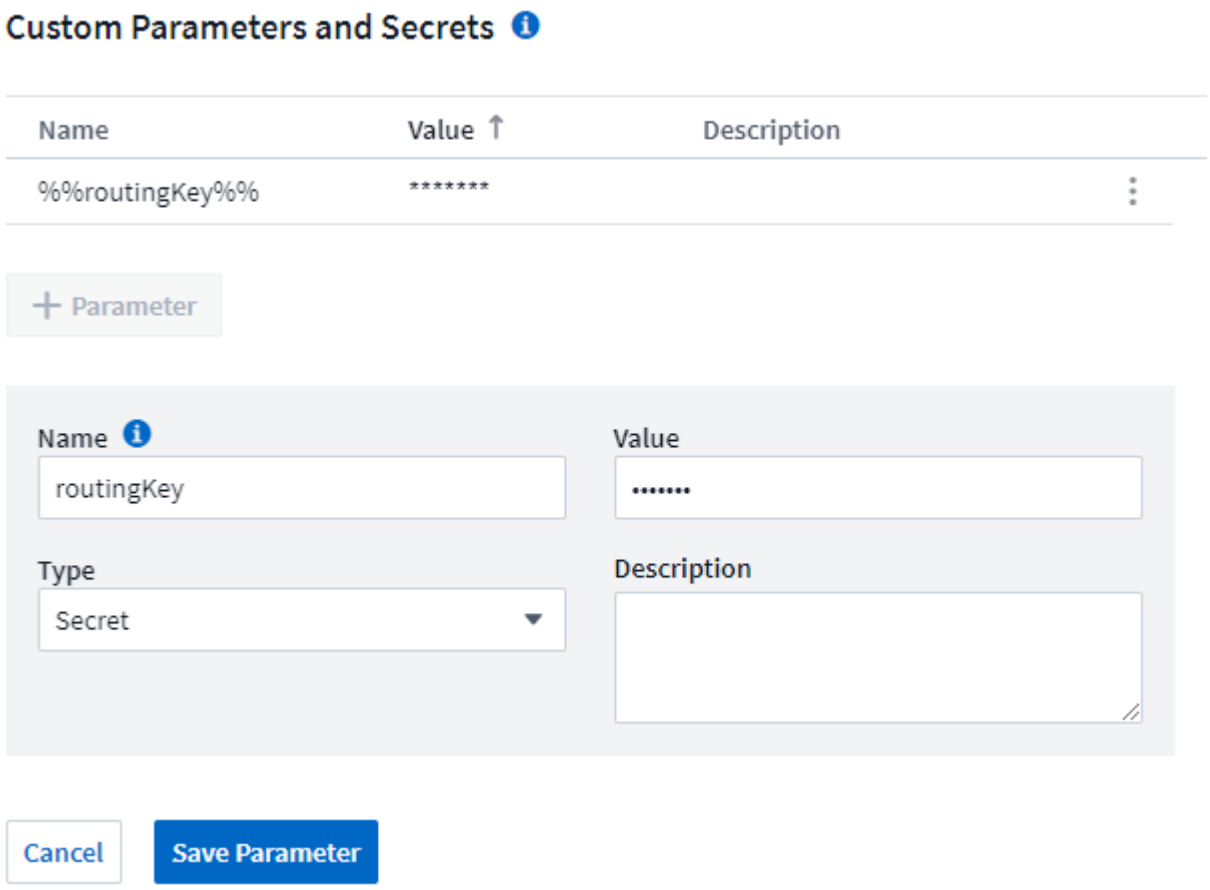


3. Cliquez sur l'onglet *Integrations* pour afficher **Integration Key**. Vous aurez besoin de cette clé lorsque vous créez le mousqueton Data Infrastructure Insights ci-dessous.
4. Accédez à **incidents** ou **Services** pour afficher les alertes.



Créer le 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 mousqueton.
2. Donnez un nom significatif au mousqueton, tel que « déclencheur PagerDuty ». Vous utiliserez ce webhook pour les événements critiques et de niveau d'avertissement.
3. Dans la liste déroulante *Template Type*, sélectionnez **PagerDuty**.
4. Créez un paramètre personnalisé secret nommé *routingKey* et définissez la valeur sur la valeur PagerDuty *Integration Key* du dessus.



Répétez ces étapes pour créer une bande-son « résolution de pagerDuty » pour les événements résolus.

Mappage du champ informations de PagerDuty vers Data Infrastructure

Le tableau et l'image suivants présentent le mappage des champs entre PagerDuty et Data Infrastructure Insights :

Service de PagerDuty	Informations exploitables sur l'infrastructure de données
Touche d'alerte	L'ID d'alerte
Source	Activé
Composant	Nom de la mesure
Groupe	Type d'objet

Service de PagerDuty	Informations exploitables sur l'infrastructure de données
Classe	Nom du moniteur

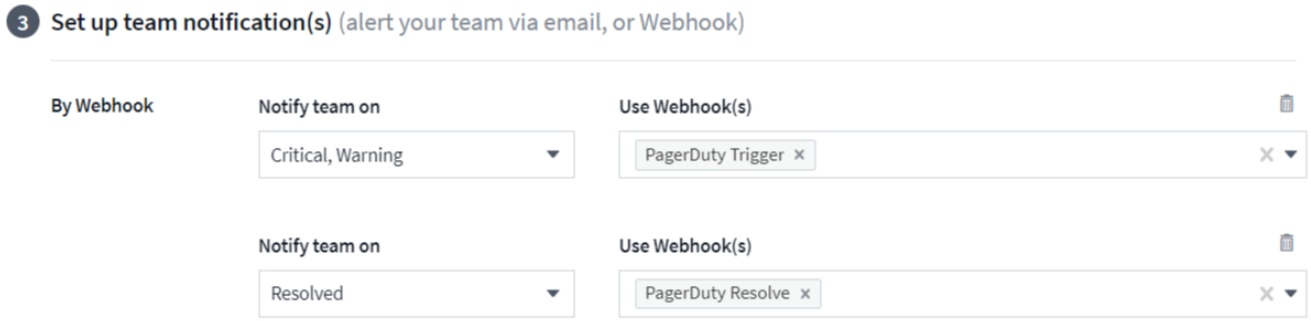
Message Body

```
{
 "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 signaler des événements via Webhook, accédez à **alertes > moniteurs** dans Data Infrastructure Insights et cliquez sur **+Monitor** pour créer un nouveau "superviser".

- Sélectionnez une mesure et définissez les conditions du moniteur.
- Sous _configurer la ou les notifications d'équipe, choisissez la méthode de livraison **Webhook**.
- Choisissez le mousqueton « PagerDuty Trigger » pour les événements de niveau critique et Avertissement.
- Choisissez la « résolution de PagerDuty » pour les événements résolus.



La définition de notifications distinctes pour les événements déclencheurs par rapport aux événements résolus est une pratique recommandée, puisque PagerDuty gère les événements déclencheurs différemment des événements résolus.

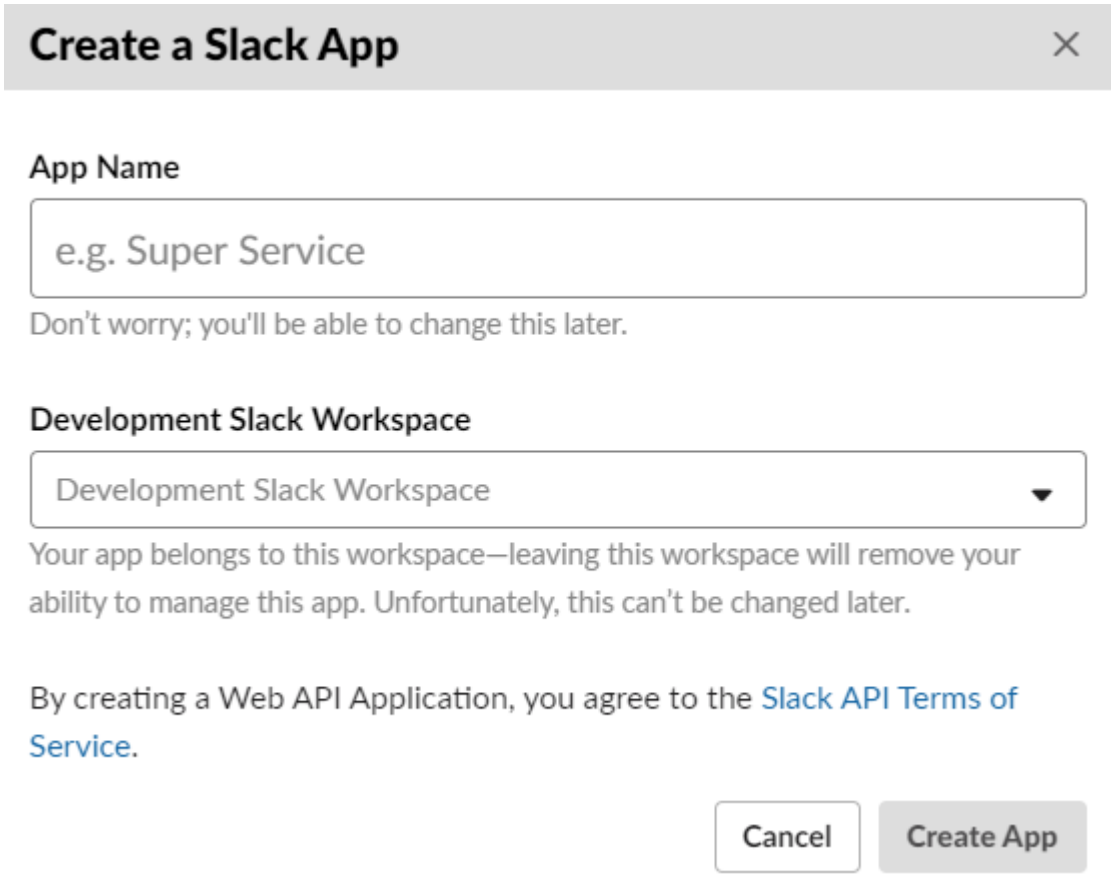
Exemple de mousqueton pour le mou

Les Webpatères permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal Web personnalisé. Cette page fournit un exemple de configuration des crochets pour le mou.

Cette page fait référence aux instructions de tiers, qui peuvent faire l'objet de modifications. Reportez-vous au "Documentation Slack" pour obtenir les informations les plus récentes.

Exemple de mou :

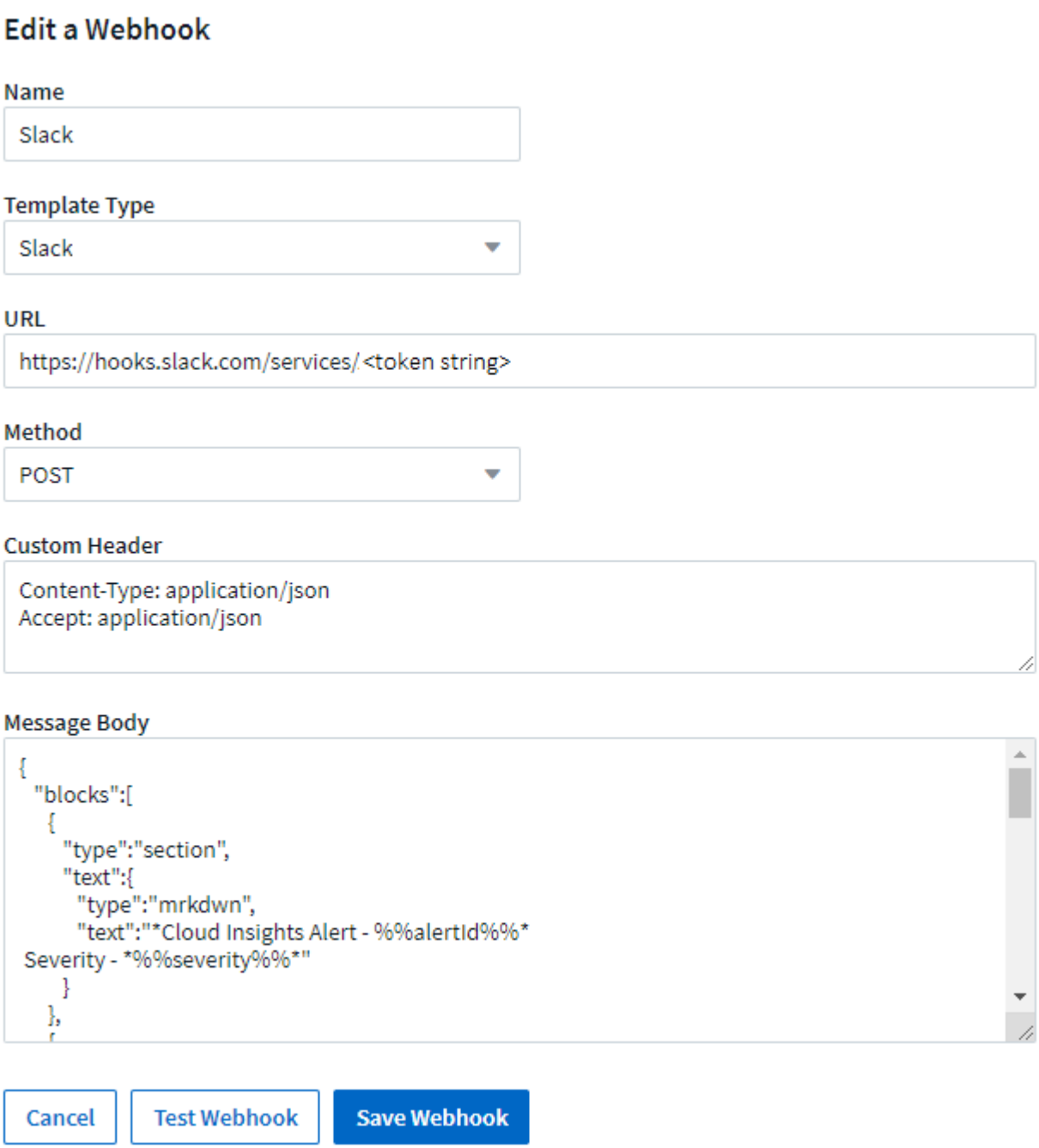
- Accédez à https://api.slack.com/apps et créez une nouvelle application Donnez un nom significatif et sélectionnez l'espace de travail Slack.



- Accédez aux Webpatères entrants, cliquez sur *Activer les Webpatères entrants*, demander à *Ajouter un nouveau Webhook* et sélectionnez le canal sur lequel envoyer.
- Copiez l'URL du Webhook. Vous devez coller cette information dans la configuration du webhook Data Infrastructure Insights.

Créer le Webhook Data Infrastructure Insights :

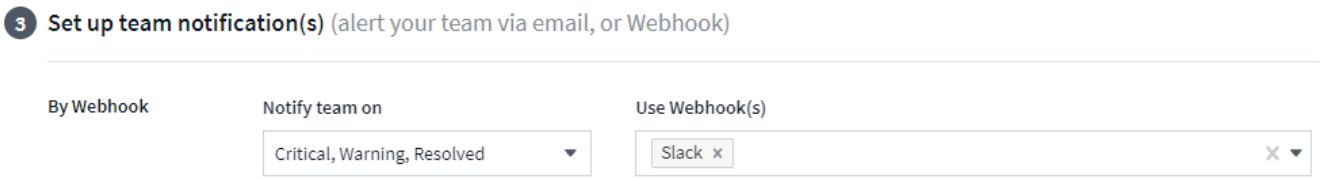
1. Dans Data Infrastructure Insights, accédez à **Admin > Notifications** et sélectionnez l'onglet **Webhooks**. Cliquez sur **+Webhook** pour créer un nouveau mousqueton.
2. Donnez au webhook un nom significatif, tel que « Slack Webhook ».
3. Dans la liste déroulante *Template Type*, sélectionnez **Slack**.
4. Collez l'URL ci-dessus dans le champ *URL*.



Notifications via Webhook

Pour signaler des événements via Webhook, accédez à **alertes > moniteurs** dans Data Infrastructure Insights et cliquez sur **+Monitor** pour créer un nouveau "superviser".

- Sélectionnez une mesure et définissez les conditions du moniteur.
- Sous _configurer la ou les notifications d'équipe, choisissez la méthode de livraison **Webhook**.
- Choisissez le crochet pour le « mou » pour les événements souhaités (critique, Avertissement, résolu)



Pour aller plus loin :

- Pour modifier le format et la disposition des messages, voir https://api.slack.com/messaging/composing
- Gestion des erreurs : https://api.slack.com/messaging/webhooks#handling_errors

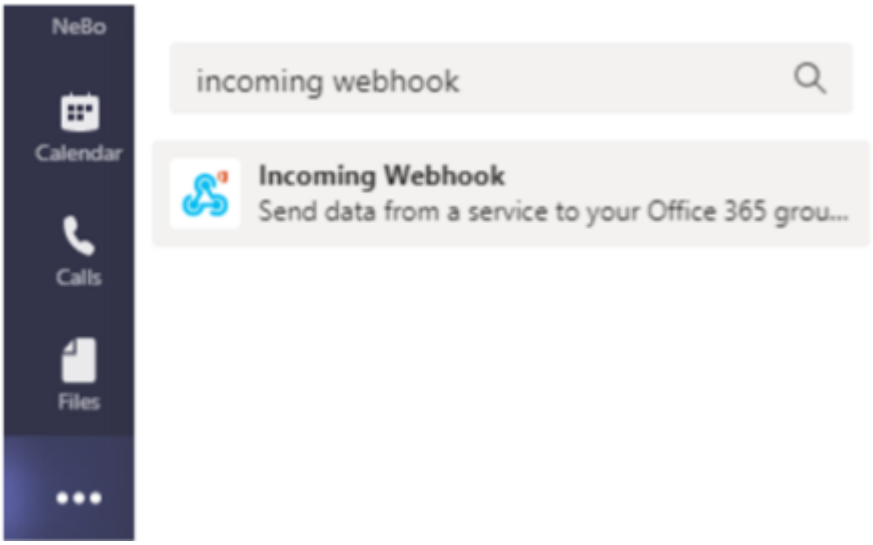
Exemple Webhook pour Microsoft Teams

Les Webpatères permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal Web personnalisé. Cette page fournit un exemple de configuration des crochets pour les équipes.

Cette page fait référence aux instructions de tiers, qui peuvent faire l'objet de modifications. Reportez-vous au "Documentation des équipes" pour obtenir les informations les plus récentes.

Configuration des équipes :

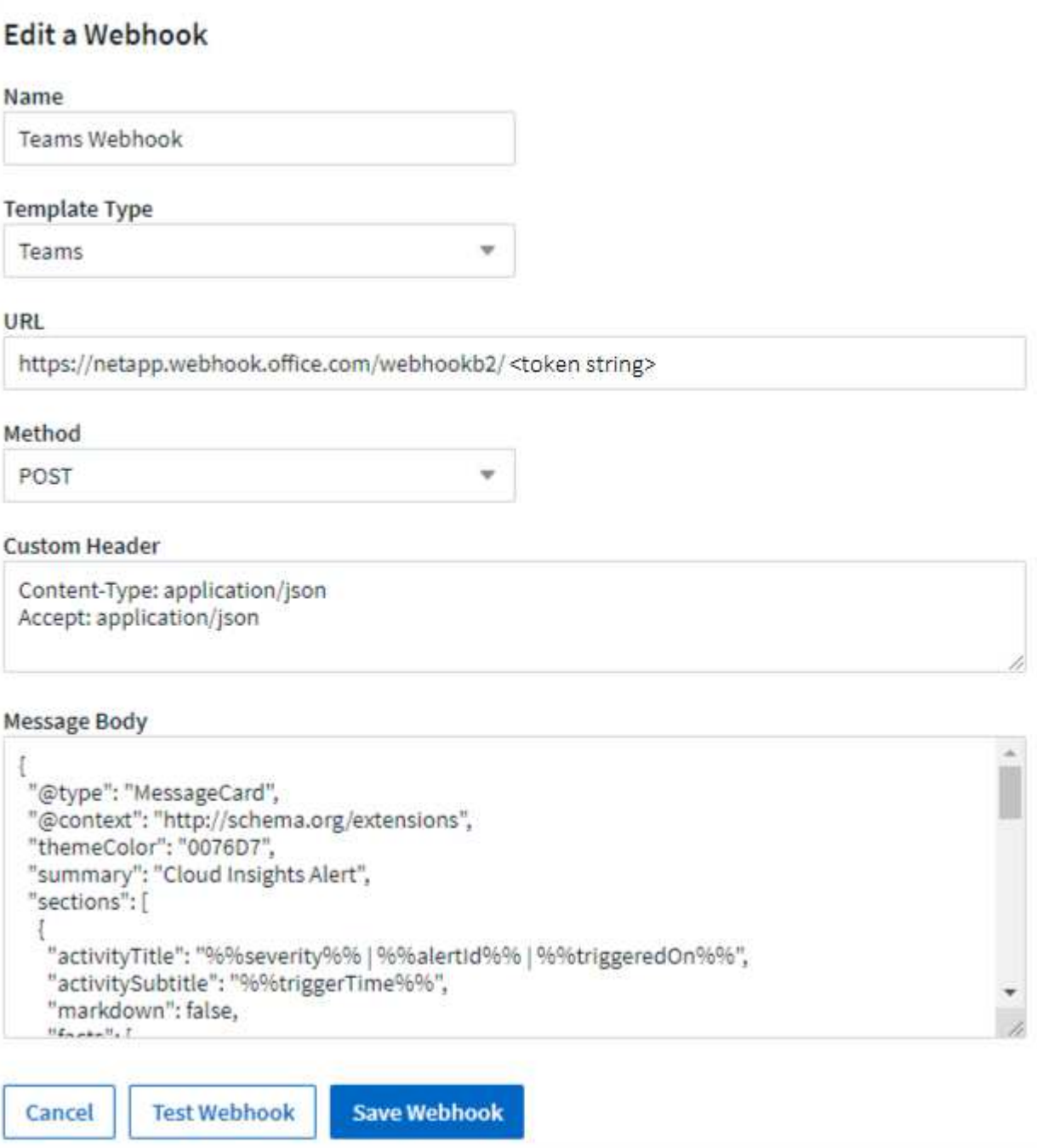
1. Dans Teams, sélectionnez le kebab et recherchez le Webhook entrant.



2. Sélectionnez **Ajouter à une association > Sélectionner une association > configurer un connecteur**.
3. Copiez l'URL du Webhook. Vous devez coller cette information dans la configuration du webhook Data Infrastructure Insights.

Créer le 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 mousqueton.
2. Donnez au webhook un nom significatif, tel que "Teams Webhook".
3. Dans la liste déroulante *Template Type*, sélectionnez **Teams**.

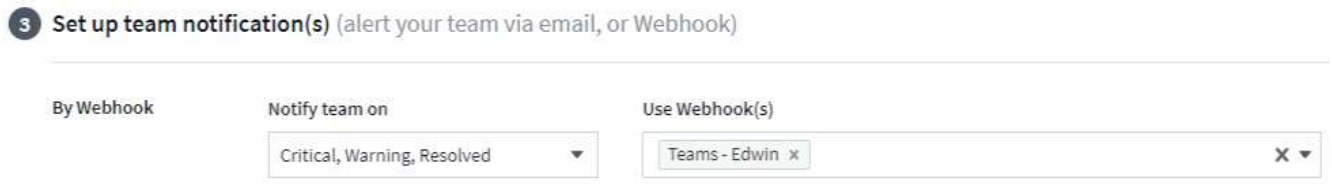


1. Collez l'URL ci-dessus dans le champ *URL*.

Notifications via Webhook

Pour signaler des événements via Webhook, accédez à **alertes > moniteurs** dans Data Infrastructure Insights et cliquez sur **+Monitor** pour créer un nouveau "superviser".

- Sélectionnez une mesure et définissez les conditions du moniteur.
- Sous _configurer la ou les notifications d'équipe, choisissez la méthode de livraison **Webhook**.
- Choisissez le « Teams » pour les événements souhaités (critique, Avertissement, résolu).



Utilisation des annotations

Définition des annotations

Lorsque vous personnalisez des informations de l'infrastructure de données pour effectuer le suivi des données en fonction des besoins de votre entreprise, vous pouvez définir des notes spécialisées, appelées annotations, et les affecter à vos ressources.

Vous pouvez attribuer des annotations à des ressources avec des informations telles que la fin de vie des ressources, le data Center, l'emplacement de construction, le Tier de stockage ou le niveau de service du volume.

L'utilisation d'annotations pour vous aider à contrôler votre environnement comprend les tâches de haut niveau suivantes :

- Création ou modification de définitions pour tous les types d'annotation.
- Affichage des pages ASSET et association de chaque ressource à une ou plusieurs annotations.

  Par exemple, si un bien est loué et que le bail expire dans un délai de deux mois, vous pouvez appliquer une annotation de fin de vie à l'actif. Cela permet d'éviter que d'autres personnes n'utilisent cette ressource 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'annotation par défaut

Data Infrastructure Insights propose 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 :

- Le cycle de vie des actifs, comme l'anniversaire, le coucher du soleil ou la fin de vie
- Informations de localisation sur un appareil, comme un centre de données, un bâtiment ou un sol
- Classification des actifs, par exemple par qualité (niveaux), par périphériques connectés (niveau du commutateur) ou par niveau de service
- État, comme les données fortement sollicitées (utilisation élevée)

Le tableau suivant répertorie les types d'annotations fournies par Data Infrastructure Insights.

Types d’annotation	Description	Type
Alias	Nom convivial pour une ressource	Texte
Calculer le groupe de ressources	Affectation de groupe utilisée par le collecteur de données systèmes de fichiers hôte et VM	Liste
Data Center	Emplacement physique	Liste
Chaud	Dispositifs en utilisation intensive sur une base régulière ou au seuil de capacité	Booléen
Remarque	Commentaires associés à une ressource	Testez
Niveau de service	Un ensemble de niveaux de service pris en charge que vous pouvez attribuer aux ressources. Le fournit une liste d’options ordonnée pour les volumes internes, qtree et volumes. Modifiez les niveaux de service pour définir des règles de performances adaptées à différents niveaux.	Liste
Coucher de soleil	Seuil défini après lequel aucune nouvelle attribution ne peut être effectuée à ce périphérique. Utile pour les migrations planifiées et autres modifications réseau en attente.	Date
Niveau du commutateur	Options prédéfinies pour la configuration des catégories de commutateurs. Généralement, ces désignations restent pour la durée de vie du périphérique, bien que vous puissiez les modifier. Disponible uniquement pour les commutateurs.	Liste
Niveau	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, Gold ou Silver). 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	Classer (par exemple, majeur) d’une violation (par exemple, ports hôtes manquants ou redondance manquante), dans une hiérarchie de la plus haute à la plus faible importance.	Liste

Alias, data Center, données actives, niveau de service, coucher de soleil, Niveau de commutation, niveau et gravité de violation sont des annotations au niveau du système, que vous ne pouvez pas supprimer ou renommer ; vous pouvez uniquement modifier les valeurs qui leur sont attribuées.

Création d’annotations personnalisées

Ces annotations vous permettent d’ajouter des données personnalisées spécifiques à l’entreprise qui correspondent aux ressources de votre entreprise. Même si les informations sur l’infrastructure de données proposent un ensemble d’annotations par défaut, vous pouvez souhaiter afficher les données de différentes manières. Les données contenues dans des annotations personnalisées complètent les données déjà collectées, telles que le fabricant du stockage, le nombre de volumes et les statistiques de performance. Les données que vous ajoutez à l’aide d’annotations ne sont pas découvertes par Data Infrastructure Insights.

Étapes

1. Dans le menu informations sur l'infrastructure de données, cliquez sur **gérer > Annotations**.

   La page Annotations affiche la liste des annotations.

2. Cliquez sur **+Ajouter**
3. Saisissez un **Nom** et **Description** de l'annotation.

   Ces champs peuvent comporter jusqu'à 255 caractères.

4. Cliquez sur **Type**, puis sélectionnez l'une des options suivantes qui représente le type de données autorisé dans cette annotation :

Types d'annotation

Booléen : crée une liste déroulante avec les choix de oui et de non. Par exemple, l'annotation « Direct attached » est booléenne. Date : crée un champ contenant une date. Par exemple, si l'annotation est une date, sélectionnez cette option. Liste : crée l'une des options suivantes : * Une liste déroulante fixe

+ lorsque d'autres attribuent ce type d'annotation à un périphérique, ils ne peuvent pas ajouter d'autres 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 à un périphérique, elles peuvent ajouter d'autres valeurs à la liste.

Nombre : crée un champ dans lequel l'utilisateur qui affecte l'annotation peut entrer un nombre. Par exemple, si le type d'annotation est « sol », l'utilisateur peut sélectionner le type de valeur « nombre » et saisir le numéro d'étage.

Texte : crée un champ permettant le texte libre. Par exemple, vous pouvez saisir "langue" comme type d'annotation, sélectionner "texte" comme type de valeur et entrer 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 des valeurs supplémentaires à l'annotation sur une page de ressources, ce qui crée une liste flexible.

      Par exemple, supposons que vous vous trouvez sur une page d'actifs et que l'actif comporte l'annotation City avec les valeurs Detroit, 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 la ressource au lieu de devoir aller 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. Entrez 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 de la page Annotations.

Une fois que vous avez terminé

L'annotation est immédiatement disponible dans l'interface utilisateur.

Utilisation d'annotations

Vous créez des annotations et vous les attribuez aux ressources que vous surveillez. Ces annotations sont des notes qui fournissent des informations sur une ressource, telles que l'emplacement physique, la fin de vie, le niveau de stockage ou les niveaux de service de volume.

Définition des annotations

Ces annotations vous permettent d'ajouter des données personnalisées spécifiques à l'entreprise qui correspondent aux ressources de votre entreprise. Les informations d'infrastructure de données fournissent un ensemble d'annotations par défaut, telles que le cycle de vie des ressources (date d'anniversaire ou de fin de vie), l'emplacement du bâtiment ou du data Center et le niveau, mais vous pouvez rechercher d'autres façons d'afficher les données.

Les données contenues dans des annotations personnalisées complètent les données déjà recueillies sur les périphériques, telles que le fabricant du commutateur, le nombre de ports et les statistiques de performance. Les données que vous ajoutez à l'aide d'annotations ne sont pas découvertes par Data Infrastructure Insights.

Avant de commencer

- Répertoriez toute terminologie de l'industrie à laquelle les données d'environnement doivent être associées.
- Répertorier la terminologie d'entreprise à laquelle les données d'environnement doivent être associées.
- Identifiez tout type d'annotation par défaut que vous pouvez utiliser.
- Identifiez les annotations personnalisées que vous devez créer. Vous devez créer l'annotation pour pouvoir l'affecter à une ressource.

Procédez comme suit 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. Entrez un nom, une description et un type pour la nouvelle annotation.

   Par exemple, entrez ce qui suit pour créer une annotation texte qui définit l'emplacement physique d'une ressource dans Data Center 4 :

   - Saisissez un nom pour l'annotation, tel que « emplacement »
   - Saisissez une description de l'annotation, telle que « l'emplacement physique est Data Center 4 ».
   - Entrez le type d'annotation, tel que « texte ».

Affectation manuelle d'annotations aux ressources

L'affectation d'annotations aux ressources vous permet de trier, de regrouper et de 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 affecter des annotations à une ressource individuelle à l'aide de sa page de contenu.

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 la ressource à laquelle vous souhaitez appliquer l'annotation.
    - Vous pouvez localiser les ressources en effectuant une requête, en choisissant un widget dasoard ou en effectuant une recherche. Une fois que vous avez trouvé la ressource souhaitée, cliquez sur le lien pour ouvrir la page d'accueil de la ressource.
3. Sur la page ressource, 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, en fonction du 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 texte, saisissez une valeur.
7. Cliquez sur **Enregistrer**.

Si vous souhaitez modifier la valeur de l'annotation après l'avoir affectée, cliquez sur le champ d'annotation et sélectionnez une autre valeur. Si l'annotation est de type liste pour laquelle l'option *Ajouter de nouvelles valeurs sur Fly* est sélectionnée, vous pouvez saisir une nouvelle valeur en plus de la sélection d'une valeur existante.

Affectation d'annotations à l'aide de règles d'annotation

Pour attribuer automatiquement des annotations aux ressources en fonction des critères que vous définissez, vous devez configurer des règles d'annotation. Les informations d'infrastructure de données affectent les annotations aux ressources en fonction de ces règles. Data Infrastructure Insights propose également deux règles d'annotation par défaut, que vous pouvez modifier en fonction de 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 une page de ressource individuelle ont priorité sur les annotations basées sur des règles lors de l'évaluation par Insight des règles d'annotation.

Avant de commencer

Vous devez avoir créé une requête pour la règle d'annotation.

Description de la tâche

Bien que vous puissiez modifier les types d'annotation lors de la création des 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 zone **Nom**, entrez un nom unique qui décrit la règle.

      Ce nom apparaît dans la page règles d'annotation.

   b. Cliquez sur **Query** 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 planifié régulièrement.

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. Les informations d'infrastructure de données affectent les annotations aux ressources en fonction de ces règles. Les annotations définies manuellement sur une page de ressource individuelle ont priorité sur les annotations basées sur des règles lors de l'évaluation des règles d'annotation par Cloud Insight.

Avant de commencer

Vous devez avoir créé une requête pour la règle d'annotation.

Étapes

1. Dans le menu informations sur l'infrastructure de données, 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 zone **Nom**, entrez un nom unique qui décrit la règle.

      Le nom apparaît dans la page règles d'annotation.

   b. Cliquez sur **Query** et sélectionnez la requête utilisée par Data Infrastructure Insights pour identifier les actifs auxquels 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 planifié régulièrement.

> Dans un environnement Data Infrastructure Insights volumineux, vous remarquerez peut-être que l'exécution de règles d'annotation semble prendre un certain temps. Ceci est dû au fait que l'indexeur s'exécute en premier et doit se terminer avant d'exécuter les règles. L'indexeur permet à Data Infrastructure Insights 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 modifier le nom de la règle, son annotation, la valeur de l'annotation ou la requête associée à la règle.

Étapes

1. Dans le menu informations sur l'infrastructure de données, 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 à modifier.

   Vous pouvez filtrer les règles d'annotation en entrant 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 au bas. Pour modifier l'ordre de traitement d'une règle, procédez comme suit :

Étapes

1. Cliquez sur l'icône de menu correspondant à la règle que vous souhaitez déplacer.
2. Cliquez sur **déplacer vers le haut** ou **déplacer vers le bas** selon les besoins jusqu'à ce que la règle s'affiche à l'emplacement souhaité.

Notez que lors de l'exécution de plusieurs règles qui mettent à jour la même annotation sur une ressource, la première règle (exécutée depuis le haut vers le bas) applique l'annotation et met à jour la ressource, la seconde règle s'applique mais ne modifie pas toute annotation qui a déjà été définie par la règle précédente.

Suppression de règles d'annotation

Vous pouvez supprimer les règles d'annotation qui ne sont plus utilisées.

Étapes

1. Dans le menu informations sur l'infrastructure de données, 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 à supprimer.

   Vous pouvez filtrer les règles d'annotation en entrant 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 à supprimer.
4. Cliquez sur **Supprimer**

   Un message de confirmation s'affiche, vous invitant à supprimer la règle.

5. Cliquez sur **OK**

Importation d'annotations

Data Infrastructure Insights inclut une API pour importer des annotations ou des applications à partir d'un fichier CSV et les attribuer aux objets que vous spécifiez.

L'API Data Infrastructure Insights est disponible dans **Data Infrastructure Insights Premium Edition**.

Importation

Les liens **Admin > API Access** contiennent "documentation" pour l'API **Assets/Import**. Cette documentation contient des informations sur le format de fichier .CSV.

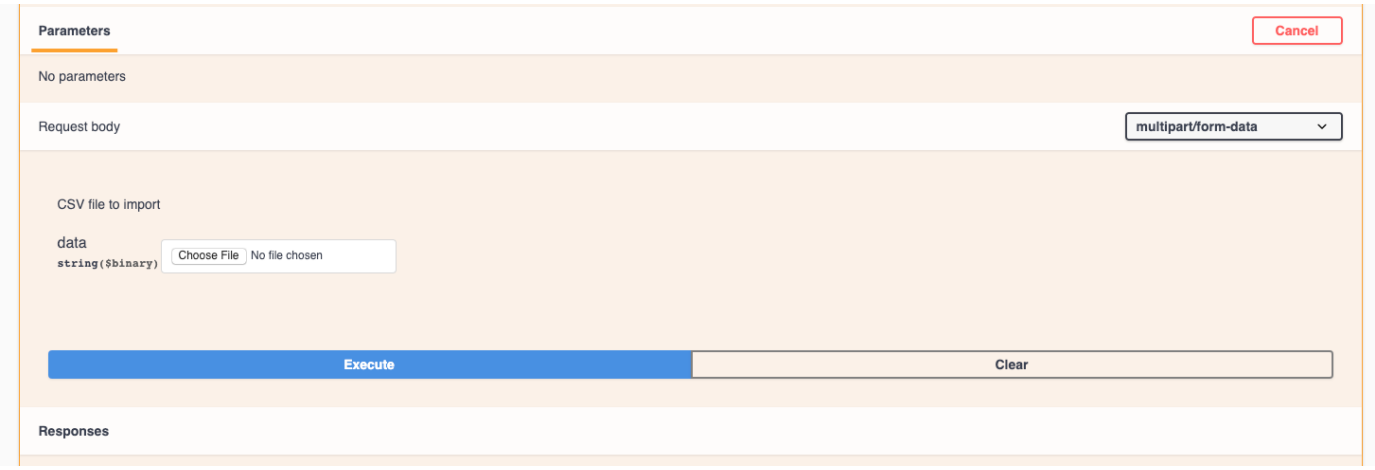


Format de fichier .CSV

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. Cette opération est suivie de lignes distinctes pour chaque annotation ou application. Il n'est pas nécessaire de définir chaque champ. Toutefois, 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]
Reportez-vous à la documentation API pour des exemples de fichiers .CSV.
```

Vous pouvez importer et attribuer des annotations à partir d'un fichier .CSV à partir de l'outil de swagger de l'API lui-même. Il vous suffit de choisir le fichier à utiliser et de cliquer sur le bouton *Execute* :



Comportement d'importation

Lors de l'importation, des données sont ajoutées, fusionnées ou remplacées, en fonction des objets et des types d'objets en cours d'importation. 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 avec 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 du même nom existe dans le système cible.

  Remarque : si une annotation portant le même nom mais avec un type différent existe dans le système cible, l'importation échoue. Si les objets dépendent de l'annotation qui a échoué, ces objets peuvent afficher des informations incorrectes ou indésirables. Vous devez vérifier toutes les dépendances des annotations 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 de date doivent être transmises en millisecondes sous forme d'heure unix.
- Lors de l'annotation des volumes ou des volumes internes, le nom de l'objet combine le nom du stockage et le nom du volume en utilisant le séparateur «-> ». Par exemple : *<Nom du stockage>-><Nom du volume>*
- Si un nom d'objet contient une virgule, le nom entier doit être entre guillemets. Par exemple : *« NetApp1,NetApp2 »-> 023F*
- Lorsque vous fixez des annotations aux stockages, commutateurs et ports, la colonne « application » est ignorée.

- Locataire, secteur_d'activité, entité_commerciale et/ou projet fait une entité commerciale. Comme pour toutes les entités métier, toutes les valeurs peuvent être vides.

Les types d'objet suivants peuvent être annotés.

TYPE D'OBJET	NOM OU TOUCHE
Hôte	id-><ID> ou <Nom> ou <IP>
VM	id-><ID> ou <Nom>
Poolde stockage	id-><ID> ou <Nom du stockage>-><Nom du pool de stockage>
Volume interne	id-><ID> ou <Nom du stockage>-><Nom du volume interne>
Volumétrie	id-><ID> ou <Nom du stockage>-><Nom du volume>
Stockage	id-><ID> ou <Nom> ou <IP>
Commutateur	id-><ID> ou <Nom> ou <IP>
Port	id-><ID> ou <WWN>
Qtree	id-><ID> ou <Nom du stockage>-><Nom du volume interne>-><Nom du qtree>
Partagez	id-><ID> ou <Nom du stockage>-><Nom du volume interne>-><Nom du partage>-><Protocole>[-><Nom du qtree (facultatif en cas de qtree par défaut)>]

Utilisation des applications

Suivi de l'utilisation des ressources par application

Connaître les applications utilisées dans l'environnement de votre entreprise vous aide à surveiller l'utilisation des ressources et les coûts.

Avant de pouvoir suivre les données associées aux applications s'exécutant 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, les partages et les hyperviseurs.

Cette rubrique fournit un exemple de suivi de l'utilisation des machines virtuelles que l'équipe marketing utilise pour son courrier électronique Exchange.

Vous pouvez créer un tableau similaire à celui ci-dessous pour identifier les applications utilisées sur votre tenant et noter le groupe ou l'unité commerciale utilisant chaque application.

Locataire	Secteur d'activité	Unité commerciale	Projet	En termes de latence
NetApp	Stockage des données	Légal	Brevets	Oracle Identity Manager, Oracle On Demand, PatentWiz

NetApp	Stockage des données	Marketing	Événements commerciaux	Exchange, base de données partagée Oracle, planificateur d'événements BlastOff

Le tableau indique que l'équipe marketing utilise l'application Exchange. Nous souhaitons suivre l'utilisation de leurs ordinateurs virtuels pour Exchange, afin que nous puissions prévoir quand il nous faudra ajouter du stockage. Nous pouvons associer l'application Exchange à toutes les machines virtuelles de Marketing :

1. Créez une application nommée *Exchange*
2. Accédez à **Queries > +New Query** pour créer une nouvelle requête pour les machines virtuelles (ou sélectionnez une requête VM existante, le cas échéant).

   En supposant que les ordinateurs virtuels de l'équipe Marketing aient tous un nom contenant la chaîne "**mkt**", créez votre requête pour filtrer le nom de la machine virtuelle pour "mkt".

3. Sélectionnez les VM.
4. Associez les machines virtuelles à l'application *Exchange* à l'aide de **actions groupées > Ajouter des applications**.
5. Sélectionnez l'application souhaitée et cliquez sur **Enregistrer**.
6. Lorsque vous avez terminé, **Enregistrer** la requête.

Création d'applications

Pour suivre les données associées à des applications spécifiques s'exécutant sur votre locataire, vous pouvez définir les applications dans Data Infrastructure Insights.

Description de la tâche

Les informations sur l'infrastructure de données vous permettent de suivre les données des ressources associées aux applications, par exemple pour l'utilisation ou le reporting des coûts.

Étapes

1. Dans le menu informations sur l'infrastructure de données, cliquez sur **observabilité > enrichir > applications**. Sélectionnez

   La boîte de dialogue Ajouter une application s'affiche.

2. Saisissez 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 aux ressources

Cette procédure attribue l'application à un hôte comme exemple. Vous pouvez affecter un hôte, une machine virtuelle, un volume ou des volumes internes à une application.

Étapes

1. Recherchez la ressource à attribuer à l'application :
2. Cliquez sur **Queries > +New Query** et recherchez Host.
3. Cochez la case à gauche de l'hôte que vous souhaitez associer à l'application.
4. Cliquez sur **actions groupées > Ajouter une application**.
5. Sélectionnez l'application à laquelle vous affectez la ressource.

Toutes les nouvelles applications que vous attribuez remplacent toutes les applications de la ressource dérivées d'une autre ressource. Par exemple, les volumes héritent des applications des hôtes. Lorsque de nouvelles applications sont attribuées à un volume, la nouvelle application est prioritaire sur l'application dérivée.

Pour les environnements disposant d'un grand nombre de ressources associées, l'héritage des affectations d'applications peut prendre plusieurs minutes. Veuillez laisser plus de temps à l'héritage si vous disposez de nombreux biens connexes.

Une fois que vous avez terminé

Après avoir affecté l'hôte à l'application, vous pouvez affecter les ressources restantes à l'application. Pour accéder à la page d'accueil de l'application, cliquez sur **gérer > application** et sélectionnez l'application que vous avez créée.

Résolution automatique des périphériques

Présentation de la résolution automatique des périphériques

Vous devez identifier tous les dispositifs que vous souhaitez contrôler avec Data Infrastructure Insights. L'identification est nécessaire pour effectuer un suivi précis des performances et de l'inventaire de votre locataire. Généralement, la majorité des périphériques découverts sur votre locataire sont identifiés par *Automatic Device Resolution*.

Une fois que vous avez configuré des collecteurs de données, les périphériques de votre locataire, y compris les switchs, les baies de stockage et votre infrastructure virtuelle d'hyperviseurs et de VM, sont identifiés. Cependant, cela ne permet généralement pas d'identifier 100 % des périphériques de votre locataire.

Une fois les périphériques de type collecteur de données configurés, il est recommandé d'exploiter les règles de résolution des périphériques pour identifier les périphériques inconnus restants de votre locataire. La résolution de périphérique peut vous aider à résoudre les périphériques inconnus comme étant les types de périphériques suivants :

- Hôtes physiques
- Les baies de stockage
- Les bandes

Les périphériques qui restent inconnus après la résolution du périphérique sont considérés comme des périphériques 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 périphériques ayant des attributs similaires au fur et à mesure qu'ils sont ajoutés à votre environnement. Dans certains cas, la résolution des périphériques permet également une identification manuelle en contournant les règles de résolution des

périphériques pour les périphériques non détectés dans Data Infrastructure Insights.

Une identification incomplète des périphériques peut entraîner des problèmes, notamment :

- Chemins incomplets
- Connexions à chemins d'accès multiples non identifiées
- L'incapacité à regrouper les applications
- Vues topologiques inexactes
- Données inexactes dans l'entrepôt de données et les rapports

La fonction de résolution du périphérique (gérer > résolution du périphérique) inclut les onglets suivants, chacun jouant un rôle dans la planification de la résolution du périphérique et dans l'affichage des résultats :

- **Fibre Channel Identify** contient une liste des WWN et des informations de port des périphériques Fibre Channel qui n'ont pas été résolus par la résolution automatique des périphériques. L'onglet identifie également le pourcentage de périphériques qui ont été identifiés.
- **IP Address Identify** contient une liste de périphériques accédant aux partages CIFS et aux partages NFS qui n'ont pas été identifiés par la résolution automatique des périphériques. L'onglet identifie également le pourcentage de périphériques qui ont été identifiés.
- **Règles de résolution automatique** contient la liste des règles qui sont exécutées lors de l'exécution de la résolution de périphérique Fibre Channel. Il s'agit de règles que vous créez pour résoudre les périphériques Fibre Channel non identifiés.
- **Préférences** fournit des options de configuration que vous utilisez pour personnaliser la résolution de périphérique pour votre environnement.

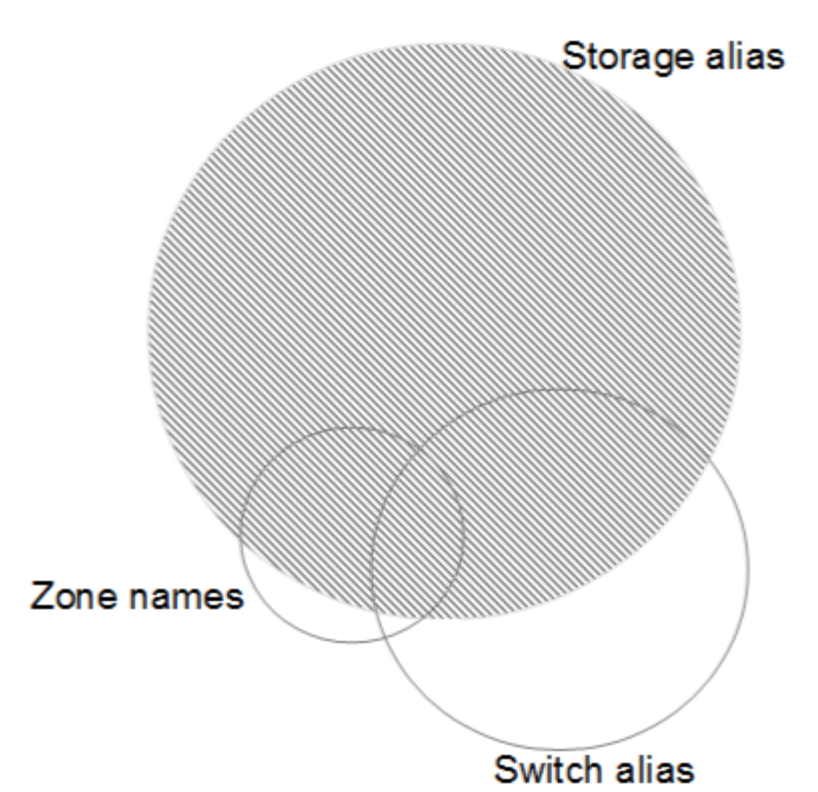
Avant de commencer

Vous devez savoir comment votre environnement est configuré avant de définir les règles d'identification des périphériques. Plus vous en saurez sur votre environnement, plus il sera facile d'identifier les périphériques.

Vous devez répondre à des questions similaires aux suivantes pour vous aider à créer des règles précises :

- Votre environnement respecte-t-il des normes de dénomination pour les zones ou les hôtes, et quel est le pourcentage exact de ces zones ?
- Votre environnement utilise-t-il un alias de commutateur ou un alias de stockage et correspond-il au nom d'hôte ?
- À quelle fréquence les schémas de dénomination changent-ils pour votre locataire ?
- Y a-t-il eu des acquisitions ou des fusions qui ont introduit différents systèmes de dénomination ?

Après l'analyse de votre environnement, vous devriez être en mesure d'identifier les normes de dénomination existantes que vous pouvez vous attendre à des rencontres de fiabilité. Les informations que vous avez rassemblées peuvent être représentées graphiquement dans un chiffre similaire à ce qui suit :



Dans cet exemple, le plus grand nombre de périphériques sont représentés de manière fiable par des alias de stockage. Les règles permettant d'identifier les hôtes utilisant des alias de stockage doivent d'abord être écrites, 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 d'identification des périphériques

En général, vous utilisez un flux de travail similaire à celui ci-dessous pour identifier les périphériques de votre locataire. L'identification est un processus itératif qui peut nécessiter plusieurs étapes de planification et de raffinage des règles.

- Environnement de recherche
- Règles de plan
- Créer/réviser des règles
- Passez en revue les résultats
- Créer des règles supplémentaires ou identifier manuellement les périphériques
- L'a fait

> Si vous avez des périphériques non identifiés (ou des 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 ou comptés comme périphériques génériques.

Relié : "Création de règles de résolution de périphérique" "Résolution de périphérique Fibre Channel" "Résolution de périphérique IP" "Définition des préférences de résolution du périphérique"

Règles de résolution du périphérique

Vous créez des règles de résolution des périphériques 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 dans votre environnement et identifient également les périphériques similaires ajoutés à votre environnement.

Création de règles de résolution de périphérique

Lorsque vous créez des règles, vous commencez par identifier la source des informations sur lesquelles la règle s'exécute, la méthode utilisée pour extraire des informations et si la recherche DNS est appliquée aux résultats de la règle.

Source utilisée pour identifier le périphérique	* 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 qu'il est (extrait un nom d'un SRM) * Delimters * expressions régulières
Recherche DNS	Indique 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 hôte** ou **+ règle 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 pour créer des expressions régulières.

3. Dans la liste **Type**, sélectionnez le périphérique à identifier.

   Vous pouvez sélectionner *Host* ou *Tape*.

4. Dans la liste **Source**, sélectionnez la source à utiliser pour identifier l'hôte.

   Selon la source que vous avez choisie, Data Infrastructure Insights affiche la réponse suivante :

   a. **Zones** répertorie les zones et le WWN devant 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 le 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 à utiliser pour identifier l'hôte.

Source	Méthode
SRM	Tout comme les 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'hôte longs ou plus.

     Pour les règles utilisant des délimitateurs, la chaîne d'entrée est tokenisée par le délimiteur et une liste de candidats de noms d'hôte est créée en faisant plusieurs combinaisons du jeton adjacent. La liste est ensuite triée, la plus grande à la plus petite. Par exemple, pour un sring d'entrée de *vipsnq03_hba3_emc3_12ep0*, la liste se traduit par ce qui suit :

     - 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 sensibilité des cas.
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 des périphériques

Une mise à jour de la résolution du périphérique valide les modifications manuelles qui ont été ajoutées depuis la dernière exécution de la 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 de périphérique. Aucune résolution complète du périphérique n'est exécutée.

Procédure

1. Connectez-vous à l'interface utilisateur Web Data Infrastructure Insights.
2. Cliquez sur **gérer > résolution du périphérique**
3. Dans l'écran **Device Resolution**, cliquez sur la flèche vers le bas du bouton **Run AR**.
4. Cliquez sur **Update** pour lancer la mise à jour.

Identification manuelle assistée par des règles

Cette fonction est utilisée dans des cas particuliers où vous souhaitez exécuter une règle spécifique ou une liste de règles (avec ou sans réorganisation unique) pour résoudre des hôtes inconnus, des périphériques de stockage et de bande.

Avant de commencer

Vous avez un certain nombre de périphériques qui n'ont pas été identifiés et vous disposez également de plusieurs règles qui ont identifié d'autres périphériques avec succès.

> 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 utilisateur Web Data Infrastructure Insights.
2. Cliquez sur **gérer > résolution du périphérique**
3. Cliquez sur l'onglet **Fibre Channel Identify**.

   Le système affiche les périphériques avec leur état de résolution.
4. Sélectionnez plusieurs périphériques non identifiés.
5. Cliquez sur **actions groupées** 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 les périphériques avec succès.
6. Modifiez l'ordre des règles en un ordre qui répond à vos besoins.

   L'ordre des règles est modifié dans l'écran identifier, mais ne sont pas modifiés globalement.
7. Sélectionnez la méthode qui répond à vos besoins.

Data Infrastructure Insights exécute le processus de résolution des hôtes dans l'ordre dans lequel les méthodes apparaissent, en commençant par celles situées en haut.

Lorsque des règles s'appliquent, les noms de règles s'affichent dans la colonne règles et sont identifiés comme étant manuels.

Relié : "Résolution de périphérique Fibre Channel" "Résolution de périphérique IP" "Définition des préférences de résolution du périphérique"

Résolution de 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 la résolution manuelle des périphériques.

Les périphériques qui ont été résolus par résolution manuelle contiennent un état de *OK* et identifient la règle utilisée pour identifier le périphérique. Les périphériques manquants ont le statut *non identifié*. Les appareils qui sont spécifiquement exclus de l'identification ont le statut *excluded*. La couverture totale pour l'identification des périphériques est indiquée sur cette page.

Vous effectuez des actions en bloc en sélectionnant plusieurs périphériques sur le côté gauche de l'écran d'identification Fibre Channel. Vous pouvez effectuer des actions sur un seul périphérique en passant le pointeur de la souris sur un périphérique et en sélectionnant les boutons *Identify* ou *Unidentifier* à l'extrême droite de la liste.

Le lien *Total Coverage* affiche la liste du nombre de périphériques identifiés/nombre de périphériques 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 fonction *Manual Add* disponible dans l'onglet Device Resolution Fibre Channel Identify. Ce processus peut être utilisé pour la pré-identification d'un périphérique qui devrait être découvert à l'avenir.

Avant de commencer

Pour ajouter une identification de périphérique au système, vous devez connaître l'adresse WWN ou IP et le nom du périphérique.

Description de la tâche

Vous pouvez ajouter manuellement un hôte, un périphérique de stockage, une bande ou un périphérique Fibre Channel inconnu.

Procédure

1. Connectez-vous à l'interface utilisateur Web Data Infrastructure Insights
2. Cliquez sur **gérer > résolution du périphérique**
3. Cliquez sur l'onglet **Fibre Channel Identify**.
4. Cliquez sur le bouton **Ajouter**.

   La boîte de dialogue **Ajouter un périphérique** s'affiche

5. Entrez le WWN ou l'adresse IP, le nom du périphérique et sélectionnez le type de périphérique.

   Le périphérique que vous entrez est ajouté à la liste des périphériques dans l'onglet Fibre Channel Identify. La règle est identifiée comme *Manual*.

Importation de l'identification du périphérique Fibre Channel à partir d'un fichier .CSV

Vous pouvez importer manuellement l'identification des périphériques Fibre Channel dans la résolution des périphériques 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 importer des identifications de périphérique directement dans la résolution du périphérique. Le fichier .CSV pour les périphériques Fibre Channel requiert les informations suivantes :

WWN	IP	Nom	Type

Les champs de données doivent être entre guillemets, comme illustré 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"
```

Dans le cadre des meilleures pratiques, il est recommandé d'exporter d'abord les informations d'identification Fibre Channel vers un fichier .CSV, de procéder aux modifications souhaitées dans ce fichier, puis de réimporter le fichier dans Fibre Channel identifient. Cela permet de s'assurer que les colonnes attendues sont présentes et dans le bon ordre.

Pour importer les informations d'identification de Fibre Channel :

1. Connectez-vous à l'interface utilisateur Web Data Infrastructure Insights.
2. Cliquez sur **gérer > résolution du périphérique**
3. Sélectionnez l'onglet **Fibre Channel Identify**.
4. Cliquez sur le bouton **identifier > identifier à partir du fichier**.
5. Naviguez jusqu'au dossier contenant vos fichiers .CSV pour les importer et sélectionnez le fichier souhaité.

   Les périphériques que vous entrez sont ajoutés à la liste des périphériques dans l'onglet Fibre Channel Identify. La « règle » est identifiée comme Manuel.

Exportation des identifications de périphérique Fibre Channel vers un fichier .CSV

Vous pouvez exporter les identifications de périphériques Fibre Channel existantes vers un fichier .CSV à partir de la fonction de résolution de périphériques Data Infrastructure Insights. Vous pouvez exporter une identification de périphérique pour la modifier, puis l'importer à nouveau dans Data Infrastructure Insights, où elle est ensuite utilisée pour identifier les périphériques similaires à ceux qui correspondent à l'origine à l'identification exportée.

Description de la tâche

Ce scénario peut être utilisé lorsque les périphériques ont des attributs similaires qui peuvent être facilement modifiés dans le fichier .CSV, puis importés à nouveau dans le système.

Lorsque vous exportez une identification de périphérique Fibre Channel dans un fichier .CSV, le fichier contient

les informations suivantes dans l'ordre indiqué :

WWN	IP	Nom	Type

Procédure

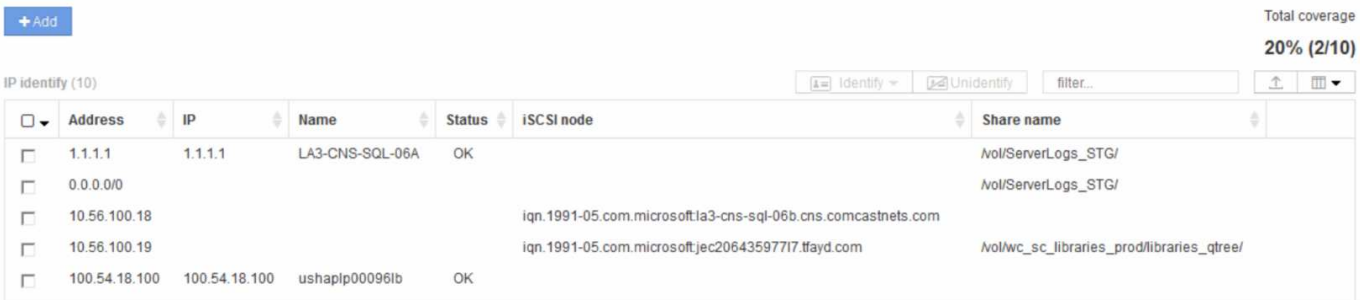
1. Connectez-vous à l'interface utilisateur Web Data Infrastructure Insights.
2. Cliquez sur **gérer > résolution du périphérique**
3. Sélectionnez l'onglet **Fibre Channel Identify**.
4. Sélectionnez le ou les périphériques Fibre Channel dont vous souhaitez exporter l'identification.
5. Cliquez sur le bouton *Exporter* .

   Indiquez si vous souhaitez ouvrir le fichier .CSV ou enregistrer le fichier.

Relié : "Résolution de périphérique IP" "Création de règles de résolution de périphérique" "Définition des préférences de résolution du périphérique"

Résolution du périphérique IP

L'écran IP Identify affiche tous les partages iSCSI et CIFS ou NFS identifiés par la résolution automatique du périphérique ou par la résolution manuelle des périphériques. Les périphériques non identifiés sont également affichés. L'écran comprend l'adresse IP, le nom, l'état, le nœud iSCSI et le nom de partage des périphériques. Le pourcentage de périphériques 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 IP Identify.

Procédure

1. Connectez-vous à l'interface utilisateur Web Data Infrastructure Insights.
2. Cliquez sur **gérer > résolution du périphérique**
3. Cliquez sur l'onglet **IP Address Identify**.
4. Cliquez sur le bouton **Ajouter**.

   La boîte de dialogue Ajouter un périphérique s'affiche

5. Entrez l'adresse, l'adresse IP et un nom de périphérique unique.

Résultat

Le périphérique que vous entrez est ajouté à la liste des périphériques dans l'onglet IP Address Identify (identification de l'adresse IP).

Importation de l'identification du périphérique IP à partir d'un fichier .CSV

Vous pouvez importer manuellement des identifications de périphérique IP dans la fonction résolution de périphérique à l'aide d'une liste d'identifications de périphérique dans un fichier .CSV.

1. Avant de commencer

Vous devez disposer d'un fichier .CSV correctement formaté pour importer des identifications de périphérique directement dans la fonction résolution de périphérique. Le fichier .CSV pour les périphériques IP requiert les informations suivantes :

Adresse	IP	Nom

Les champs de données doivent être entre guillemets, comme illustré dans l'exemple ci-dessous.

```
"Address","IP","Name"
"ADDRESS6447","IP6447","NAME-6447"
"ADDRESS3211","IP3211","NAME-3211"
"ADDRESS593","IP593","NAME-593"
```

Il est recommandé d'exporter d'abord les informations d'identification de l'adresse IP dans un fichier .CSV, d'effectuer les modifications souhaitées dans ce fichier, puis de réimporter le fichier dans IP Address identifier. Cela permet de s'assurer 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 des identifications de périphériques IP existants vers un fichier .CSV à partir de la fonction de résolution de périphériques Data Infrastructure Insights. Vous pouvez exporter une identification de périphérique pour la modifier, puis l'importer à nouveau dans Data Infrastructure Insights, où elle est ensuite utilisée pour identifier les périphériques similaires à ceux qui correspondent à l'origine à l'identification exportée.

Description de la tâche

1. Ce scénario peut être utilisé lorsque les périphériques ont des attributs similaires qui peuvent être facilement modifiés dans le fichier .CSV, puis importés à nouveau dans le système.

Lorsque vous exportez une identification de périphérique IP dans un fichier .CSV, le fichier contient les informations suivantes dans l'ordre indiqué :

Adresse	IP	Nom

Procédure

1. Connectez-vous à l'interface utilisateur Web Data Infrastructure Insights.
2. Cliquez sur **gérer > résolution du périphérique**

3. Sélectionnez l'onglet **IP Address Identify**.
4. Sélectionnez le ou les périphériques IP dont vous souhaitez exporter l'identification.
5. Cliquez sur le bouton *Exporter* .

   Indiquez si vous souhaitez ouvrir le fichier .CSV ou enregistrer le fichier.

Relié : "Résolution de périphérique Fibre Channel" "Création de règles de résolution de périphérique" "Définition des préférences de résolution du périphérique"

Configuration des options dans l'onglet Préférences

L'onglet Préférences de résolution du périphérique permet de créer un programme de résolution automatique, de spécifier des venders de stockage et de bande à inclure ou exclure de l'identification, et de définir des options de recherche DNS.

Planning de résolution automatique

Un planning de résolution automatique peut indiquer quand la résolution automatique du périphérique est exécutée :

Option	Description
Toutes les	Utilisez cette option pour exécuter la résolution automatique des périphériques aux intervalles de jours, heures ou minutes.
Tous les jours	Utilisez cette option pour exécuter la résolution automatique du périphérique tous les jours à une heure donnée.
Manuellement	Utilisez cette option pour exécuter uniquement la résolution automatique des périphériques manuellement.
Sur chaque changement d'environnement	Utilisez cette option pour exécuter la résolution automatique des périphériques lorsqu'un changement d'environnement est apporté.

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 fonctions 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 adresses IP : pour activer la résolution automatique des hôtes pour les initiateurs et les hôtes iSCSI qui accèdent aux partages NFS à l'aide de la recherche DNS. Si ce n'est pas spécifié, seule la résolution FC est effectuée.
- Vous pouvez choisir d'autoriser des traits de soulignement dans les noms d'hôte et d'utiliser un alias « connecté à » au lieu de l'alias de port standard dans les résultats.

Y compris les fournisseurs spécifiques de systèmes de stockage et de bandes, ou l'exclusion de ces fournisseurs

Vous pouvez inclure ou exclure certains fournisseurs de stockage et de bandes pour la résolution automatique. Vous pouvez exclure des fournisseurs spécifiques si vous savez, par exemple, qu'un hôte spécifique deviendra un hôte hérité et qu'il doit être exclu de votre nouvel environnement. Vous pouvez également réajouter des fournisseurs que vous avez précédemment exclus mais qui ne souhaitez plus exclure.

> Les règles de résolution des périphériques pour bande ne fonctionnent que pour les WWN où le fournisseur pour ce WWN est défini sur *inclus comme bande uniquement* dans les préférences des fournisseurs.

Voir aussi : "Exemples d'expression régulière"

Exemples d'expression régulière

Si vous avez sélectionné l'approche expression régulière comme stratégie de nommage 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

Lorsque vous créez des expressions régulières pour la résolution automatique de Data Infrastructure Insights, vous pouvez configurer le format de sortie en entrant 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. Le 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 d'appellation 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
```

La sortie peut être au format suivant :

```
 [hostname]-[data center]-[device type]
Pour ce faire, vous devez capturer les champs de nom d'hôte, de centre de
données et de type de périphérique dans les variables et les utiliser dans
la sortie. L'expression régulière suivante ferait ceci :
```

```
 .*?_([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 les sorties au format de votre choix :

```
 \2-\1-\3
Votre résultat sera le suivant :
```

```
hostname1-Miami-filer
hostname2-Tampa-switch
hostname3-Boston-windows2K
hostname4-Raleigh-solaris
```

Les tirets entre les variables fournissent un exemple de texte constant 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 pouvez utiliser pour capturer le nom d'hôte est :

```
 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 d'une combinaison de chiffres , suivie d'un trait de
soulignement, du nom d'hôte alphanumérique (myComputer1Name), d'un trait
de soulignement ou d'un tiret, des lettres en majuscule HBA et d'un seul
chiffre (0-9). Le nom d'hôte seul est stocké dans la variable *\1*.
```

L'expression régulière peut être divisée en ses composants :

- "S" représente le nom de la zone et commence l'expression. Ceci 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.
- Le signe + indique que l'occurrence des informations entre crochets précédents doit exister 1 fois ou plus.

- Le _ (trait de soulignement) signifie que les chiffres après S doivent être suivis immédiatement par un caractère de soulignement dans le nom de 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 motif contenu dans sera stocké dans la variable \1.
- Les caractères entre crochets [a-ZA-Z0-9] indiquent que les caractères correspondants sont tous des lettres (indépendamment du cas) et des chiffres.
- Le * (astérisque) suivant les crochets indique que les caractères entre crochets se produisent 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 se produire dans le nom de la zone.
- Le jeu final de caractères entre parenthèses [0-9] correspond à un chiffre unique de 0 à 9 inclus.

Exemple 2

Dans cet exemple, passez au premier trait de soulignement "*", puis faites correspondre E et tout ce qui suit jusqu'au second "*", puis sautez tout après cela.

ZONE: Z_E2FHDBS01_E1NETAPP

NOM D'HÔTE: E2FHDBS01

RegExp: .***?(E.?)**.*?

Exemple 3

Les parenthèses "( )" autour de la dernière section de l'expression régulière (ci-dessous) identifie la partie qui est le nom d'hôte. Si vous souhaitez que VSAN3 soit le nom d'hôte, il s'agit de : _([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 :

- MyComputerName123-HBA1_Symm1_FA3
- MyComputerName123-HBA2_Symm1_FA5
- MyComputerName123-HBA3_Symm1_FA7

L'expression régulière que vous pouvez utiliser pour capturer ces expressions est :

```
 ([a-zA-Z0-9]*)_.*
La variable \1 ne contiendra que _myComputerName123_ après avoir été
évaluée par cette expression.
```

L'expression régulière peut être divisée en ses composants :

- Les parenthèses indiquent que le motif contenu dans sera stocké dans la variable \1.
- Les caractères entre crochets [a-ZA-Z0-9] signifient que toute lettre (quel que soit le cas) ou tout chiffre correspond.
- Le * (astérisque) suivant les crochets indique que les caractères entre crochets se produisent 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 qui correspond aux crochets précédents.
- Le . (point) correspond à n'importe quel caractère (caractère générique).
- L'astérisque (*) indique que le caractère générique de la période précédente peut se produire 0 fois ou plus.

  En d'autres termes, la combinaison .* indique n'importe quel caractère, n'importe quel nombre de fois.

Exemple 5 montrant les noms de zone sans motif

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 pouvez utiliser pour capturer ces expressions est :

```
 (.*?)_.*
La variable \1 contiendra _myComputerName_ (dans le premier exemple de nom
de zone) ou _myComputerName123_ (dans le second exemple de nom de zone).
Cette expression régulière correspond donc à tout ce qui précède le
premier trait de soulignement.
```

L'expression régulière peut être divisée en ses composants :

- Les parenthèses indiquent que le motif contenu dans sera stocké dans la variable \1.
- Le .* (astérisque de point) correspondent à n'importe quel caractère, à n'importe quel nombre de fois.
- Le * (astérisque) suivant les crochets indique que les caractères entre crochets se produisent 0 fois ou plus.
- Le caractère ? rend le match non-avide. Cela la force 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 les noms d'ordinateur avec un motif

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 pouvez utiliser pour capturer ces expressions est :

```
 .*?_.*?_([a-zA-Z0-9]*[ABT])_.*
Comme la convention de nom de zone comporte davantage de motifs, nous
pouvons utiliser l'expression ci-dessus, qui correspond 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 divisée en ses composants :

- Le .* (astérisque de point) correspondent à n'importe quel caractère, à n'importe quel nombre de fois.
- Le caractère ? rend le match non-avide. Cela la force 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 l'exemple de nom de première zone.
- La seconde combinaison .*?_ se comporte comme la première, mais correspond à Switch1_ dans l'exemple de nom de première zone.
- Les parenthèses indiquent que le motif contenu dans sera stocké dans la variable \1.
- Les caractères entre crochets [a-ZA-Z0-9] signifient que toute lettre (quel que soit le cas) ou tout chiffre correspond.
- Le * (astérisque) suivant les crochets indique que les caractères entre crochets se produisent 0 fois ou plus.
- Les caractères entre crochets dans l'expression régulière [ABT] correspondent à un seul caractère dans le nom de zone qui doit être A, B ou T.
- Le symbole _ (trait de soulignement) suivant les parenthèses indique que la correspondance [ABT] doit être suivie d'un trait de soulignement.
- Le .* (astérisque de point) correspondent à n'importe quel caractère, à n'importe quel nombre de fois.

Par conséquent, la variable \1 contient toute chaîne alphanumérique qui :

- a été précédé d'un certain nombre de caractères alphanumériques et de deux traits de soulignement
- a été suivi d'un trait de soulignement (puis d'un nombre quelconque de caractères alphanumériques)
- Avait un caractère final de A, B ou T, avant le troisième trait de soulignement.

Exemple 7

Zone: myComputerName123_HBA1_Symm1_FA1

NOM D'HÔTE: myComputerName123

RegExp: ([a-ZA-Z0-9]+).*

Exemple 8

Cet exemple trouve tout avant le premier _.

Zone : MyComputerName_HBA1_Symm1_FA1

MyComputerName123_HBA1_Symm1_FA1

Nom d'hôte : MyComputerName

Regexp: (.**?)_.**

Exemple 9

Cet exemple trouve tout après le 1er _ et jusqu'au second _.

Zone: Z_MyComputerName_StorageName

Nom d'hôte: MyComputerName

RegExp: .**?*(.?)***.*?

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 ^ (circumflex ou caret) **à l'intérieur des crochets** nient l'expression, par exemple, [^FF] signifie tout sauf majuscules ou minuscules F, et [^a-z] signifie tout sauf la minuscule a à z, et dans le cas ci-dessus, tout sauf le

_. L’instruction format ajoute dans le "-" au nom d’hôte de sortie.

Zone: mhs_apps44_d_A_10a0_0429

Nom d’hôte: mhs-apps44-d

RegExp: ()_([AB]).*format dans les informations de l'infrastructure de données : \1-\2 ([^_])_ ()_([^_]).*format dans les informations de l’infrastructure de données : \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 en fait "\" utilisé dans la chaîne, et que ceux-ci 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

RegExp: -(.*-\d).*

Exemple 15

Le paramètre de format dans ce cas ajoute le paramètre « US-BV- » au nom d’hôte.

ZONE: SRV_USBVM11_F1

NOM D’HÔTE: US-BV-M11

RegExp: SRV_USBV([A-Za-z0-9]+)_F[12]

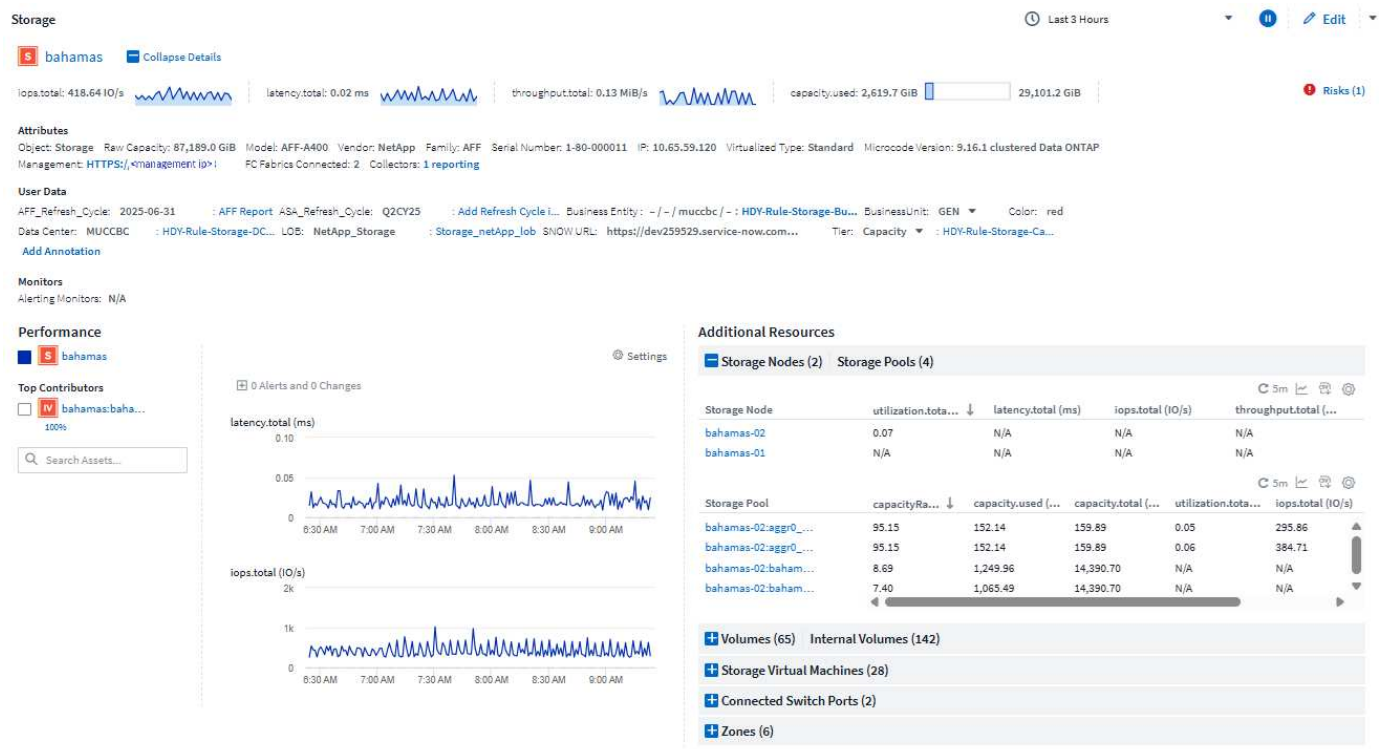
Format: US-BV-\1

Informations sur la page de ressources

Présentation de la page de ressources

Les pages d’accueil des ressources résument l’état actuel d’une ressource et contiennent des liens vers des informations supplémentaires sur la ressource et ses ressources associées.

Les pages d’accueil vous donnent une vue d’une page de l’objet, avec des informations de résumé, de performances et de ressources associées.



Résumé

En haut d'une page d'accueil se trouve la section Synthèse expansible, qui inclut plusieurs graphiques sparkline affichant des tendances de données récentes pour des éléments tels que le débit ou la latence, ainsi que des informations et des attributs d'objet, et tous les moniteurs susceptibles d'alerter l'objet.

La section Résumé s'affiche également et vous permet de modifier les annotations affectées à la ressource.

Section performances

La section Performance affiche les données de performances de l'objet. Sélectionnez *Settings* pour ajouter des graphiques supplémentaires à l'affichage, tels que débit ou capacité, ou sélectionnez des ressources corrélées ou contribuant pour tracer leurs données avec celles de l'objet. Les périphériques susceptibles de provoquer des conflits sont également répertoriés dans la section performances. Les données des graphiques sont actualisées automatiquement lorsque les collecteurs de données interrogent et que les données mises à jour sont acquises.

Vous pouvez sélectionner le metrics que vous souhaitez afficher dans le graphique de performances pour la période sélectionnée. Cliquez sur le menu déroulant *Settings* et choisissez parmi les mesures répertoriées.

Outre les données de performances, toutes les alertes qui sont ou étaient actives dans la plage horaire de page sélectionnée s'affichent également.



Vous pouvez choisir parmi les périphériques suivants qui peuvent être répertoriés dans la section performances :

- Meilleure corrélation

  Indique les ressources dont la corrélation est élevée (pourcentage) avec un ou plusieurs metrics de performance à l'ressource de base.

- Principaux contributeurs

  Affiche les actifs qui contribuent (pourcentage) à l'actif de base.

- Top change

  Ressources liées aux modifications récentes.

- Contentions de charge de travail

  Indique les ressources qui affectent ou sont affectées par d'autres ressources partagées, telles que les hôtes, les réseaux et le stockage. Ces ressources sont parfois appelées *greedy* et *dégraded*.

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 tables afin de vous concentrer sur des ressources spécifiques. Sélectionnez l'icône en forme 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 de ressources. Les widgets que vous ajoutez apparaîtront sur les pages de contenu pour tous les objets de ce type. Par exemple, l'ajout d'un widget personnalisé à une page d'actifs de stockage affichera ce widget sur les pages d'actifs de toutes les

ressources de stockage.

Les widgets personnalisés sont placés au bas d'une page d'accueil, sous les sections performances et ressources.

Types de pages de biens

Data Infrastructure Insights fournit des pages de ressources pour les ressources suivantes :

- Ordinateur virtuel
- Storage Virtual machine (SVM)
- Volumétrie
- Volume interne
- Hôte (hyperviseur compris)
- Pool de stockage
- Stockage
- Datastore
- Client supplémentaire
- Nœud de stockage
- Qtree
- Disque
- VMDK
- Port
- Commutateur
- Structure
- Hôte
- Zone

Modification de la plage horaire des données affichées

Par défaut, une page d'inventaire affiche les 3 dernières heures de données. Cependant, vous pouvez modifier le segment de temps des données affichées à l'aide d'une option située sur chaque page d'inventaire, 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 de temps suivants :

- Dernières 15 minutes
- Dernières 30 minutes
- Dernières 60 minutes
- Dernières 2 heures
- Les 3 dernières heures (il s'agit de la valeur par défaut)
- Dernières 6 heures
- Dernières 12 heures
- Dernières 24 heures

- 2 derniers jours
- 3 derniers jours
- 7 derniers jours
- 14 derniers jours
- 30 derniers jours
- Plage horaire personnalisée

La plage de temps 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 12:00 AM le premier jour sélectionné et l'heure de fin par défaut est 11:59 PM le dernier jour sélectionné. Cliquez sur appliquer pour appliquer la plage horaire personnalisée à la page ressource.

Les informations de la page sont automatiquement actualisées en fonction de la plage horaire sélectionnée. La fréquence de rafraîchissement actuelle s'affiche dans le coin supérieur droit de la section Résumé, ainsi que dans 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 mesure est affichée dans son propre graphique de performances. Vous pouvez ajouter ou supprimer des mesures et des ressources associées dans les graphiques en fonction des données que vous souhaitez voir ; les mesures que vous pouvez choisir varient en fonction du type d'actif.

Métrique	Description
BB crédit zéro Rx, Tx	Nombre de fois que le nombre de crédits de la mémoire tampon de réception/transmission est passé à zéro pendant la période d'échantillonnage. Cette mesure représente le nombre de fois que le port connecté a dû cesser de transmettre car ce port était en dehors des crédits à fournir.
BB crédit zéro durée Tx	Temps en millisecondes pendant lequel le crédit BB de transmission était égal à zéro pendant l'intervalle d'échantillonnage.
Taux d'accès au cache (total, lecture, écriture) %	Pourcentage de demandes ayant des résultats dans le cache. Plus le nombre d'accès au volume est élevé, plus les performances sont élevées. Cette colonne est vide pour les matrices de stockage qui ne collectent pas les informations d'accès au cache.
Utilisation du cache (total) %	Pourcentage total de demandes de cache qui entraînent des taux d'accès au cache
Discards de classe 3	Nombre de cartes de transport de données Fibre Channel classe 3.
Taux d'utilisation du processeur (total) %	Quantité de ressources CPU utilisées activement, en pourcentage du total disponible (sur l'ensemble des processeurs virtuels).

Erreur CRC	Nombre d’images avec vérifications cycliques de redondance non valides (CRCS) détectées par le port pendant la période d’échantillonnage
Fréquence d’image	Vitesse d’image de transmission en images par seconde (FPS)
Taille moyenne des trames (Rx, Tx)	Rapport entre le trafic et la taille de la trame. Cette mesure vous permet de déterminer s’il existe des cadres en hauteur dans le tissu.
Taille du châssis 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 des E/S (Total, lecture, écriture)	Nombre d’IOPS divisé par la capacité utilisée (tel qu’acquise lors de l’enquête d’inventaire la plus récente de la source de données) pour le volume, le volume interne ou l’élément de stockage. Mesures réalisées en nombre d’opérations d’E/S par seconde et par To.
IOPS (total, lecture, écriture)	Nombre de demandes de service d’E/S en lecture/écriture qui passent 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 : taux agrégé auquel les données IP ont été transmises et reçues en mégaoctets par seconde.
Débit IP (réception) :	Taux moyen de réception des données IP en mégaoctets par seconde.
Écriture : débit IP (transmission) :	Vitesse moyenne à laquelle les données IP ont été transmises en mégaoctets par seconde.
Latence (total, lecture, écriture)	Latence (R&W) : vitesse à laquelle les données sont lues ou écrites sur les machines virtuelles dans un délai fixe. La valeur est mesurée en mégaoctets par seconde.
Latence :	Temps de réponse moyen provenant des ordinateurs virtuels dans un magasin de données.
Latence principale :	Le temps de réponse le plus élevé des ordinateurs virtuels dans un datastore.
Échec de la liaison	Nombre d’échecs de liaison détectés par le port pendant la période d’échantillonnage.
Link reset Rx, Tx	Nombre de réinitialisations de liaison de réception ou de transmission pendant la période d’échantillonnage. Cette mesure représente le nombre de réinitialisations de liaison émises par le port connecté à ce port.
Utilisation de la mémoire (totale) %	Seuil de mémoire utilisé par l’hôte.

R/W partiel (total) %	Nombre total de fois qu'une opération de lecture/écriture franchit une limite de bande sur un module de disque dans un LUN RAID 5, RAID 1/0 ou RAID 0 en général, les croisements de bandes ne sont pas bénéfiques, car chacun nécessite une E/S supplémentaire Un pourcentage faible indique une taille d'élément de bande efficace et indique un alignement incorrect d'un volume (ou d'une 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/période donnée.
Décompte des 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 il existe un problème physique.
Taux de swap (taux total, taux d'entrée, taux de sortie)	Vitesse à laquelle la mémoire est échangée en entrée, en sortie ou les deux du disque vers la mémoire active pendant la période d'échantillonnage. Ce compteur s'applique aux machines virtuelles.
Synchroniser le nombre de pertes	Nombre d'erreurs de perte de synchronisation. Si une erreur de perte de synchronisation se produit, le matériel ne peut pas détecter le trafic ou le verrouiller. Il est possible que tous les équipements n'utilisent pas le même débit de données, ou que les câbles optiques ou les connexions physiques soient de mauvaise qualité. Le port doit resynchroniser après chaque erreur, ce qui a un impact sur la performance du système. Mesurée en Ko/s.
Débit (total, lecture, écriture)	Vitesse à laquelle les données sont transmises, reçues ou les deux en un temps fixe en réponse aux demandes de service d'E/S (mesurée en Mo par seconde).
Délai d'expiration des trames - Tx	Nombre de trames de transmission rejetées causées par le délai d'attente.
Débit de trafic (total, lecture, écriture)	Trafic transmis, reçu ou les deux reçu 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 de réception/transmission/totale pendant la période d'échantillonnage.
Taux d'utilisation (total, 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'écriture d'E/S en attente.

Filtrage des objets dans le contexte

Lors de la configuration d'un widget sur la page d'accueil d'une ressource, vous pouvez définir des filtres *dans-contexte* pour afficher uniquement les objets directement liés à l'actif actuel. Par défaut, lorsque vous ajoutez un widget, les objets *all* du type sélectionné sur votre locataire s'affichent. Les filtres dans le contexte vous permettent d'afficher uniquement les données pertinentes pour votre ressource actuelle.

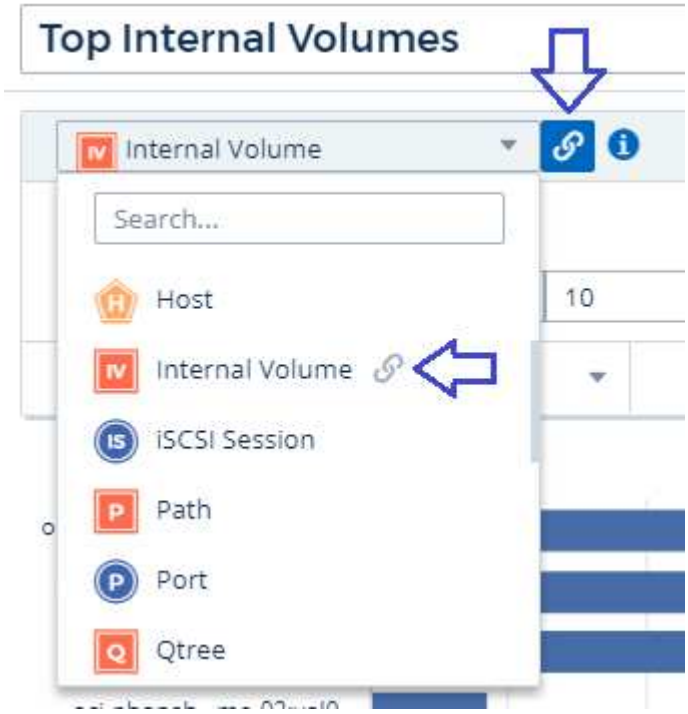
Sur la plupart des pages d'accueil des ressources, les widgets vous permettent de filtrer les objets associés à la ressource actuelle. Dans les listes déroulantes de filtres, les types d'objets qui affichent une icône de lien peuvent être filtrés dans le contexte de l'actif actuel.

Par exemple, sur une page Storage Asset, vous pouvez ajouter un widget Bar Chart pour afficher les IOPS les plus élevées sur les volumes internes uniquement sur ce stockage. Par défaut, lorsque vous ajoutez un widget, *all* volumes internes sur votre tenant s'affichent.

Pour afficher uniquement les volumes internes de l'actif de stockage actuel, procédez comme suit :

Étapes

1. Ouvrez une page de ressources pour toute ressource **Storage**.
2. Cliquez sur **Modifier** pour ouvrir la page de ressources en mode Édition.
3. Cliquez sur **Ajouter un widget** et sélectionnez *BarBar Chart*.
4. Sélectionnez **Volume interne** pour le type d'objet à afficher dans le graphique à barres. Notez que le type d'objet de volume interne est associé à une icône de lien. L'icône « lié » est activée par défaut.



5. Choisissez *IOPS - Total* et définissez les filtres supplémentaires que vous souhaitez.
6. Réduisez le champ **remonter** en cliquant sur [X] en regard de celui-ci. Le champ **Afficher** s'affiche.
7. Choisissez d'afficher le Top 10.

8. Enregistrez le widget.

   Le graphique à barres indique uniquement les volumes internes résidant sur l'actif de stockage actuel.

Le widget s'affiche sur les pages d'actifs de tous les objets de stockage. Lorsque le lien In-context est activé dans le widget, le graphique à barres affiche les données des volumes internes liés uniquement à l'actif de stockage actuellement affiché.

Pour dissocier les données de l'objet, modifiez le widget et cliquez sur l'icône de lien en regard du type d'objet. Le lien devient désactivé et le graphique affiche les données de *tous* objets sur votre locataire.

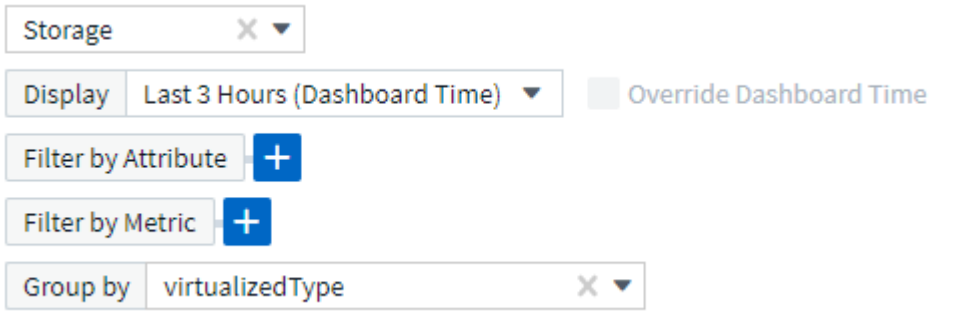
Vous pouvez également utiliser **"variables spéciales dans les widgets"** pour afficher les informations relatives aux ressources sur les pages d'accueil.

Virtualisation du stockage

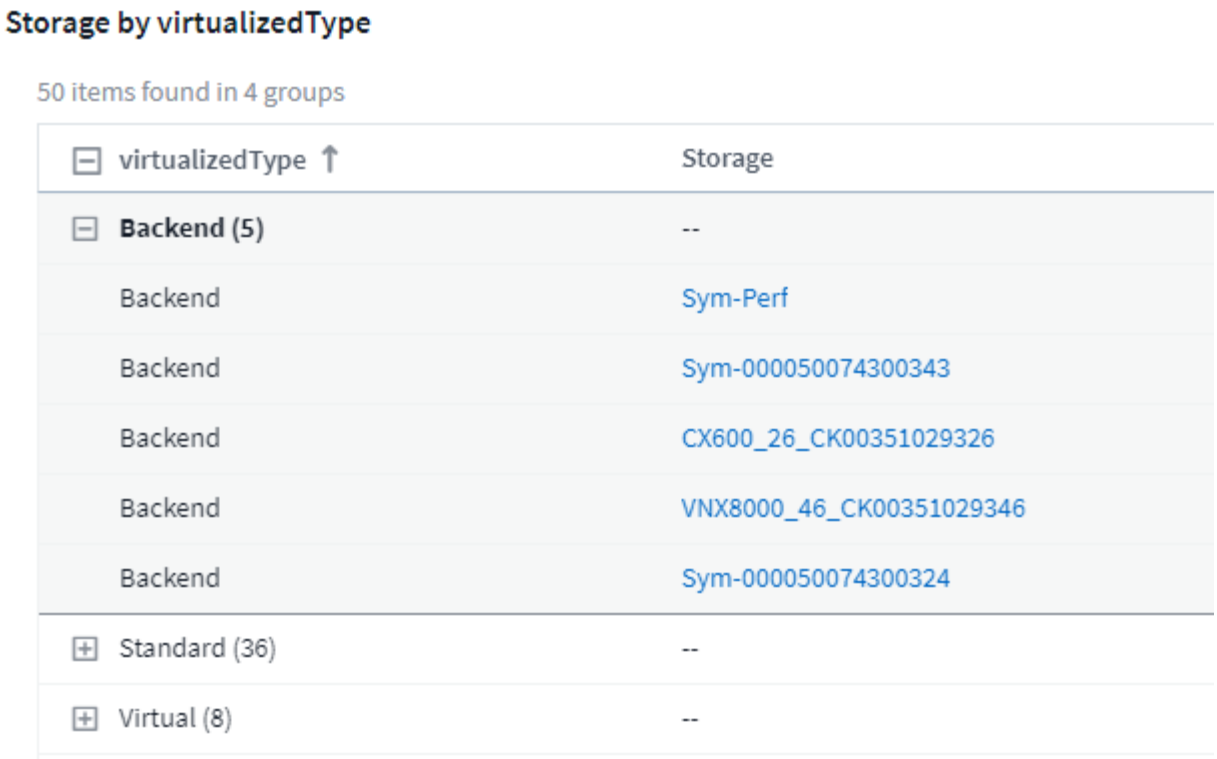
Les informations d'infrastructure de données permettent de différencier une baie de stockage dotée d'un stockage local ou de la virtualisation d'autres baies de stockage. Vous pouvez ainsi établir le lien entre les coûts et distinguer les performances du stockage frontal et du stockage interne de votre infrastructure.

Virtualisation dans un widget Table

L'un des moyens les plus simples de commencer à examiner votre virtualisation du stockage est de créer un widget de tableau de bord montrant le type virtualisé. Lors de la création de la requête pour le widget, ajoutez simplement "virtualizedType" à votre groupement ou filtre.

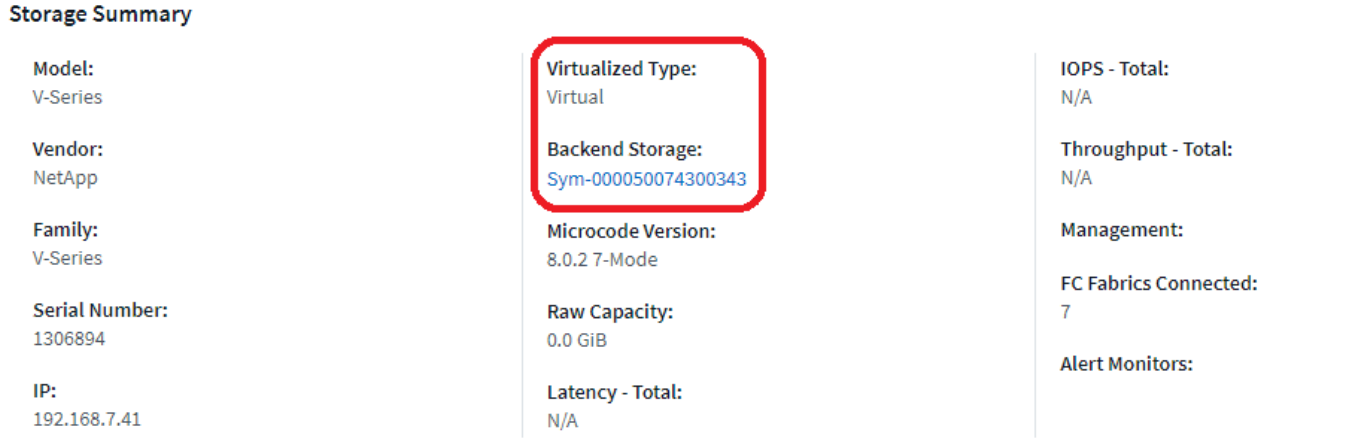


Le widget de table qui en résulte affiche les stockages *Standard*, *Backend* et *Virtual* de votre locataire.



Les pages d'accueil affichent des informations virtualisées

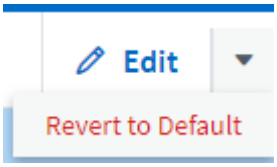
Sur une page de stockage, de volume, de volume interne ou de disque, vous pouvez consulter les informations pertinentes sur la virtualisation. Par exemple, sur la page d'accueil du stockage ci-dessous, vous pouvez voir qu'il s'agit d'un stockage virtuel et quel système de stockage back-end s'applique. Tous les tableaux pertinents figurant sur les pages d'accueil indiqueront également des informations sur la virtualisation, le cas échéant.



Pages d'accueil et tableaux de bord existants

Sachez que si vous disposez actuellement de pages d'accueil 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 à la valeur par défaut* tout tableau de bord ou page d'accueil personnalisé (vous devrez à nouveau mettre en œuvre vos personnalisations), ou modifier les widgets pertinents pour inclure les attributs ou mesures de virtualisation souhaités.

Rétablir par défaut est disponible dans le coin supérieur droit d'un tableau de bord personnalisé ou d'un écran de page d'accueil.



Conseils et astuces pour rechercher des ressources et des alertes

Plusieurs techniques de recherche peuvent être utilisées pour rechercher des données ou des objets dans votre environnement surveillé.

- **Recherche de caractères génériques**

  Vous pouvez effectuer une recherche par caractère générique à l'aide du caractère *. Par exemple, *applic*n* renverra *application*.

- **Phrases utilisées dans la recherche**

  Une expression est un groupe de mots entouré de guillemets, par exemple "VNX LUN 5". Vous pouvez utiliser des guillemets doubles pour rechercher des documents contenant des espaces dans leurs noms ou attributs.

- **Opérateurs booléens**

  En utilisant des 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 OR est utilisé.

  L'opérateur OR lie deux termes et trouve un document correspondant si l'un des termes existe dans un document.

  Par exemple, *stockage OU netapp* recherche des documents contenant *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, *stockage ET netapp* recherchent des documents contenant à la fois *stockage* et *netapp*.

  Vous pouvez utiliser le symbole **&&&&** au lieu du mot ET.

  PAS

  Lorsque vous utilisez L'opérateur NOT, tous les documents contenant le terme après NE sont pas exclus des résultats de la recherche. Par exemple, *stockage ET NON netapp* recherche des documents qui ne

contiennent que *Storage* et non *netapp*.

Vous pouvez utiliser le symbole **!** au lieu du mot NON.

La recherche n’est pas sensible à la casse.

Recherche à l’aide de termes indexés

Les recherches qui correspondent à davantage de termes indexés entraînent des scores plus élevés.

La chaîne de recherche est divisée en termes de recherche séparés par espace. Par exemple, la chaîne de recherche « stockage aurora netapp » est divisée en trois mots clés : « stockage », « aurora » et « netapp ». La recherche s’effectue à l’aide des trois termes. Les documents qui correspondent à la plupart de ces termes auront le score le plus élevé. Plus vous fournissez d’informations, mieux les résultats de recherche sont nombreux. Par exemple, vous pouvez rechercher un stockage par son nom et son modèle.

L’interface utilisateur affiche les résultats de la recherche dans les différentes catégories, avec les trois meilleurs résultats par catégorie. Si vous n’avez pas trouvé d’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 du fournisseur de noms « stockage »
Poolde stockage	Nom du nom « storagepool » des adresses IP de stockage du numéro de série du stockage du fournisseur de stockage pour tous les noms de volumes internes associés pour tous les disques associés
Volume interne	Nom interne du nom des adresses IP de stockage du numéro de série de stockage du fournisseur de stockage du nom de modèle de stockage du pool de stockage de tous les partages associés de toutes les applications associées
Volumétrie	Noms d’étiquette de nom « volume » de tous les volumes internes nom du pool de stockage nom des adresses IP de stockage du numéro de série de stockage du modèle de stockage du fournisseur de stockage
Nœud de stockage	Nom de « storagenode » des adresses IP de stockage du numéro de série de stockage du modèle de stockage du fournisseur
Hôte	Nom « hôte » adresses IP noms de toutes les applications associées
Datastore	Nom du « datastore » : noms IP du centre virtuel de tous les volumes, noms de tous les volumes, de tous les volumes internes

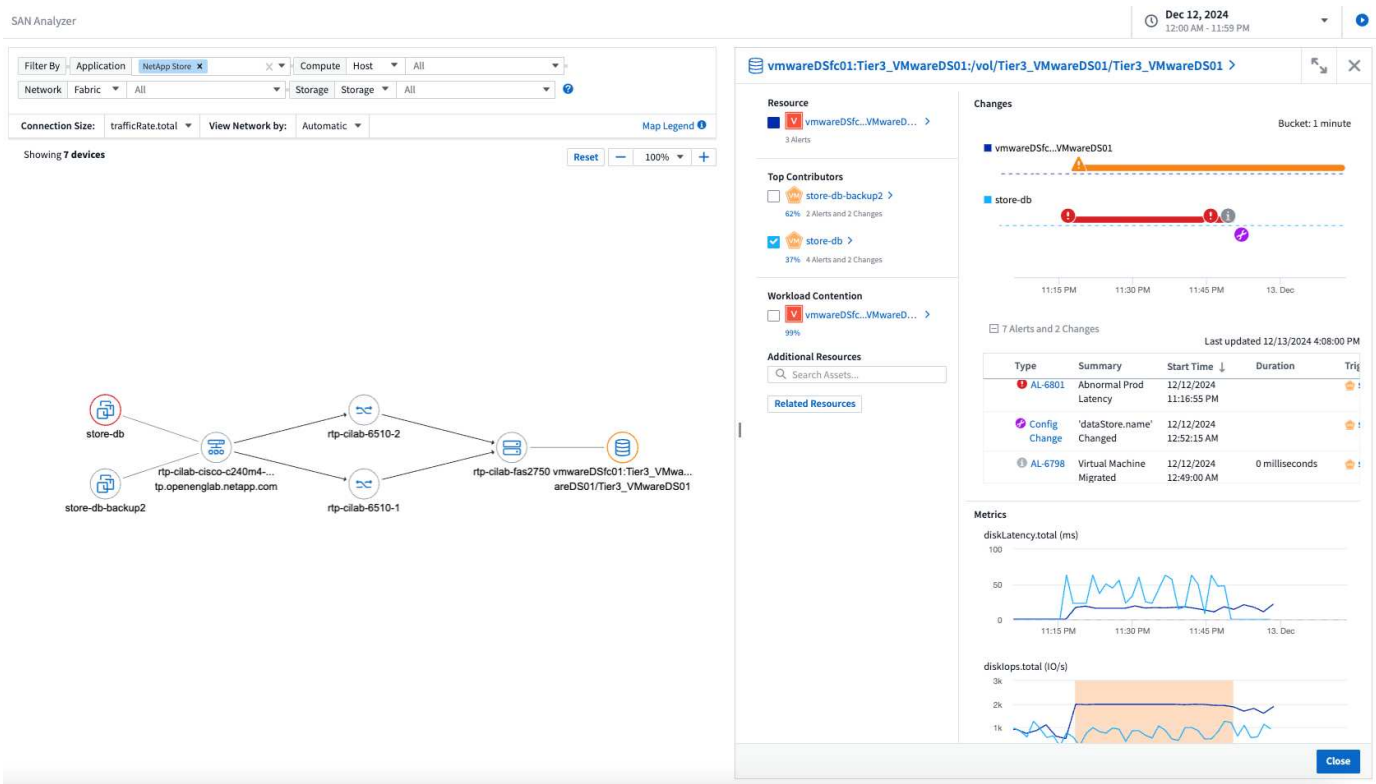
Catégorie	Termes indexés
Ordinateurs virtuels	Nom de "virtualmachine" Nom DNS adresses IP nom de l'hôte adresses IP des noms d'hôte de tous les datastores noms de toutes les applications associées
Commutateurs (standard et NPV)	« Switch » adresse IP wwn nom numéro de série modèle ID de domaine nom de la structure wwn de la structure
Client supplémentaire	nom du locataire secteur d'activité projet de l'unité commerciale
Bande	Nom de l'adresse IP « bande » fournisseur du numéro de série
Port	nom wwn « port »
Structure	nom wwn de la « structure »
Storage Virtual machine (SVM)	UUID de nom « storagevirtualmachine »

Analyse des données

Présentation de SAN Analyzer

LE SAN joue un rôle crucial dans la gestion des charges de travail stratégiques, mais sa complexité peut entraîner des pannes importantes et des perturbations pour les clients. Grâce à **SAN Analyzer** de DII, la gestion du SAN devient plus simple et plus efficace. Cet outil puissant offre une visibilité de bout en bout, en mappant les dépendances entre les ordinateurs virtuels/l'hôte et le réseau vers les LUN et le stockage.

Grâce à une carte topologique interactive, SAN Analyzer vous permet de repérer les problèmes, de comprendre les modifications et d'améliorer la compréhension du flux de données. Rationalisez la gestion SAN dans des environnements IT complexes avec SAN Analyzer et augmentez votre visibilité sur les charges de travail en mode bloc.



Explorer les connexions entre vos ressources

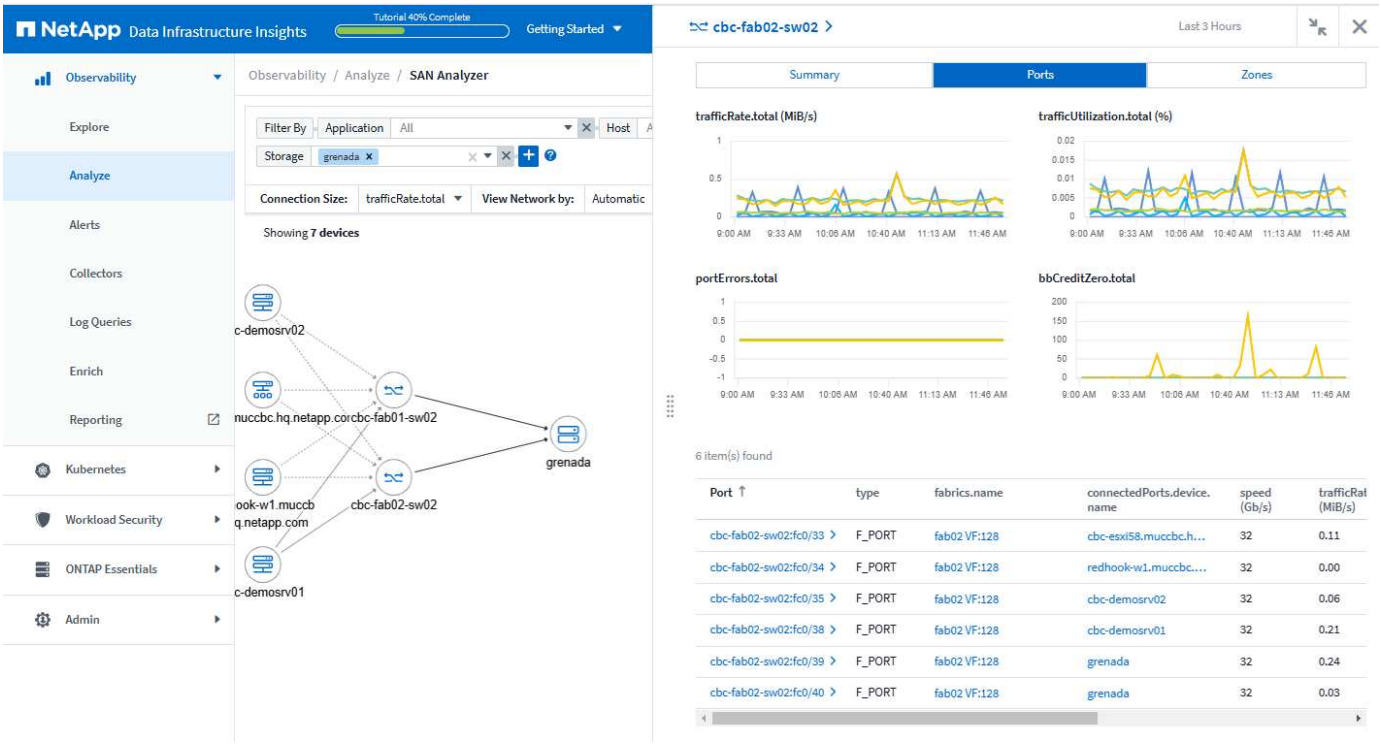
Sélectionnez **observabilité > analyse > analyseur SAN** pour afficher l'analyseur SAN. Définissez un filtre pour l'application, l'hôte, la structure et/ou le stockage. La carte des objets s'affiche, affichant les objets connectés. Passez le curseur sur un objet pour afficher les mesures de trafic pour ces connexions.



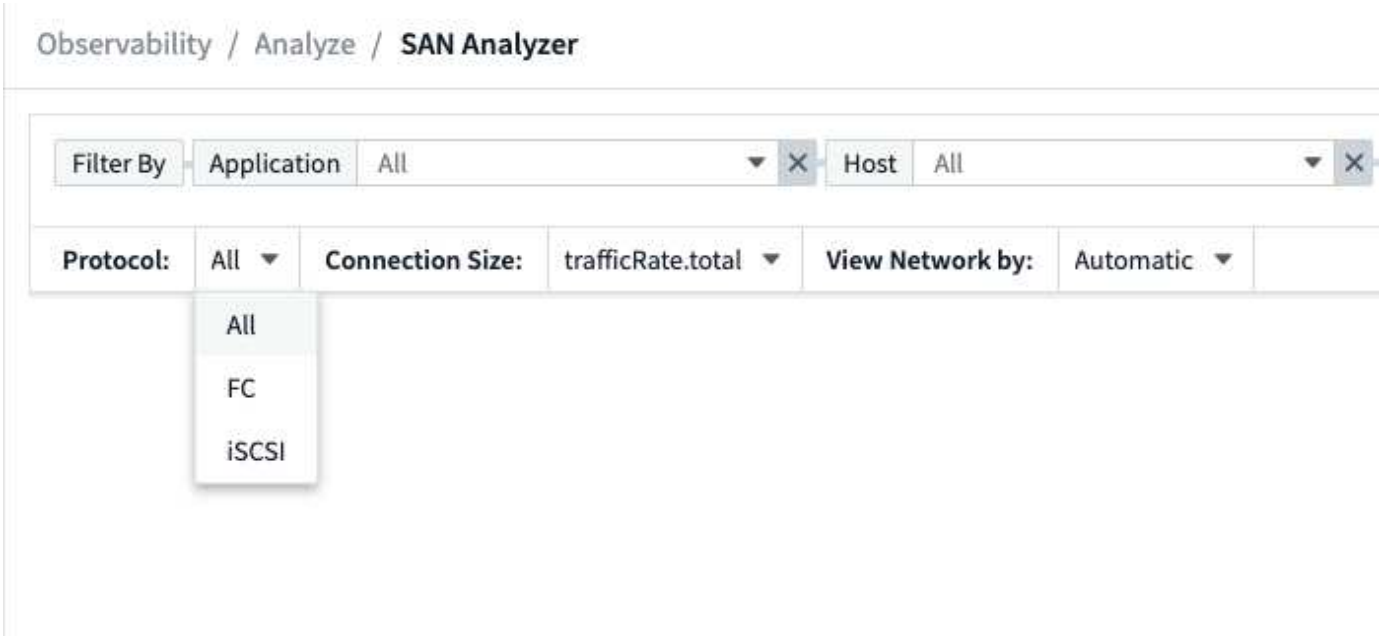
La plupart des filtres SAN Analyzer (y compris ceux que vous pouvez ajouter) sont contextuels ; lorsque vous sélectionnez un objet dans l'un de ces filtres, les choix présentés dans les autres listes déroulantes de filtre sont actualisés en contexte avec le ou les objets sélectionnés. Les seules exceptions 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 récapitulatif qui fournit des détails sur l'objet sélectionné (par exemple, IP, hyperviseur, structures connectées, etc., en fonction du type d'objet), ainsi que des graphiques affichant les mesures pour l'objet, telles que la latence ou les IOPS, et les modifications et alertes, le cas échéant. Vous pouvez également choisir d'afficher les mesures des objets Top Correlation sur les graphiques, si vous le souhaitez.

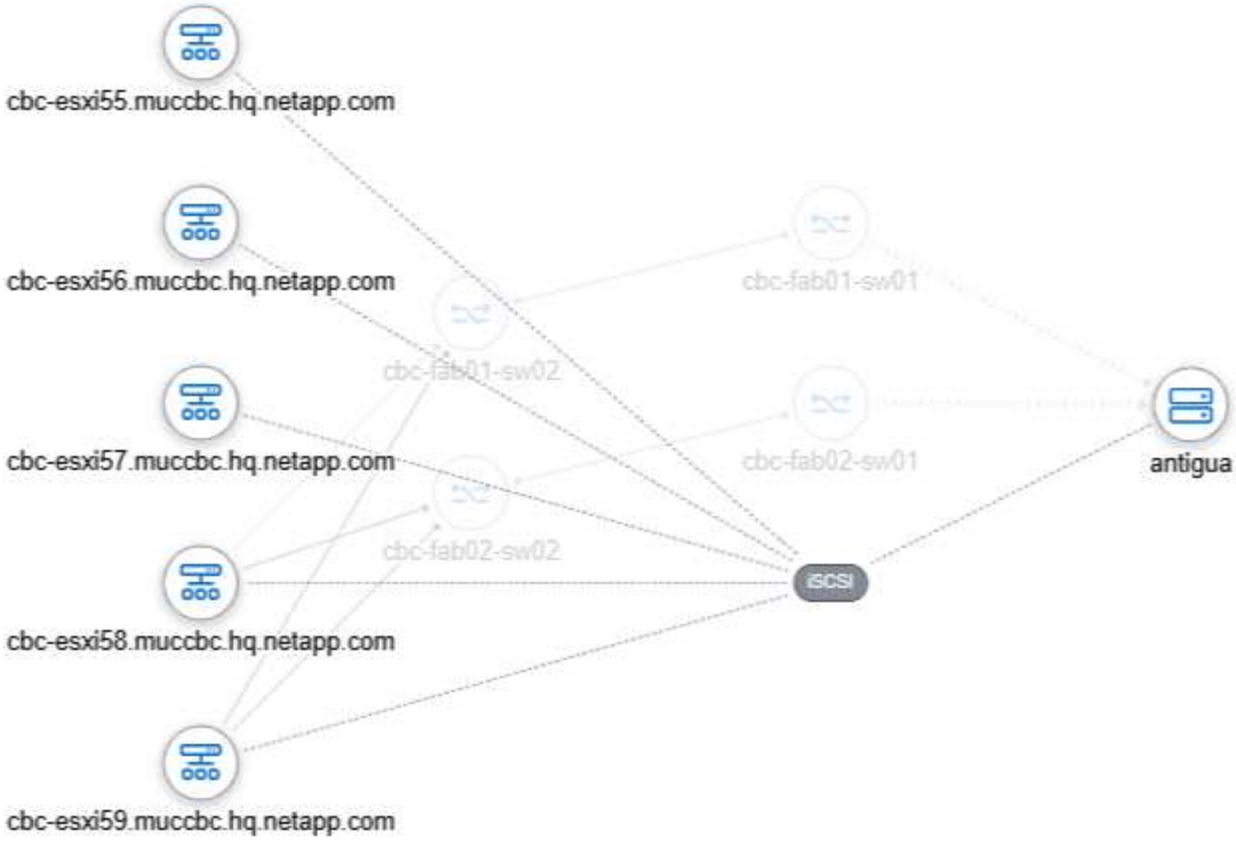
En plus de l'onglet Résumé, le panneau coulissant affiche des onglets pour des éléments tels que les détails de port ou les informations de zone, s'il s'applique à l'objet choisi.



Si votre environnement possède des protocoles différents, vous pouvez filtrer par iSCSI ou FC :



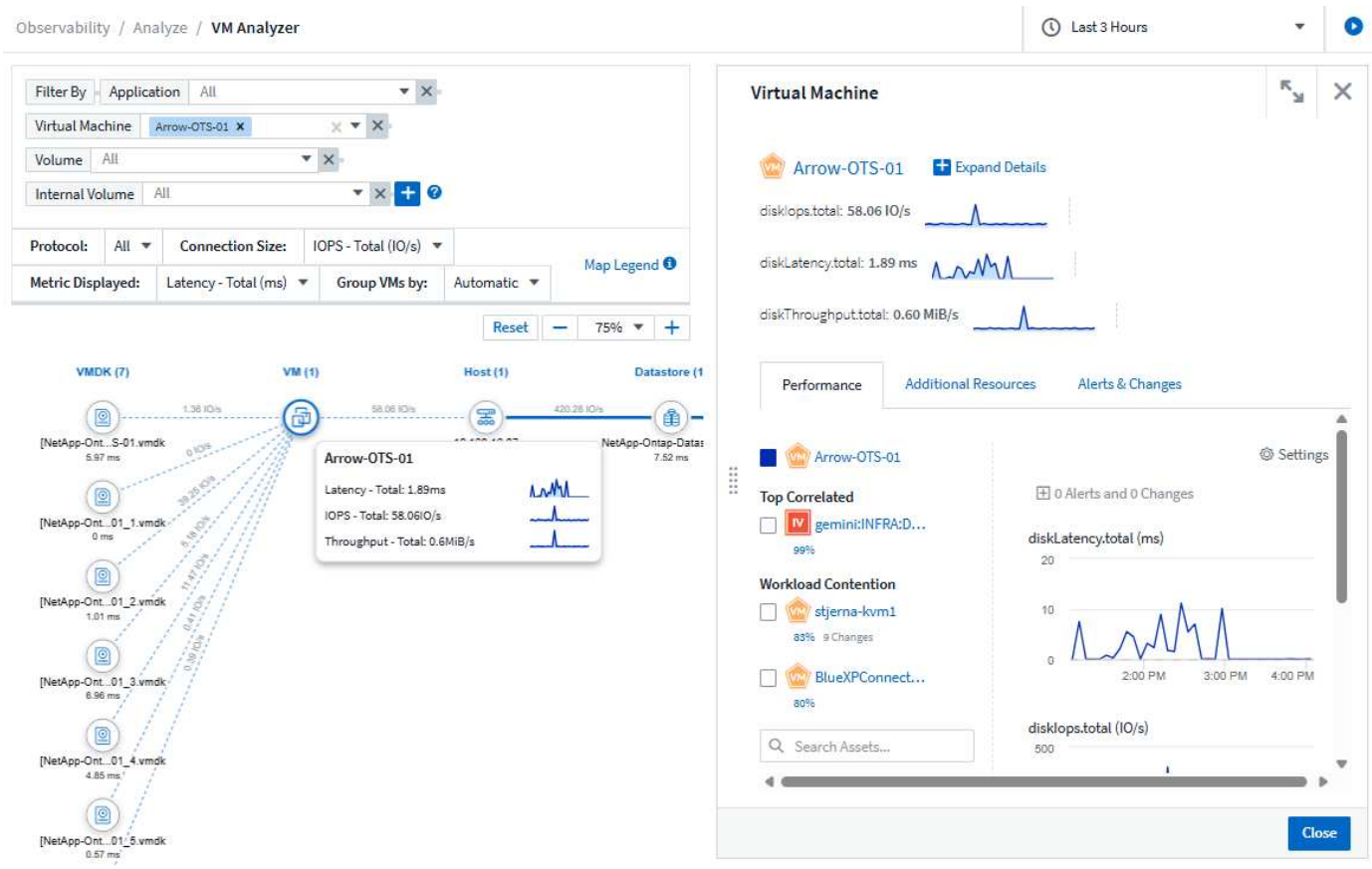
Si votre environnement inclut des périphériques iSCSI, passez la souris sur l'objet *iSCSI* pour mettre en évidence les connexions associées aux périphériques iSCSI concernés.



Présentation de VM Analyzer

Avec **VM Analyzer** de DII, la gestion de vos ressources virtuelles devient plus simple et plus efficace. Cet outil puissant offre une visibilité de bout en bout, mappant les dépendances du VMDK/VM à l'hôte, au datastore, au volume interne/volume et au stockage.

Grâce à une carte topologique interactive, VM Analyzer vous permet de repérer les problèmes, de comprendre les modifications 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.



Explorer les connexions entre vos ressources

Sélectionnez **observabilité > analyse > analyseur VM** pour afficher l'analyseur 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, affichant les objets connectés. Passez le curseur 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 filtre sont actualisés en contexte avec le 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 détaillé de l'objet sélectionné (par exemple, le débit ou l'utilisation, selon le type d'objet), ainsi que des graphiques présentant des métriques telles que la latence ou les IOPS. Des onglets supplémentaires vous permettent d'explorer des ressources supplémentaires, des modifications et des alertes. Vous pouvez également choisir d'afficher les métriques des

objets les plus corrélés ou en conflit sur les graphiques, si vous le souhaitez.

Voyez-le en action

"Dépannage simplifié avec VM Analyzer (vidéo)"

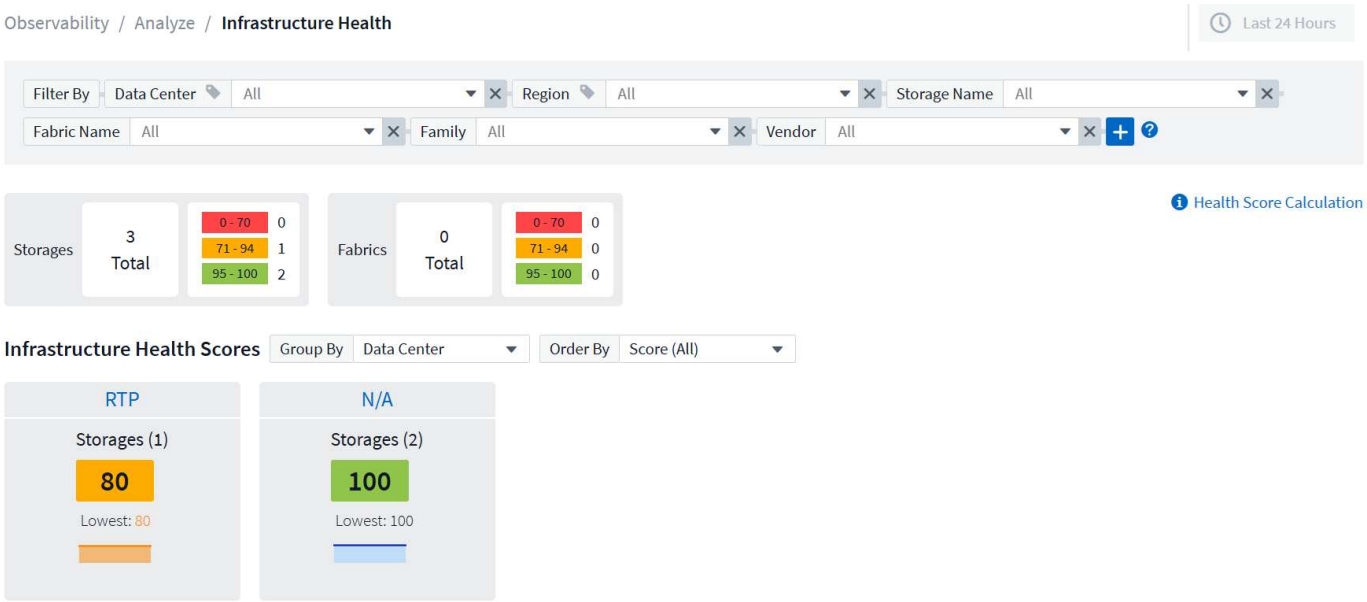
Surveiller la santé de l'infrastructure

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.

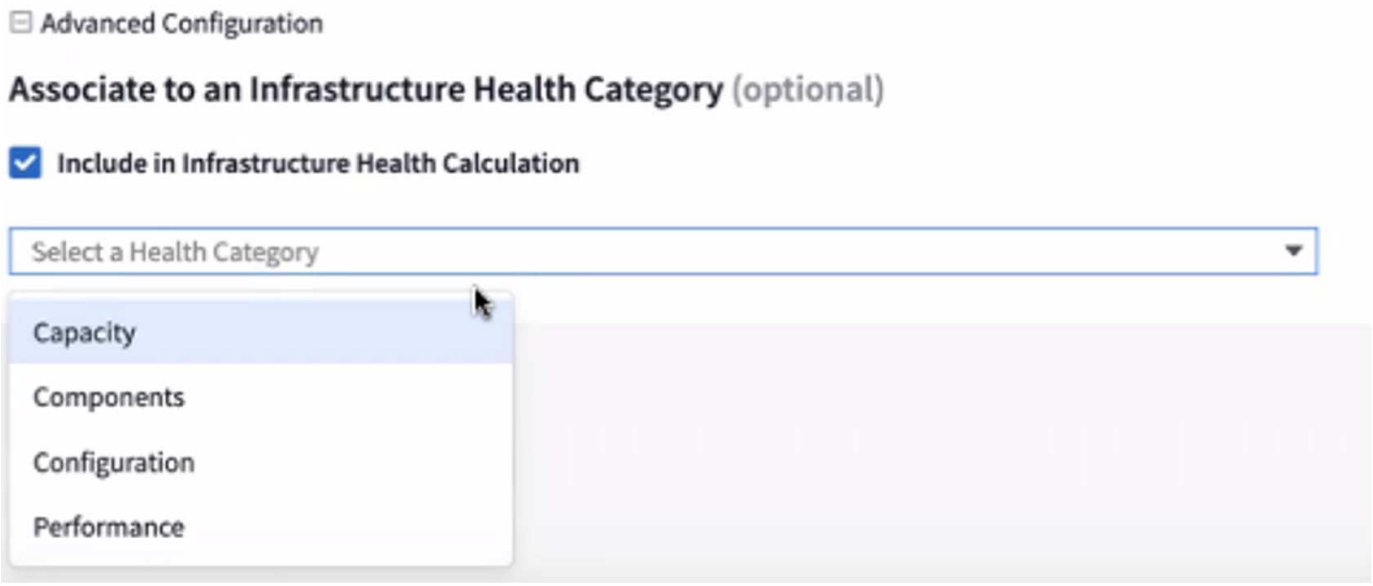
Configurer les moniteurs à utiliser pour la santé de l'infrastructure

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.

Création de rapports

Présentation des rapports sur les informations d'infrastructure de données

Le reporting Data Infrastructure Insights est un outil de veille stratégique qui vous permet d'afficher des rapports prédéfinis ou de créer des rapports personnalisés.

> La fonction de génération de rapports 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.

Les rapports Data Infrastructure Insights vous permettent d'effectuer les tâches suivantes :

- Exécuter un rapport prédéfini
- Créer un rapport personnalisé
- Personnalisez le format et la méthode de livraison d'un rapport
- Planifiez l'exécution automatique des rapports
- Rapports par e-mail
- Utilisez des couleurs pour représenter des seuils sur les données

Le reporting Data Infrastructure Insights permet de générer des rapports personnalisés pour différents domaines tels que la facturation interne, l'analyse de consommation et la prévision. Il aide également à répondre à plusieurs questions :

- Quel inventaire ai-je à faire ?
- Où est mon inventaire?
- Qui utilise nos ressources ?
- Quelle est la refacturation du stockage alloué à une unité commerciale ?
- Combien de temps me faut-il pour acquérir de la capacité de stockage supplémentaire ?
- Les unités commerciales sont-elles alignées sur les niveaux de stockage appropriés ?
- Dans quelle mesure les allocations de stockage sont-elles changeantes en un mois, un trimestre ou une année ?

Accès au reporting Data Infrastructure Insights

Vous pouvez accéder au rapport Data Infrastructure Insights en cliquant sur le lien **Rapports** dans le menu.

Vous serez redirigé vers l'interface de génération de rapports. Data Infrastructure Insights utilise IBM Cognos Analytics pour son moteur de reporting.

Qu'est-ce que le CÉC?

Lorsque vous travaillez avec les rapports, vous entendrez les termes « entrepôt de données » et « ETL ». ETL signifie « extraire, transformer et charger ». Le processus ETL récupère les données collectées dans Data Infrastructure Insights et les transforme dans un format pour les utiliser dans Reporting. « Entrepôt de données » fait référence aux données collectées disponibles pour la génération de rapports.

Le processus ETL comprend les processus individuels suivants :

- **Extract** : prend des données à partir de Data Infrastructure Insights.
- **Transform** : applique des règles ou des fonctions de logique applicative aux données lorsqu'elles sont extraites de Data Infrastructure Insights.
- **Load**: Enregistre les données transformées dans l'entrepôt de données pour utilisation dans Reporting.

Rôles utilisateur du reporting Data Infrastructure Insights

Si vous disposez de Data Infrastructure Insights Premium Edition avec Reporting, chaque utilisateur Data Infrastructure Insights de votre locataire dispose également d'un login SSO (Single Sign-On) pour l'application Reporting (Cognos, par exemple). Il vous suffit de cliquer sur le lien **Rapports** dans le menu pour vous connecter automatiquement à Reporting.

Votre rôle d'utilisateur dans Data Infrastructure Insights détermine votre rôle d'utilisateur Reporting :

Rôle informations exploitables sur l'infrastructure de données	Rôle de génération de rapports	Autorisations liées aux rapports
Invité	Grand public	Permet d'afficher, de planifier et d'exécuter des rapports et de définir des préférences personnelles telles que celles pour les langues et les fuseaux horaires. Les clients ne peuvent pas créer de rapports ni effectuer des tâches administratives.
Utilisateur	Auteur	Peut exécuter toutes les fonctions de l'utilisateur ainsi que créer et gérer des rapports et des tableaux de bord.
Administrateur	Administrateur	Peut exécuter toutes les fonctions auteur ainsi que toutes les tâches administratives telles que la configuration des rapports et l'arrêt et le redémarrage des tâches de rapport.

Le tableau suivant présente les fonctions disponibles pour chaque rôle de rapport.

Fonction	Grand public	Auteur	Administrateur
Afficher les rapports dans l'onglet contenu de l'équipe	Oui	Oui	Oui
Exécuter des rapports	Oui	Oui	Oui
Planifier des rapports	Oui	Oui	Oui

Téléchargez des fichiers externes	Non	Oui	Oui
Créer des travaux	Non	Oui	Oui
Créez des histoires	Non	Oui	Oui
Créer des rapports	Non	Oui	Oui
Créer des modules de données et des modules de données	Non	Oui	Oui
Effectuer des tâches administratives	Non	Non	Oui
Ajouter/Modifier un élément HTML	Non	Non	Oui
Exécuter le rapport avec l'élément HTML	Oui	Oui	Oui
Ajouter/Modifier SQL personnalisé	Non	Non	Oui
Exécutez des rapports avec Custom SQL	Oui	Oui	Oui

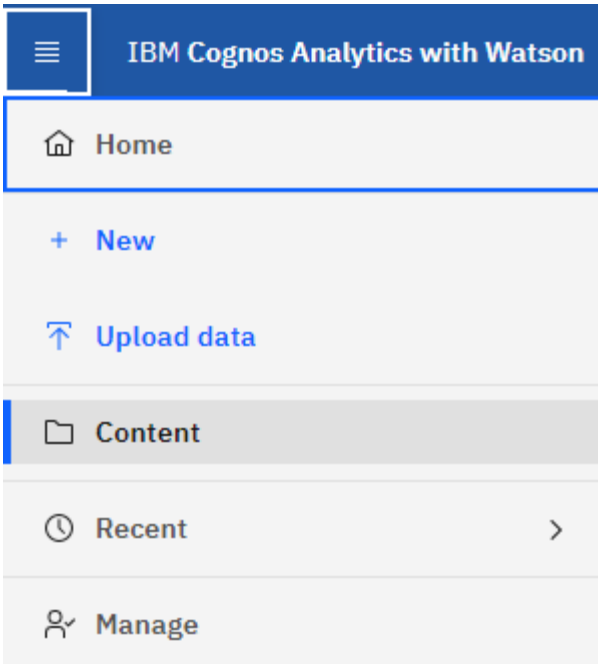
Définition des préférences de notification (Cognos)

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 de Cognos et de nouveau vous permettront de réinitialiser vos préférences de courriel.

Quelles mesures dois-je prendre pour préparer mon environnement existant à l'activation de la fonctionnalité SSO ?

Pour vous assurer que vos rapports sont conservés, migrez tous les rapports de *mon contenu* à *contenu* de l'équipe en suivant les étapes ci-dessous. Vous devez effectuer cette opération avant d'activer SSO sur votre locataire :

1. Accédez à **Menu > contenu**



1. Créez un nouveau dossier dans ***Team Content***
   a. Si plusieurs utilisateurs ont été créés, créez un dossier distinct pour chaque utilisateur afin d'éviter d'écraser des 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 nouveau dossier créé dans *Team Content*
6. Collez les rapports dans le nouveau dossier créé à l'aide des boutons Copier vers ou déplacer vers
7. Une fois la connexion SSO activée pour Cognos, connectez-vous à Data Infrastructure Insights à l'aide de 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 *My Content*.

Les rapports prédéfinis sont faciles à réaliser

Le reporting sur les informations de l'infrastructure de données inclut des rapports prédéfinis qui répondent à un certain nombre d'exigences courantes en matière de reporting, fournissant aux parties prenantes une vision critique nécessaire pour prendre des décisions avisées concernant leur infrastructure de stockage.

La fonction de génération de rapports est disponible dans Data Infrastructure Insights "Édition Premium".

Vous pouvez générer des rapports prédéfinis à partir du portail de rapports Data Infrastructure Insights, les envoyer par e-mail à d'autres utilisateurs et même les modifier. Plusieurs rapports vous permettent de filtrer par périphérique, entité commerciale ou niveau. Les outils de création de rapports utilisent IBM Cognos comme fondation et vous donnent de nombreuses options de présentation de données.

Les rapports prédéfinis indiquent votre inventaire, vos capacités de stockage, votre facturation interne, vos

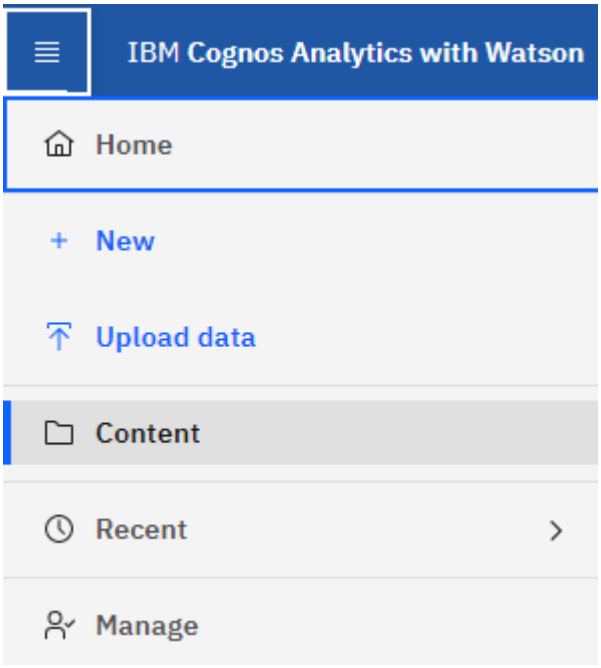
performances, votre efficacité du stockage, et les données de coût du cloud. Vous pouvez modifier ces rapports prédéfinis et enregistrer vos modifications.

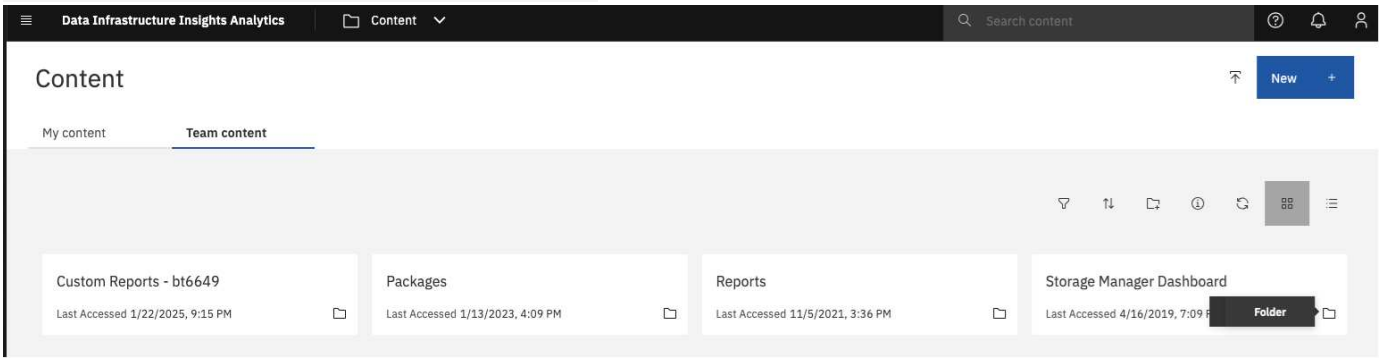
Vous pouvez générer des rapports sous différents formats, notamment HTML, PDF, CSV, XML, Et Excel.

Accès aux rapports prédéfinis

Lorsque vous ouvrez le portail de rapports, le dossier *Team Content* vous permet de 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.





Utilisation de rapports prédéfinis pour répondre aux questions courantes

Les rapports prédéfinis suivants sont disponibles dans **contenu de l'équipe > Rapports**.

Performance et capacité des applications au niveau de service

Le rapport capacité et performances des niveaux de service d'applications offre une vue d'ensemble de vos applications. Vous pouvez utiliser ces informations pour planifier la capacité ou pour élaborer un plan de migration.

Refacturation

Le rapport Chargeback fournit des informations sur la refacturation de la capacité de stockage et la comptabilité par hôte, application et entité commerciale, et inclut des données actuelles et historiques.

Pour éviter le double comptage, n'incluez pas les serveurs ESX, uniquement surveiller les machines virtuelles.

Sources des 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 le démarrage du dépannage des sources de données. Les sources de données défectueuses ont une incidence sur l'exactitude des rapports et sur l'utilisation générale du produit.

Performances ESX et VM

Le rapport ESX/VM Performance compare les serveurs ESX et les ordinateurs virtuels. Il présente les IOPS, le débit, la latence et l'utilisation des serveurs ESX et des VM en moyenne et en pics. Pour éviter le double comptage, exclure les serveurs ESX ; n'incluez que les VM. Une version mise à jour de ce rapport est disponible sur le site NetApp Storage Automation Store.

Synthèse de la structure

Le rapport Fabric Summary identifie les switchs et les switchs, y compris le nombre de ports, les versions du firmware et l'état des licences. Le rapport n'inclut pas les ports de commutateur NPV.

HBA hôtes

Le rapport Host HBA fournit une vue d'ensemble des hôtes dans l'environnement et fournit le fournisseur, le modèle et la version du micrologiciel des HBA, ainsi que le niveau de 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 hôte

Le rapport capacité et performances du niveau de service hôte fournit une vue d'ensemble de l'utilisation du stockage par hôte pour les applications en mode bloc uniquement.

Récapitulatif de l'hôte

Le rapport Host Summary fournit une vue d'ensemble de l'utilisation du stockage par chaque hôte sélectionné avec des informations sur les hôtes Fibre Channel et iSCSI. Ce rapport vous permet de comparer les ports et les chemins, la capacité Fibre Channel et ISCSI, ainsi que le nombre de violations.

Détails de licence

Le rapport Détails de la licence indique la quantité de ressources autorisées pour tous les sites avec des licences actives. Le rapport montre également une somme de la quantité réelle sur tous les sites avec des licences actives. La somme peut inclure des chevauchements de baies de stockage gérées par plusieurs serveurs.

Volumes mappés mais pas 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 donné, mais n'est pas masqué pour cet hôte. Dans certains cas, ces LUN peuvent être désaffectées. Les volumes non masqués sont accessibles par n'importe quel hôte, ce qui les

rend vulnérables à la corruption des données.

Capacité et performances NetApp

Le rapport capacité et performances de NetApp fournit des données globales pour la capacité allouée, utilisée et engagée, avec des données d'tendances et de performances pour la capacité NetApp.

Tableau de bord

Le rapport de la carte de performances fournit un résumé et un état général de tous les actifs acquis par Data Infrastructure Insights. L'état est indiqué par des indicateurs verts, jaunes et rouges :

- Le vert indique un état normal
- Le jaune indique un problème potentiel dans l'environnement
- Le rouge indique un problème nécessitant une intervention

Tous les champs du rapport sont décrits dans le dictionnaire de données fourni avec le rapport.

Récapitulatif du stockage

Le rapport Storage Summary fournit une synthèse globale des données de capacité utilisées et inutilisées pour les volumes, les pools de stockage et les volumes bruts, alloués et alloués. Ce rapport offre une vue d'ensemble de l'ensemble du stockage découvert.

Capacité et performances des machines virtuelles

Décrit l'environnement de machine virtuelle et son utilisation de la capacité. Les outils des machines virtuelles doivent être activés pour afficher certaines données, par exemple lorsque les machines virtuelles ont été hors tension.

Chemins d'accès aux VM

Le rapport VM Paths fournit des mesures de performances et de capacité de stockage des données pour lesquelles la machine virtuelle est exécutée sur quel hôte, quels hôtes accèdent aux volumes partagés, au contenu du chemin d'accès actif et aux éléments qui comprennent l'allocation et l'utilisation de la capacité.

Capacité HDS en fonction du pool fin

Le rapport HDS Capacity par thin Pool indique la quantité de capacité utilisable sur un pool de stockage provisionné.

Capacité NetApp par agrégat

Le rapport capacité NetApp par agrégat indique l'espace brut, total, utilisé, disponible et engagé d'agrégats.

Capacité Symmetrix par Thick Array

Le rapport Symmetrix Capacity by Thick Array affiche la capacité brute, la capacité utilisable, la capacité libre, mappée, masquée, et capacité libre totale.

Capacité Symmetrix par thin Pool

Le rapport Symmetrix Capacity by Thin Pool indique la capacité brute, la capacité utilisable, la capacité utilisée, la capacité libre, le pourcentage utilisé, capacité souscrite et taux d'abonnement.

Capacité XIV par baie

Le rapport XIV Capacity by Array indique les capacités utilisées et inutilisées pour la baie.

Capacité XIV par pool

Le rapport XIV Capacity by Pool indique la capacité utilisée et non utilisée pour les pools de stockage.

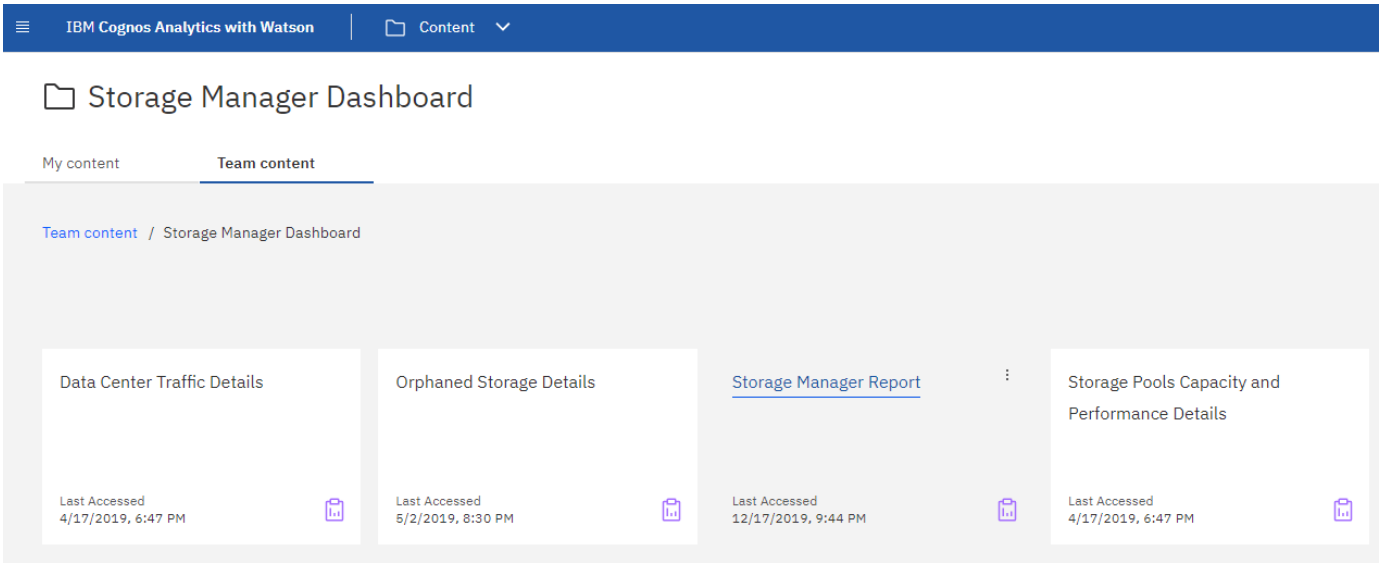
Tableau de bord de Storage Manager

Le tableau de bord de Storage Manager vous offre une visualisation centralisée qui vous permet de comparer et de comparer l'utilisation des ressources dans le temps par rapport aux plages acceptables et aux jours précédents d'activité. En ne présentant que les indicateurs de performance clés pour vos services de stockage, vous pouvez prendre des décisions sur la maintenance de vos data centers.

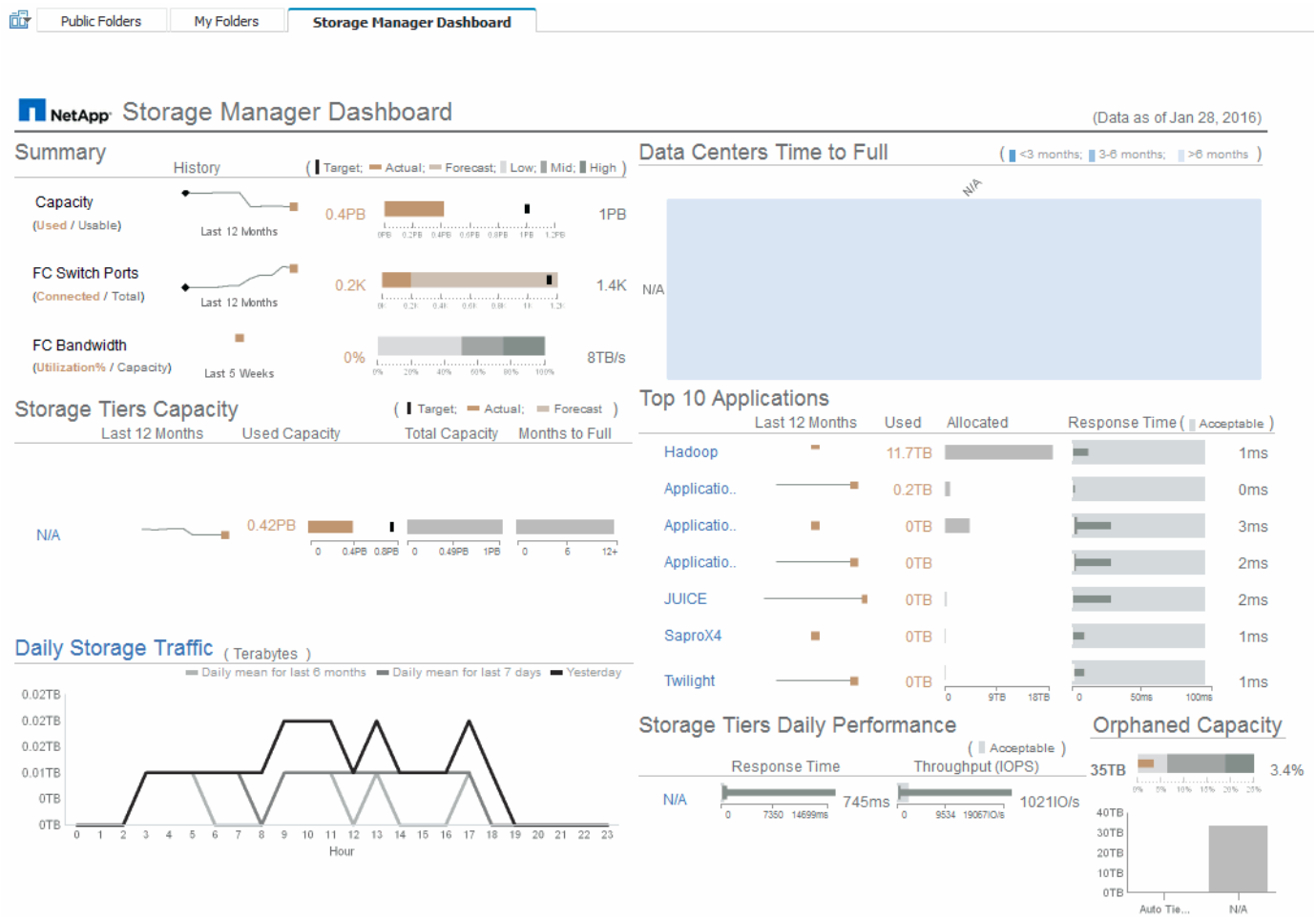
La fonction de génération de rapports est disponible dans Data Infrastructure Insights "Édition Premium".

Récapitulatif

La sélection de **Storage Manager Dashboard** à partir du contenu de l'équipe vous donne plusieurs rapports qui fournissent des informations sur votre trafic et votre stockage.



Pour une vue d'ensemble, le **Storage Manager Report** comprend sept composants qui contiennent des informations contextuelles sur de nombreux aspects de votre environnement de stockage. Vous pouvez approfondir vos différents aspects de vos services de stockage afin d'effectuer une analyse approfondie d'une section qui vous intéresse le plus.



Ce composant montre l'utilisation par rapport à la capacité de stockage utilisable, le nombre total de ports de switch par rapport au nombre total de ports de switch connectés, et l'utilisation totale des ports de switch connectés par rapport à la bande passante totale, et la façon dont chacune de ces tendances est dans le temps. Vous pouvez afficher l'utilisation réelle par rapport aux gammes basse, moyenne et élevée, ce qui vous permet de comparer et de comparer l'utilisation entre les projections et les valeurs réelles souhaitées, en fonction d'une cible. Pour les ports de capacité et 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 prévision de l'utilisation future, dépasse la cible, une alerte (cercle rouge Uni) apparaît à côté de la capacité.

Capacité des niveaux de stockage

Ce composant indique 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 à sa capacité maximale. L'utilisation de la capacité s'affiche avec les 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 prévision de l'utilisation future, dépasse la capacité cible, une alerte (cercle rouge Uni) apparaît à côté d'un niveau.

Vous pouvez cliquer sur n'importe quel niveau pour afficher le rapport Storage pools Capacity and Performance Details (informations disponibles par rapport aux capacités utilisées, nombre de jours avant saturation et performance (IOPS et temps de réponse) pour tous les pools du niveau sélectionné. Vous pouvez également cliquer sur n'importe quel nom de pool de stockage ou de stockage dans ce rapport pour afficher la page des ressources résumant l'état actuel de cette ressource.

Trafic quotidien de stockage

Ce composant indique les performances de l'environnement, s'il existe une forte croissance, des changements ou des problèmes potentiels par rapport aux six mois précédents. Il indique également le trafic moyen par rapport au trafic des sept jours précédents et pour la veille. Vous pouvez visualiser les anomalies de l'infrastructure sur son fonctionnement, car elles fournissent des informations qui mettent en évidence à la fois les variations cycliques (sept jours précédents) et saisonnières (six mois précédents).

Vous pouvez cliquer sur le titre (Daily Storage Traffic) pour afficher le rapport Storage Traffic Details (informations sur le trafic de stockage quotidien), qui affiche la carte des points chauds du trafic de stockage horaire pour la veille de chaque système de stockage. Cliquez sur un nom de stockage dans ce rapport pour afficher la page des ressources résumant l'état actuel de cette ressource.

Temps plein pour les data centers

Cette partie montre l'ensemble des data centers par rapport à tous les niveaux, ainsi que la quantité de capacité restante dans chaque data Center, sur la base des taux de croissance prévus. Le niveau de capacité de niveau est affiché en bleu ; plus la couleur est foncée, moins le niveau restant à l'emplacement avant qu'il soit plein.

Vous pouvez cliquer sur une section d'un niveau pour afficher le rapport « jours des pools de stockage complets », qui indique la capacité totale, la capacité disponible et le nombre de jours à pleins pour tous les pools du niveau sélectionné et du centre de données. Cliquez sur un nom de pool de stockage ou de stockage dans ce rapport pour afficher la page des ressources résumant l'état actuel de cette ressource.

10 applications principales

Ce composant représente les 10 applications principales 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 le partage de l'infrastructure. Vous pouvez visualiser l'éventail de l'expérience utilisateur au cours des sept derniers jours afin de voir si les temps de réponse des clients sont acceptables (ou plus important, inacceptables).

Cette zone montre également les tendances, qui indiquent si les applications répondent à leurs objectifs de niveau de service (SLO) de performance. Vous pouvez afficher le temps de réponse minimum de la semaine précédente, le premier quartile, le troisième quartile et le temps de réponse maximal, avec une médiane indiquée par rapport à un objectif SLO acceptable que vous pouvez configurer. Lorsque le temps de réponse médian d'une application est en dehors de la plage d'objectifs SLO acceptable, une alerte (cercle rouge Uni) s'affiche à côté de l'application. Vous pouvez cliquer sur une application pour afficher la page de ressources résumant l'état actuel de cette ressource.

Tiers de stockage performances quotidiennes

Ce composant récapitule les performances du niveau en matière de temps de réponse et d'IOPS pour les sept jours précédents. Ces performances sont comparées à celles d'un objectif SLO que vous pouvez configurer. Vous pouvez donc voir s'il est possible de consolider les niveaux, d'réaligner les charges de travail exécutées à partir de ces tiers ou d'identifier les problèmes liés à des tiers spécifiques. Lorsque le temps de réponse médian ou les IOPS médianes ne se situe pas dans la plage d'objectifs SLO acceptable, une alerte (cercle rouge Uni) s'affiche en regard d'un niveau.

Vous pouvez cliquer sur le nom d'un niveau pour afficher le rapport Storage pools Capacity and Performance Details (informations disponibles par rapport aux capacités utilisées, nombre de jours avant saturation et performance (IOPS et temps de réponse) pour tous les pools du niveau sélectionné. Cliquez sur un pool de stockage ou un pool de stockage dans ce rapport pour afficher la page des ressources résumant l'état actuel de cette ressource.

Capacité orpheline

Ce composant affiche la capacité totale orpheline et la capacité orpheline par niveau, par rapport aux plages acceptables pour la capacité totale utilisable et par rapport à la capacité réelle orpheline. La capacité orpheline est définie par configuration et par performance. Le stockage orphelin par configuration décrit une situation dans laquelle le stockage est alloué à un hôte. Toutefois, la configuration n'a pas été correctement effectuée et l'hôte ne peut pas accéder au système de stockage. La fonction orpheline par performance se trouve lorsque le stockage est correctement configuré pour être accessible par un hôte. Cependant, il n'y a eu aucun trafic de stockage.

La barre empilée horizontale indique les plages acceptables. Plus le gris est foncé, plus la situation est inacceptable. La situation réelle est indiquée par une barre de bronze étroite indiquant la capacité réelle orpheline.

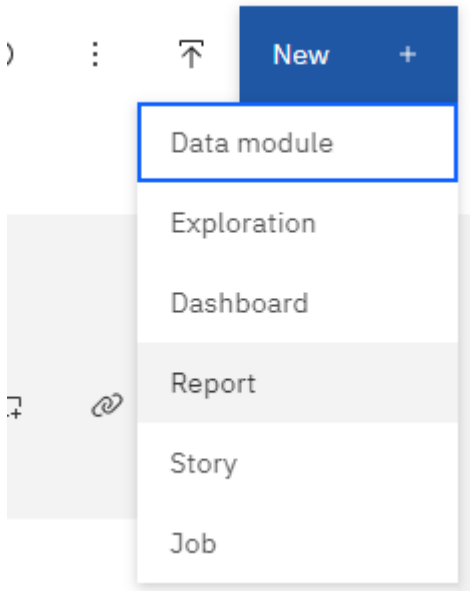
Vous pouvez cliquer sur un niveau pour afficher le rapport des détails du stockage orphelin, qui affiche tous les volumes identifiés comme orphelins par la configuration et les performances du niveau sélectionné. Cliquez sur n'importe quel stockage, pool de stockage ou volume de ce rapport pour afficher la page des ressources résumant l'état actuel de la ressource en question.

Création d'un rapport (exemple)

Utilisez les étapes de cet exemple pour générer un rapport simple sur la capacité physique des pools de stockage et de stockage dans plusieurs data centers.

Étapes

1. Accédez à **Menu > contenu > contenu de l'équipe > Rapports**
2. Dans le coin supérieur droit de l'écran, sélectionnez **[Nouveau +]**
3. Sélectionnez **Rapport**



4. Dans l'onglet **Templates**, sélectionnez *Blank*

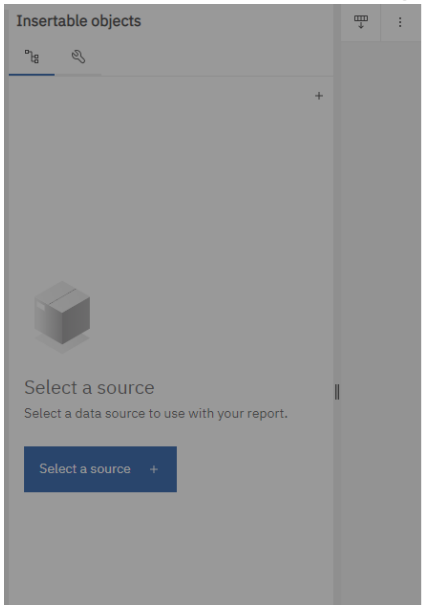
   Les onglets Source et données s'affichent

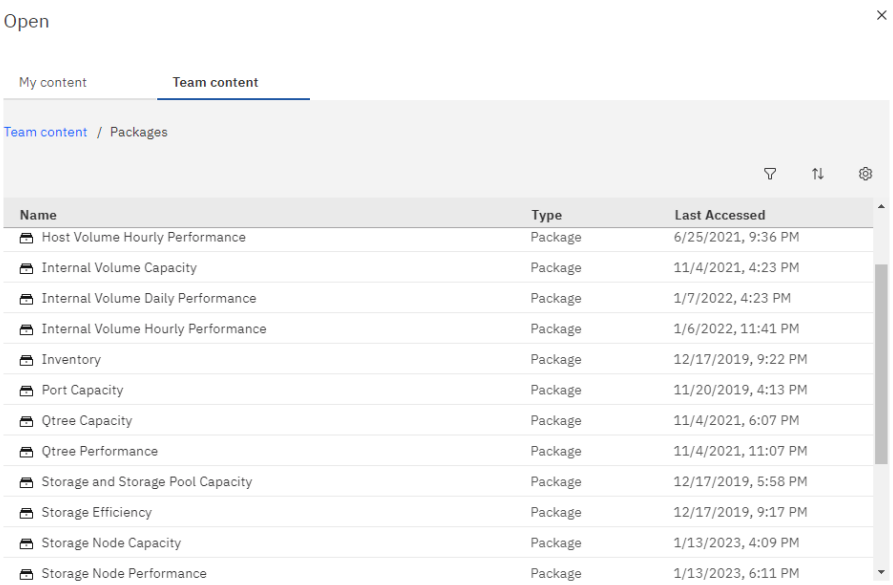
5. Ouvrir **sélectionnez une source +**

6. Sous **contenu de l'équipe**, ouvrez **Packages**

   La liste des packages disponibles s'affiche.

7. Choisissez **capacité de stockage et de pool de stockage**





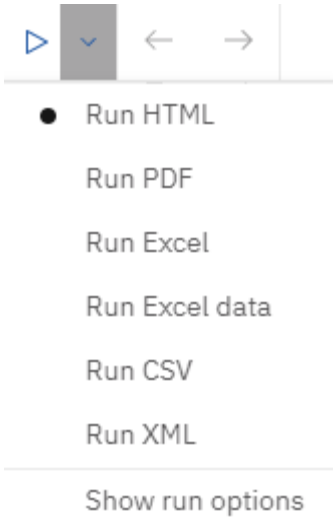
8. Sélectionnez **Ouvrir**

   Les styles disponibles pour votre rapport sont affichés.

9. Sélectionnez **liste**

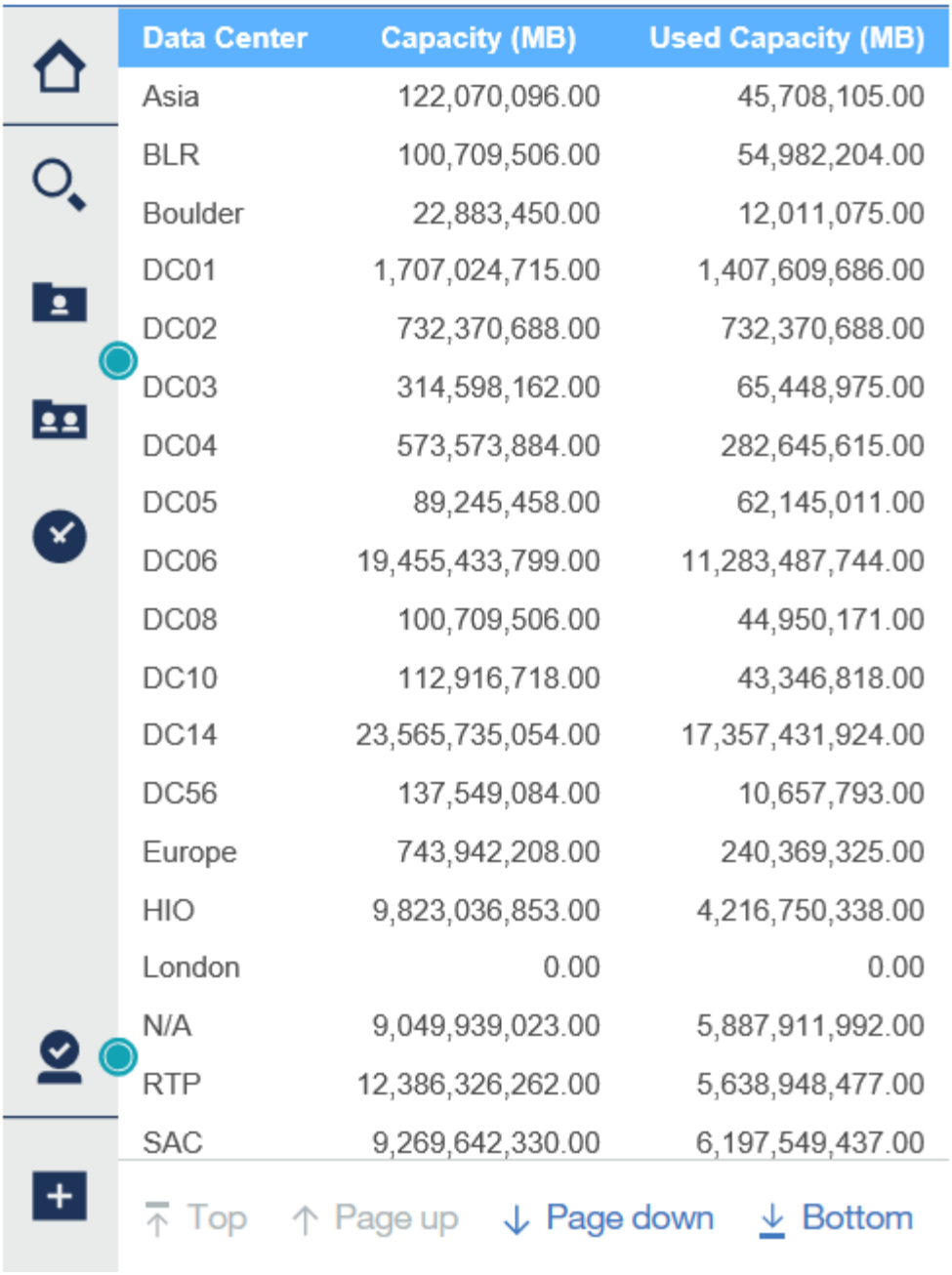
   Ajoutez des noms appropriés pour la liste et la requête

10. Sélectionnez **OK**
11. Développez *la capacité physique*
12. Développez jusqu'au niveau le plus bas de *Data Center*
13. Faites glisser *Data Center* vers le palais de reporting.
14. Développez *Capacity (Mo)*
15. Faites glisser *Capacity (Mo)* vers le palais de reporting.
16. Faites glisser *used Capacity (MB)* vers le palais de reporting.
17. Exécutez le rapport en sélectionnant un type de sortie dans le menu **Exécuter**.



Résultat

Un rapport similaire à ce qui suit 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 distribution d'un rapport, définir les propriétés ou les plannings de rapport et envoyer des rapports par e-mail.

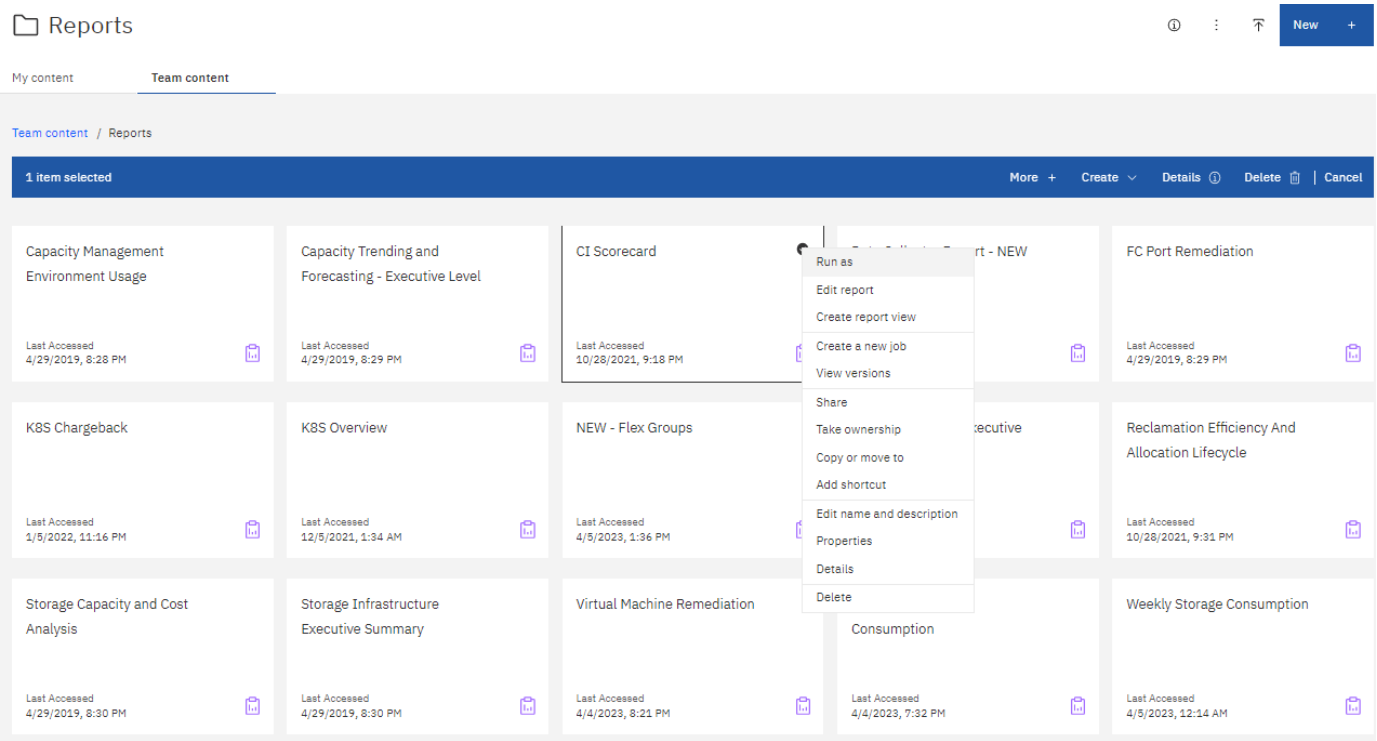
La fonction de génération de rapports est disponible dans Data Infrastructure Insights "Édition Premium".

Avant d'apporter des modifications aux autorisations ou à la sécurité des rapports, vous devez copier les rapports « mon contenu » dans le dossier « contenu de l'équipe » pour vous assurer que les rapports sont enregistrés.

Personnalisation du format de sortie et de l'envoi d'un rapport

Vous pouvez personnaliser le format et la méthode de diffusion des rapports.

1. Dans le portail de génération de rapports Data Infrastructure Insights, accédez à **Menu > contenu > mon contenu/contenu d'équipe**. Placez le pointeur de la souris sur le rapport que vous souhaitez personnaliser et ouvrez le menu « trois points ».

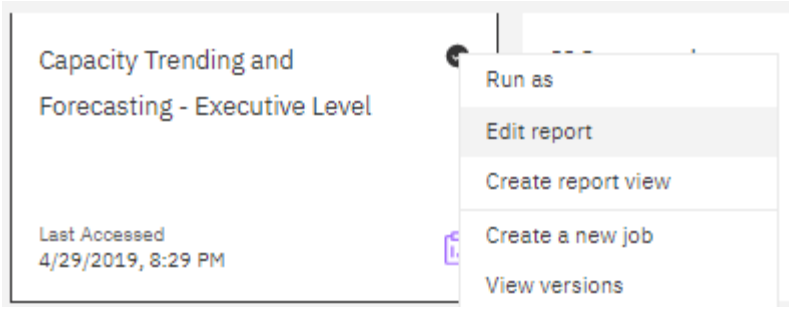


1. Cliquez sur **Propriétés > Programme**
2. Vous pouvez définir les options suivantes :
   - **Planifier** lorsque vous souhaitez que les rapports s'exécutent.
   - Choisissez **Options** pour le format et la livraison du rapport (Enregistrer, Imprimer, E-mail) et les langues du rapport.
3. Cliquez sur **Enregistrer** pour produire le rapport à l'aide des sélections que vous avez effectuées.

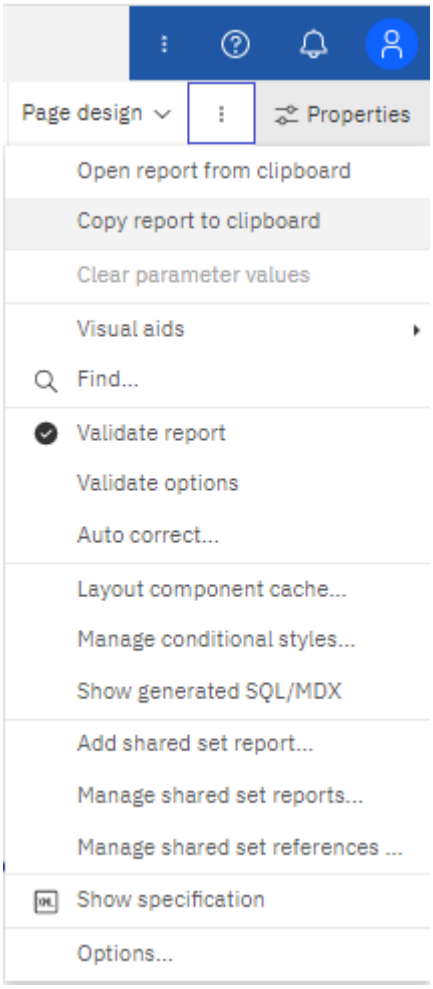
Copie d'un rapport dans le presse-papiers

Utilisez ce processus pour copier un rapport dans le presse-papiers.

1. Sélectionnez un rapport à copier à partir de (**Menu > contenu > mon contenu ou contenu d'équipe**)
2. Choisissez *Modifier le rapport* dans le menu déroulant du rapport



3. Dans le coin supérieur droit de l'écran, ouvrez le menu « trois points » à côté de « Propriétés ».
4. Sélectionnez **Copier le rapport dans le presse-papiers**.

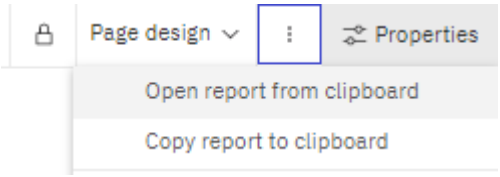


Ouverture de rapports à partir du presse-papiers

Vous pouvez ouvrir une spécification de rapport qui a été précédemment copiée dans le presse-papiers.

A 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. Dans le coin supérieur droit 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 un nom significatif au nouveau rapport et sélectionnez **Enregistrer**.

Modification d'un rapport existant

N'oubliez pas que la modification des fichiers à leur emplacement par défaut risque d'écraser ces rapports 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 à la création de rapports.

Problème:	**Essayez ceci:**
Lorsque vous planifiez l'envoi d'un rapport par e-mail, le nom de l'utilisateur connecté est pré-renseigné dans le champ « à » de l'e-mail. Toutefois, le nom est sous la forme de "prénom nom lastname" (prénom, espace, nom de famille). Étant donné que cette adresse e-mail n'est pas valide, l'e-mail ne peut pas être envoyé lorsque le rapport programmé est exécuté.	Lorsque vous planifiez l'envoi du rapport par e-mail, effacez le nom pré-rempli et saisissez une adresse e-mail valide et correctement formatée dans le champ « à ».
Mon rapport planifié est envoyé par e-mail, mais il n'est pas possible d'y accéder si l'origine provient du dossier « mon contenu ».	Pour éviter cela, le rapport ou la vue de rapport doit être enregistré dans le dossier « contenu de l'équipe > Rapports personnalisés - xxxxxx » et le programme 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 de 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" où vous n'avez pas accès à l'écriture.	La solution consiste à créer un nouveau dossier portant un nom unique (c.-à-d. "NewFolder") et à l'enregistrer, ou à enregistrer dans "mon contenu", puis à 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 planning régulier. Les résultats des rapports peuvent être automatiquement envoyés par e-mail à vous-même et à d'autres personnes.

La fonction de génération de rapports est disponible dans Data Infrastructure Insights "Édition Premium".

Les exemples de cette section présentent le processus suivant, qui peut être utilisé pour n'importe quel modèle de données de reporting Data Infrastructure Insights :

- Identifier une question à répondre avec un rapport
- Déterminer les données nécessaires pour soutenir les résultats
- Sélection d'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 peuvent être imprécis ou incomplets.

Par exemple, si vous n'avez pas terminé le processus d'identification du périphérique, vos rapports de capacité ne seront pas précis. Ou, si vous ne terminez pas de définir des annotations (par exemple, des niveaux, des unités commerciales et des data centers), vos rapports personnalisés peuvent ne pas générer des rapports précis sur les données de votre domaine ou indiquer « N/A » pour certains points de données.

Avant de concevoir vos rapports, effectuez les tâches suivantes :

- Tout configurer "collecteurs de données"correctement.
- Entrez des annotations (telles que des niveaux, des data centers et des entités commerciales) sur les périphériques et les ressources de votre locataire. Il est avantageux d'avoir des annotations stables avant de générer des rapports, car le reporting Data Infrastructure Insights collecte des informations d'historique.

Processus de création de rapports

Le processus de création de rapports personnalisés (également appelés « ad hoc ») implique plusieurs tâches :

- Planifiez les résultats de votre rapport.
- Identifiez les données à l'appui de vos résultats.
- Sélectionnez le modèle de données (par exemple, le modèle de données Chargeback, le modèle de données Inventory, etc.) qui contient les données.
- Sélectionnez les éléments de données pour le rapport.
- Vous pouvez éventuellement formater, trier et filtrer les résultats du rapport.

Planifier les résultats de votre rapport personnalisé

Avant d'ouvrir les outils de création de rapports, vous pouvez planifier les résultats souhaités à partir du rapport. Avec les outils de création de rapports, vous pouvez facilement créer des rapports et peut ne pas avoir besoin de beaucoup de planification. Cependant, il est bon d'obtenir un bon sens de la part du demandeur de rapport sur les exigences du rapport.

- Identifiez la question que vous souhaitez répondre. Par exemple :
  - Quelle est la capacité restante ?
  - Quels sont les coûts de refacturation par unité commerciale ?
  - Quelle est la capacité par niveau pour s'assurer que les unités commerciales sont alignées sur le niveau de stockage approprié ?

    - Comment puis-je prévoir les besoins en énergie et en climatisation ? (Ajoutez des métadonnées personnalisées en ajoutant des annotations aux ressources.)
- Identifiez les éléments de données dont vous avez besoin pour prendre en charge une réponse.
- Identifiez les relations entre les données que vous voulez voir dans la réponse. N'incluez pas de relations illogiques dans votre question, par exemple, « Je veux voir les ports qui se rapportent à la capacité ».
- Identifier tous les calculs nécessaires sur les données.
- Déterminez les types de filtrage 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.
- Identifier la manière dont le rapport sera distribué. Par exemple, doit-il être envoyé par e-mail à un horaire fixe ou inclus dans la zone du dossier contenu de l'équipe ?
- Déterminez qui sera responsable du rapport. Cela peut affecter la complexité de la conception.
- Créer une maquette du rapport.

Conseils pour concevoir des rapports

Plusieurs conseils peuvent être utiles lors de la conception de rapports.

- Déterminez si vous devez utiliser des données actuelles ou historiques.

  La plupart des rapports n'ont besoin que de générer des rapports sur les données les plus récentes disponibles dans les informations sur l'infrastructure de données.

- Les rapports Data Infrastructure Insights fournissent des informations historiques sur la capacité et les performances, mais pas sur l'inventaire.
- Chacun voit l'ensemble des données. Cependant, vous devrez peut-être limiter ces données à des publics spécifiques.

  Pour segmenter les informations des différents utilisateurs, vous pouvez créer des rapports et définir des autorisations d'accès.

Modèles de données de création de rapports

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 comprend un simple data Mart et un Data Mart avancé :

- Le magasin de données simple permet d'accéder rapidement aux éléments de données les plus couramment utilisés et ne comprend que le dernier instantané des données de l'entrepôt de données ; il n'inclut pas les données historiques.
- Le data Mart avancé fournit toutes les valeurs et tous les détails disponibles dans le simple data Mart et inclut l'accès aux valeurs de données historiques.

Modèles de données de capacité

Vous aide à répondre aux questions concernant la capacité de stockage, l'utilisation du système de fichiers, la capacité de volume interne, la capacité de port, la capacité 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 du pool de stockage et du pool de stockage

Vous permet de répondre aux questions concernant la planification des ressources de stockage, y compris les pools de stockage et les pools, et inclut à la fois les données des pools de stockage physiques et virtuels. Avec ce modèle de données simple, vous pouvez répondre à toutes les questions relatives à la capacité sur place et à l'utilisation de la capacité des pools de stockage par niveau et par data Center à long terme. Si les nouveaux rapports sur la capacité vous servent, vous devez commencer par le modèle de données, car il s'agit d'un modèle de données plus simple et ciblé. Vous pouvez répondre à des questions similaires à ce qui suit à l'aide de 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 d'une baie pour un niveau donné ?
- Quelle est ma capacité de stockage par fabricant et par famille, ainsi que par data Center ?
- Quelle est la tendance à l'utilisation du stockage sur une baie pour tous les niveaux ?
- Quels sont mes 10 principaux systèmes de stockage avec un taux d'utilisation optimal ?
- Quelle est la tendance à l'utilisation du stockage par les pools de stockage ?
- Quelle est la capacité déjà allouée ?
- Quelle est la capacité disponible pour l'allocation ?

Modèle de données d'utilisation du système de fichiers

Ce modèle de données permet de contrôler 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 tendances par type de système de fichiers. Vous pouvez répondre aux questions suivantes à l'aide de ce modèle de données :

- Quelle est la taille du système de fichiers ?
- Où les données sont-elles conservées et comment elles sont accessibles, par exemple, en local ou en SAN ?
- Quelles sont les tendances historiques de la capacité du système de fichiers ? Alors, en se basant sur ce fait, que pouvons-nous prévoir pour les besoins futurs ?

Modèle de données de capacité de volume interne

Répond à des questions sur le volume interne utilisé, 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 de port

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 comme suit pour vous aider à planifier l'achat de nouveaux commutateurs : comment créer une prévision de consommation des ports qui prévoit la disponibilité des ressources (port) (selon le data Center, le fournisseur des commutateurs et la vitesse du port)

?

- Quels ports sont susceptibles de manquer de capacité pour fournir la vitesse des données, les data centers, le fournisseur et le nombre de ports hôtes et de stockage ?
- Quelles sont les tendances de capacité des ports de commutation au fil du temps ?
- Quelle est la vitesse des ports ?
- Quel type de capacité de port est nécessaire et quelle entreprise est sur le point de sortir d'un certain type de port ou fournisseur ?
- Quel est le délai optimal pour acheter cette capacité et la rendre disponible ?

Modèle de données de capacité qtree

Permet de tendances de l'utilisation des qtrees (avec des données telles que la capacité utilisée par rapport à la capacité allouée) dans le temps. Vous pouvez afficher ces informations en fonction de différentes dimensions (par exemple, par entité commerciale, application, niveau et niveau de service). Vous pouvez répondre aux questions suivantes à l'aide de 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 en matière de capacité utilisée et libre afin de pouvoir planifier la capacité ?
- Quelles entités commerciales utilisent le plus de capacités ?
- Quelles applications consomment le plus de capacité ?

Modèle de données de capacité de la machine virtuelle

Permet de générer des rapports sur l'utilisation de la capacité de votre environnement virtuel. Ce modèle de données vous permet de créer des rapports sur l'évolution de l'utilisation de la capacité au fil du temps pour les machines virtuelles et les datastores. Le modèle de données offre également le provisionnement fin et les données de refacturation des machines virtuelles.

- Comment déterminer la refacturation des capacités en fonction de la capacité provisionnée aux machines virtuelles et aux datastores ?
- Quelle capacité n'est pas utilisée par les ordinateurs virtuels et quelle partie des ressources inutilisées est disponible, orpheline ou autre ?
- De quoi devons-nous acheter en fonction des tendances de consommation ?
- Quelles sont les économies réalisées en termes d'efficacité du stockage grâce aux technologies de déduplication et de provisionnement fin du stockage ?

Capacités dans le modèle de données VM Capacity sont extraites de disques virtuels (VMDK). Cela signifie que la taille provisionnée d'une machine virtuelle qui utilise le modèle de données de capacité de la machine virtuelle correspond à la taille de ses disques virtuels. Cette configuration est différente de la capacité provisionnée dans la vue Virtual machines des informations sur l'infrastructure de données, qui indique la taille provisionnée de la machine virtuelle elle-même.

Modèle de données Volume Capacity

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 data Center.

Vous pouvez afficher la capacité des volumes orphelins, des volumes inutilisés et des volumes de protection

(utilisés pour la réplication). Vous pouvez également voir différentes technologies de volumes (iSCSI ou FC) et comparer des volumes virtuels à des volumes non virtuels pour des problèmes de virtualisation de baies.

Vous pouvez répondre à des questions similaires à celles qui suivent avec ce modèle de données :

- Quels volumes ont une utilisation supérieure à un seuil prédéfini ?
- Quelle est la tendance de mon data Center à analyser la capacité de volumes orphelins ?
- Quelle part de ma capacité de data Center est virtualisée ou provisionnée ?
- Quelle part de la capacité de mon data Center doit être réservée à la réplication ?

Modèle de données de refacturation

Répond 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 de comptabilité et de refacturation de la capacité de stockage par hôte, application et entités commerciales, et inclut des données actuelles et historiques. Les données de rapports peuvent être classées par niveau de service et par niveau de stockage.

Vous pouvez utiliser ce modèle de données pour générer des rapports de refacturation en identifiant la capacité utilisée par une entité business. Ce modèle de données vous permet de créer des rapports unifiés sur plusieurs protocoles (notamment NAS, SAN, FC et iSCSI).

- Pour le stockage sans volumes internes, les rapports de refacturation indiquent la refacturation par volumes.
- Pour le stockage avec volumes internes :
  - Si les entités commerciales sont attribuées aux volumes, les rapports de refacturation affichent la refacturation par volume.
  - Si les entités business ne sont pas affectées aux volumes mais qu'elles sont attribuées aux qtrees, les rapports de refacturation sont indiqués par les qtrees.
  - Si les entités business ne sont pas affectées aux volumes et ne sont pas affectées aux qtrees, les rapports de refacturation affichent le volume interne.
  - La décision d'afficher la refacturation 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 refacturation à différents niveaux.

Les données de capacité sont supprimées après un intervalle de temps par défaut. Pour plus de détails, voir processus d'entrepôt de données.

Les rapports utilisant le modèle de données Chargeback peuvent afficher des valeurs différentes de celles qui utilisent 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 identiques.
- Pour les systèmes de stockage NetApp et Celerra, le modèle de données Chargeback utilise une seule couche (de volumes, de volumes internes ou de qtrees) pour établir leurs factures, tandis que le modèle de données Storage Capacity utilise plusieurs couches (de volumes et de volumes internes) pour établir les frais.

Modèle de données d'inventaire

Réponses à des questions sur les ressources d'inventaire, notamment les hôtes, les systèmes de stockage,

les commutateurs, les disques, les bandes qtrees, quotas, machines virtuelles et serveurs, ainsi que périphériques génériques. Le modèle de données Inventory inclut plusieurs sous-marins qui vous permettent d'afficher des informations concernant les réplications, les chemins FC, les chemins iSCSI, les chemins NFS et les violations. Le modèle de données d'inventaire n'inclut pas les données historiques. Questions auxquelles vous pouvez répondre avec ces données

- Quels sont les ressources dont je dispose et où sont-elles?
- Qui utilise ces ressources ?
- Quels sont les types d'appareils dont je dispose et quels sont les composants de ces appareils ?
- Combien d'hôtes par système d'exploitation puis-je disposer et combien de ports existent sur ces hôtes ?
- Quelles baies de stockage existent par fournisseur dans chaque data Center ?
- Combien de commutateurs par fournisseur y a-t-il dans chaque data Center ?
- Combien de ports ne sont pas sous licence ?
- Quelles bandes de fournisseurs utilisons-nous et combien de ports existent sur chaque bande ?re tous les périphériques génériques 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 ou les bandes de stockage ?
- Combien de violations de chaque type possède-t-il par data Center ?
- Pour chaque volume répliqué, quels sont les volumes source et cible ?
- Ai-je des incompatibilités de micrologiciel ou des discordances de vitesse de port entre les HBA et les commutateurs hôte Fibre Channel ?

Modèle de données de performance

Répond aux questions de performances des volumes, des volumes d'application, des volumes internes, des commutateurs, des applications Ordinateurs virtuels, VMDK, ESX par rapport aux machines virtuelles, aux hôtes et aux nœuds d'applications. Nombre de ces données de rapport *Hourly*, *Daily* ou les deux. Grâce à 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 au cours d'une période spécifique ?
- Pouvons-nous identifier les erreurs de configuration potentielles du stockage d'une application (non utilisée) ?
- Quel était le comportement d'accès global d'une application ?
- Les volumes hiérarchisés sont-ils affectés de manière appropriée pour une application donnée ?
- Pouvons-nous utiliser un stockage moins coûteux pour une application en cours d'exécution sans affecter les performances des applications ?
- Quelles sont les applications produisant plus d'accès au stockage actuellement configuré ?

Lorsque vous utilisez les tables de performances du commutateur, vous pouvez obtenir les informations suivantes :

- Mon trafic hôte via des ports connectés est-il équilibré ?
- Quels commutateurs ou ports présentent un grand nombre d'erreurs ?
- Quels sont les commutateurs les plus utilisés en fonction des performances du port ?

- Quels sont les commutateurs sous-utilisés basés sur les performances du port ?
- Quel est le débit des tendances hôtes en fonction des performances du port ?
- Quelle est l'utilisation des performances des X derniers jours pour un hôte, un système de stockage, une bande ou un commutateur spécifié ?
- Quels sont les périphériques générant du trafic sur un commutateur spécifique (par exemple, quels sont les périphériques responsables de l'utilisation d'un commutateur hautement utilisé) ?
- Quel est le débit d'une unité commerciale spécifique de notre environnement ?

Lorsque vous utilisez les tables de performances des disques, vous pouvez obtenir les informations suivantes :

- Quel est le débit d'un pool de stockage spécifié basé sur les 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 à l'utilisation d'un système de stockage ou d'un pool de stockage basé sur des données de performances sur disque ?
- Quelles sont les tendances d'utilisation des disques pour un pool de stockage spécifique ?

Lorsque vous utilisez des tables de performances VM et VMDK, vous pouvez obtenir les informations suivantes :

- Mon environnement virtuel fonctionne-t-il de manière optimale ?
- Quels VMDK correspondent aux charges de travail les plus élevées ?
- Comment utiliser les performances rapportées par des VMD mappées sur différents datastores pour prendre des décisions concernant la réorganisation de niveaux.

Le modèle de données performances comprend des informations qui vous aident à déterminer la pertinence des niveaux, les erreurs de configuration du stockage pour les applications, ainsi que les heures de dernier accès des volumes et des volumes internes. Ce modèle de données fournit des données telles que les temps de réponse, les IOPS, le débit, le nombre d'écritures en attente et l'état accédé.

Modèle de données d'efficacité du stockage

Vous permet de suivre le score et le potentiel en matière d'efficacité du stockage dans le temps. Ce modèle de données stocke les mesures de la capacité provisionnée et de la quantité utilisée ou consommée (la mesure physique). Par exemple, lorsque le provisionnement fin est activé, Data Infrastructure Insights indique la capacité prélevée sur le périphérique. Vous pouvez également utiliser ce modèle afin de déterminer l'efficacité lorsque la déduplication est activée. Vous pouvez répondre à diverses questions à l'aide du magasin de données Storage Efficiency :

- Quels sont les économies que nous pouvons réaliser en termes d'efficacité du stockage grâce à l'implémentation des technologies de provisionnement fin et de déduplication ?
- Quelles sont les économies de stockage réalisées dans l'ensemble des data centers ?
- Sur la base des tendances historiques de capacité, à quel moment faut-il acheter du stockage supplémentaire ?
- Quel serait le gain de capacité si nous avions activé des technologies telles que le provisionnement fin et la déduplication ?
- Concernant la capacité de stockage, suis-je en danger maintenant ?

Tableaux de faits et de dimensions des modèles de données

Chaque modèle de données comprend à la fois des tables de faits et de dimensions.

- Tableaux de faits : contiennent des données mesurées, par exemple la quantité, la capacité brute et utilisable. Contiennent des clés étrangères pour les tables de cotes.
- Tables de dimensions : contiennent des informations descriptives sur les faits, par exemple, les centres de données et les business units. Une dimension est une structure, souvent composée de hiérarchies, qui catégorise les données. Les attributs dimensionnels permettent de décrire les valeurs dimensionnelles.

À l'aide d'attributs de cotes différents ou multiples (vus comme des colonnes dans les rapports), vous créez des rapports qui accèdent aux données pour chaque dimension décrite dans le modèle de données.

Couleurs utilisées dans les éléments de modèle de données

Les couleurs des éléments de modèle de données ont des indications différentes.

- Actifs jaunes : représentent les mesures.
- Actifs non jaunes : représentent des attributs. Ces valeurs ne sont pas agrégées.

Utilisation de plusieurs modèles de données dans un rapport

Généralement, vous utilisez un modèle de données par rapport. Toutefois, vous pouvez écrire un rapport qui combine des données de plusieurs modèles de données.

Pour écrire un rapport qui combine des données 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 magasins de données supplémentaires. Vous pouvez utiliser la fonction jonction SQL pour combiner les données des différentes requêtes dans une seule requête que vous pouvez utiliser pour écrire le rapport.

Imaginons par exemple que vous souhaitiez disposer de la capacité actuelle de chaque baie de stockage et que vous souhaitez 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 et dimension actuelles et ajouter une requête SQL séparée pour accéder aux informations d'annotations dans le modèle de données Inventory. Enfin, vous pouvez combiner les données en reliant les données de stockage d'inventaire à la table 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

La puissante API de Data Infrastructure Insights permet aux utilisateurs d'interroger directement la base de données de rapports Data Infrastructure Insights, sans passer par l'environnement de reporting Cognos.

Cette documentation fait référence à la fonctionnalité de reporting Data Infrastructure Insights, disponible dans Data Infrastructure Insights Premium Edition.

OData

L'API de génération de rapports Data Infrastructure Insights suit "OData v4"la norme (Open Data Protocol) pour l'interrogation de la base de données Reporting. Pour plus d'informations ou pour en savoir plus, consultez "ce tutoriel"OData.

Toutes les demandes commenceront par l'url *https://<Data Infrastructure Insights URL>/REST/v1/dwh-*

management/odata

Génération d'une clé APIKey

En savoir plus sur "API Data Infrastructure Insights".

Pour générer une clé API, procédez comme suit :

- Connectez-vous à votre environnement Data Infrastructure Insights et sélectionnez **Admin > API Access**.
- Cliquez sur "+ jeton d'accès à l'API ".
- Entrez un nom et une description.
- Pour le type, choisissez *Data Warehouse*.
- Définir les autorisations comme lecture/écriture.
- Définissez une date d'expiration de désirs.
- Cliquez sur "Enregistrer", puis **copiez la clé et enregistrez-la** quelque part en toute sécurité. Vous ne pourrez plus accéder à la clé complète ultérieurement.

Les APIkeys sont bons pour *Sync* ou *Async*.

Requête directe des tables

Une fois la clé API en place, les requêtes directes de la base de données de rapports sont désormais possibles. Les URL longues peuvent être simplifiées vers https://…/odata/ pour l'affichage plutôt que l'URL complète https://<Data Infrastructure Insights>/REST/v1/dwh-management/odata/

Essayez des requêtes simples comme

- URL d'informations sur l'infrastructure https://<Data>/REST/v1/dwh-management/odata/dwh_custom
- URL d'informations sur l'infrastructure https://<Data>/REST/v1/dwh-management/odata/dwh_Inventory
- URL d'informations sur l'infrastructure https://<Data>/REST/v1/dwh-management/odata/dwh_Inventory/Storage
- URL de https://<Data Infrastructure Insights>/REST/v1/dwh-management/odata/dwh_Inventory/disk
- https://…/odata/dwh_custom/custom_queries

Exemples d'API REST

L'URL de tous les appels est *https://<Data Infrastructure Insights URL>/REST/v1/dwh-management/odata*.

- OBTENIR /{schema}/** - récupère les données de la base de données de rapports.

Format : *URL de l'analyse de l'infrastructure https://<Data>/REST/v1/dwh-management/odata/<schema_name>/<query>*

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 à l'esprit les éléments suivants lorsque vous utilisez des requêtes de l'API de reporting.

- 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 doivent être échappés, par exemple \"
- Les onglets sont pris en charge sous la forme \t
- Évitez les commentaires
- Les noms de tables en minuscules sont pris en charge

En outre :

- 2 en-têtes sont nécessaires :
  - Nom « X-CloudInsights-ApiKey »
  - Attribut valeur «<apikey> »

Votre clé d'API sera spécifique à votre environnement Data Infrastructure Insights.

Synchrone ou asynchrone ?

Par défaut, une commande API fonctionne en mode *synchrone*, ce qui signifie que vous envoyez la demande et que la réponse est immédiatement renvoyée. Cependant, l'exécution d'une requête peut parfois prendre un certain temps, ce qui peut entraîner la temporisation de la requête. Pour contourner ce problème, vous pouvez exécuter une requête *de manière _asynchrone*. En mode asynchrone, la demande renvoie une URL par laquelle l'exécution peut être surveillée. L'URL renvoie le résultat lorsqu'il est prêt.

Pour exécuter une requête en mode asynchrone, ajoutez l'en-tête **`Prefer: respond-async`** à la requête. 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>
```

Si vous interrogez l'URL de l'emplacement, les mêmes en-têtes seront retournés si la réponse n'est pas encore prête ou si l'état 200 est prêt. Le contenu de la réponse sera de type texte et contient l'état http de la requête d'origine et certaines métadonnées, suivies 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 afficher la liste de toutes les requêtes asynchrones et savoir lesquelles 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
       }
   ]
}
```

Conservation des données historiques pour les rapports

Data Infrastructure Insights conserve les données historiques à utiliser dans Reporting en fonction des magasins de données et de la granularité des données, comme indiqué dans le tableau suivant.

Un data Mart	Objet mesuré	Granularité	Durée de conservation
Marts de performance	Volumes et volumes internes	Horaire	14 jours
Marts de performance	Volumes et volumes internes	Tous les jours	13 mois
Marts de performance	Client supplémentaire	Horaire	13 mois
Marts de performance	Hôte	Horaire	13 mois
Marts de performance	Performances du commutateur pour le port	Horaire	35 jours
Marts de performance	Performances de commutateur pour l'hôte, le stockage et les bandes	Horaire	13 mois
Marts de performance	Nœud de stockage	Horaire	14 jours
Marts de performance	Nœud de stockage	Tous les jours	13 mois
Marts de performance	Performances des machines virtuelles	Horaire	14 jours
Marts de performance	Performances des machines virtuelles	Tous les jours	13 mois
Marts de performance	Performances de l'hyperviseur	Horaire	35 jours
Marts de performance	Performances de l'hyperviseur	Tous les jours	13 mois

Marts de performance	Performances VMDK	Horaire	35 jours
Marts de performance	Performances VMDK	Tous les jours	13 mois
Marts de performance	Performances des disques	Horaire	14 jours
Marts de performance	Performances des disques	Tous les jours	13 mois
Marts de capacité	Tous (sauf volumes individuels)	Tous les jours	13 mois
Marts de capacité	Tous (sauf volumes individuels)	Représentant mensuel	14 mois et plus
Marts d'inventaire	Volumes individuels	État actuel	1 jour (ou jusqu'au prochain CÉC)

Diagrammes de schéma de reporting des informations d'infrastructure de données

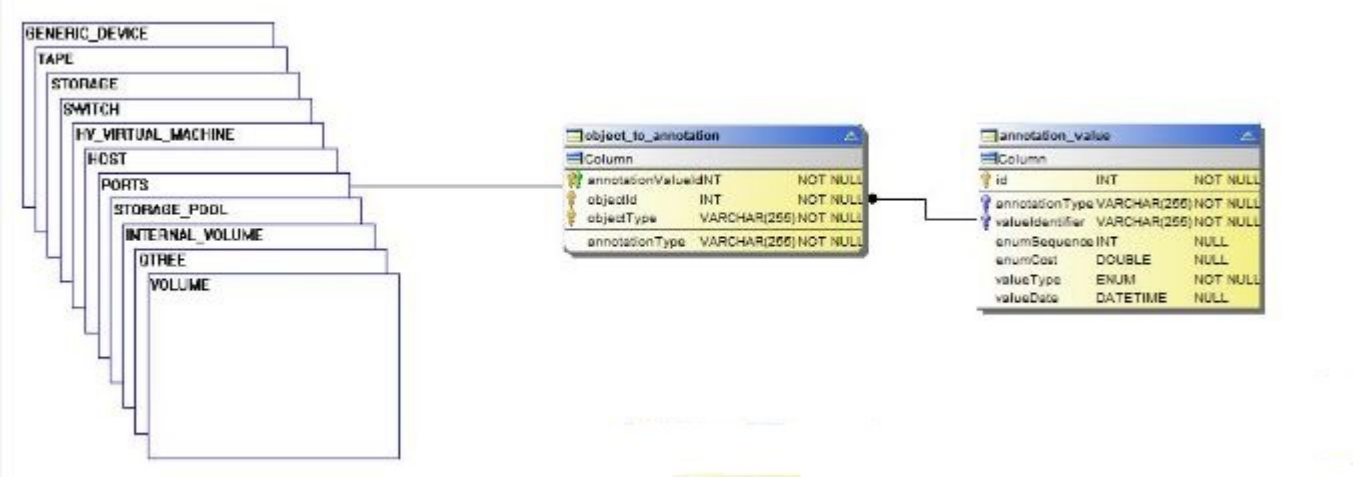
Ce document fournit des diagrammes de schéma pour la base de données de rapports.

La fonction de génération de rapports est disponible dans Data Infrastructure Insights "Édition Premium".

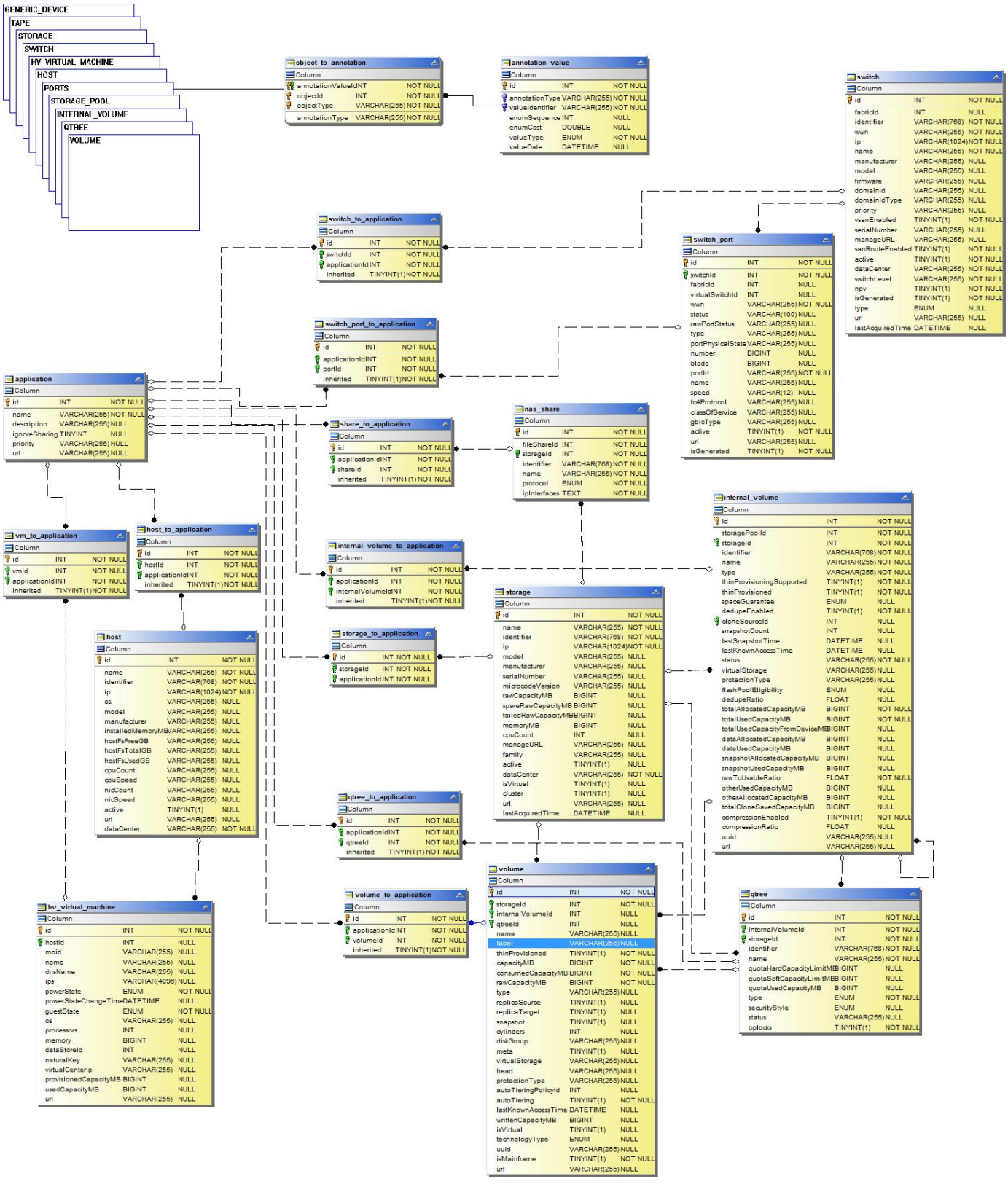
Données d'inventaire

Les images suivantes décrivent le datamart de l'inventaire.

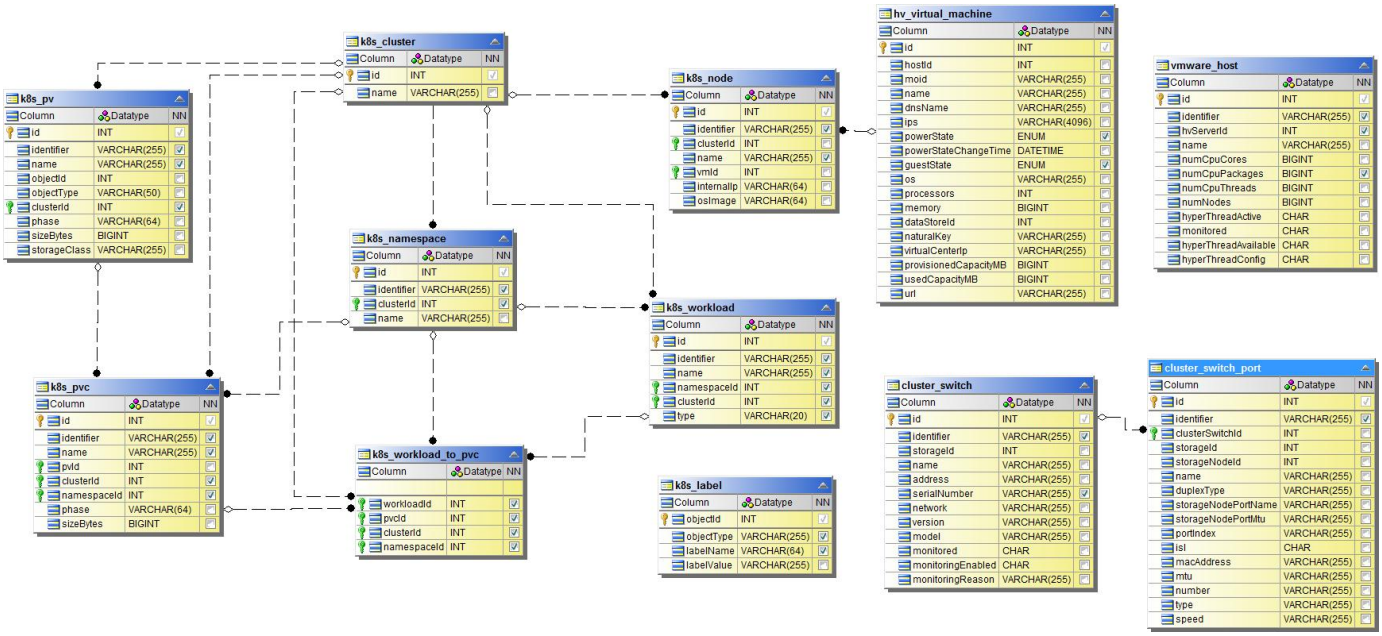
Annotations



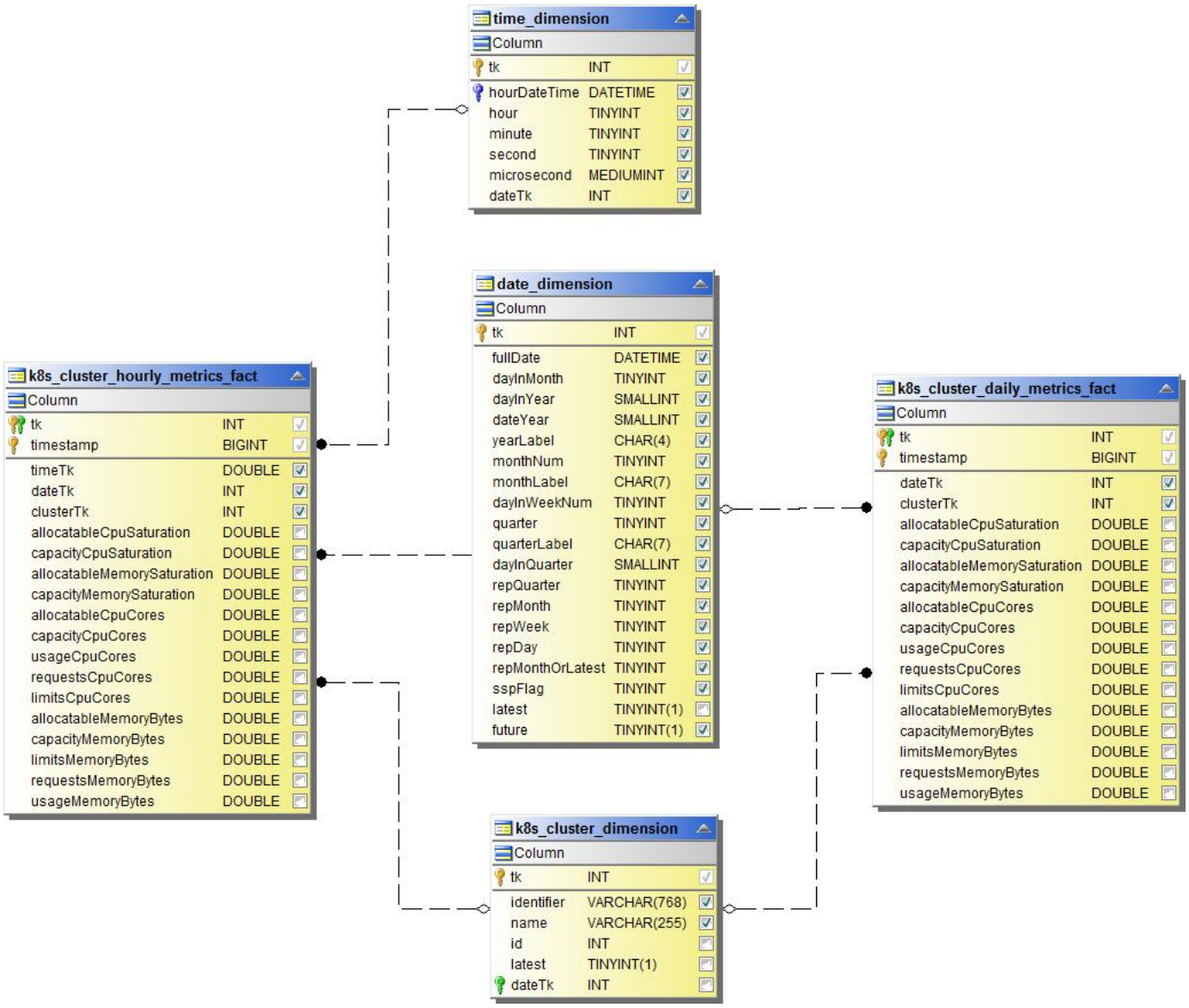
En termes de latence



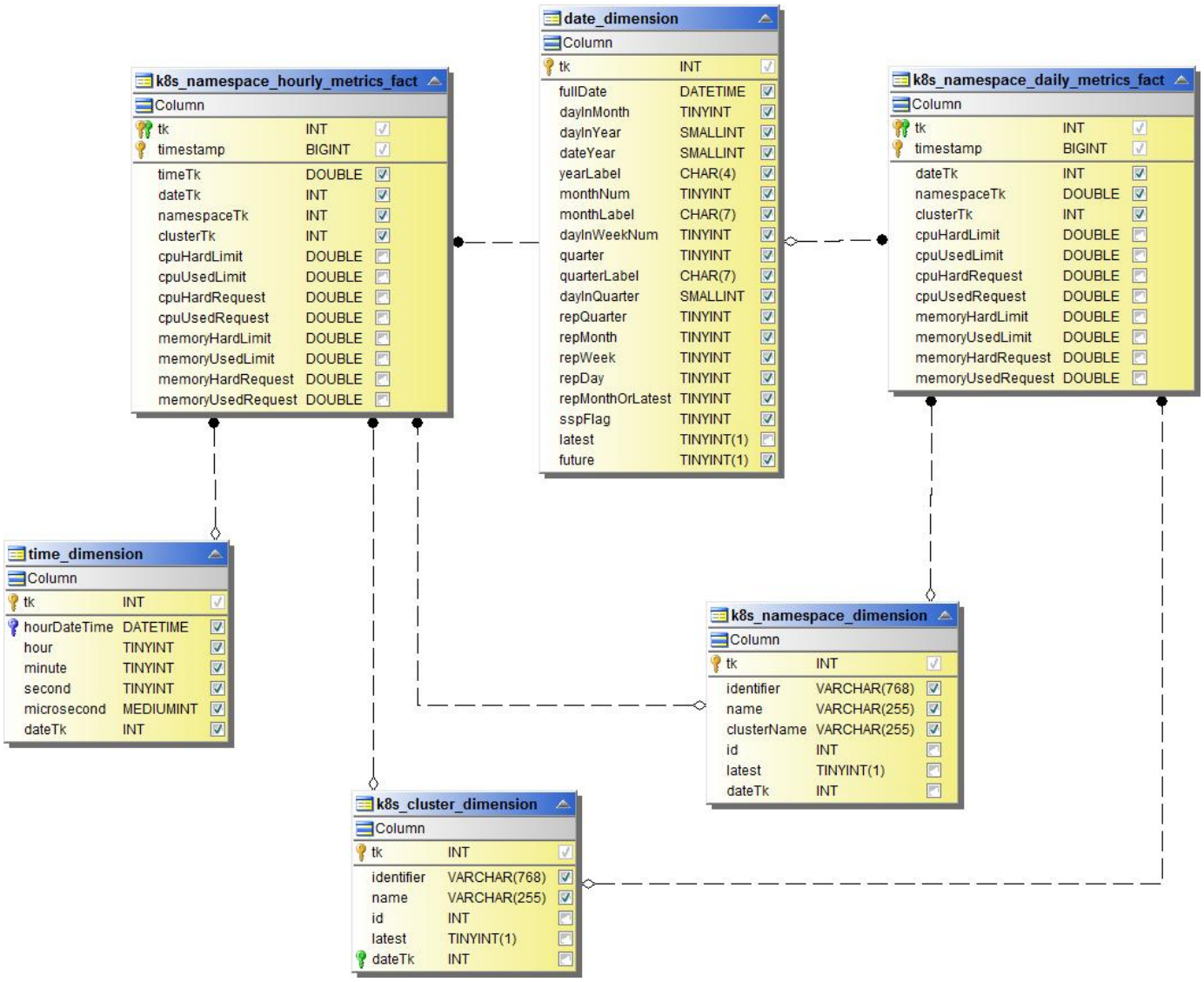
Metrics Kubernetes



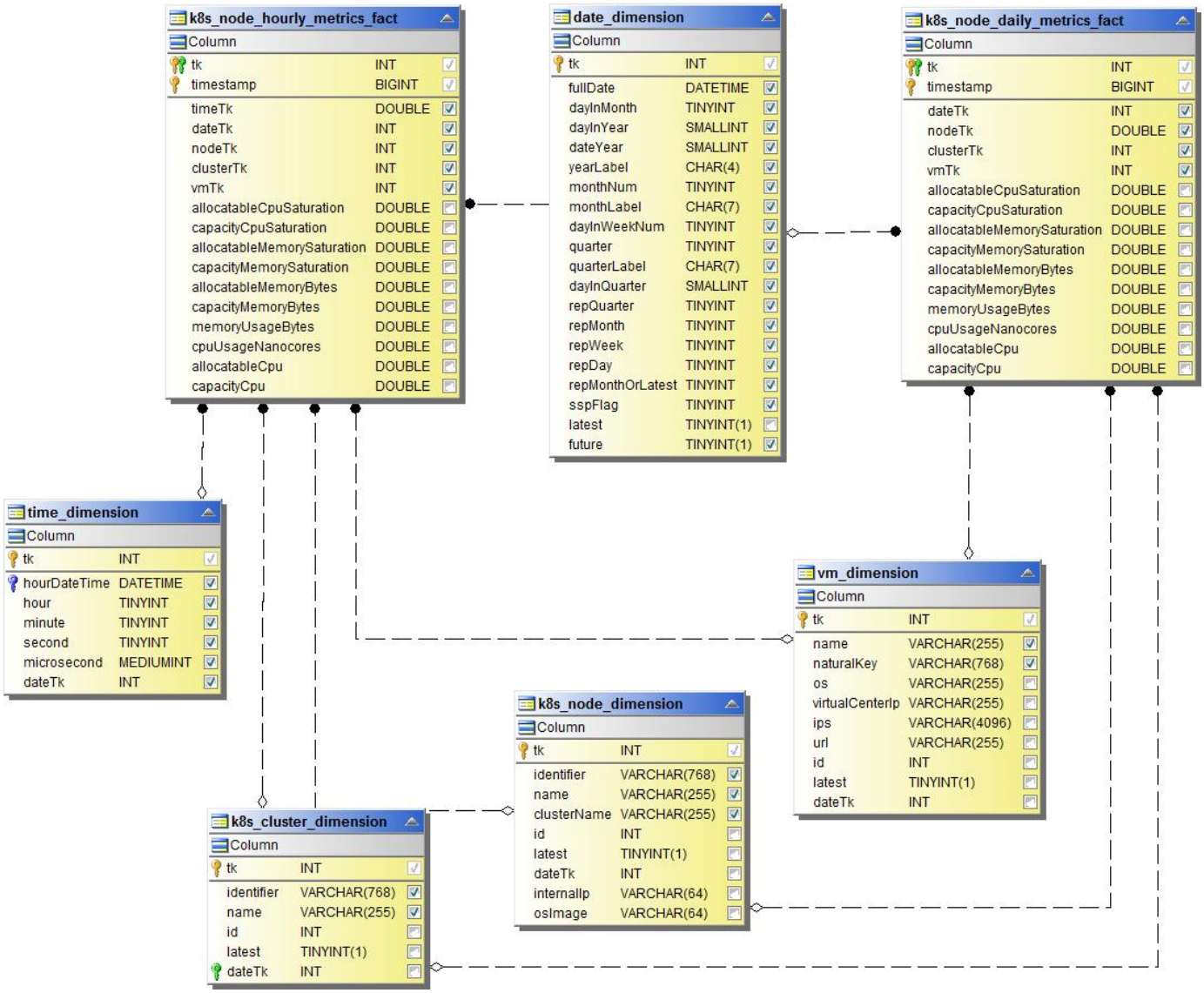
Metrics de cluster Kubernetes



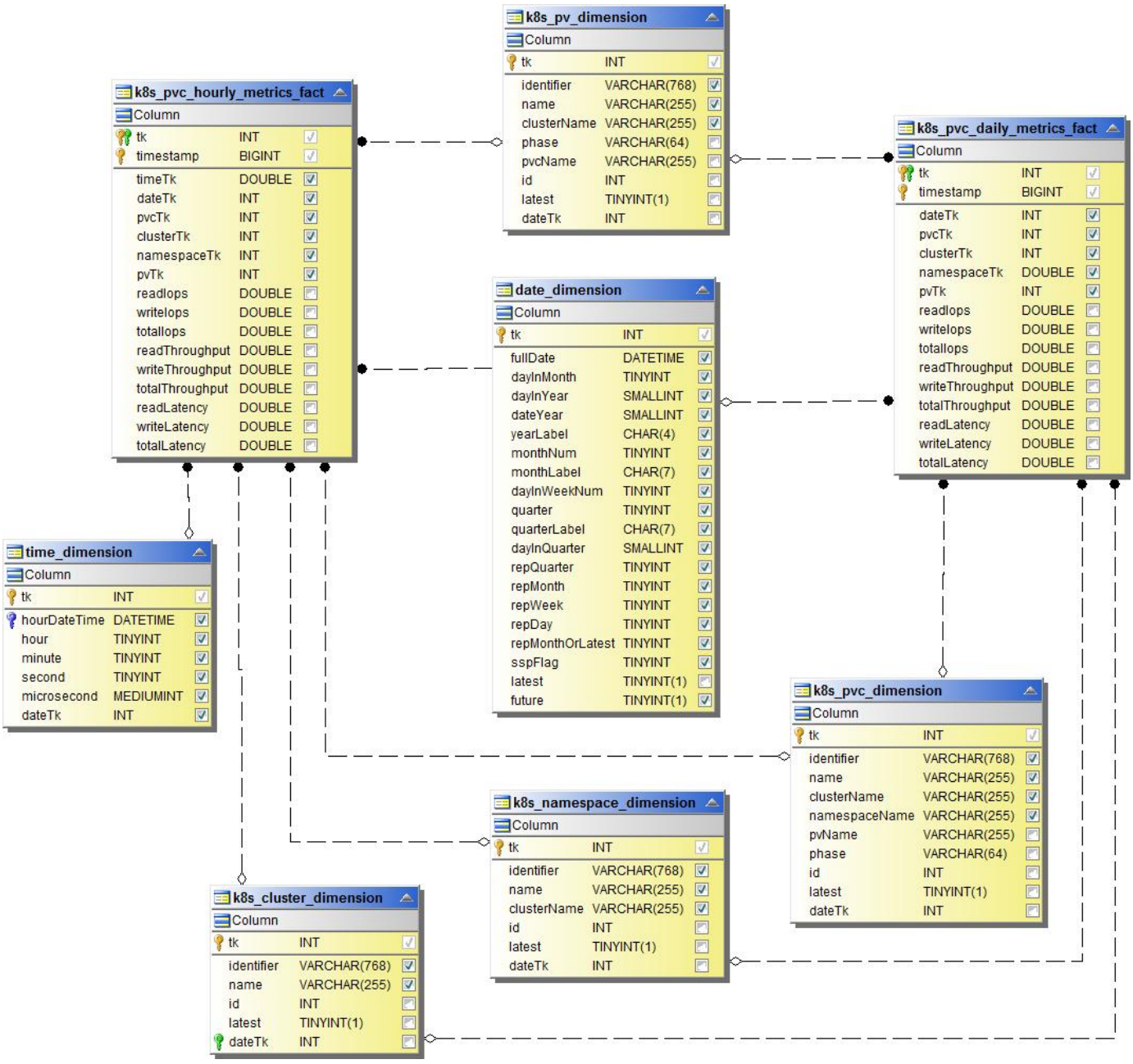
Données chiffrées de l’espace de noms Kubernetes



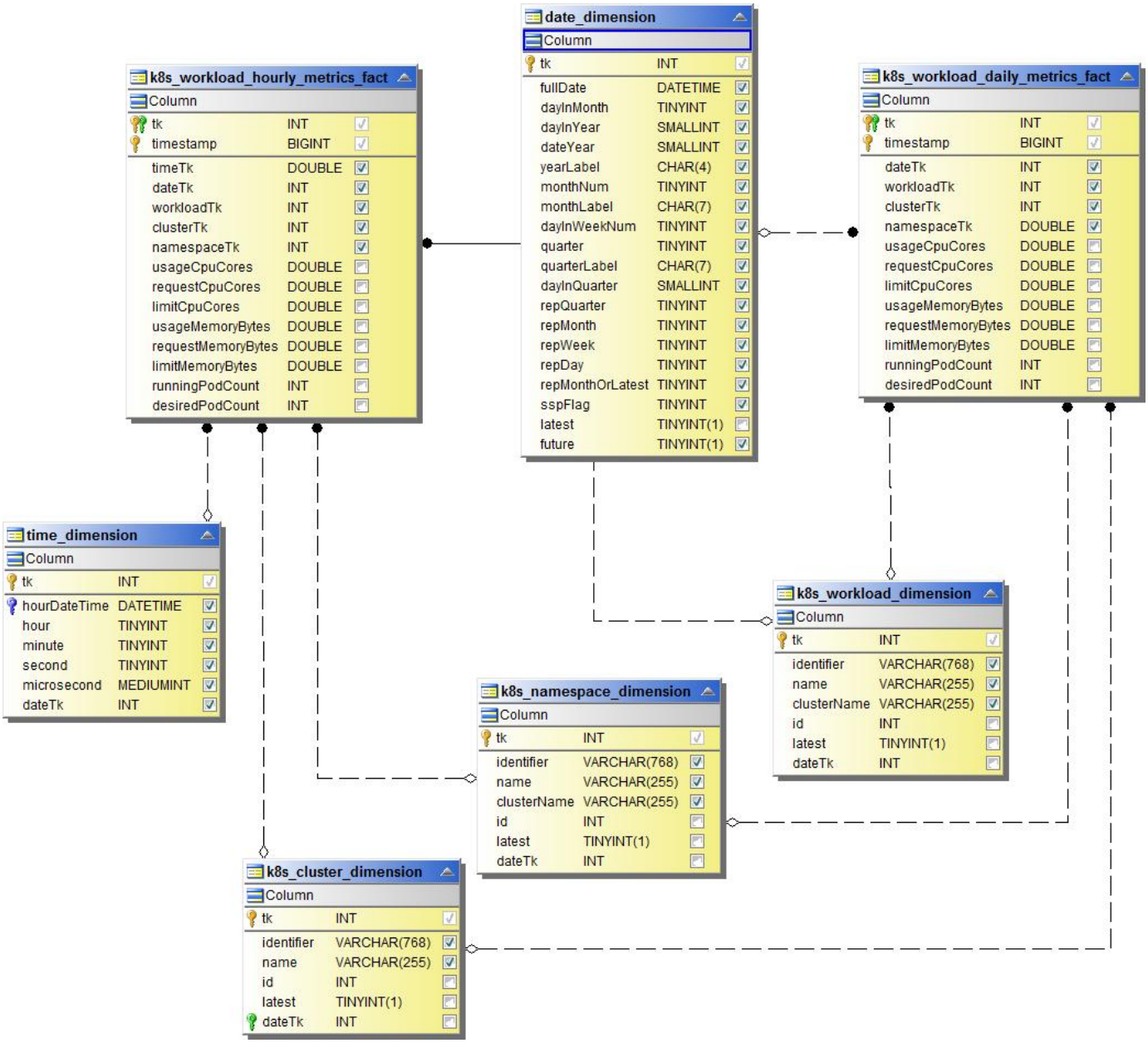
Metrics des nœuds Kubernetes



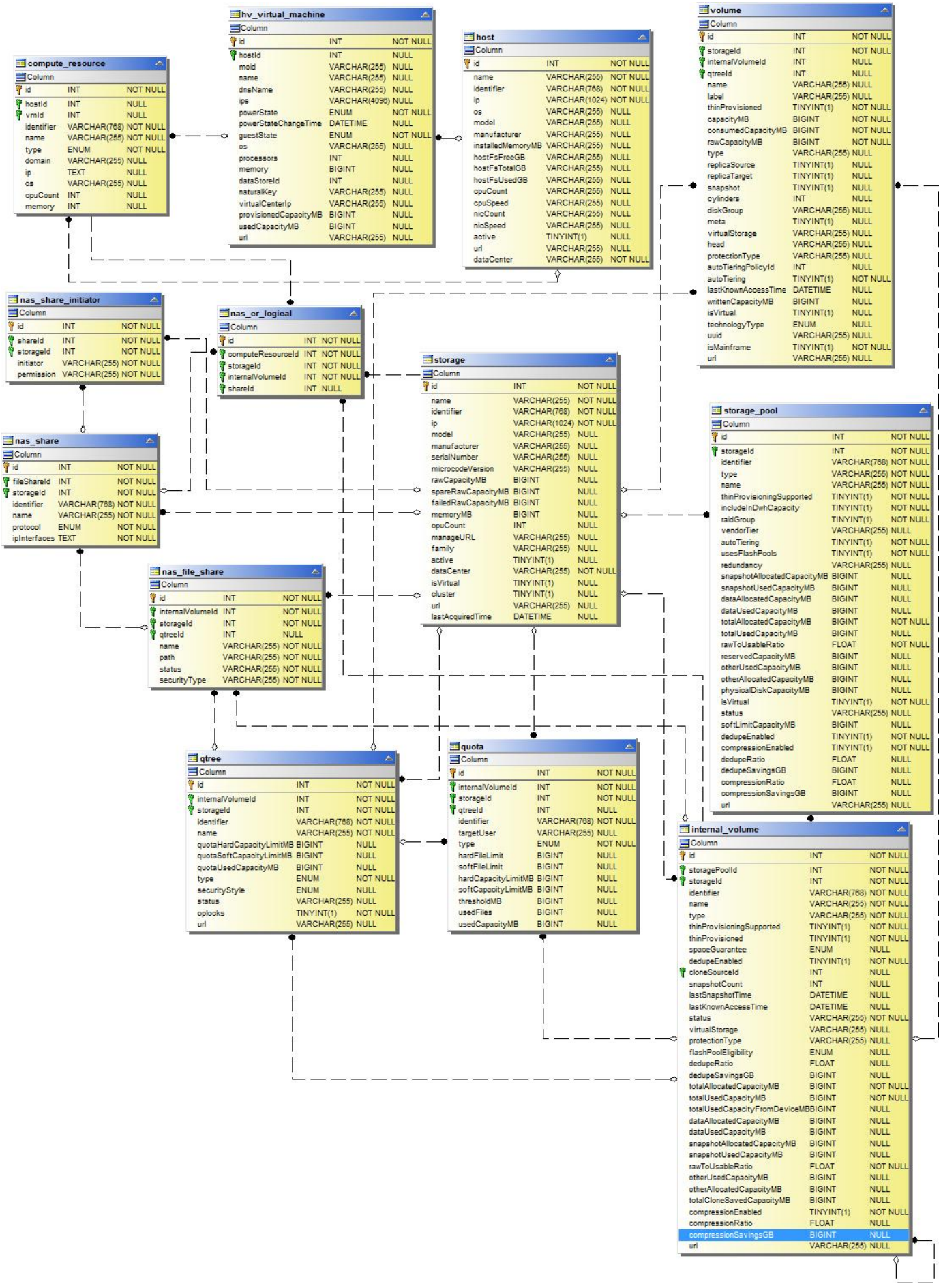
Informations sur les metrics de PVC Kubernetes



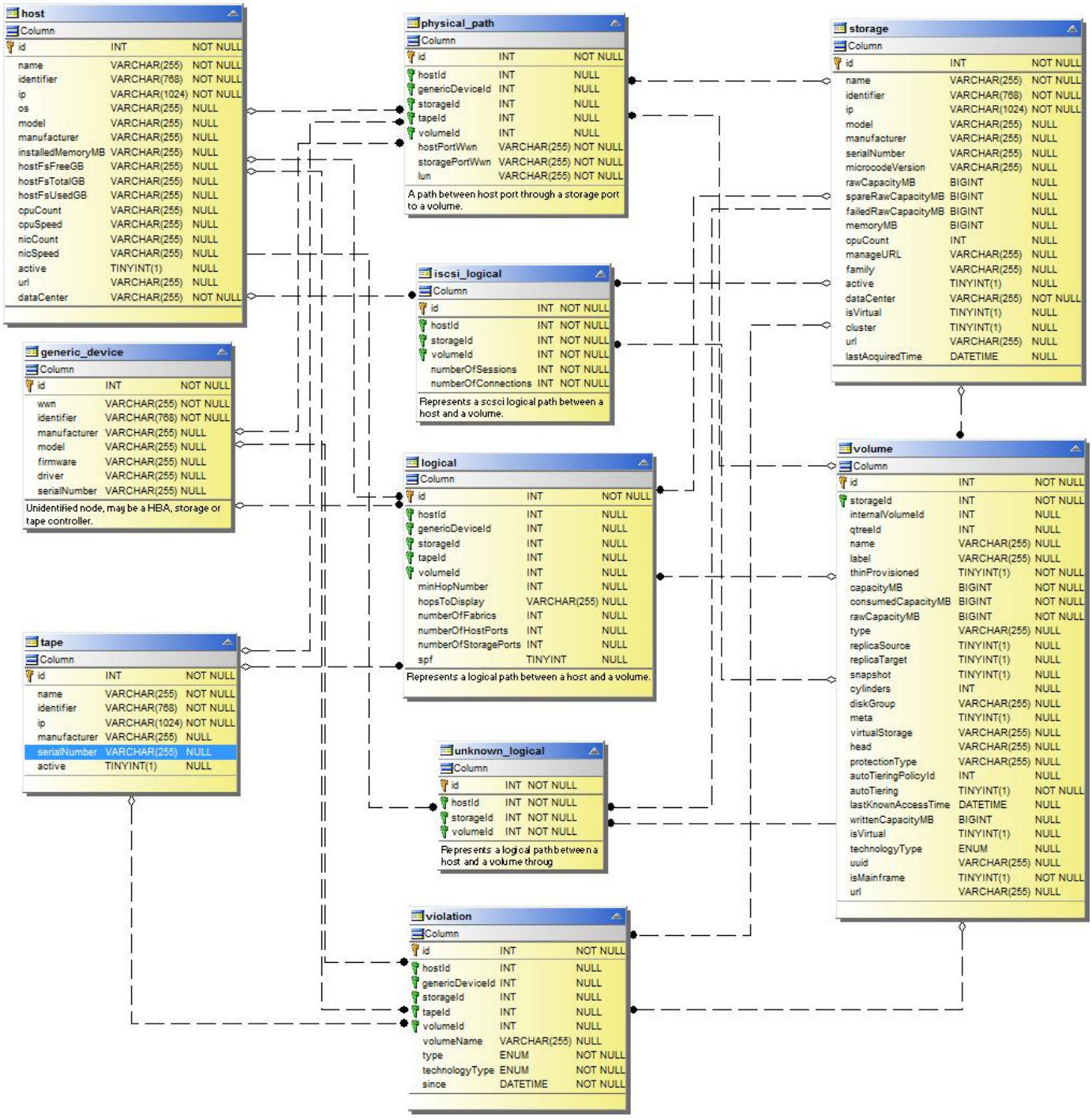
Réalité des metrics des workloads Kubernetes


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

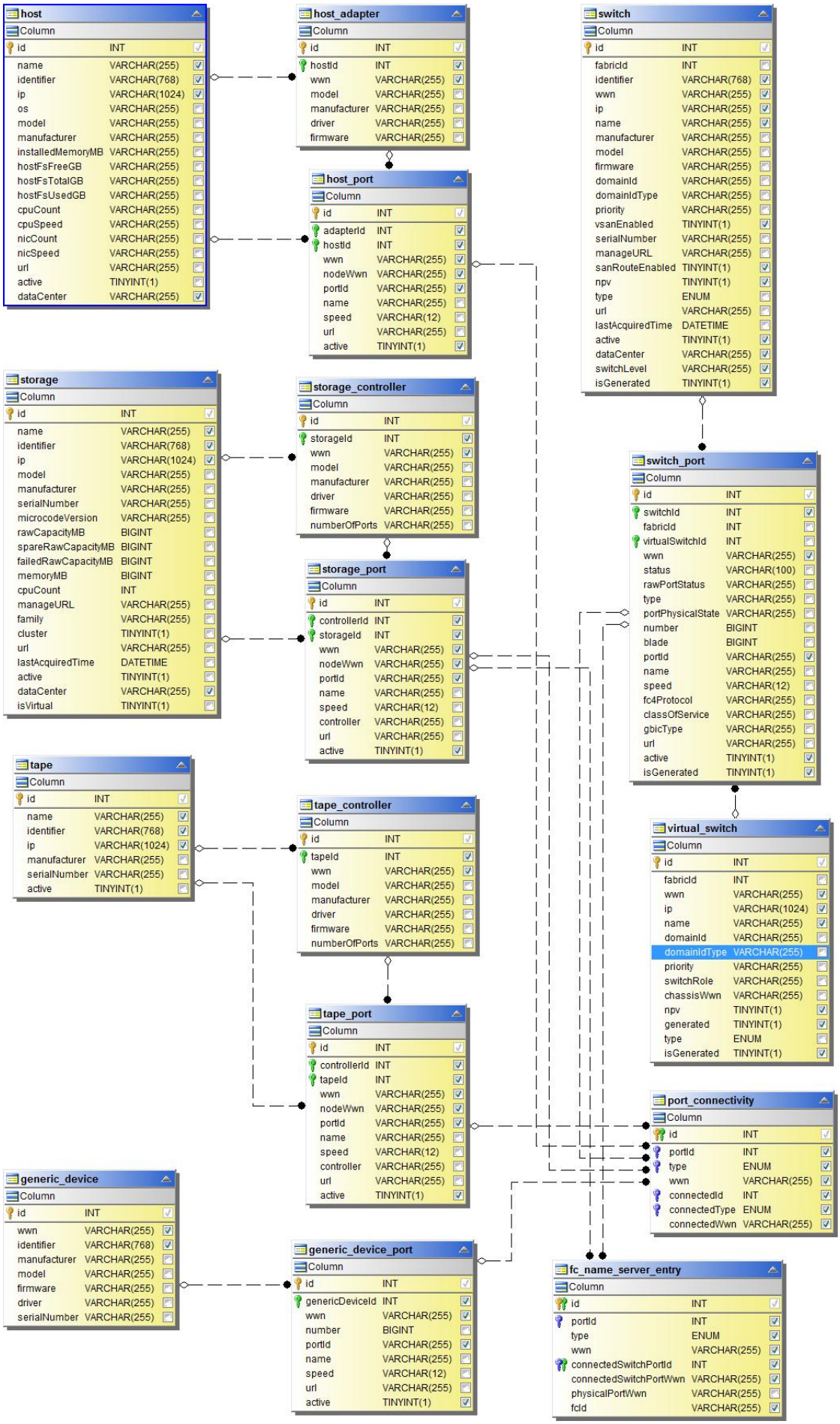
NAS


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

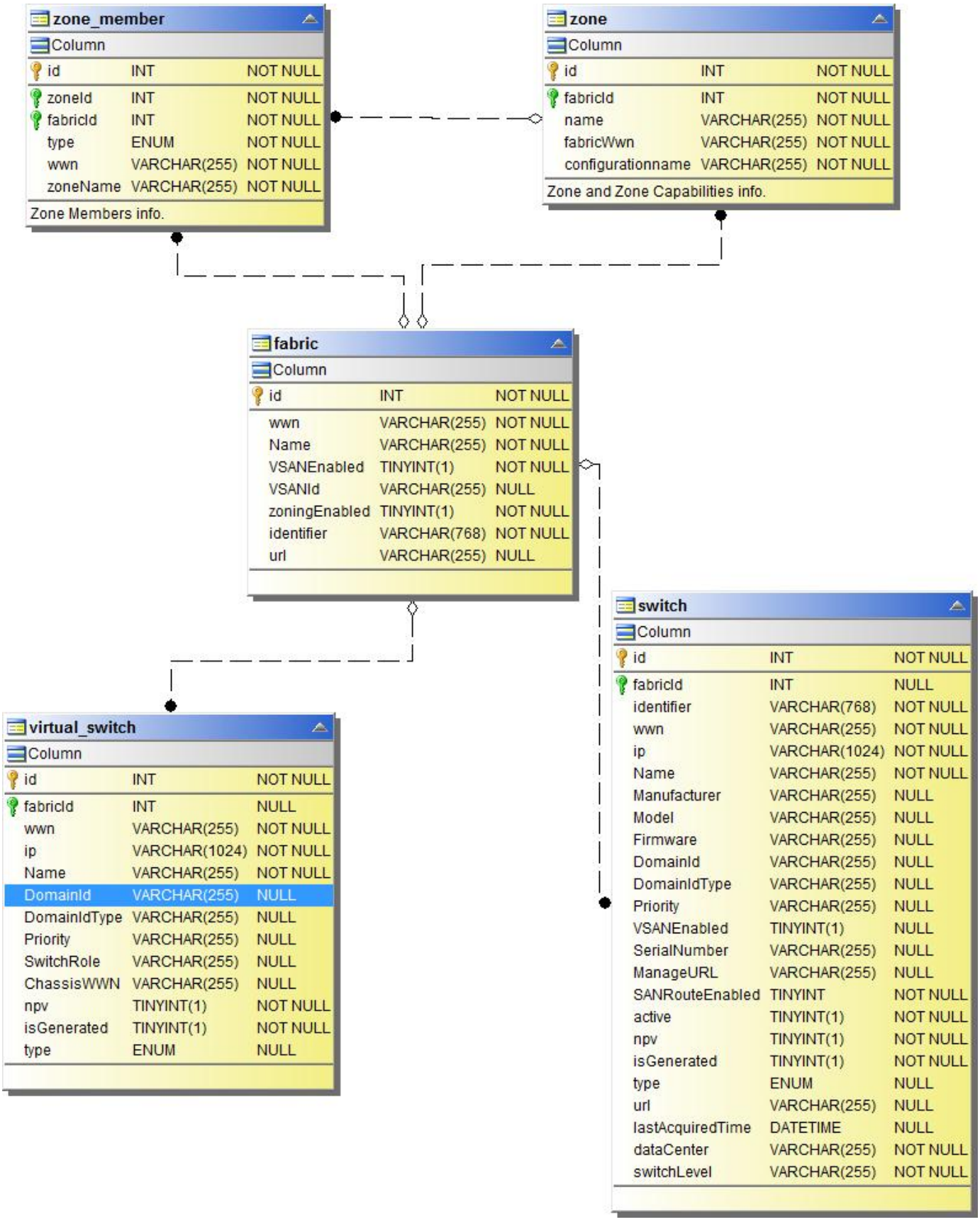
Chemins et violations



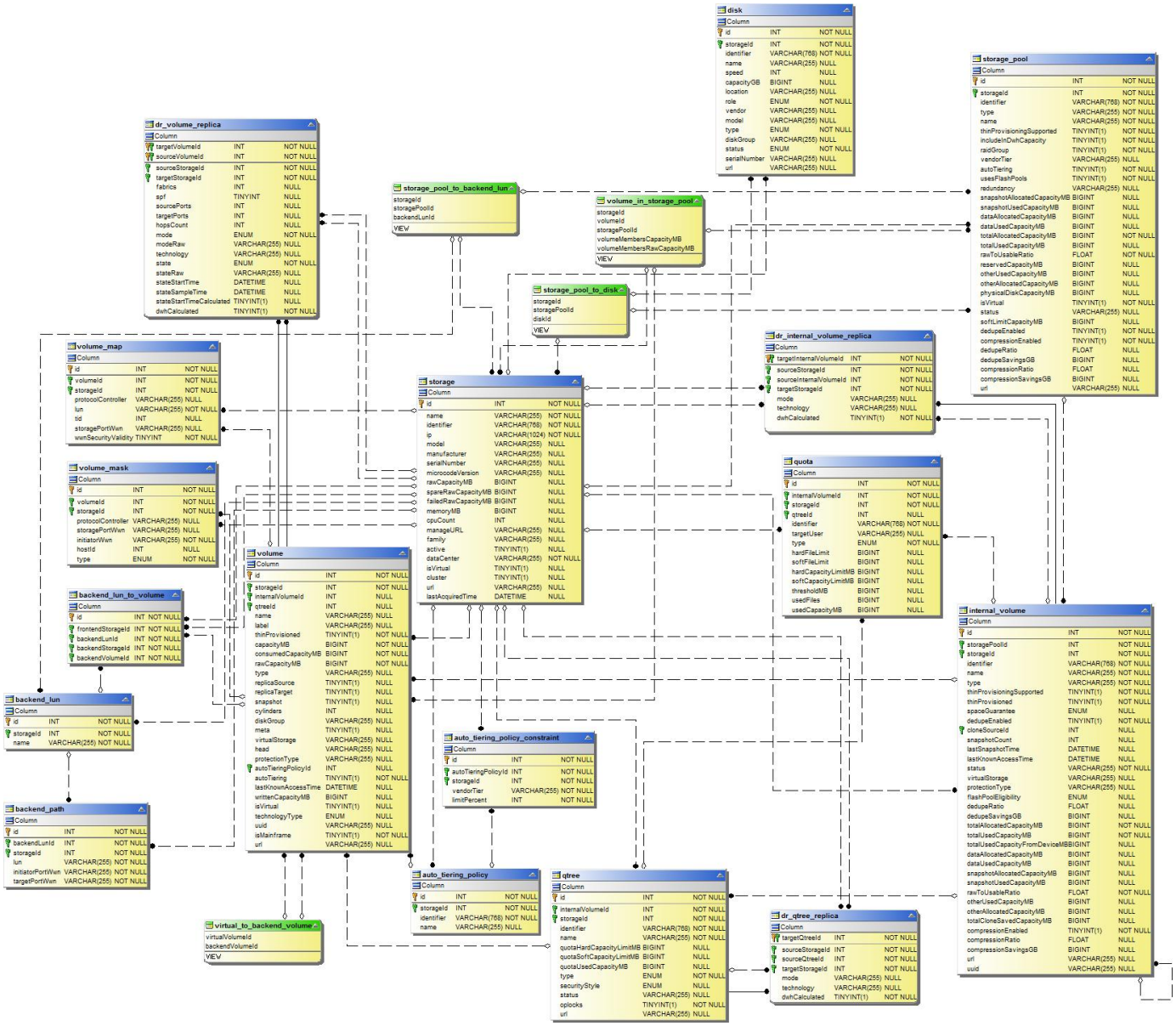
Connectivité des ports


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)
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)
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)
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)

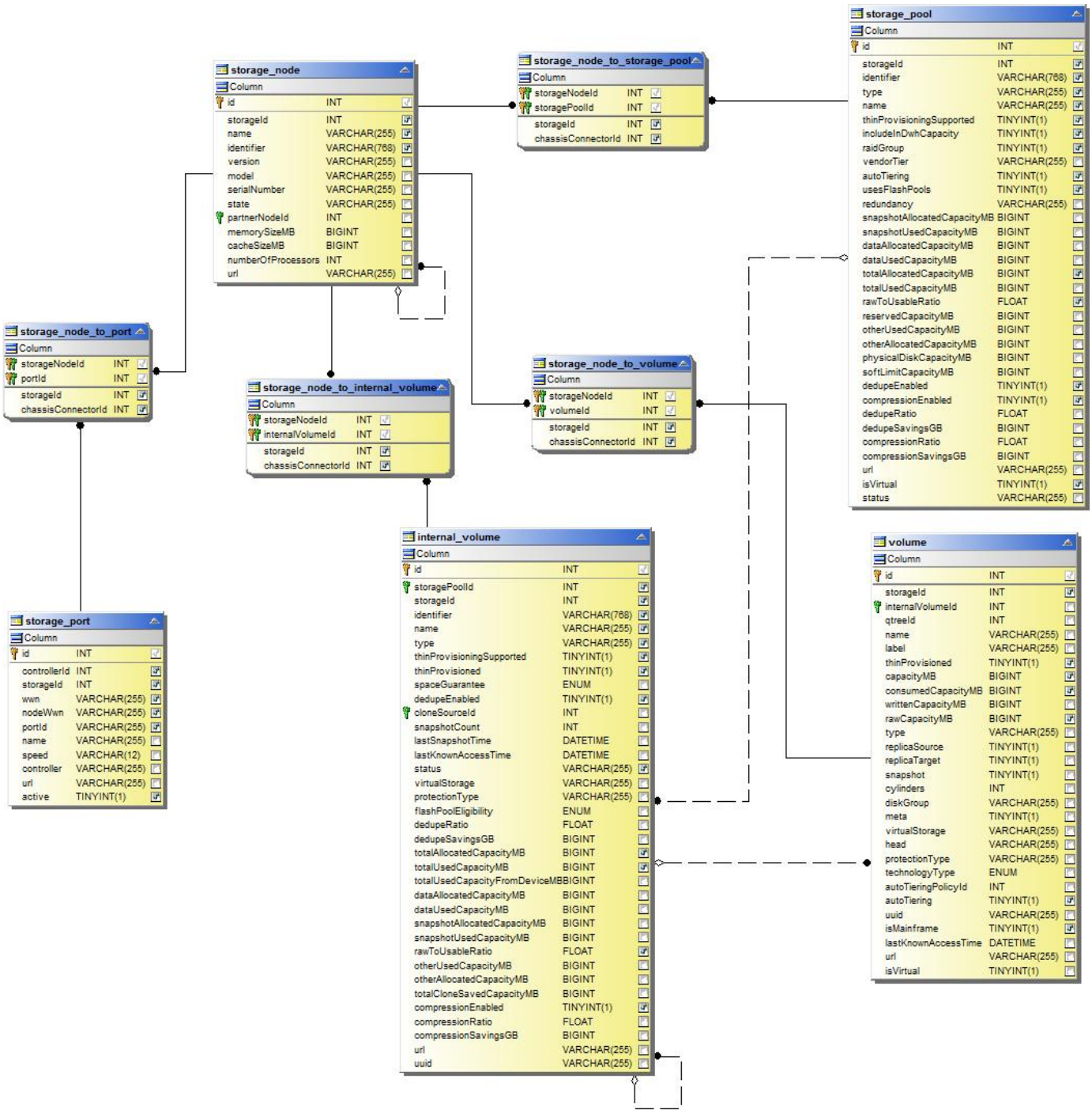
Structure SAN



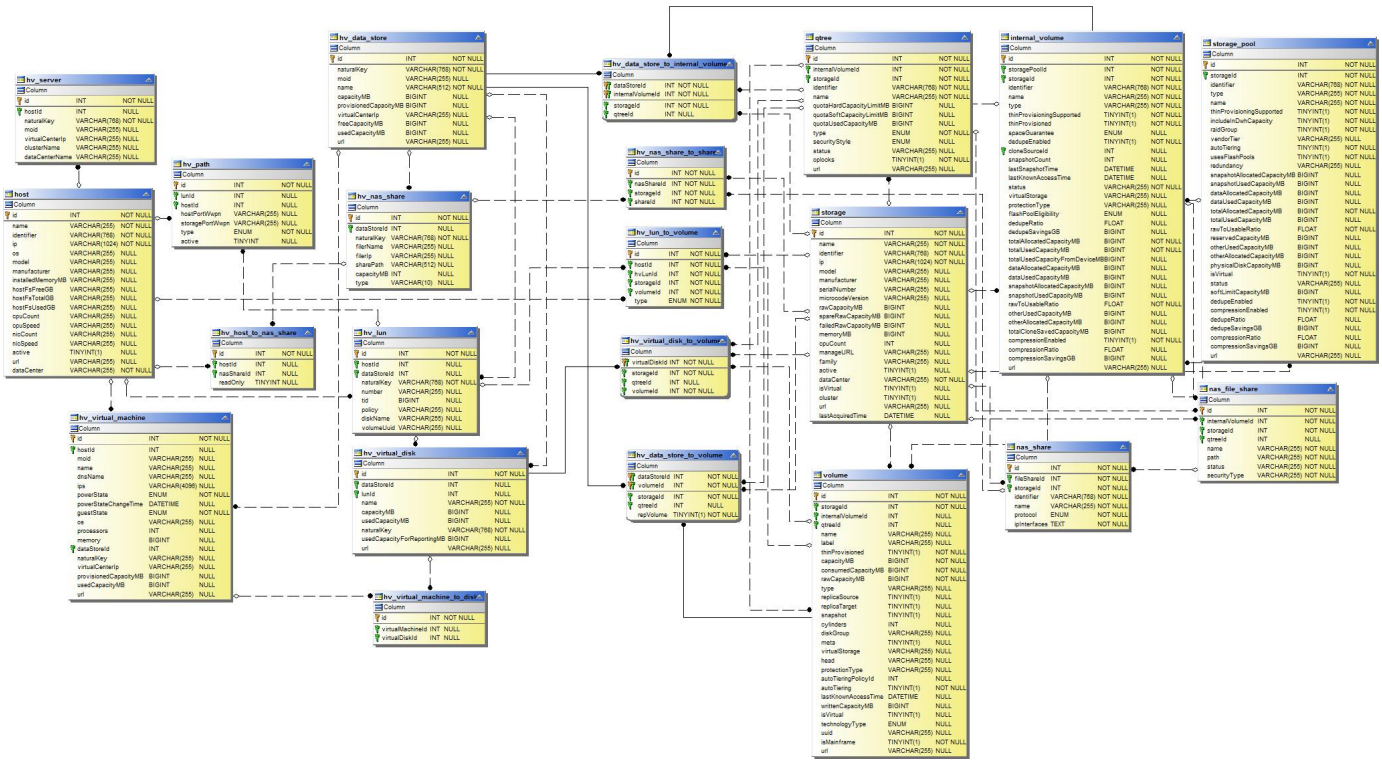
Stockage



Nœud de stockage


storage_node
Column
id INT
storageId INT
name VARCHAR(255)
identifier VARCHAR(768)
version VARCHAR(255)
model VARCHAR(255)
serialNumber VARCHAR(255)
state VARCHAR(255)
partnerNodeId INT
memorySizeMB BIGINT
cacheSizeMB BIGINT
numberOfProcessors INT
url VARCHAR(255)
storage_node_to_storage_pool
Column
storageNodeId INT
storagePoolId INT
storageId INT
chassisConnectorId INT
storage_pool
Column
id INT
storageId INT
identifier VARCHAR(768)
type VARCHAR(255)
name VARCHAR(255)
thinProvisioningSupported TINYINT(1)
includeInDwhCapacity TINYINT(1)
raidGroup TINYINT(1)
vendorTier VARCHAR(255)
autoTiering TINYINT(1)
usesFlashPools TINYINT(1)
redundancy VARCHAR(255)
snapshotAllocatedCapacityMB BIGINT
snapshotUsedCapacityMB BIGINT
dataAllocatedCapacityMB BIGINT
dataUsedCapacityMB BIGINT
totalAllocatedCapacityMB BIGINT
totalUsedCapacityMB BIGINT
rawToUsableRatio FLOAT
reservedCapacityMB BIGINT
otherUsedCapacityMB BIGINT
otherAllocatedCapacityMB BIGINT
physicalDiskCapacityMB BIGINT
softLimitCapacityMB BIGINT
dedupeEnabled TINYINT(1)
compressionEnabled TINYINT(1)
dedupeRatio FLOAT
dedupeSavingsGB BIGINT
compressionRatio FLOAT
compressionSavingsGB BIGINT
url VARCHAR(255)
isVirtual TINYINT(1)
status VARCHAR(255)
storage_node_to_port
Column
storageNodeId INT
portId INT
storageId INT
chassisConnectorId INT
storage_node_to_internal_volume
Column
storageNodeId INT
internalVolumeId INT
storageId INT
chassisConnectorId INT
storage_node_to_volume
Column
storageNodeId INT
volumeId INT
storageId INT
chassisConnectorId INT
internal_volume
Column
id INT
storagePoolId INT
storageId INT
identifier VARCHAR(768)
name VARCHAR(255)
type VARCHAR(255)
thinProvisioningSupported TINYINT(1)
thinProvisioned TINYINT(1)
spaceGuarantee ENUM
dedupeEnabled TINYINT(1)
cloneSourceId INT
snapshotCount INT
lastSnapshotTime DATETIME
lastKnownAccessTime DATETIME
status VARCHAR(255)
virtualStorage VARCHAR(255)
protectionType VARCHAR(255)
flashPoolEligibility ENUM
dedupeRatio FLOAT
dedupeSavingsGB BIGINT
totalAllocatedCapacityMB BIGINT
totalUsedCapacityMB BIGINT
totalUsedCapacityFromDeviceMB BIGINT
dataAllocatedCapacityMB BIGINT
dataUsedCapacityMB BIGINT
snapshotAllocatedCapacityMB BIGINT
snapshotUsedCapacityMB BIGINT
rawToUsableRatio FLOAT
otherUsedCapacityMB BIGINT
otherAllocatedCapacityMB BIGINT
totalCloneSavedCapacityMB BIGINT
compressionEnabled TINYINT(1)
compressionRatio FLOAT
compressionSavingsGB BIGINT
url VARCHAR(255)
uuid VARCHAR(255)
volume
Column
id INT
storageId INT
internalVolumeId INT
qtreeId INT
name VARCHAR(255)
label VARCHAR(255)
thinProvisioned TINYINT(1)
capacityMB BIGINT
consumedCapacityMB BIGINT
writtenCapacityMB BIGINT
rawCapacityMB BIGINT
type VARCHAR(255)
replicaSource TINYINT(1)
replicaTarget TINYINT(1)
snapshot TINYINT(1)
cylinders INT
diskGroup VARCHAR(255)
meta TINYINT(1)
virtualStorage VARCHAR(255)
head VARCHAR(255)
protectionType VARCHAR(255)
technologyType ENUM
autoTieringPolicyId INT
autoTiering TINYINT(1)
uuid VARCHAR(255)
isMainframe TINYINT(1)
lastKnownAccessTime DATETIME
url VARCHAR(255)
isVirtual TINYINT(1)
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)

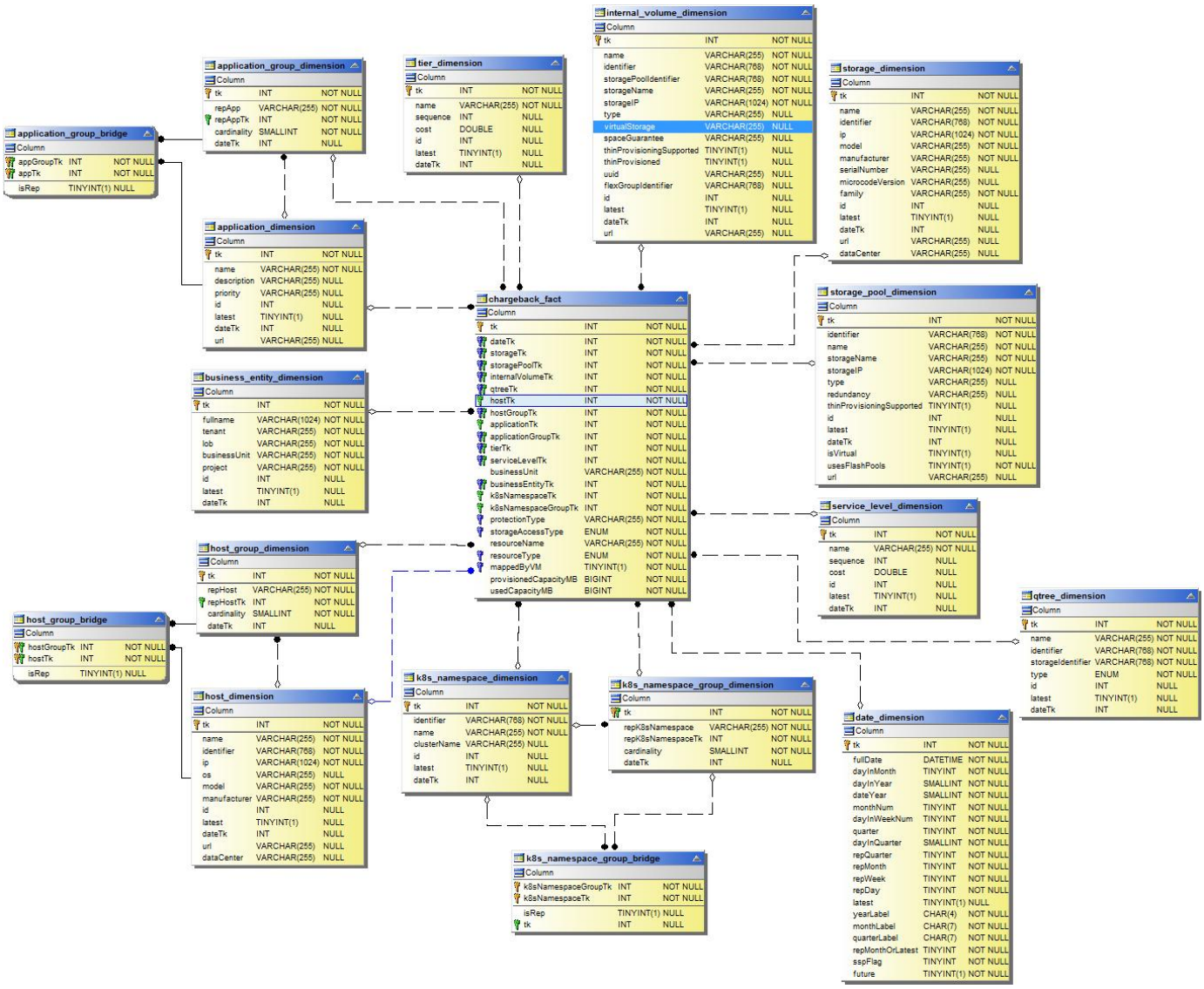
VM



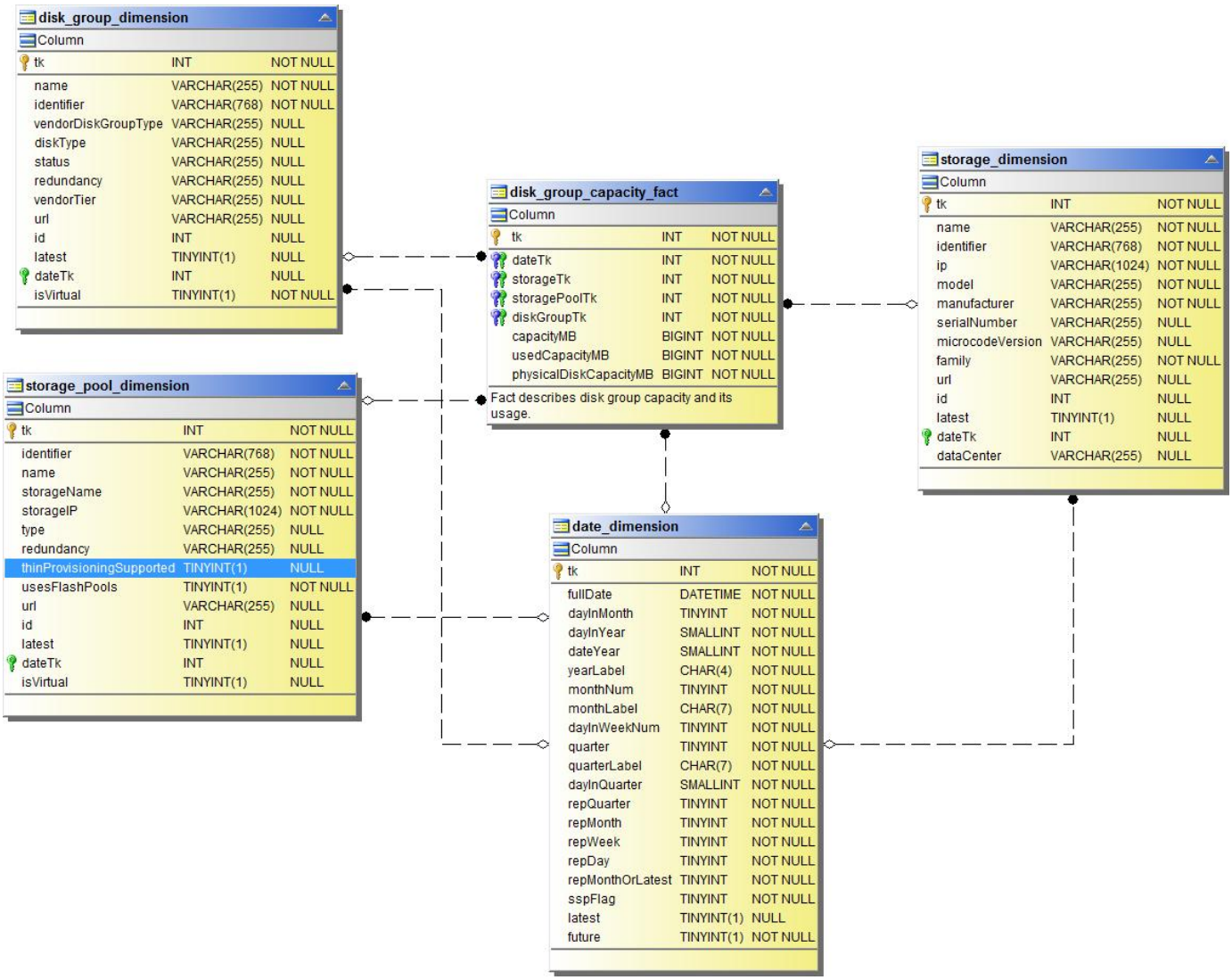
Capacité Datamart

Les images suivantes décrivent la capacité du datamart.

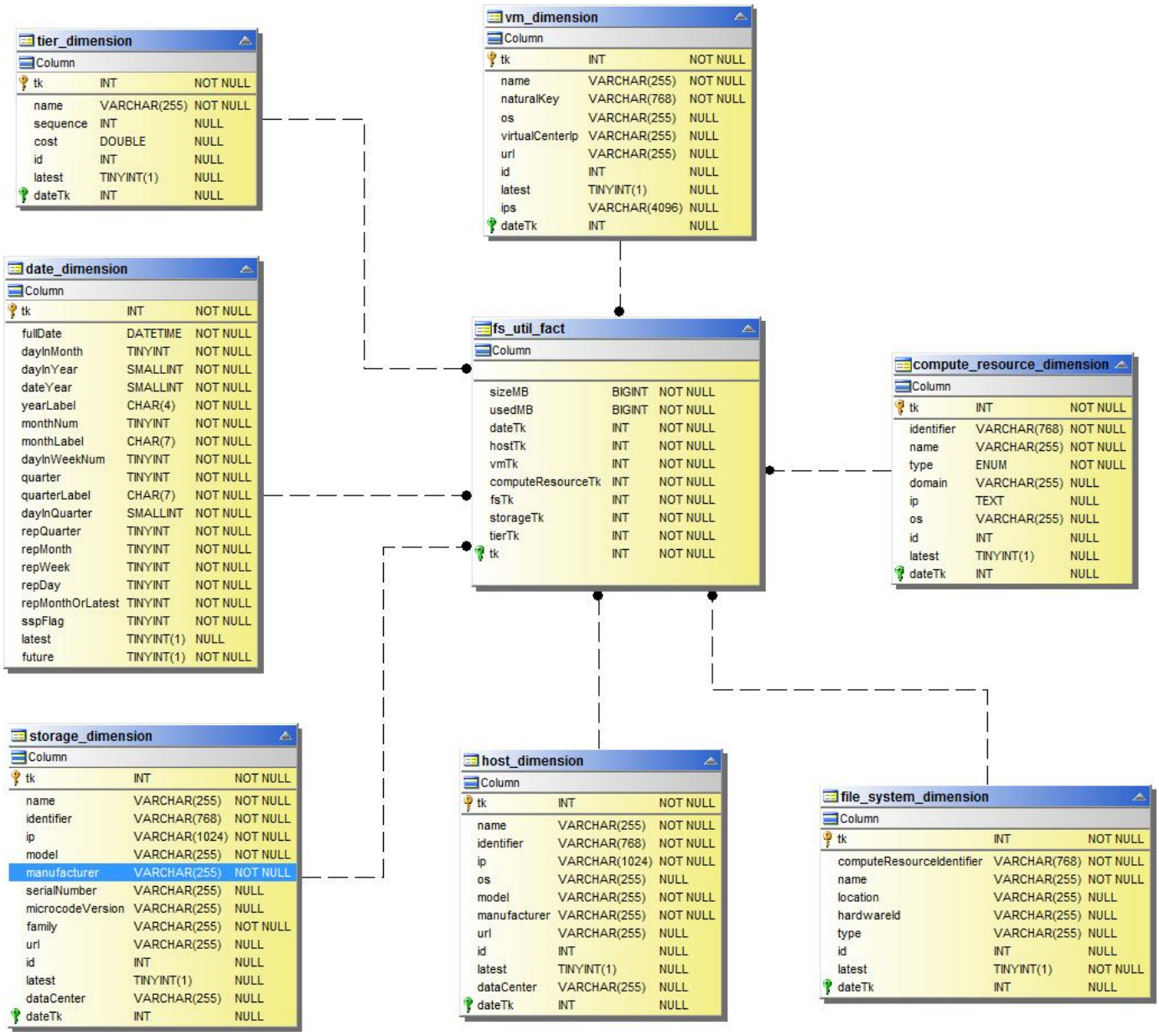
Refacturation



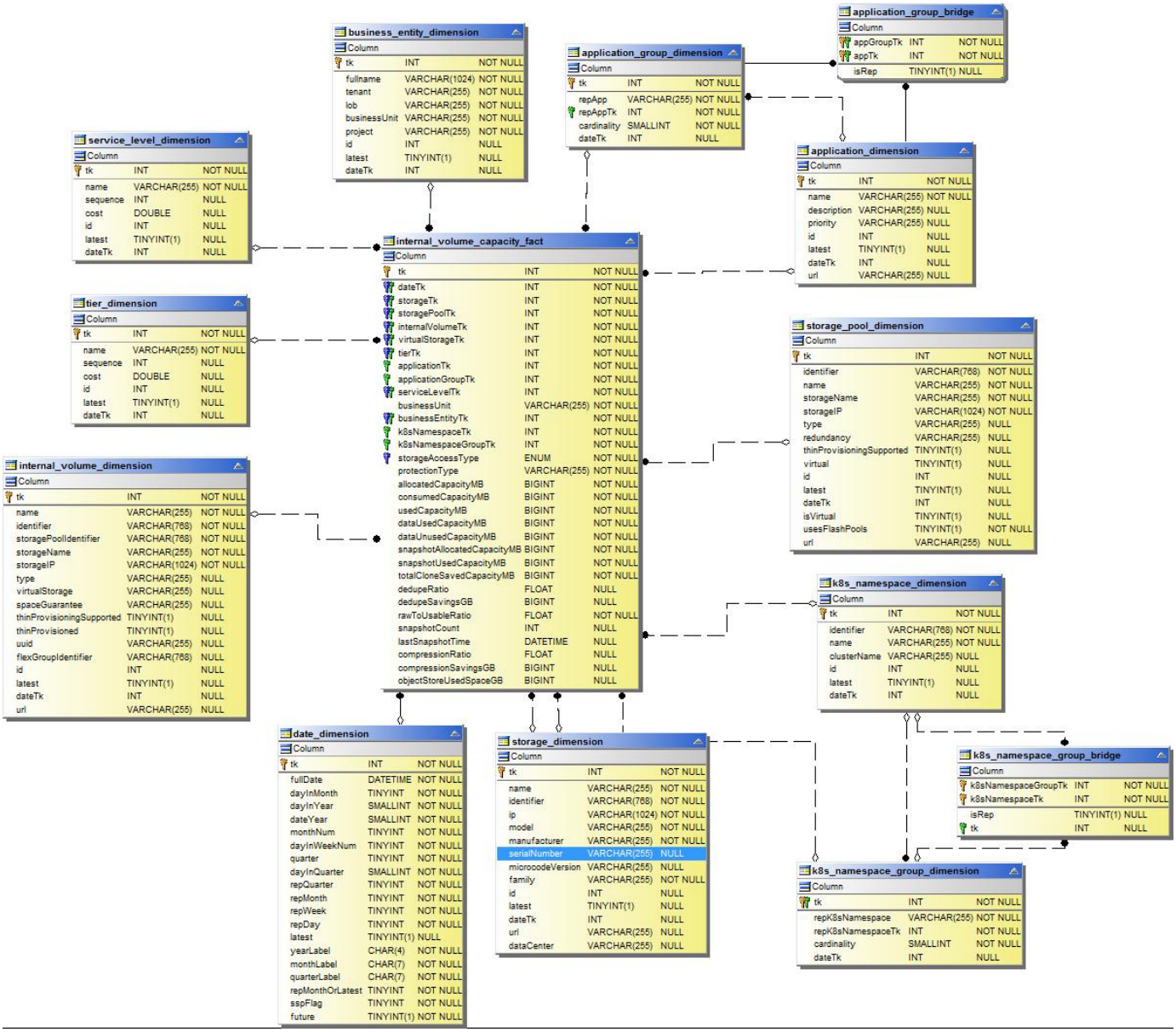
Capacité du groupe de disques



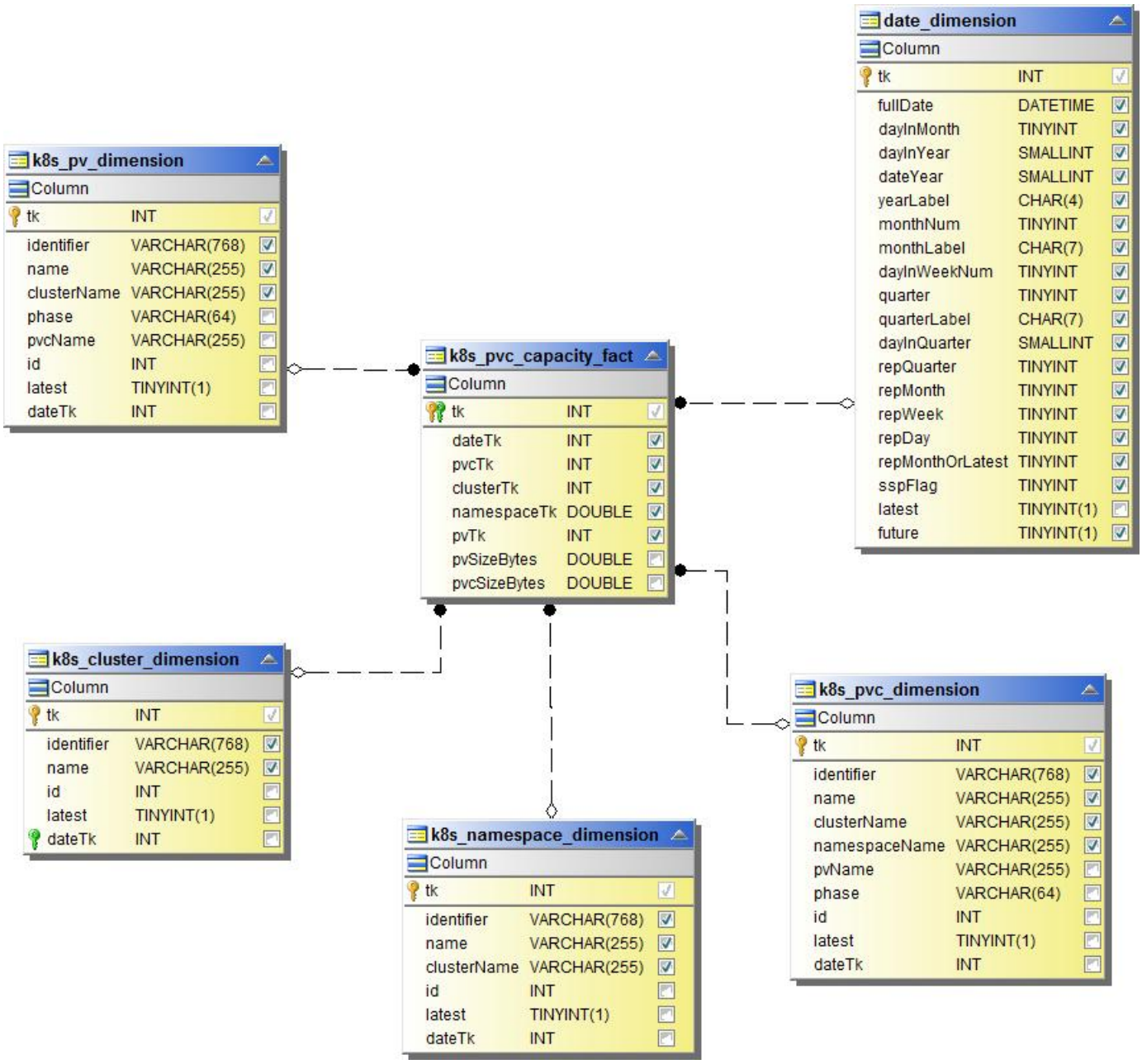
Utilisation du système de fichiers



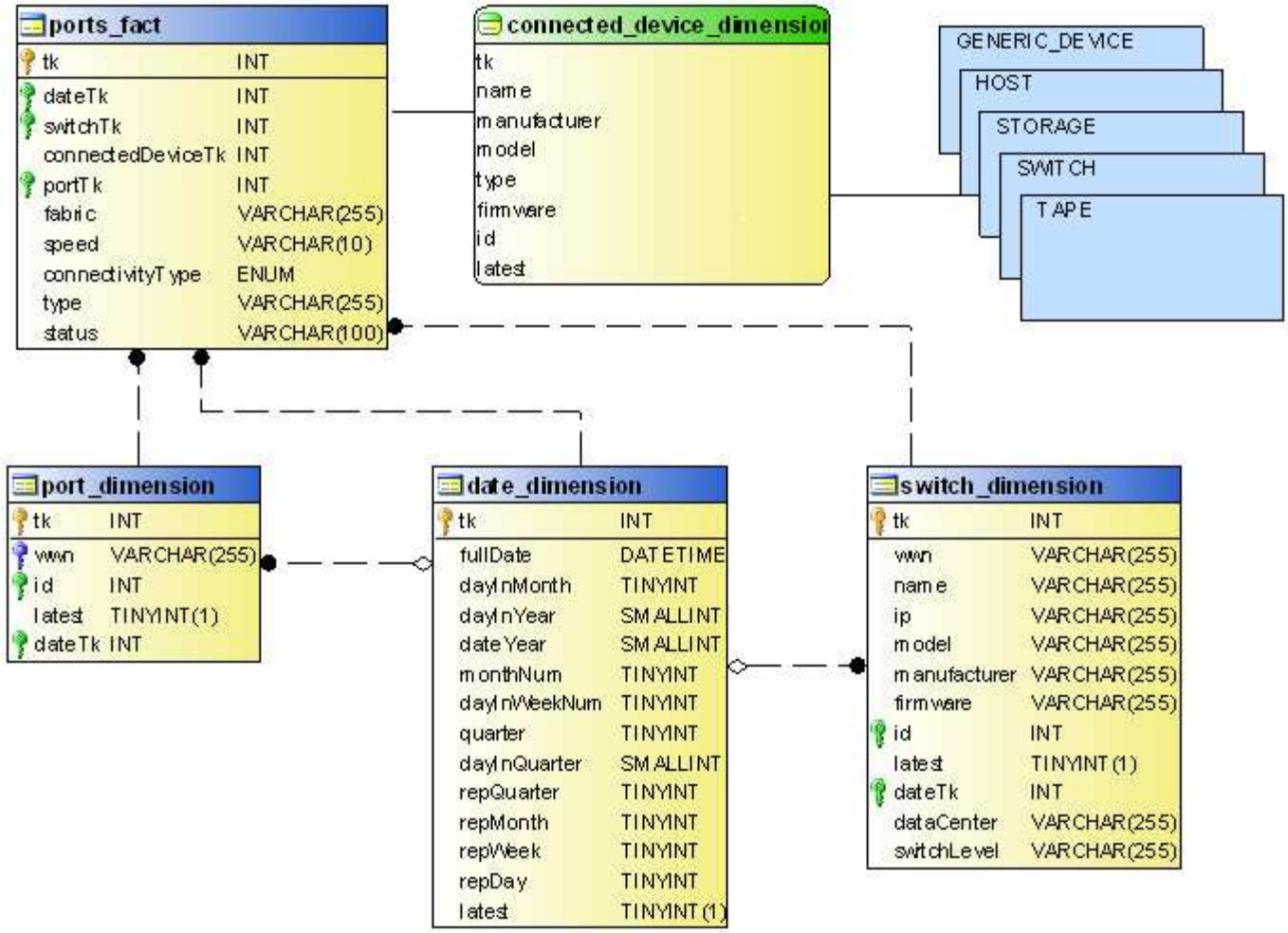
Capacité du volume interne



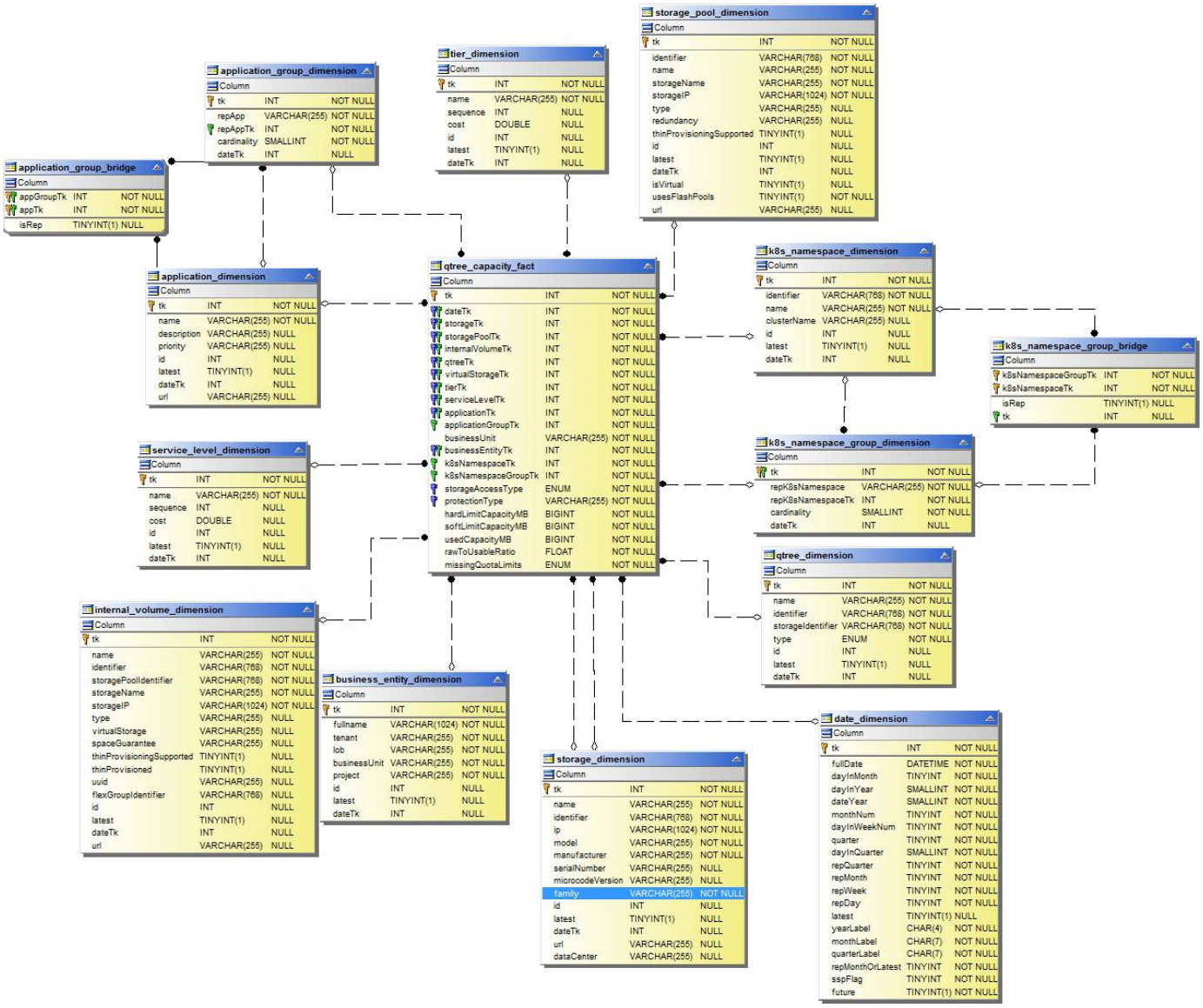
Capacité PV Kubernetes



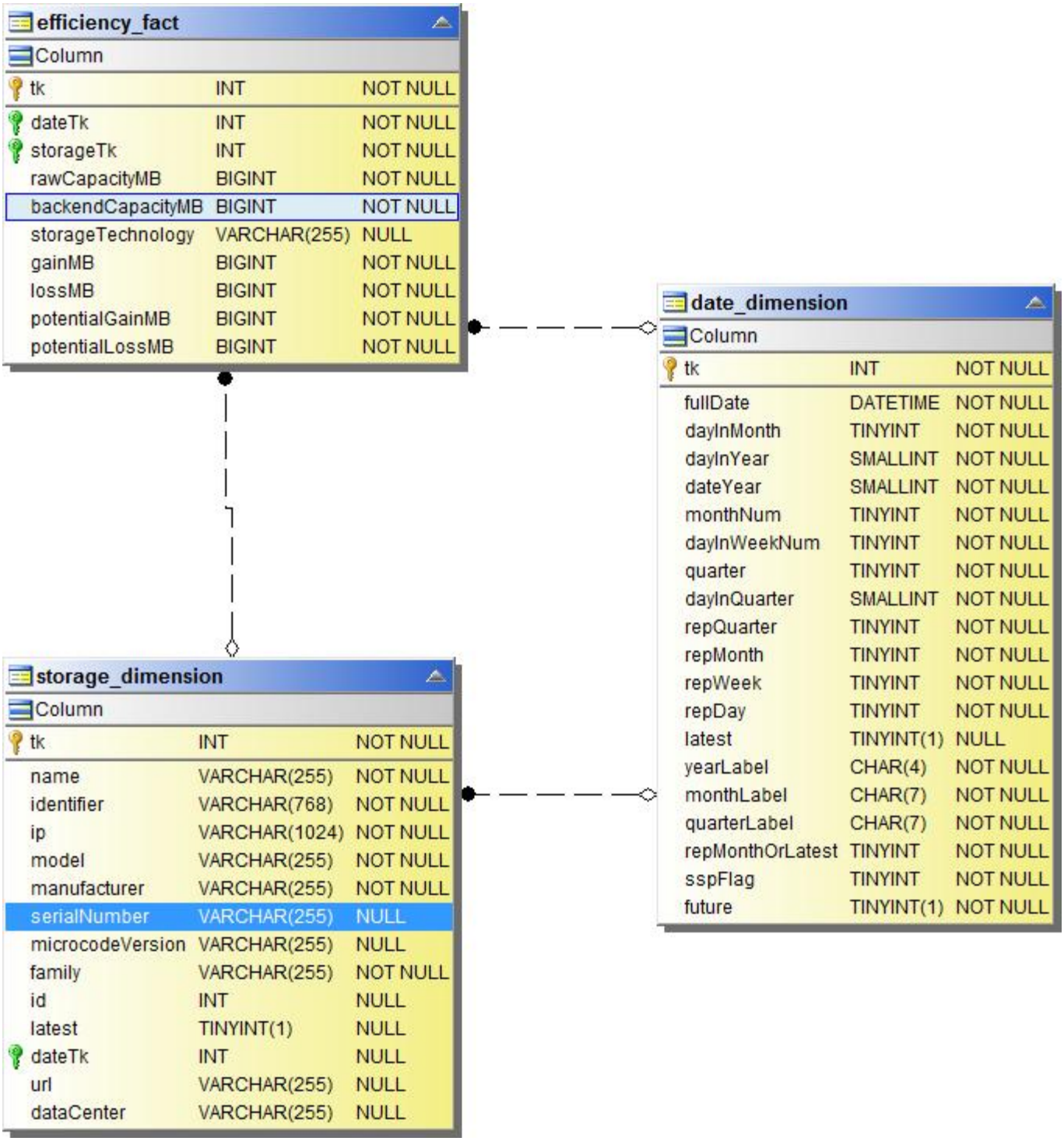
Capacité du port



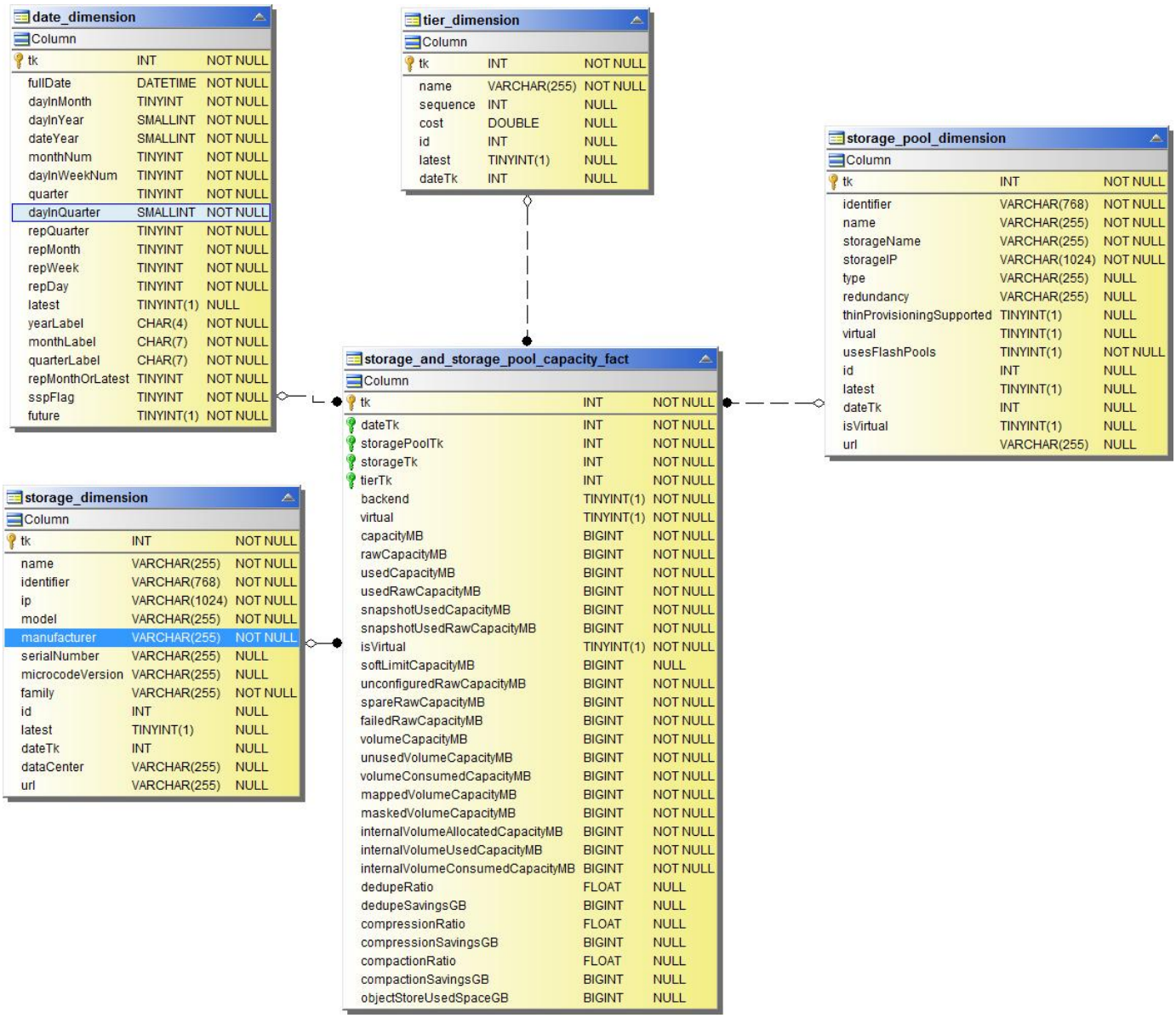
Capacité qtree



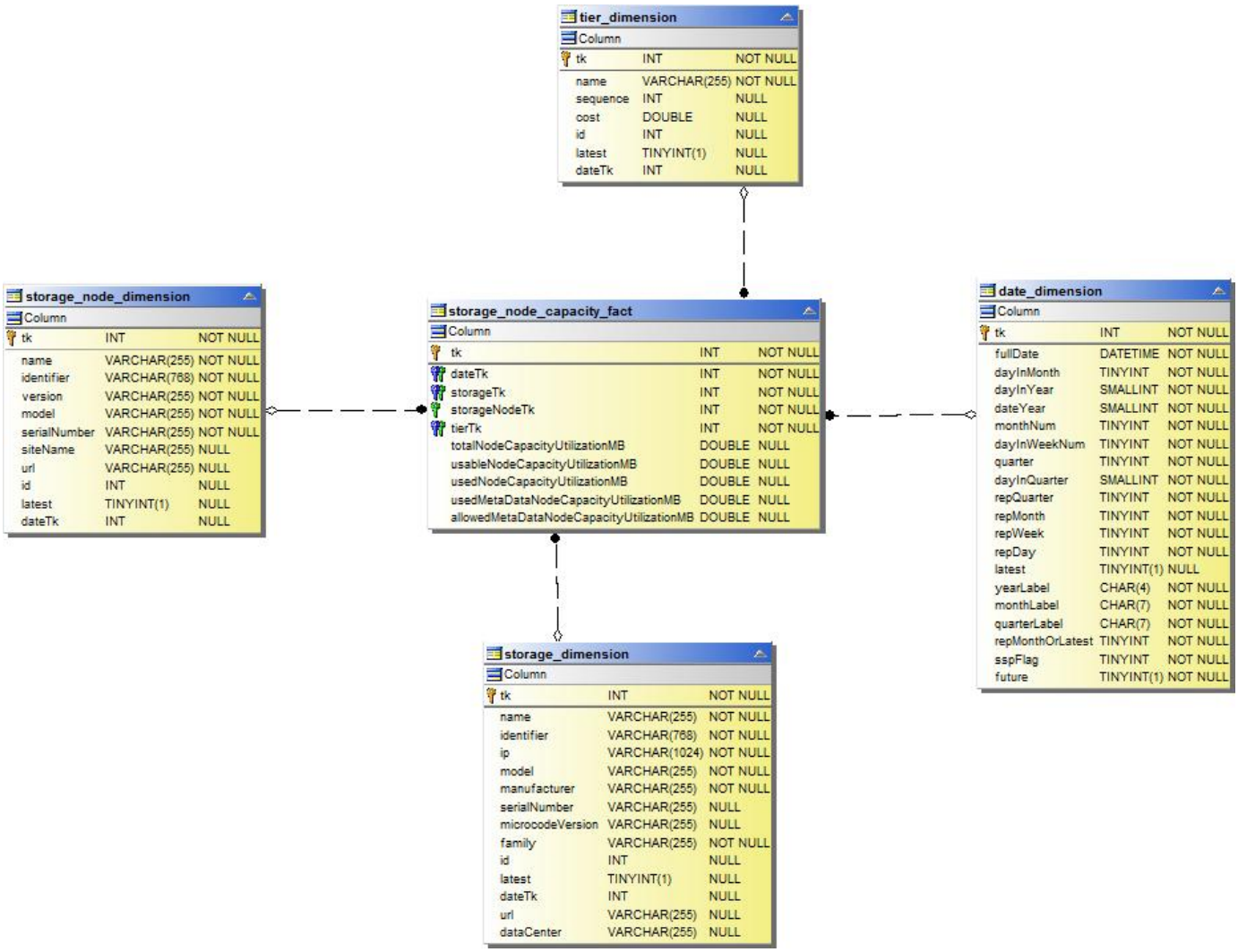
Efficacité des capacités de stockage



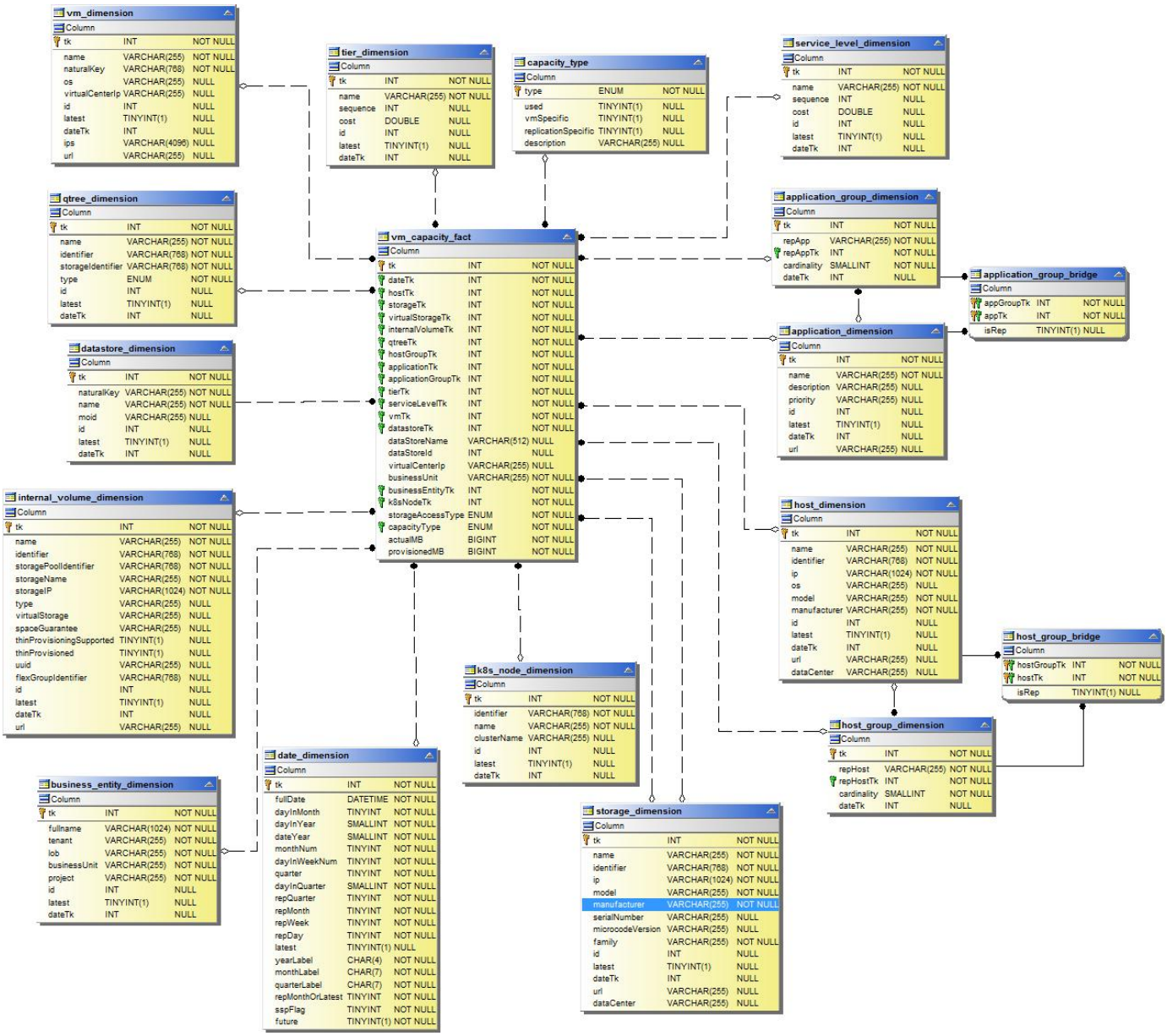
Capacité du pool de stockage et de stockage



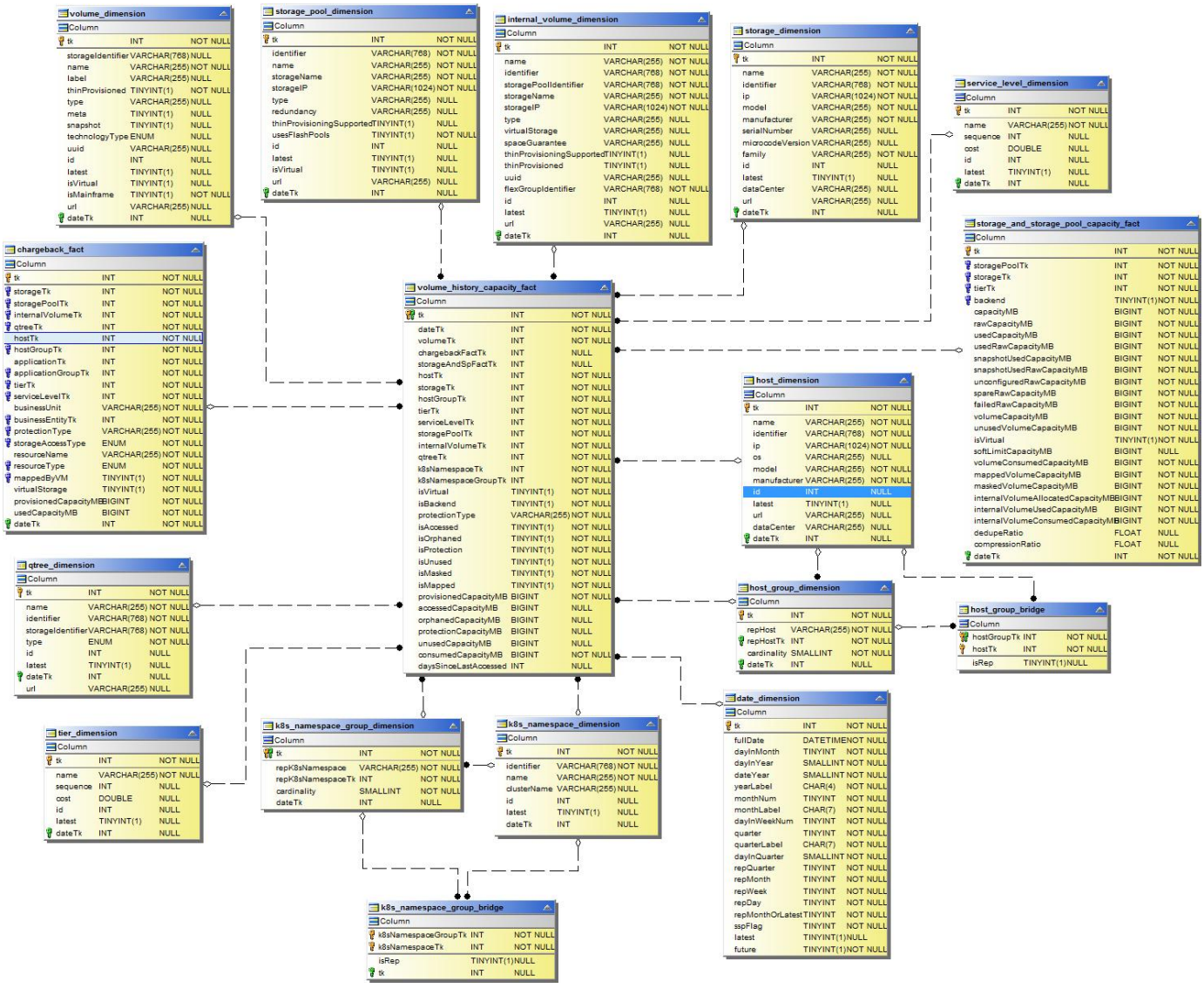
Capacité du nœud de stockage



Capacité des machines virtuelles



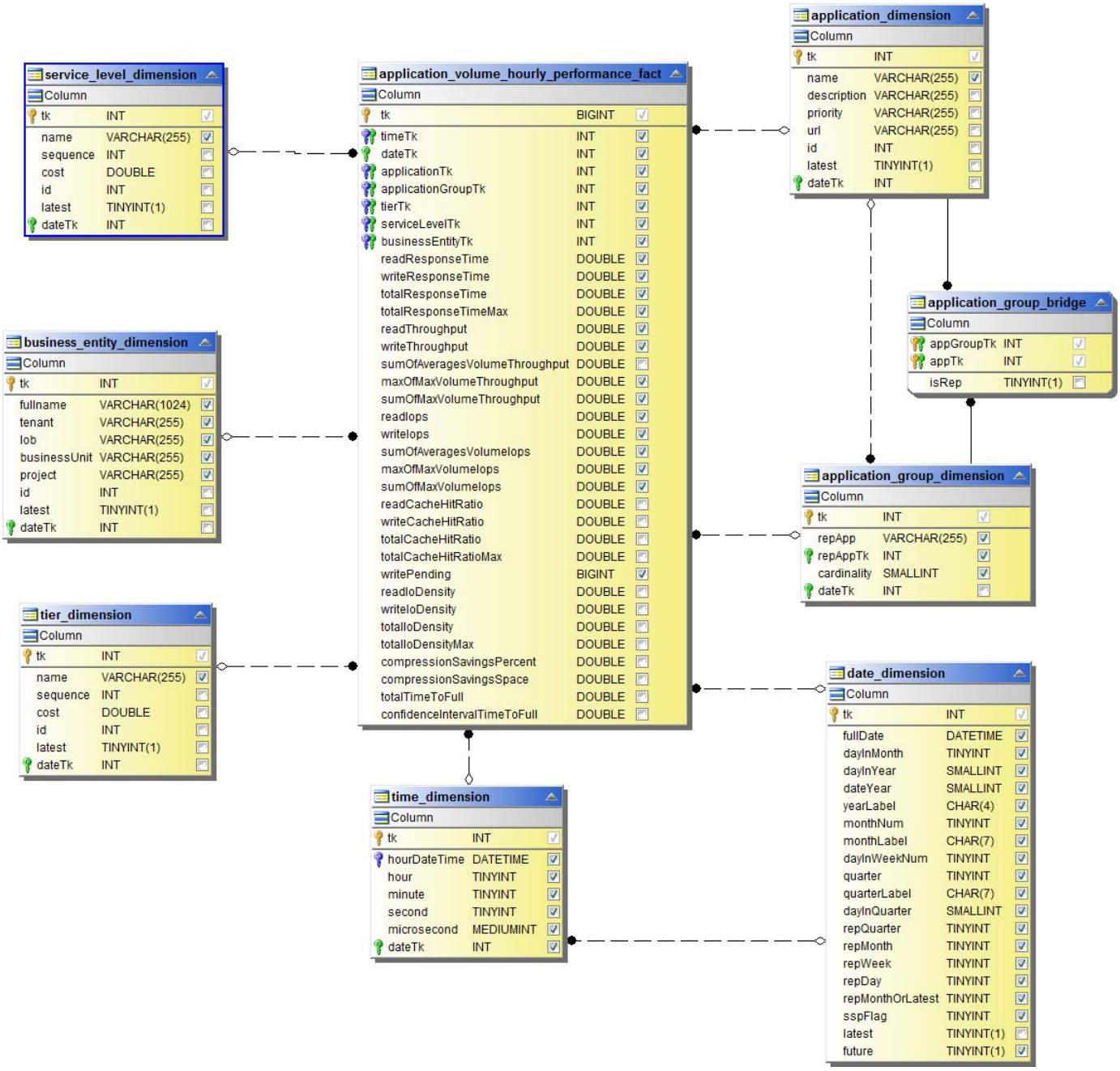
Capacité du volume



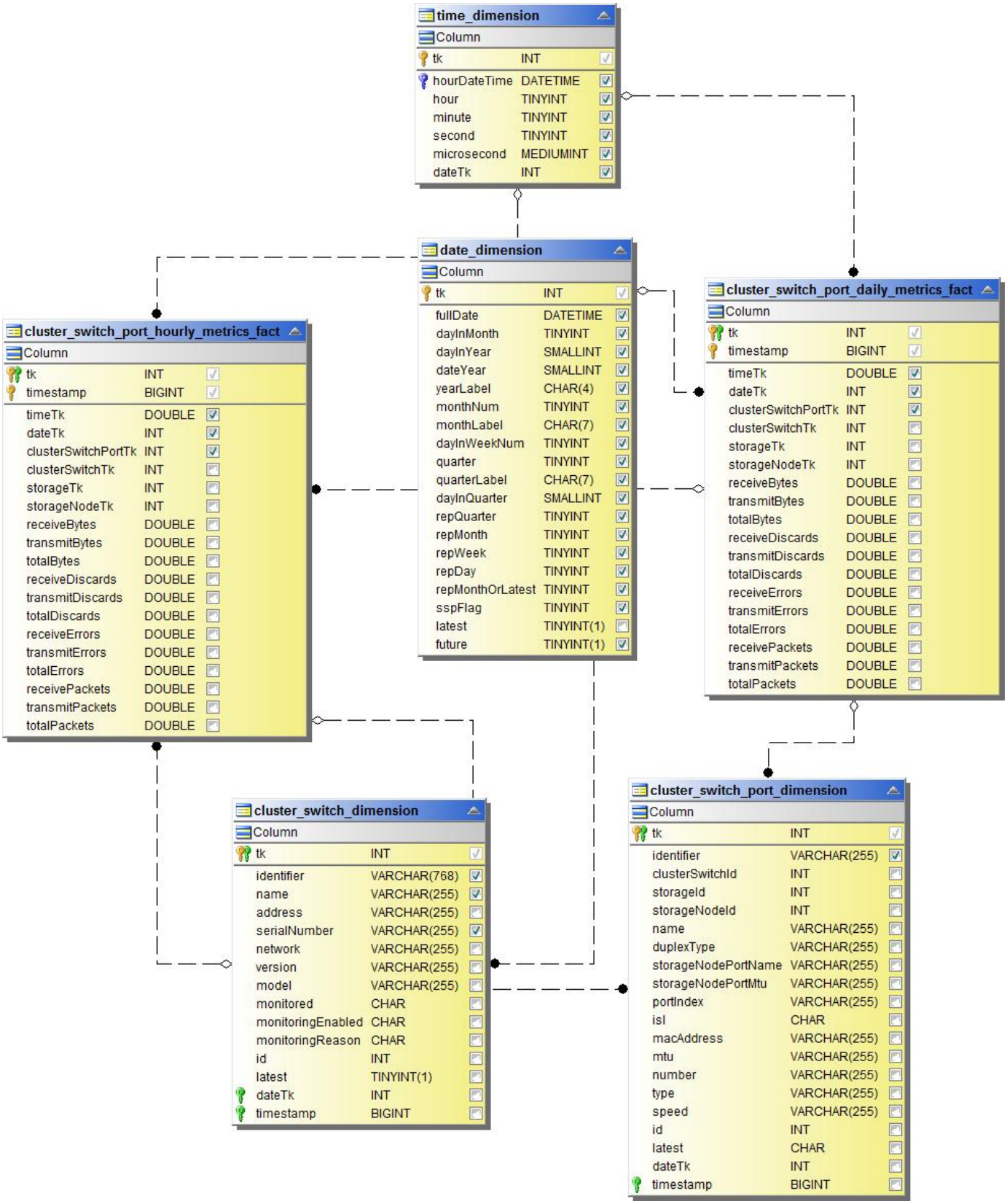
Performance Datamart

Les images suivantes décrivent le datamart de performance.

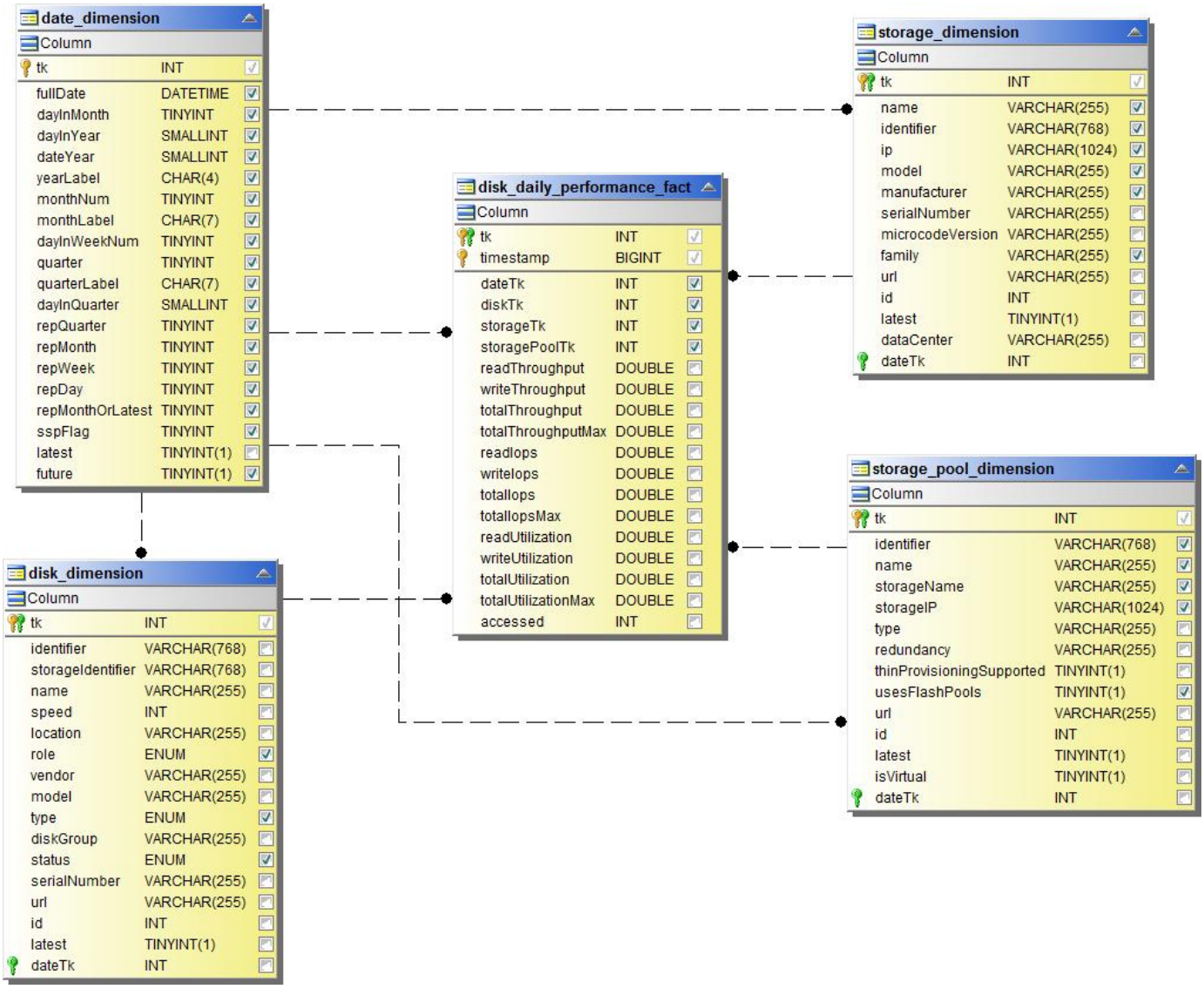
Volume de l'application performances horaires



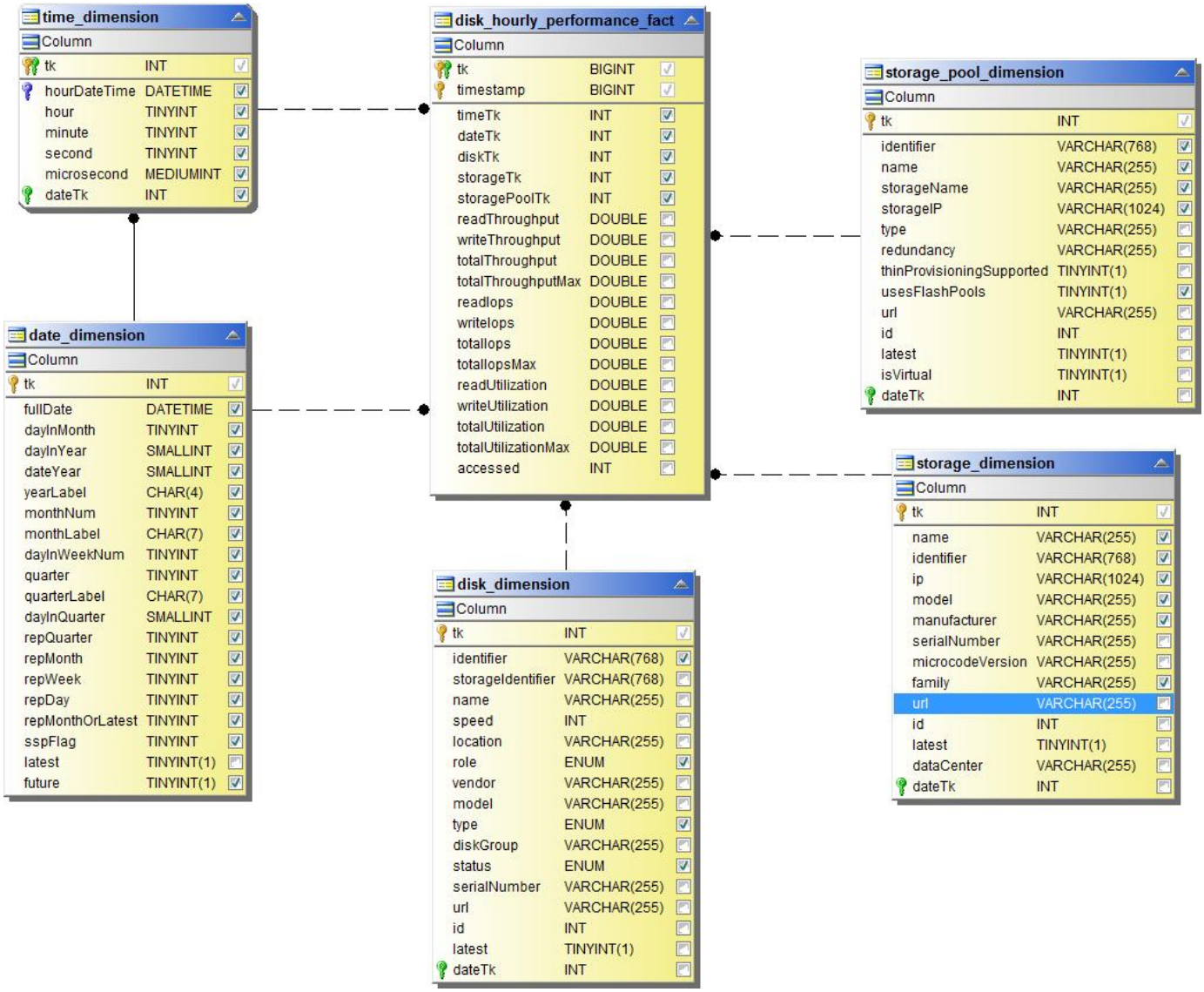
Performances des commutateurs du cluster



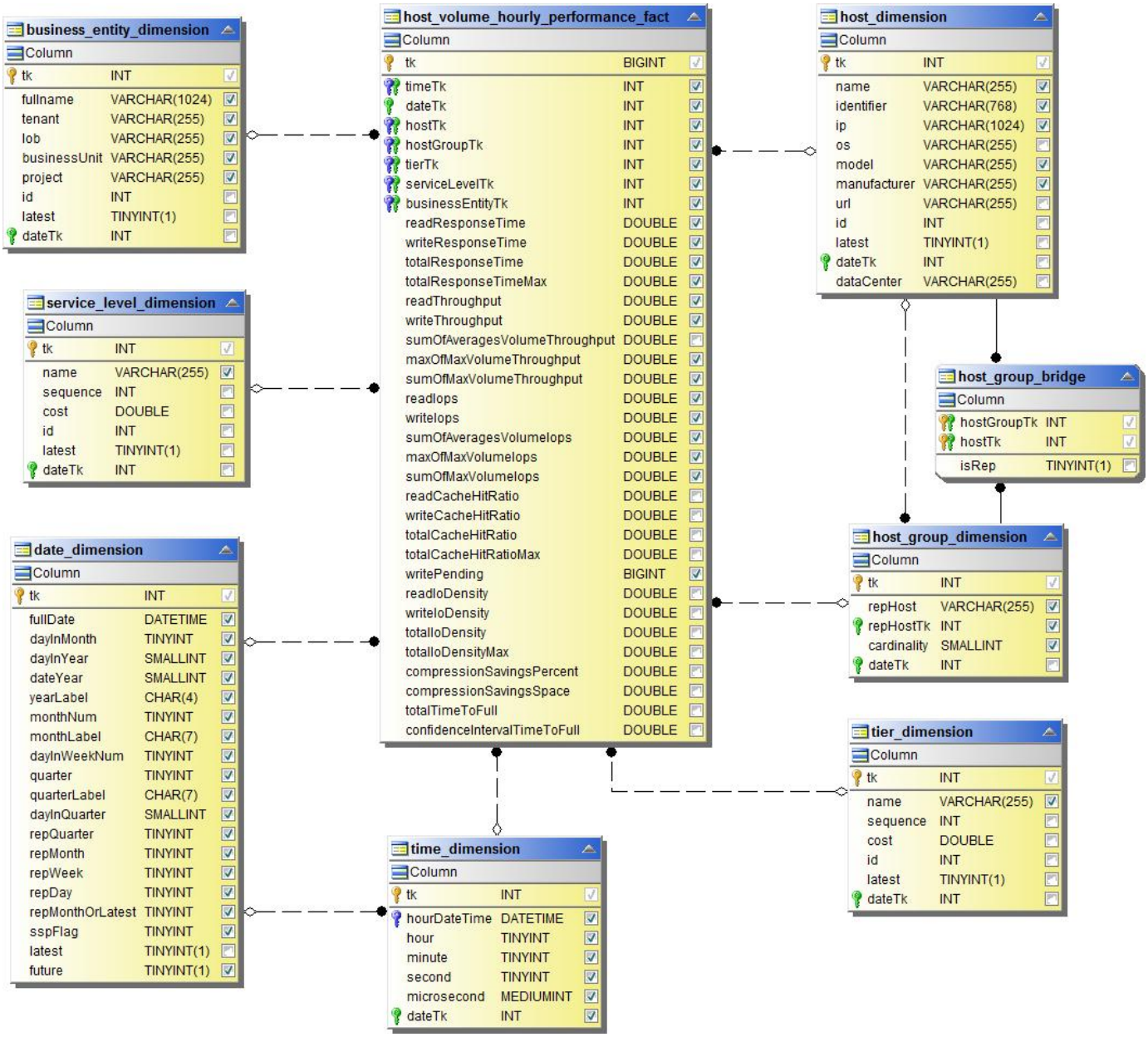
Performances quotidiennes des disques



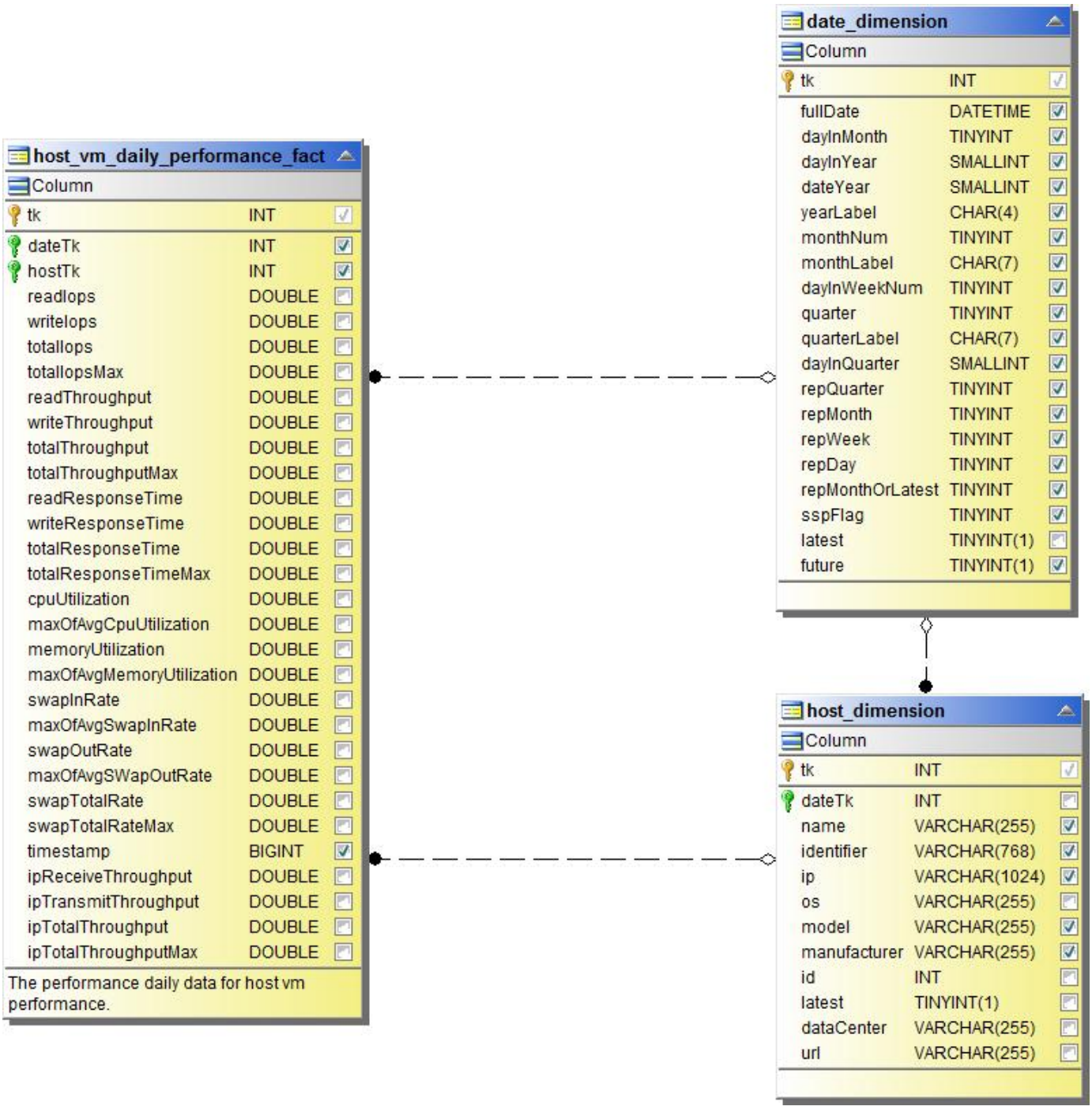
Performances des disques horaires



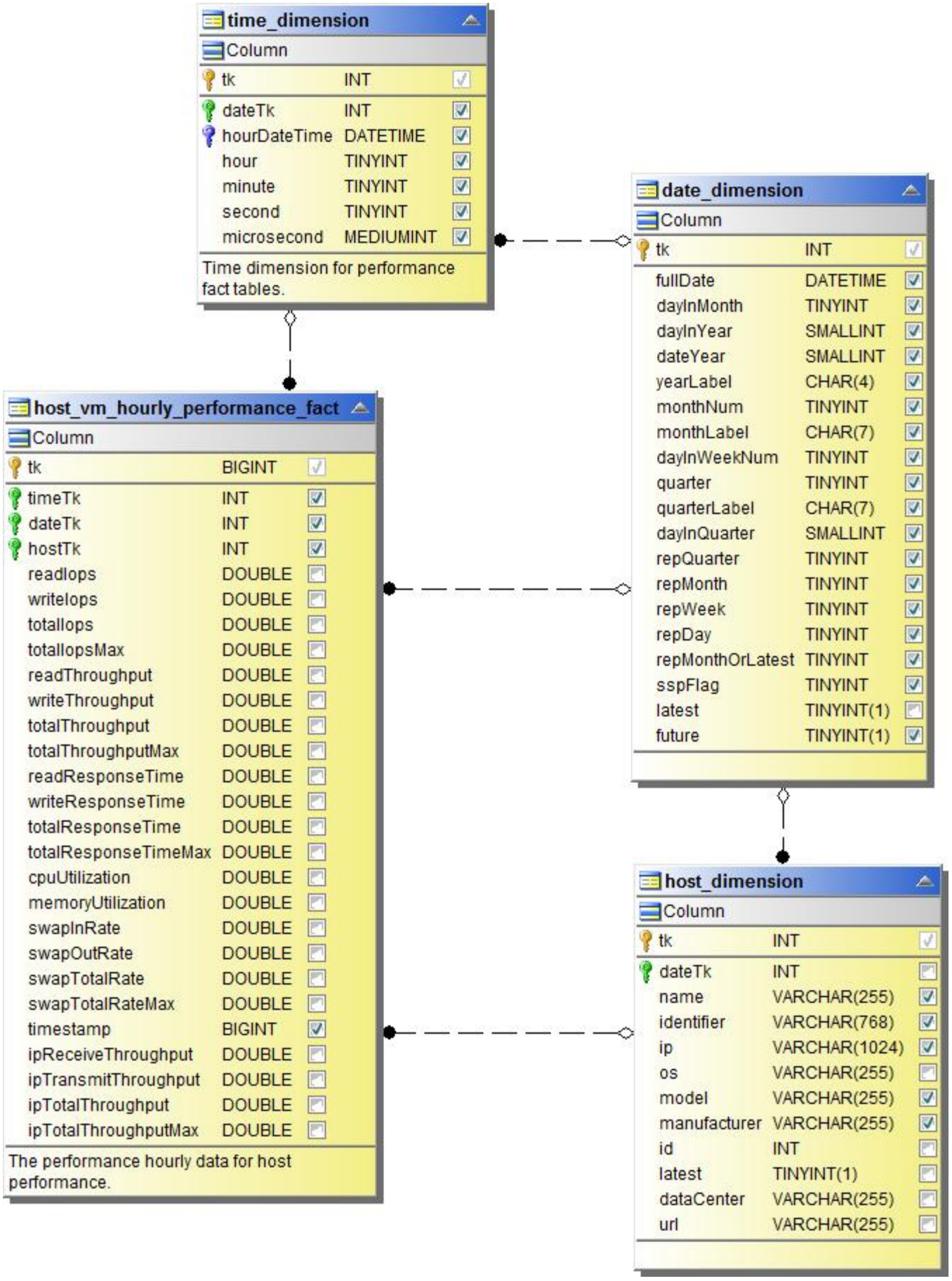
Performances de l’hôte horaire



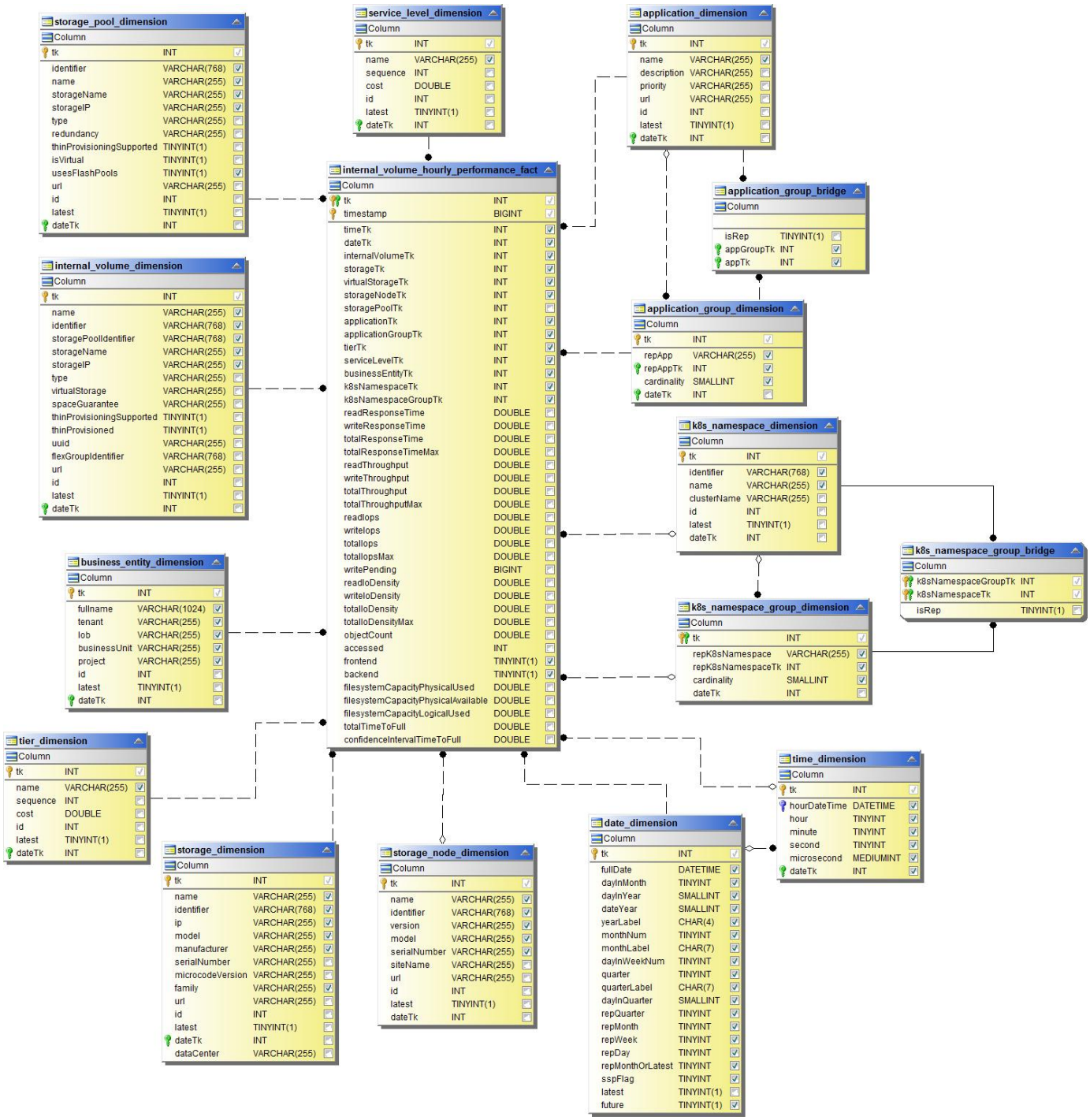
Performances quotidiennes de la machine virtuelle hôte



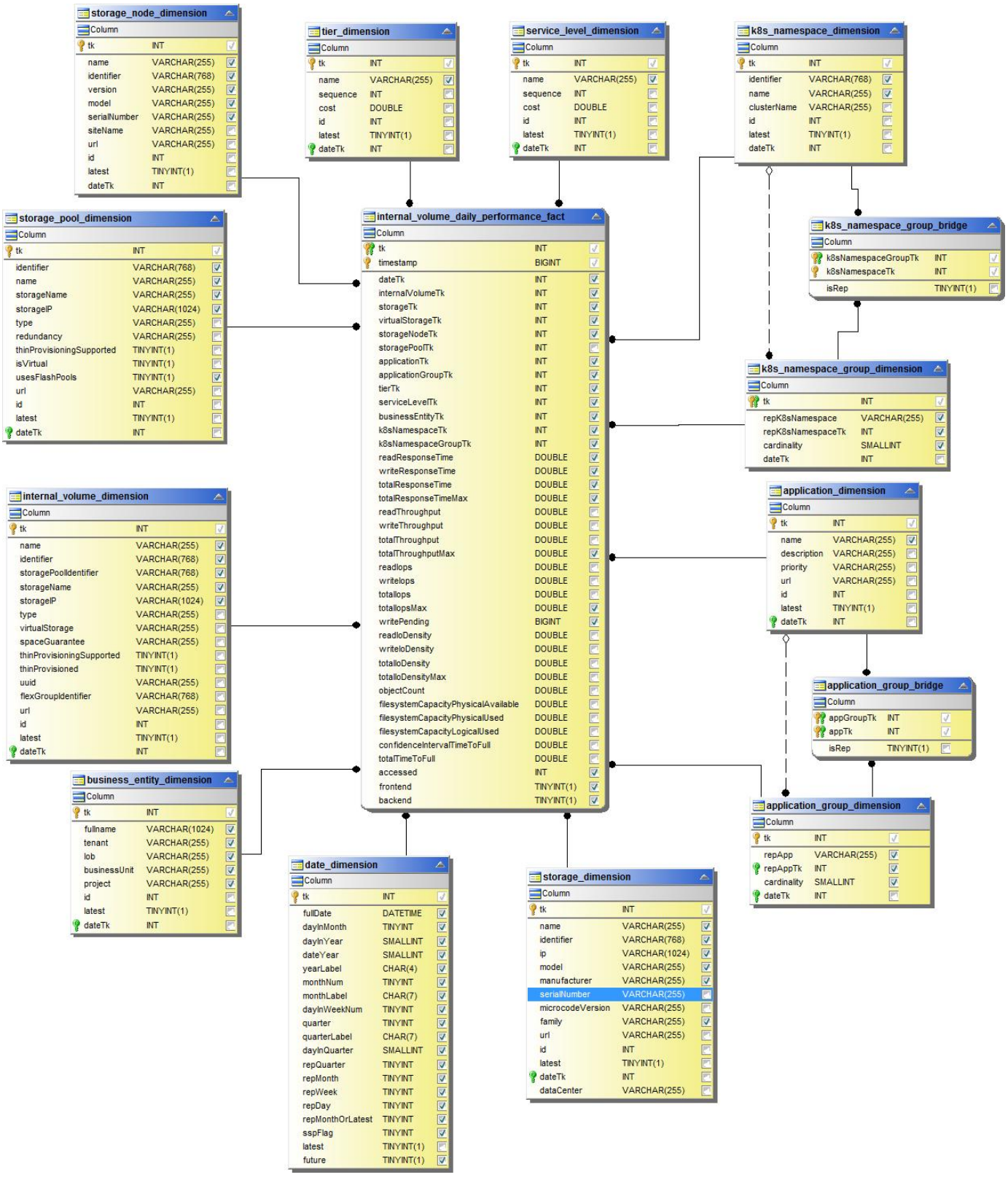
Performances horaire de l’ordinateur virtuel hôte


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)

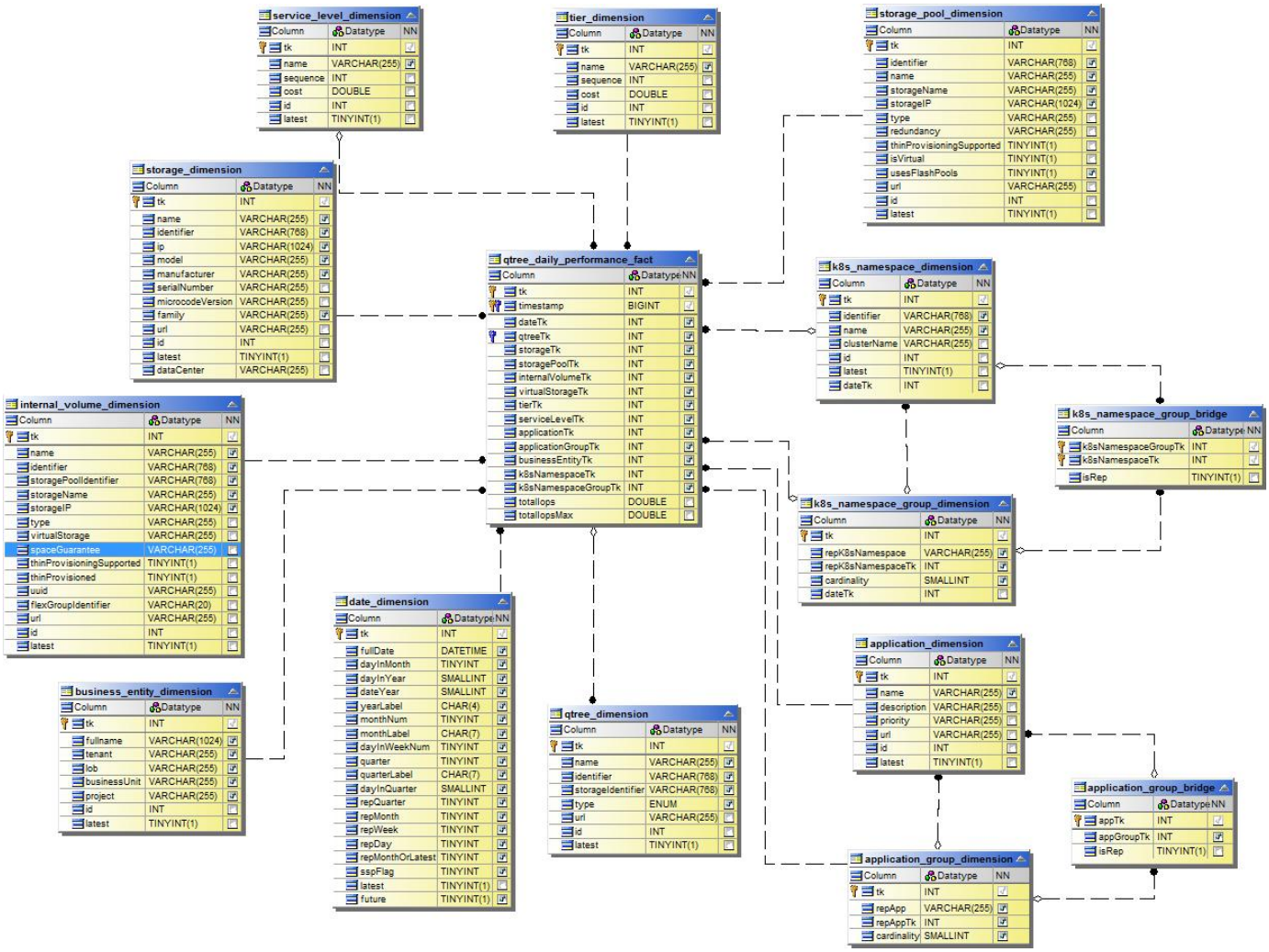
Volume interne rendement horaire



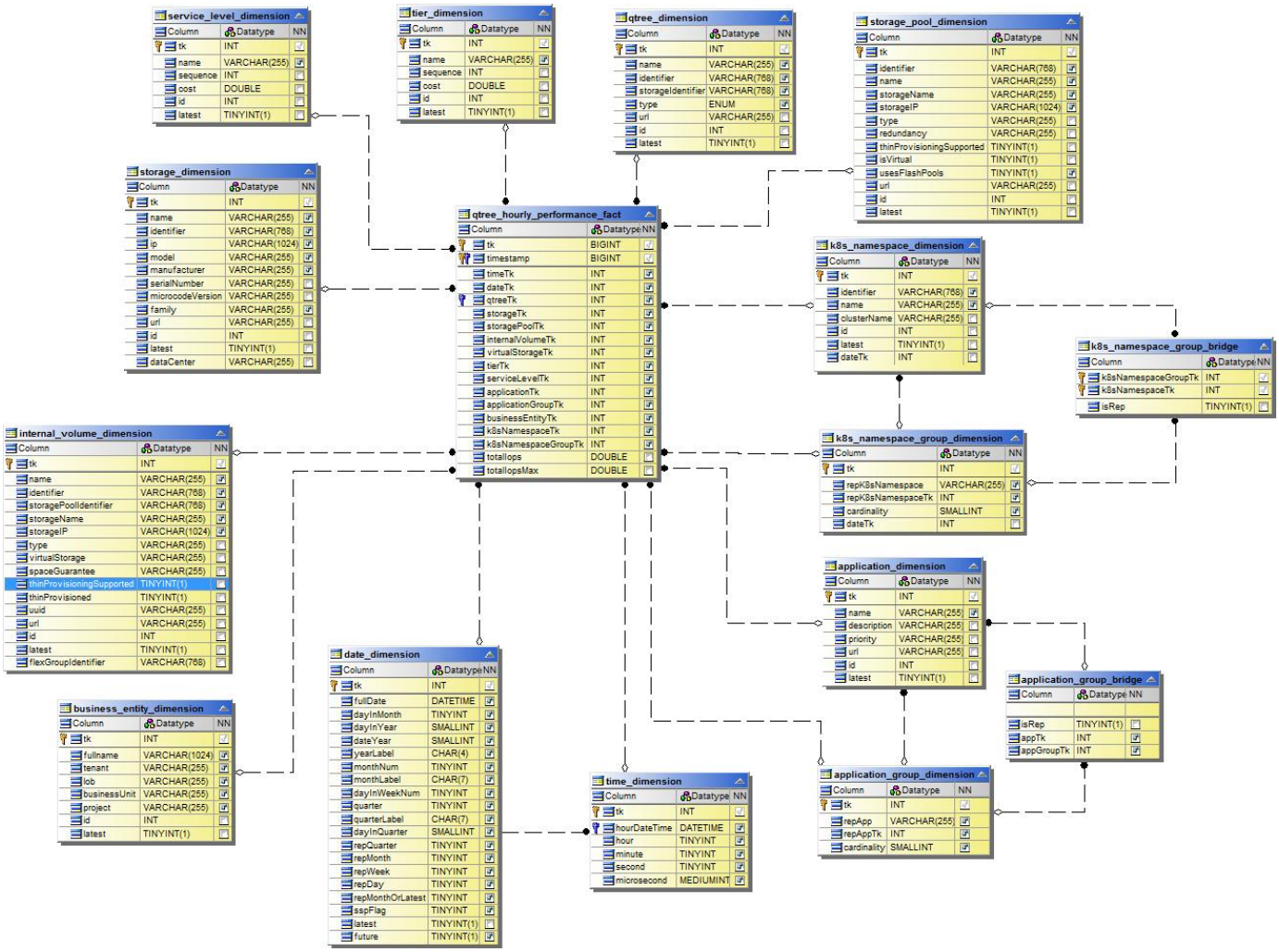
Volume interne Performance quotidienne



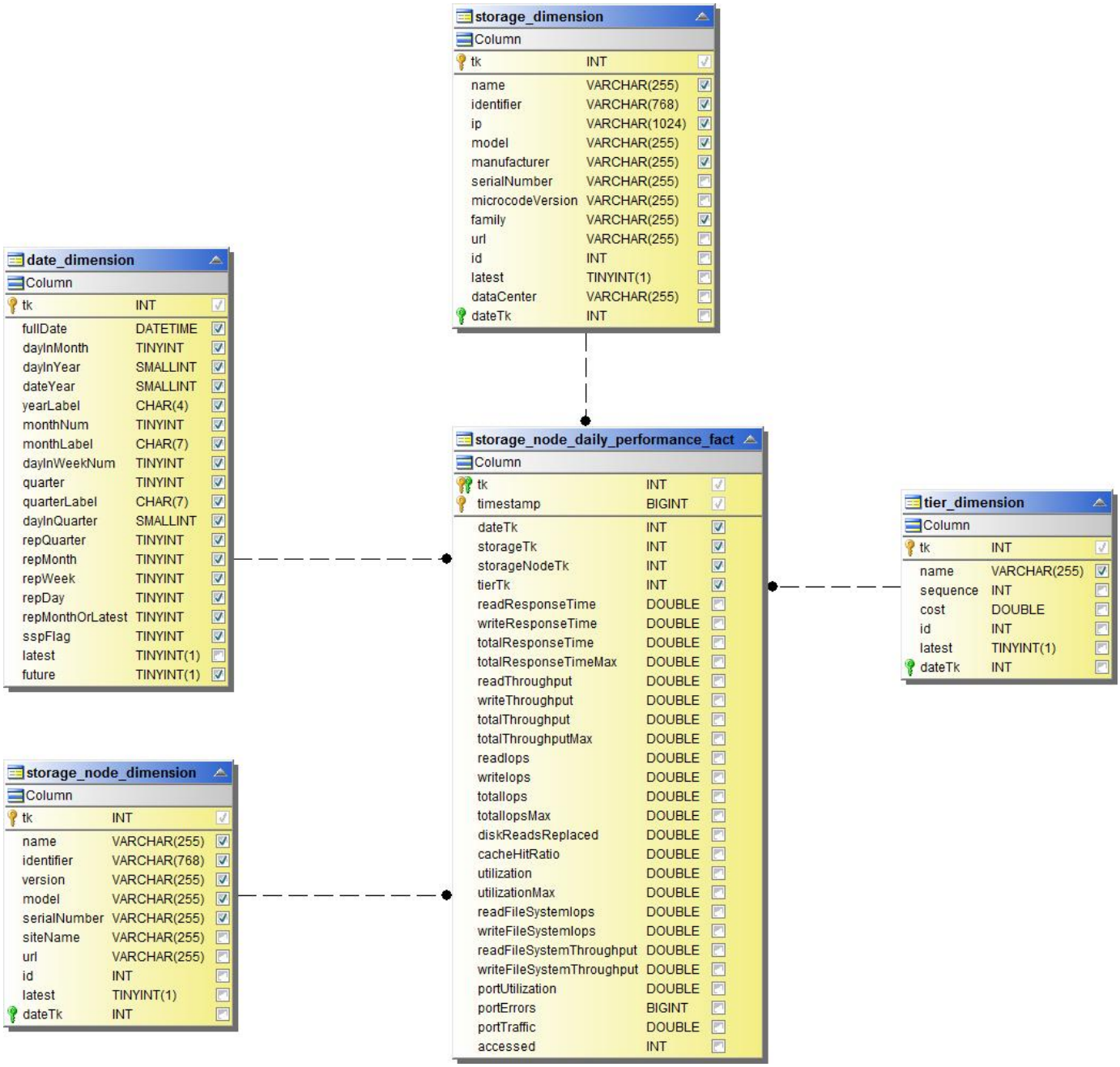
Performances quotidiennes des qtrees



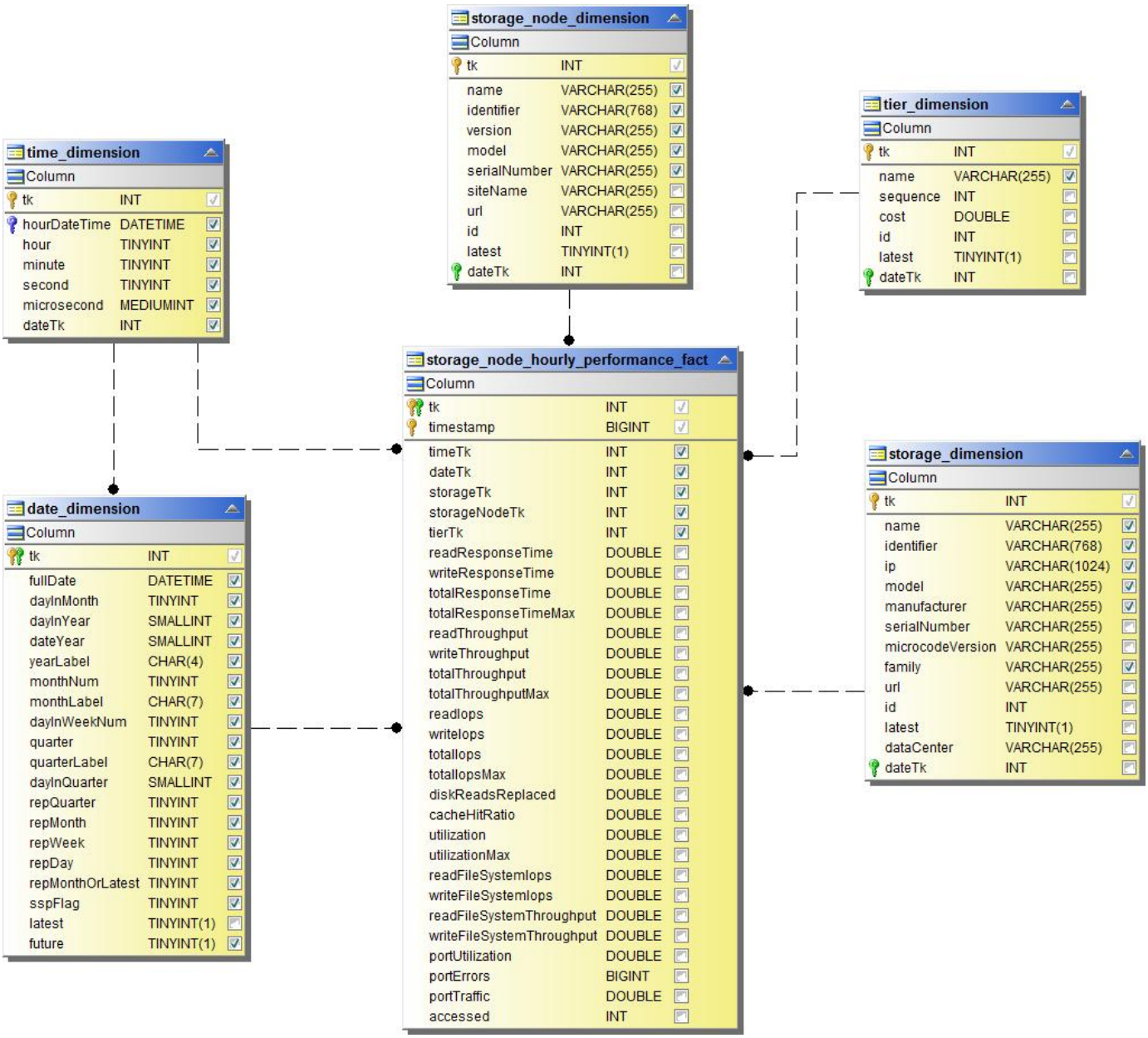
Performances qtree horaire



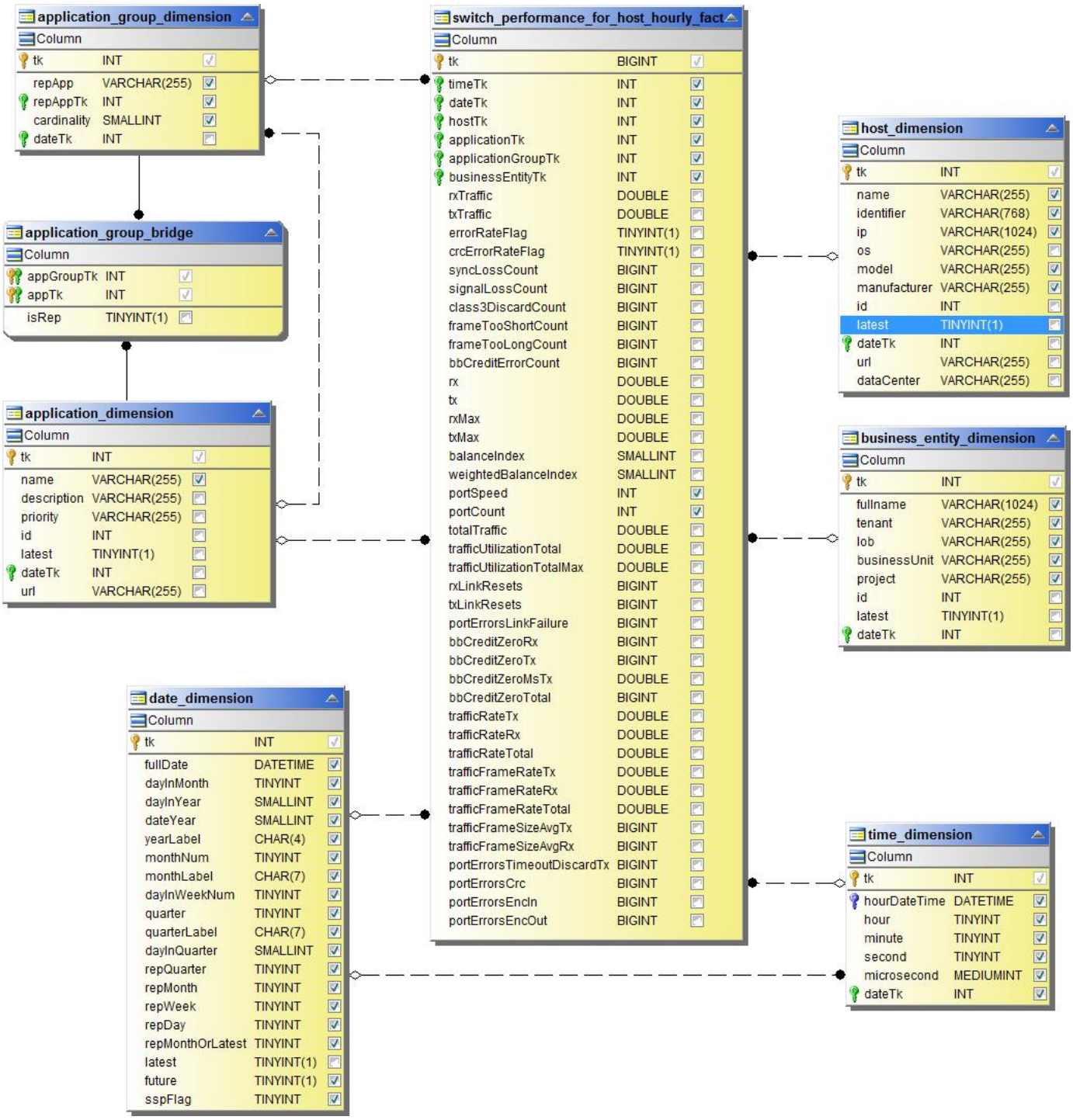
Performances quotidiennes du nœud de stockage



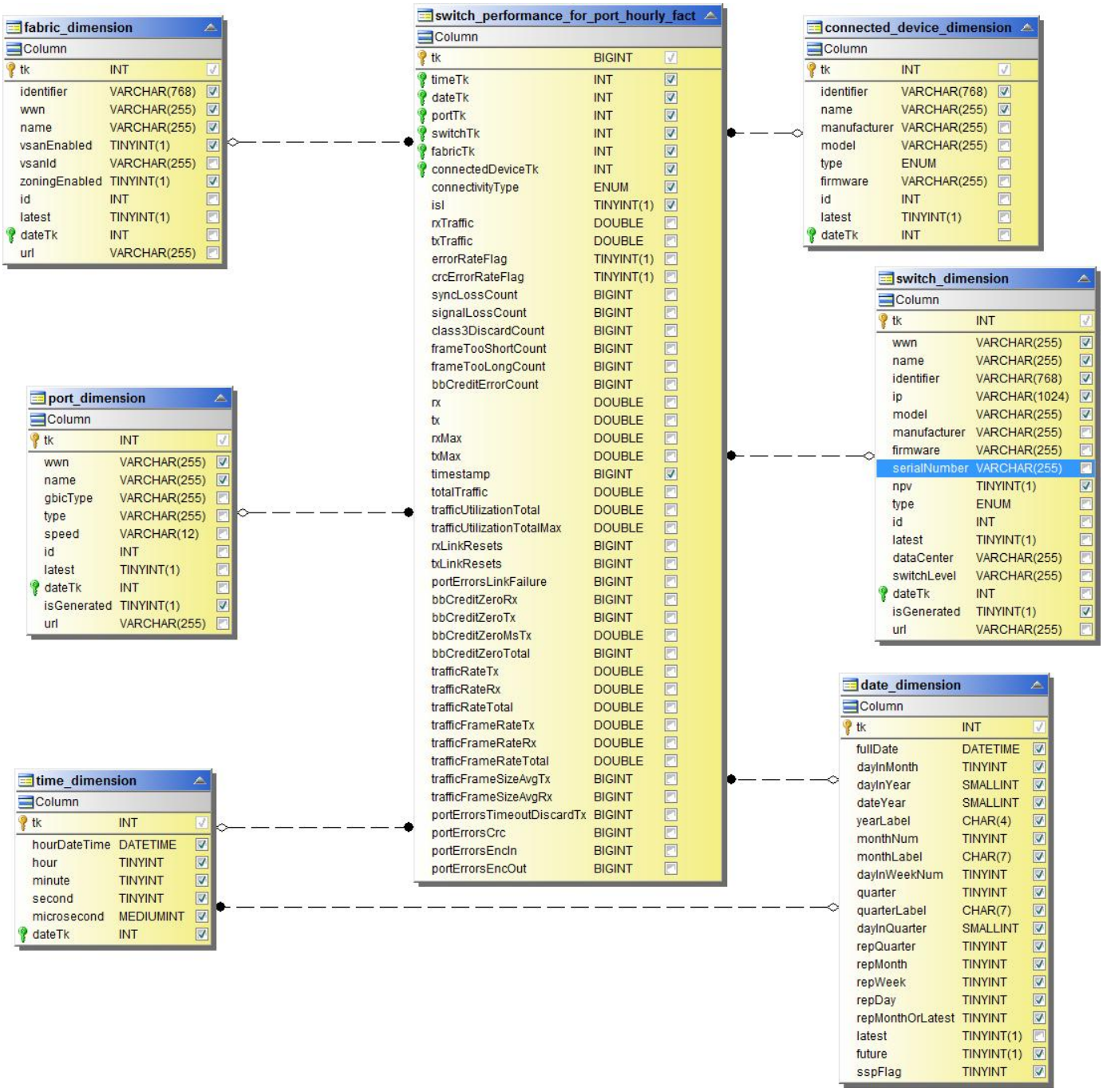
Performances du nœud de stockage horaire



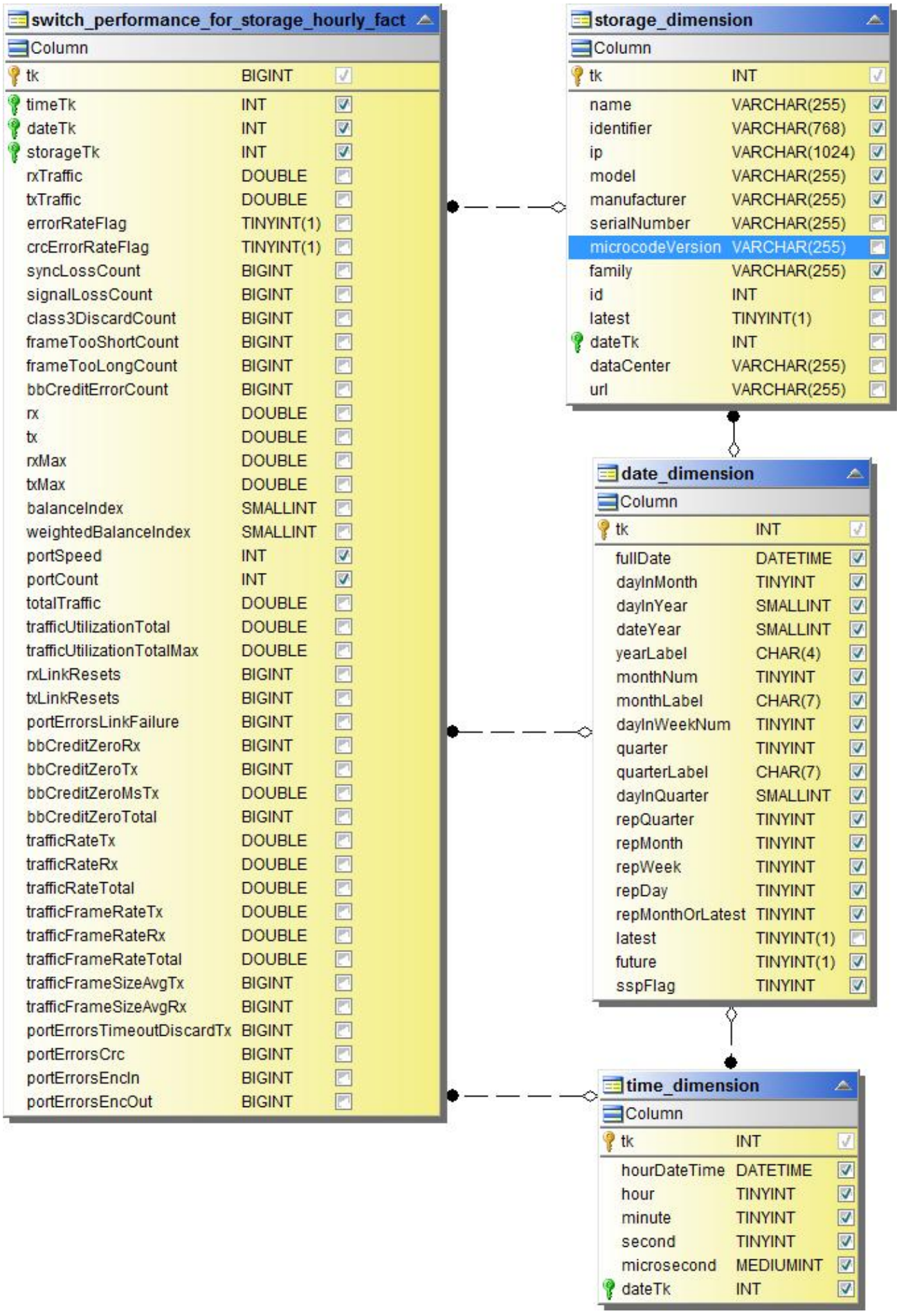
Changer les performances horaires de l’hôte



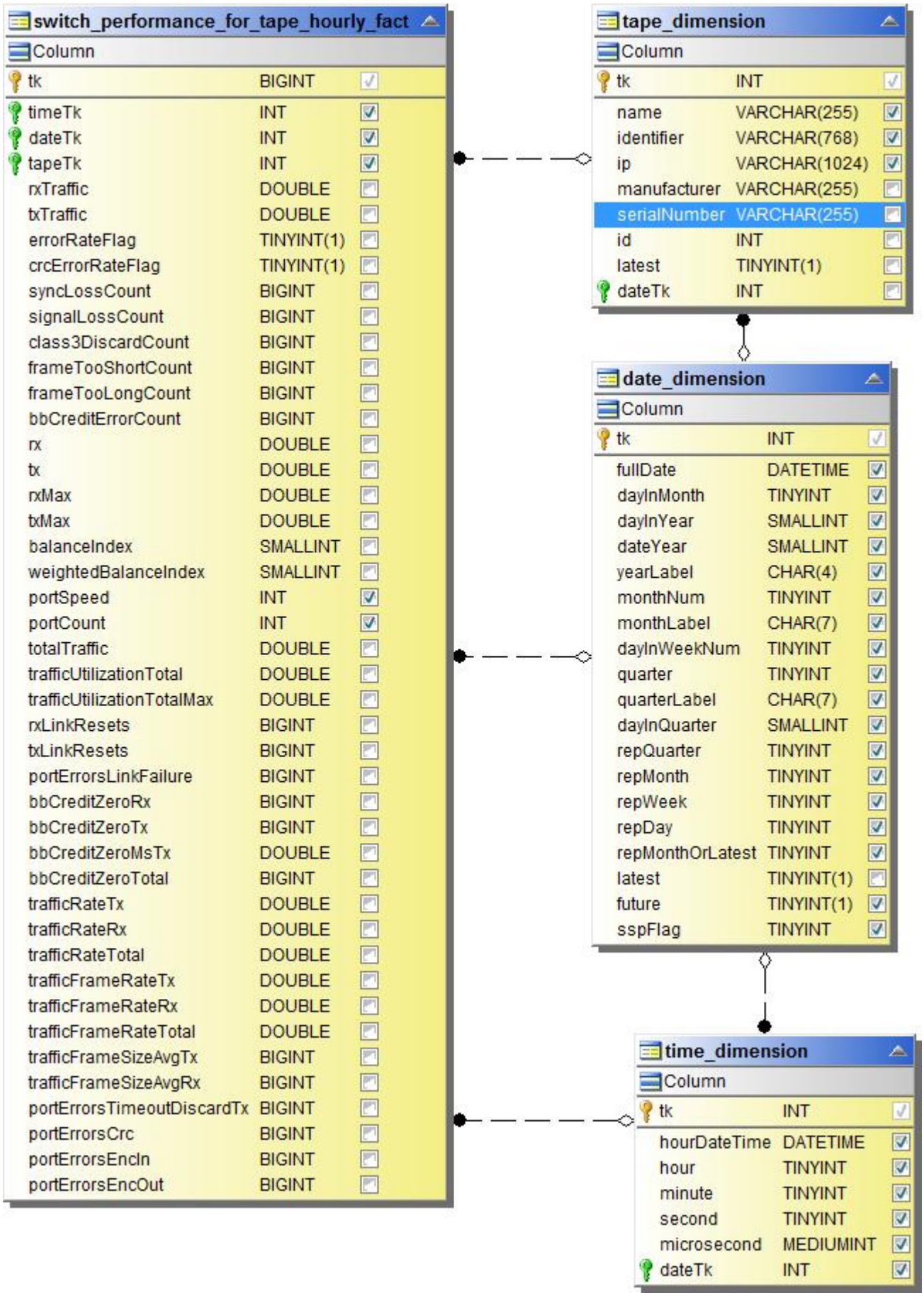
Changer les performances horaires pour le port



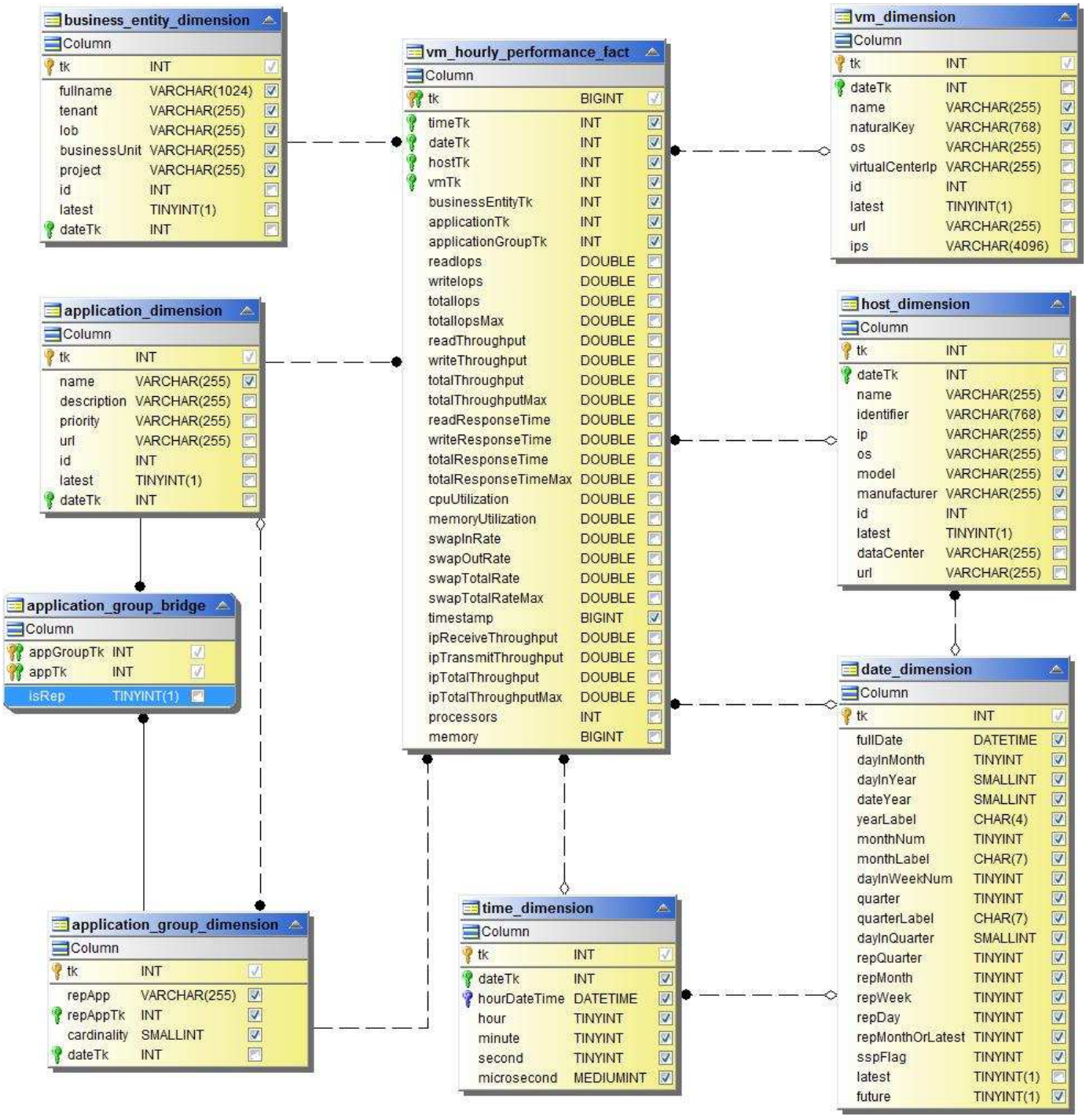
Changez les performances horaires pour le stockage


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

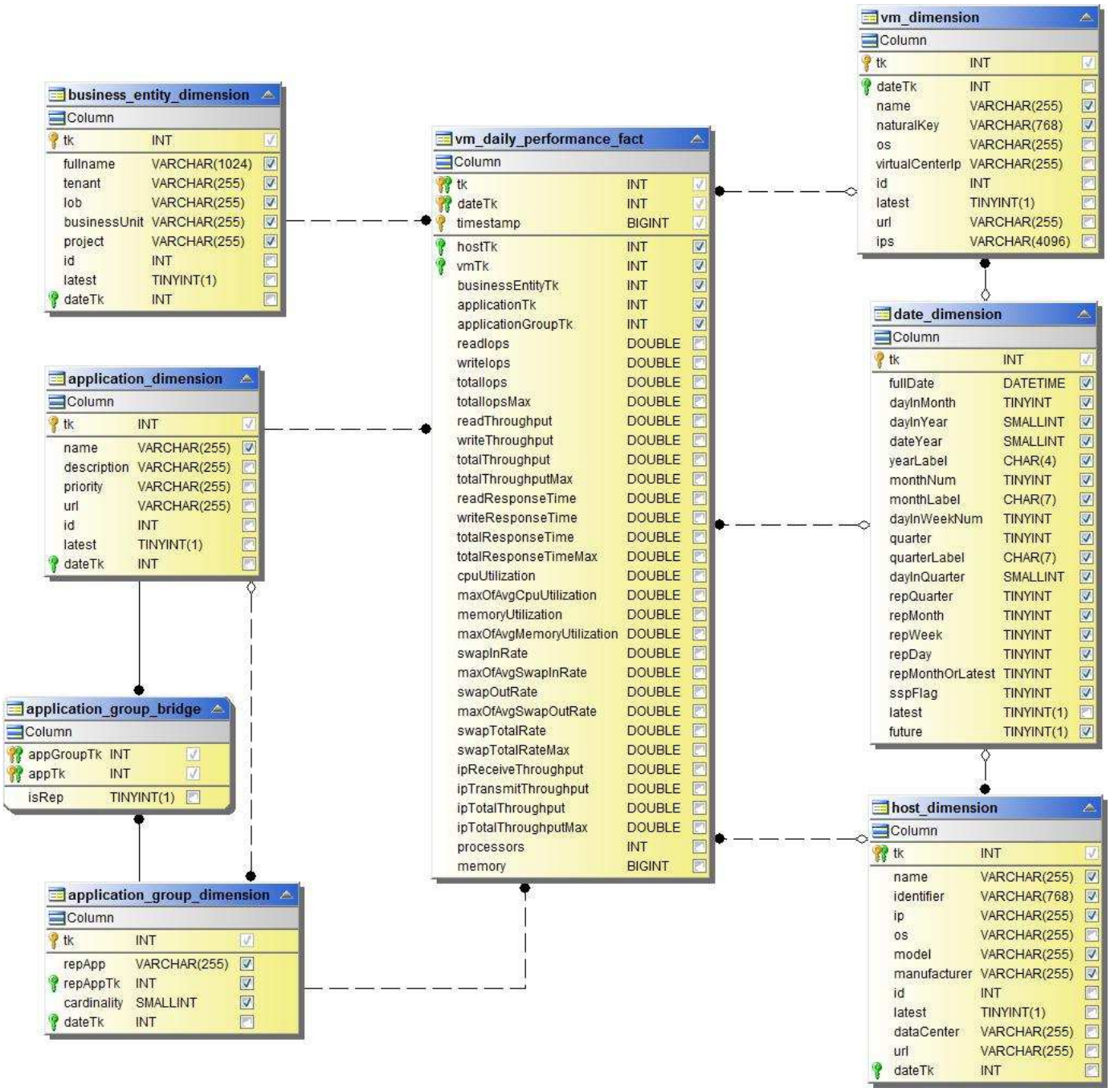
Changez les performances horaires pour les bandes



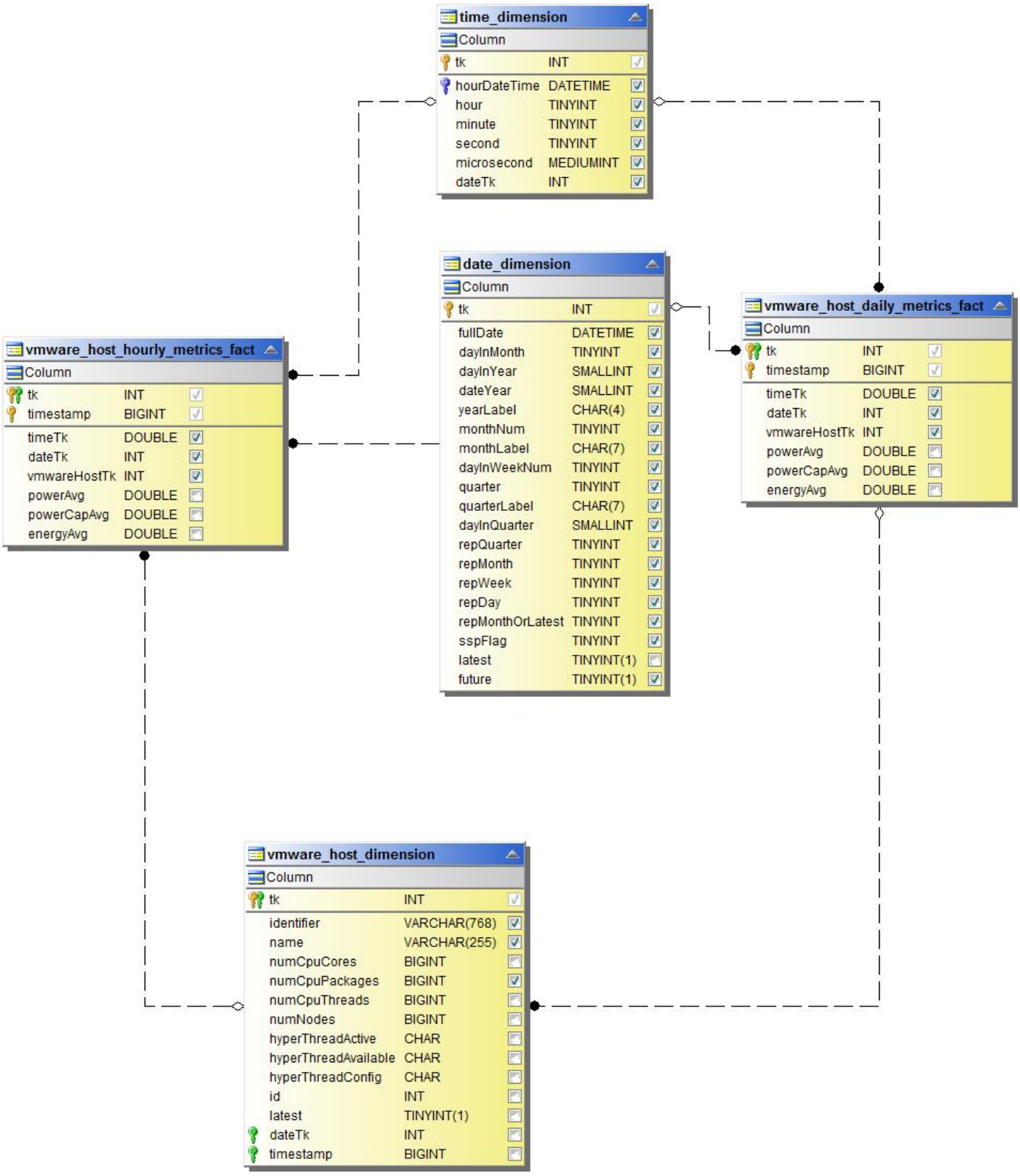
Performances des machines virtuelles



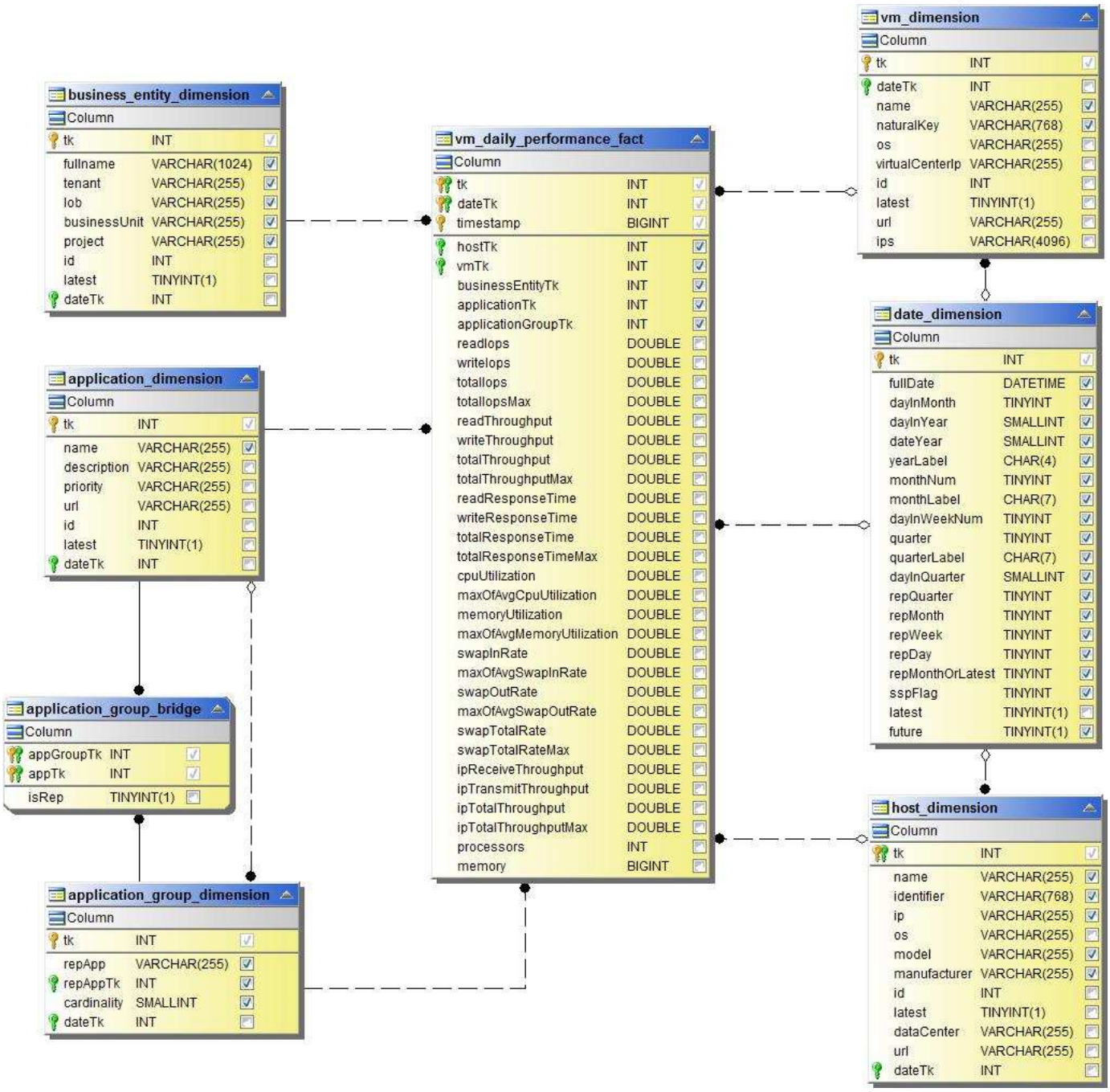
Performances quotidiennes des machines virtuelles pour l’hôte



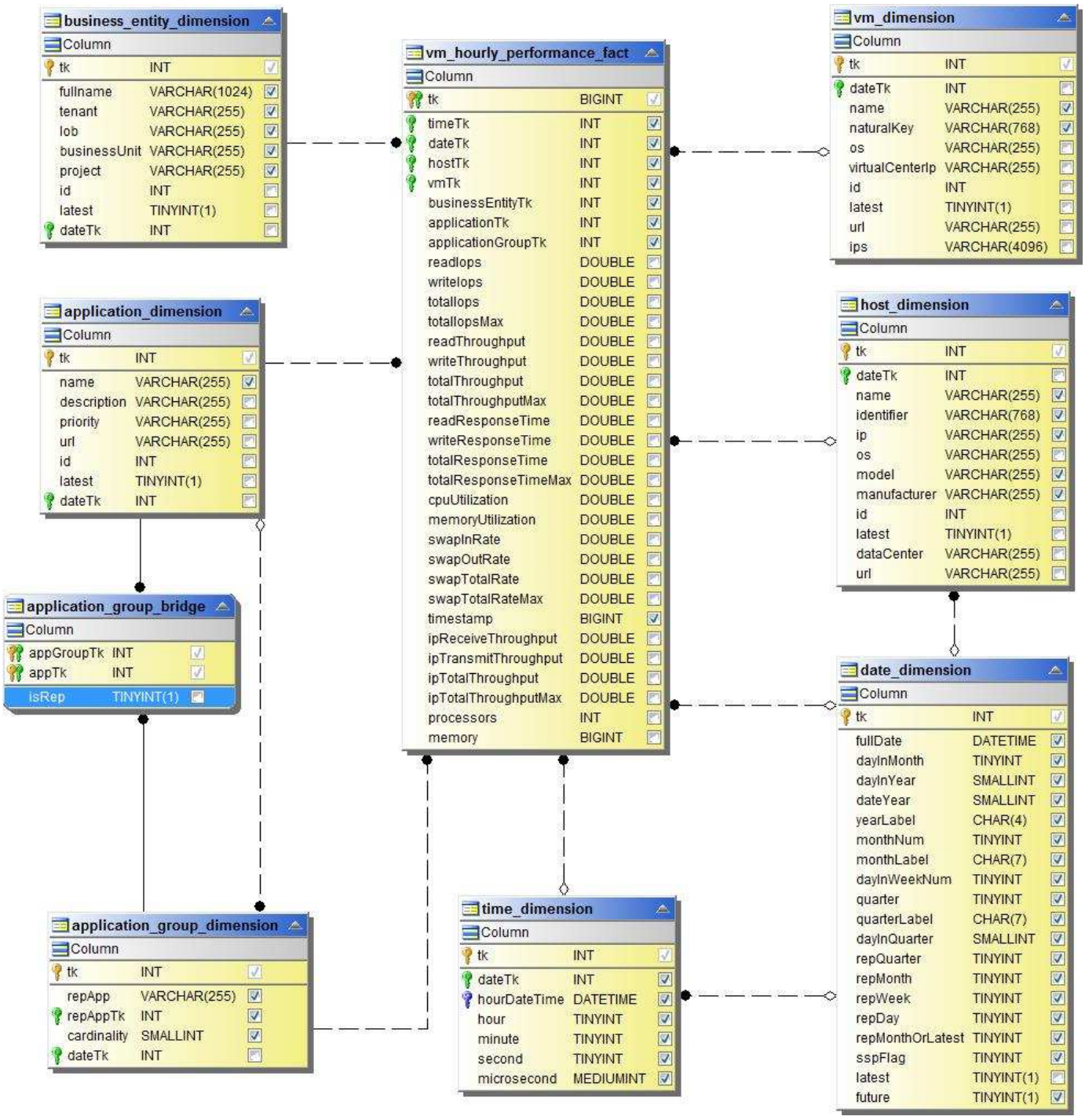
Performances des machines virtuelles horaires pour l’hôte



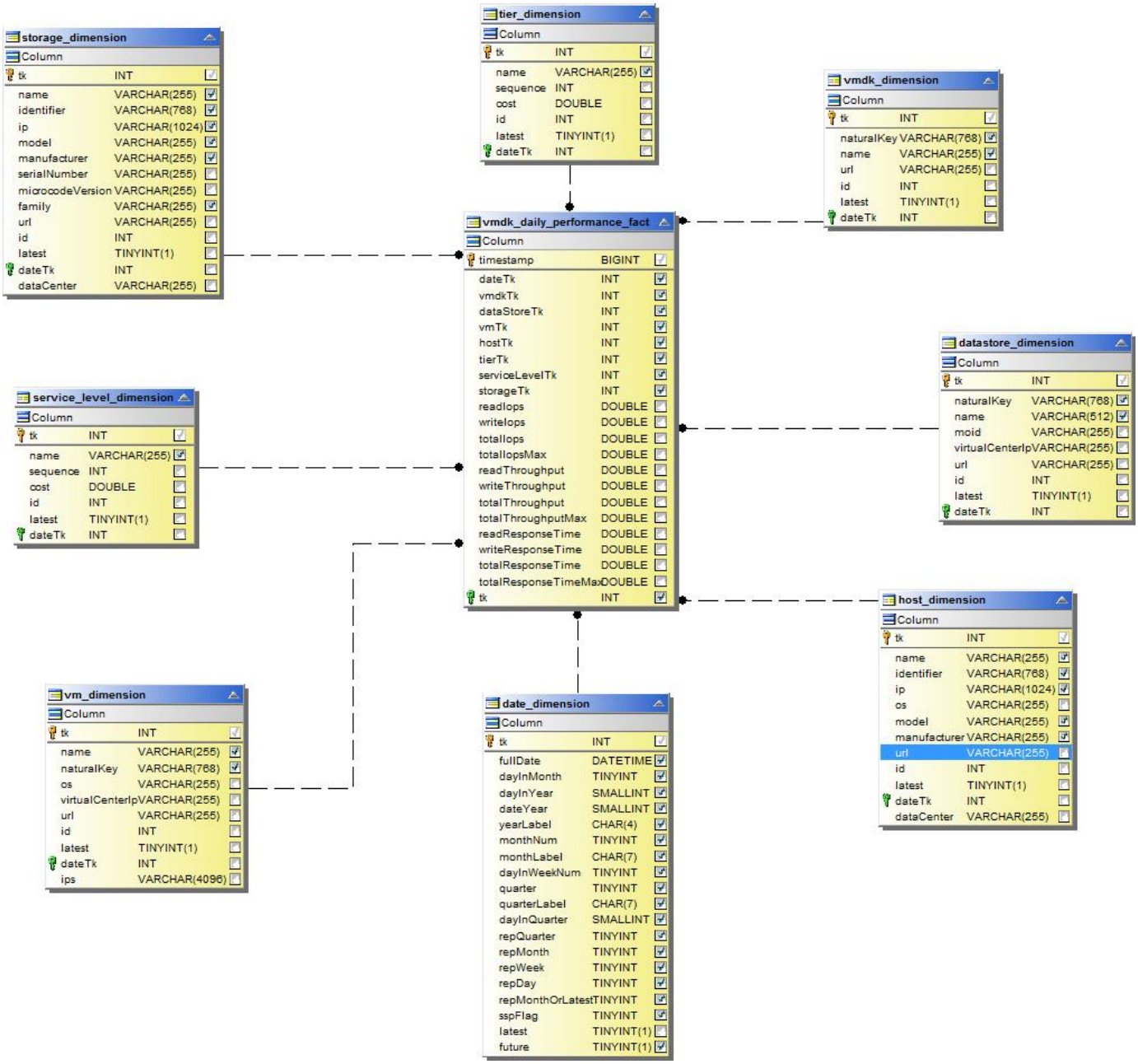
Performances quotidiennes des machines virtuelles pour l’hôte



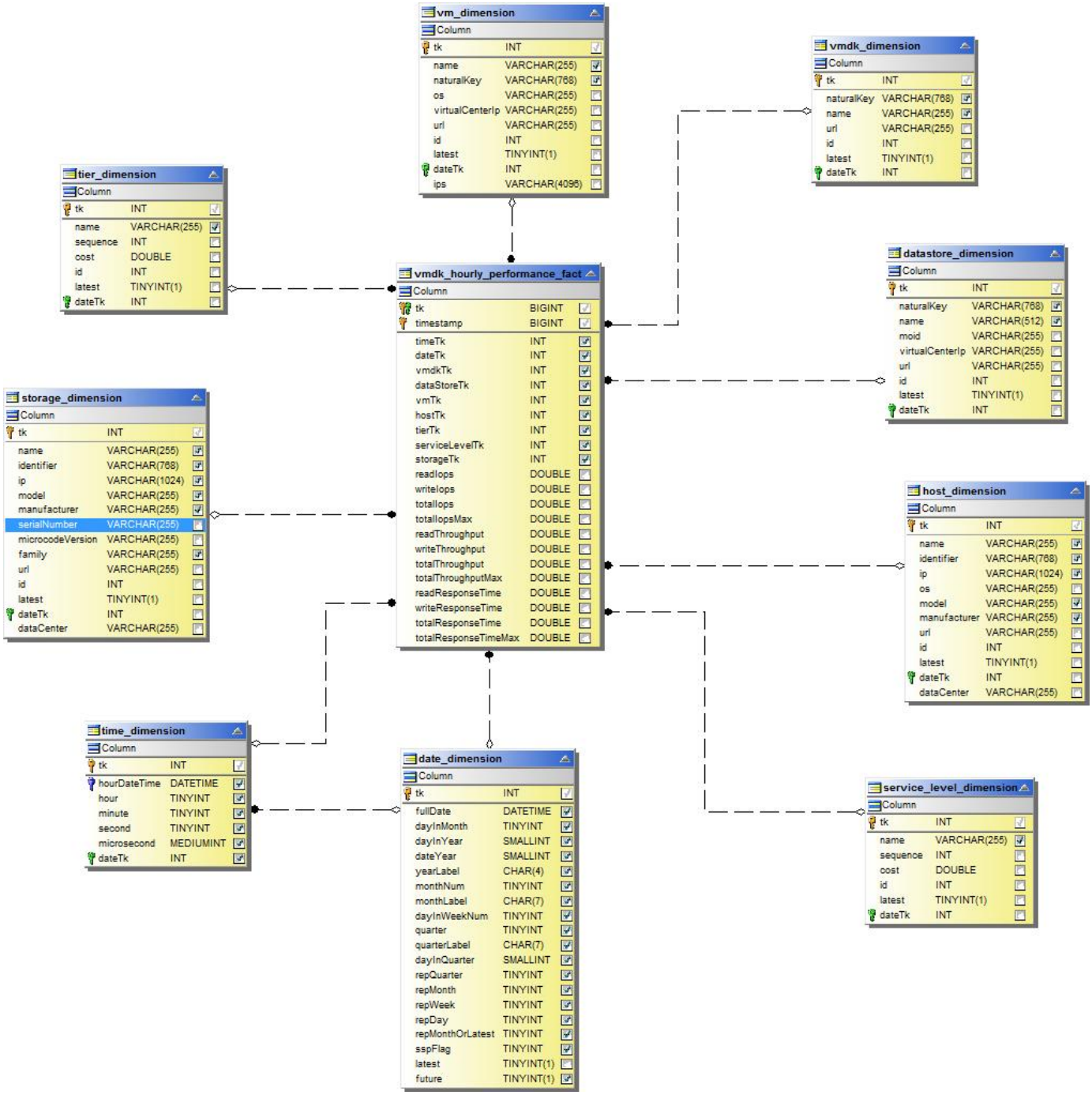
Performances des machines virtuelles horaires pour l'hôte



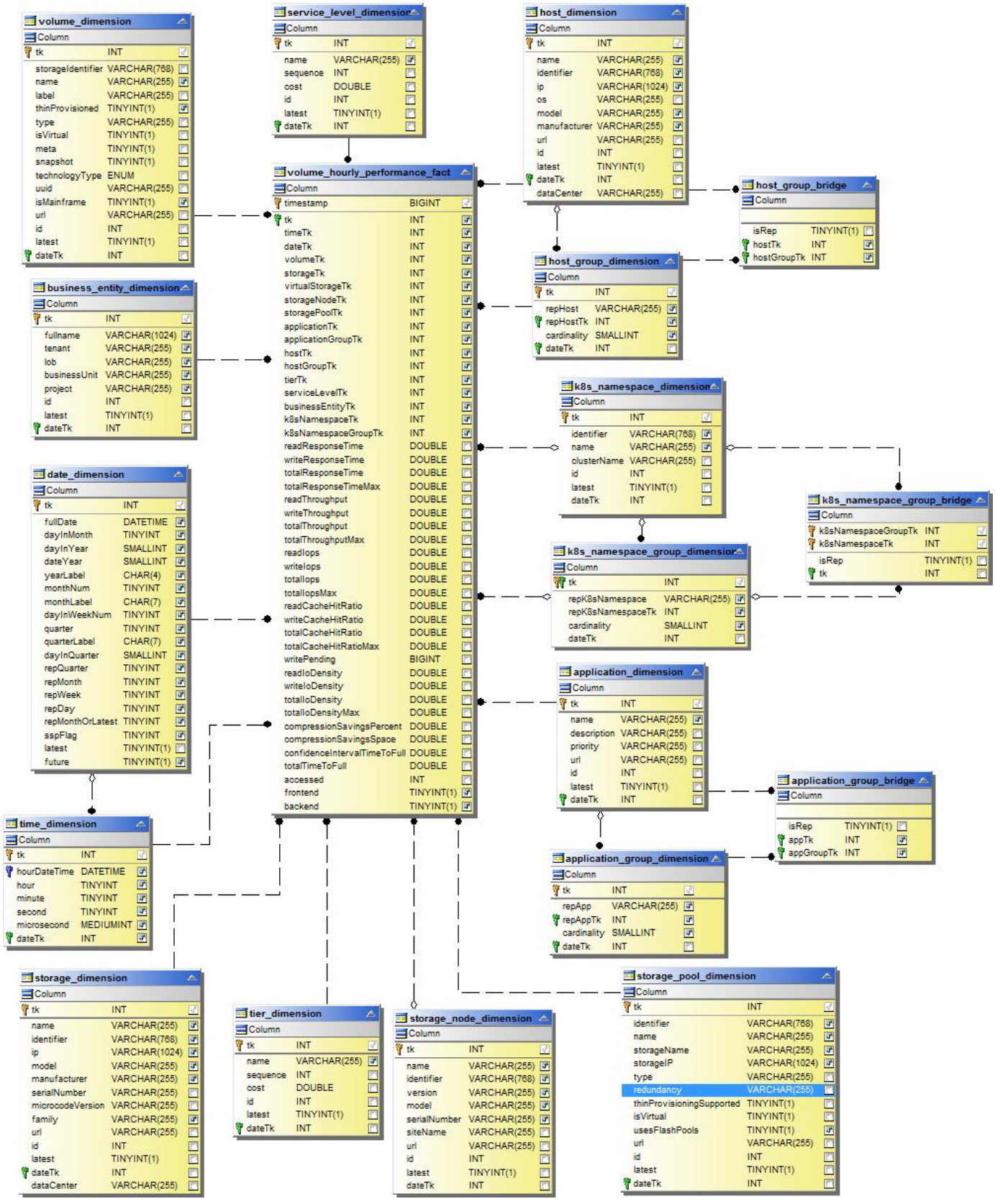
Performances quotidiennes des VMDK



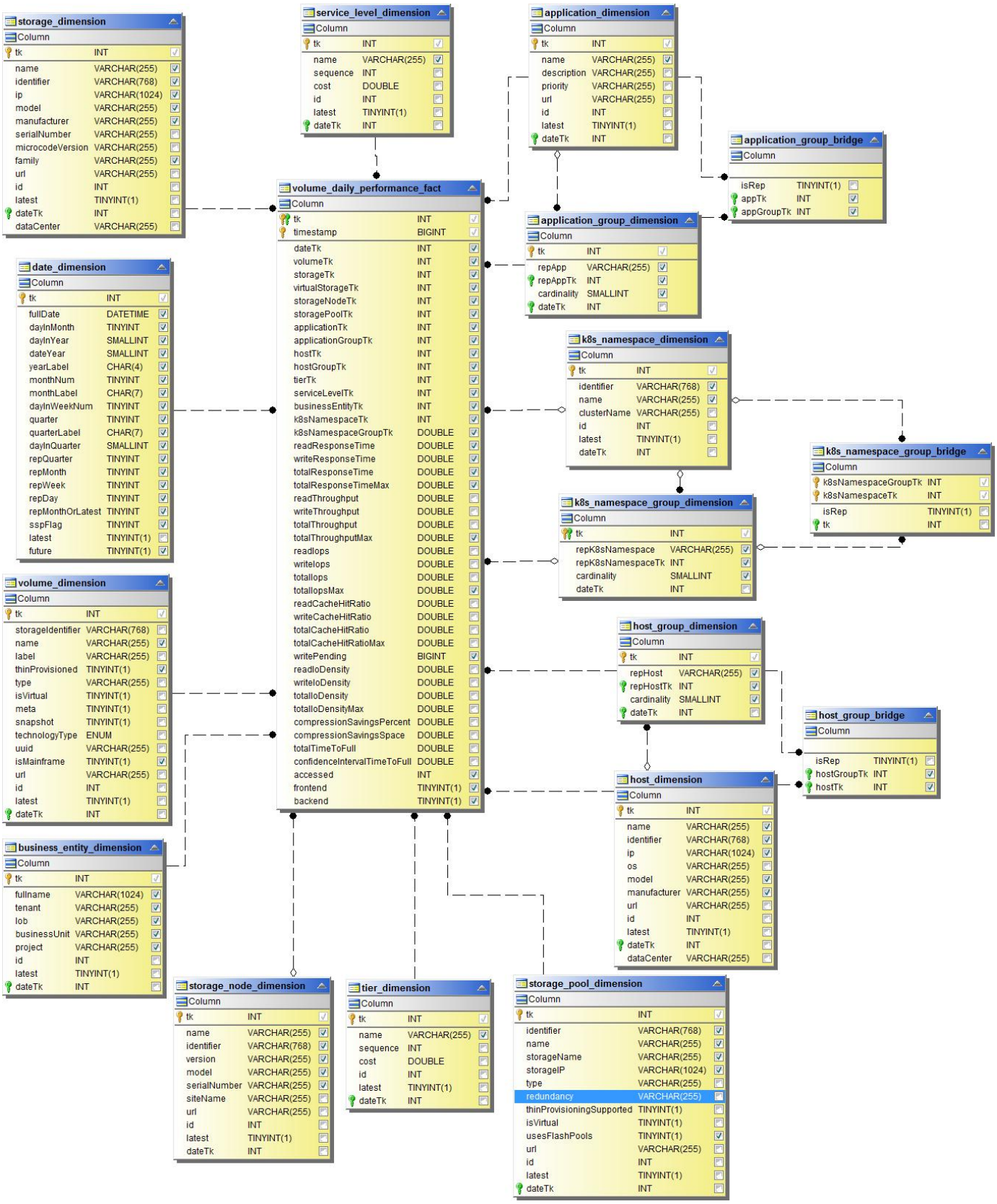
Performances VMDK à l'heure



Volume – rendement horaire



Volume performances quotidiennes



Schémas d’informations d’infrastructure de données pour le reporting

Ces tableaux et diagrammes de schéma sont fournis ici en tant que référence pour le reporting Data Infrastructure Insights.

"Tables de schémas" Au format .PDF. Cliquez sur le lien pour l'ouvrir ou cliquez avec le bouton droit de la souris et choisissez *Enregistrer sous…* pour le télécharger.

"Schémas"

La fonction de génération de rapports est disponible dans Data Infrastructure Insights "Édition Premium".

Kubernetes

Présentation du cluster Kubernetes

L'explorateur Kubernetes de Data Infrastructure Insights est un outil puissant pour afficher l'état et l'utilisation généraux de vos clusters Kubernetes. Il vous permet d'explorer facilement les domaines d'enquête.

Cliquez sur **tableaux de bord > Kubernetes Explorer** pour ouvrir la page liste des clusters Kubernetes. Cette page de présentation contient le tableau des clusters Kubernetes de votre locataire.



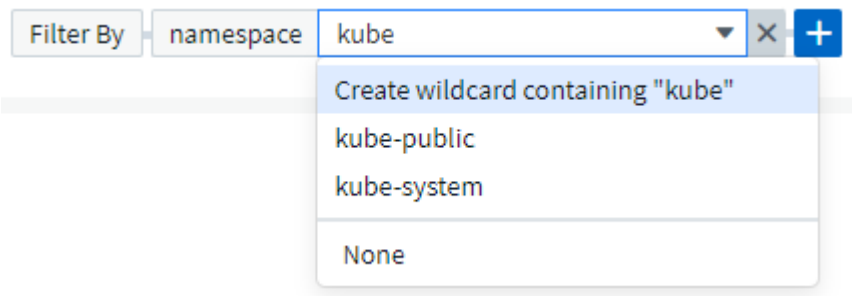
Liste des clusters

La liste des clusters affiche les informations suivantes pour chaque cluster de votre locataire :

- Nom * du cluster. Si vous cliquez sur le nom d'un cluster, le système s'ouvrira"page de détails".
- **Pourcentages de saturation**. La saturation globale est la saturation totale la plus élevée du processeur, de la mémoire ou du stockage.
- Nombre de **nœuds** dans le cluster. Cliquez sur ce numéro pour ouvrir la page liste des nœuds.
- Nombre de **Pods** dans le cluster. Cliquez sur ce numéro pour ouvrir la page de liste Pod.
- Nombre de **espaces de noms** dans le cluster. Cliquez sur ce numéro pour ouvrir la page de la liste d'espace de noms.
- Nombre de **charges de travail** dans le cluster. Cliquez sur ce numéro pour ouvrir la page de la liste des charges de travail.

Raffinage du filtre

Lorsque vous filtrez, lorsque vous commencez à taper, vous avez la possibilité de créer un **filtre générique** basé sur le texte en cours. Si vous sélectionnez cette option, tous les résultats correspondant à l'expression de caractère générique seront résélectionnés. Vous pouvez également créer **expressions** à l'aide DE NOT ou ET, ou sélectionner l'option "aucun" pour filtrer les valeurs nulles dans le champ.



Filtres basés sur des caractères génériques ou des expressions (par exemple NON, ET, « aucun », etc.) s'affichent en bleu foncé dans le champ du filtre. Les éléments que vous sélectionnez directement dans la liste s'affichent en bleu clair.



Les filtres Kubernetes sont contextuels, ce qui signifie par exemple que si vous vous trouvez sur une page de nœud spécifique, le filtre pod_name ne répertorie que les pods associés à ce nœud. De plus, si vous appliquez un filtre à un espace de noms spécifique, le filtre nom_pod répertorie uniquement les pods sur ce nœud *et* dans cet espace de noms.

Notez que le filtrage des caractères génériques et des expressions fonctionne avec du texte ou des listes, mais pas avec des valeurs numériques, des dates ou des valeurs booléennes.

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 "Opérateur de surveillance Kubernetes".

Composant	Conditions requises
Version Kubernetes	Kubernetes v1.20 et versions ultérieures.
Distributions Kubernetes	AWS Elastic Kubernetes Service (EKS) Azure Kubernetes Service (AKS) Google Kubernetes Engine (GKE) Red Hat OpenShift Rancher Kubernetes Engine (RKE) VMware Tanzu
Linux	Data Infrastructure Insights ne prend pas en charge les nœuds qui s'exécutent avec l'architecture Arm64. Surveillance réseau : doit exécuter le noyau Linux version 4.18.0 ou ultérieure. Le système d'exploitation de photons n'est pas pris en charge.
Étiquettes	Les informations d'infrastructure de données prennent en charge la surveillance des nœuds Kubernetes exécutant Linux, en spécifiant un sélecteur de nœuds Kubernetes qui recherche les étiquettes Kubernetes suivantes sur ces plateformes : Kubernetes v1.20 et versions ultérieures : Kubernetes.io/os = linux Rancher + bétail.io comme plateforme d'orchestration/Kubernetes : bétail.io/os = linux
Commandes	Les commandes curl et kubectl doivent être disponibles.; pour de meilleurs résultats, ajoutez ces commandes au CHEMIN.

Composant	Conditions requises
Connectivité	Kubectl cli est configuré pour communiquer avec le cluster K8s cible et dispose d'une connectivité Internet à votre environnement Data Infrastructure Insights. Si vous êtes derrière un proxy pendant l'installation, suivez les instructions de "Configuration du support de proxy"la section installation de l'opérateur. Pour un audit et un reporting précis des données, synchronisez l'heure sur la machine Agent à l'aide du protocole NTP (Network Time Protocol) ou SNTP (simple Network Time Protocol).
Autre	Si vous utilisez OpenShift 4.6 ou une version supérieure, vous devez suivre le en plus de vous "Instructions OpenShift"assurer que ces conditions préalables sont remplies.
Jeton d'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 d'API ; vous pouvez réutiliser le jeton précédent.

Points importants à noter avant de commencer

Si vous référentiel personnaliséutilisez un proxy, utilisez un , ou OpenShift, lisez attentivement les sections suivantes.

Lisez également à propos de Autorisations.

Configuration du support de proxy

Vous pouvez utiliser un proxy sur votre locataire à deux endroits pour installer l'opérateur de surveillance Kubernetes NetApp. Il peut s'agir de systèmes proxy identiques ou distincts :

- Proxy nécessaire lors de l'exécution de l'extrait de code d'installation (à l'aide de « curl ») pour connecter le système sur lequel l'extrait de code 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'une ou l'autre de ces versions, ou les deux, pour installer le moniteur d'exploitation NetApp Kubernetes, vous devez d'abord vous assurer que votre proxy est configuré pour permettre une bonne communication avec votre environnement Data Infrastructure Insights. Par exemple, dans les serveurs/machines virtuelles depuis lesquels vous souhaitez installer l'opérateur, vous devez être en mesure d'accéder aux informations exploitables de l'infrastructure de données et de télécharger des binaires depuis Data Infrastructure Insights.

Pour le proxy utilisé pour installer le moniteur d'exploitation NetApp Kubernetes, définissez les variables d'environnement *http_proxy/https_proxy* avant d'installer l'opérateur. Pour certains environnements proxy, il peut être nécessaire de définir la variable *no_proxy Environment*.

Pour définir la ou les variables, effectuez les opérations 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 n'a 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 la
commande suivante :
```

```
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 l'opérateur de surveillance Kubernetes NetApp après avoir lu toutes ces instructions.

Configurez la section proxy de 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
  ...
...
```

À l'aide d'un référentiel docker personnalisé ou privé

Par défaut, l'opérateur de surveillance Kubernetes NetApp extrait les images du conteneur du référentiel informations exploitables de l'infrastructure de données. Si vous utilisez un cluster Kubernetes comme cible de surveillance et que ce cluster est configuré pour extraire uniquement les 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 requis par l'opérateur de surveillance NetApp Kubernetes.

Exécutez l'extrait de code image dans la mosaïque d'installation de NetApp Monitoring Operator. Cette commande permet de se connecter au référentiel Data Infrastructure Insights, d'extraire toutes les dépendances d'image pour l'opérateur et de se déconnecter du référentiel Data Infrastructure Insights. Lorsque vous y êtes invité, saisissez le mot de passe temporaire du référentiel fourni. Cette commande permet de télécharger toutes les images utilisées par l'opérateur, y compris pour les fonctions facultatives. Voir ci-dessous pour connaître les caractéristiques auxquelles ces images sont utilisées.

Fonctionnalités centrales de l'opérateur et surveillance Kubernetes

- surveillance netapp
- proxy kube-rbac
- metrics-état-kube
- telegraf
- utilisateur-root-distroless

Journal des événements

- fluent-bit
- exportateur-événements-kubernetes

Performances et carte réseau

- ci-net-observateur

Envoyez l'image de docker de l'opérateur à votre référentiel docker privé, local ou d'entreprise, conformément aux règles de votre entreprise. Assurez-vous que les balises d'image et les chemins de répertoire vers 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 la configuration d'agentConfiguration dans Operator-config.yaml pour refléter le nouvel emplacement docker repo. Créez une nouvelle imagePullSecret pour votre référentiel privé. Pour plus de détails, voir *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 exécutez sur OpenShift 4.6 ou une version ultérieure, vous devez modifier la configuration d'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 contrôlez contient des ressources personnalisées qui n'ont pas de ClusterRole "agrégats à afficher", vous devez 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 les ressources souhaités avec les verbes ["get", "Watch", "list"]. Voir https://kubernetes.io/docs/reference/access-authn-authz/rbac/
3. Appliquez vos modifications au cluster

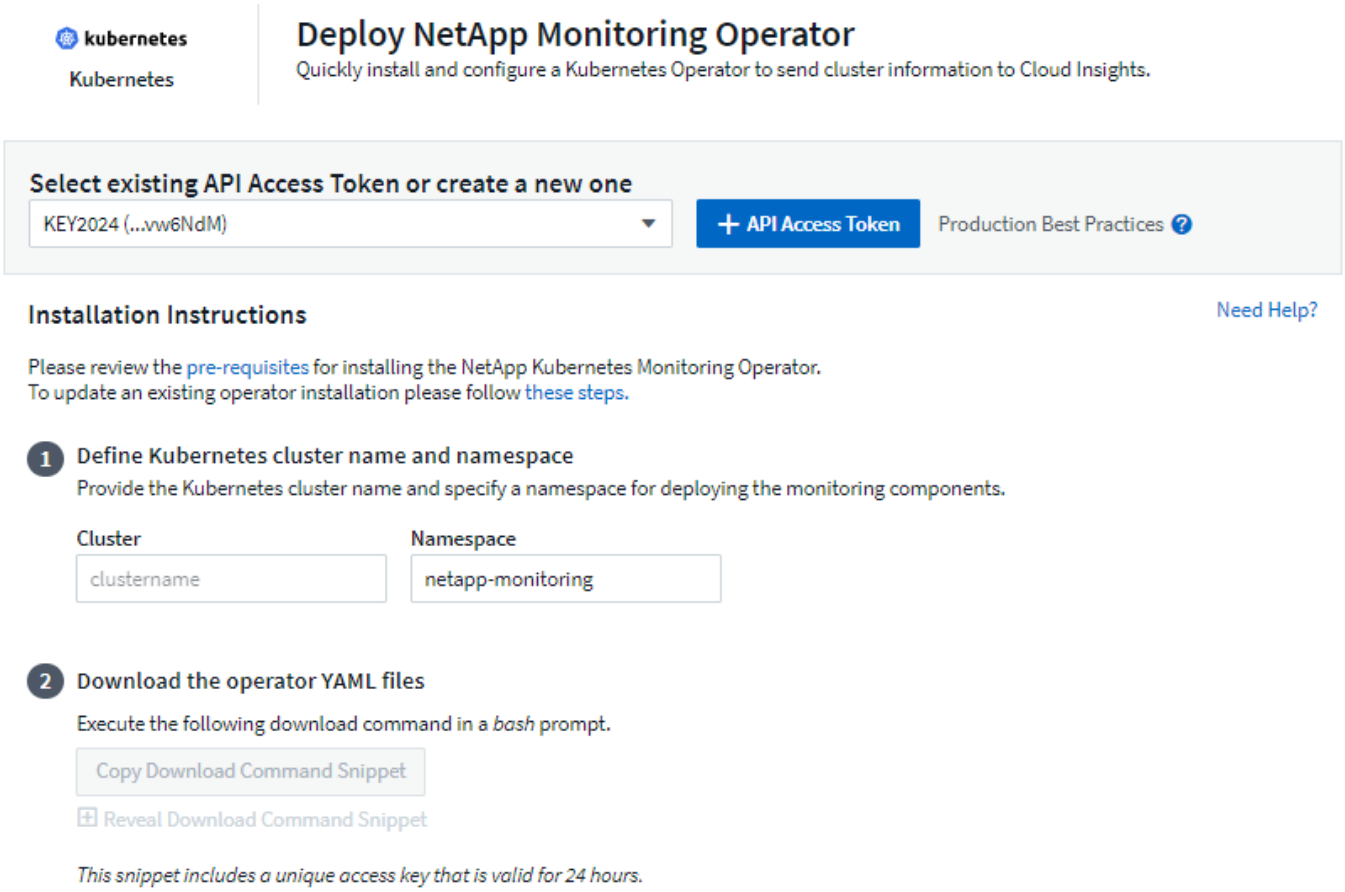
Installation et configuration de l'opérateur de contrôle Kubernetes

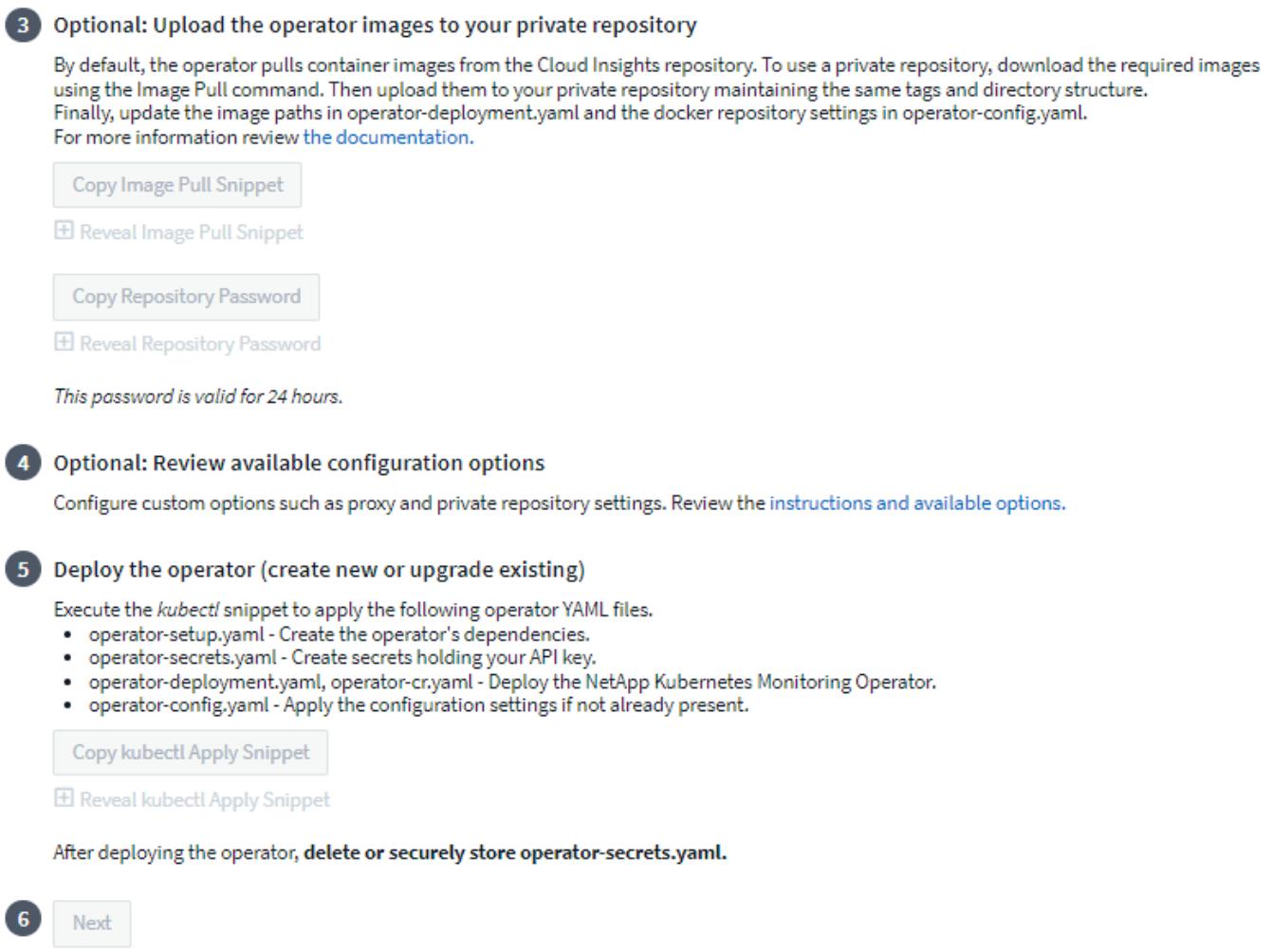
Data Infrastructure Insights propose l'opérateur **Kubernetes Monitoring Operator** pour la collecte Kubernetes. Accédez à **Kubernetes > Collectors > +Kubernetes Collector** pour déployer un nouvel opérateur.

Avant d'installer l'opérateur de surveillance Kubernetes

Consultez "Conditions préalables"la documentation avant d'installer ou de mettre à niveau l'opérateur de surveillance Kubernetes.

Installation de l'opérateur de surveillance Kubernetes





Étapes d'installation de l'agent opérateur de surveillance Kubernetes sur Kubernetes :

1. Entrez un nom de cluster et un espace de noms uniques. Si vous mise à niveauutilisez un opérateur Kubernetes précédent, utilisez le même nom de cluster et le même espace de noms.
2. Une fois ces données saisies, vous pouvez copier le fragment de commande de téléchargement dans le presse-papiers.
3. Collez le fragment dans une fenêtre *bash* et exécutez-le. Les fichiers d'installation de l'opérateur seront téléchargés. Notez que l'extrait de code possède une clé unique et est valide pendant 24 heures.
4. Si vous disposez d'un référentiel personnalisé ou privé, copiez le fragment facultatif image Pull, 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, passez en revue 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 le fragment kubectl Apply, en le téléchargeant et en l'exécutant.
7. L'installation se poursuit 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 propos de à l'aide d'un référentiel docker

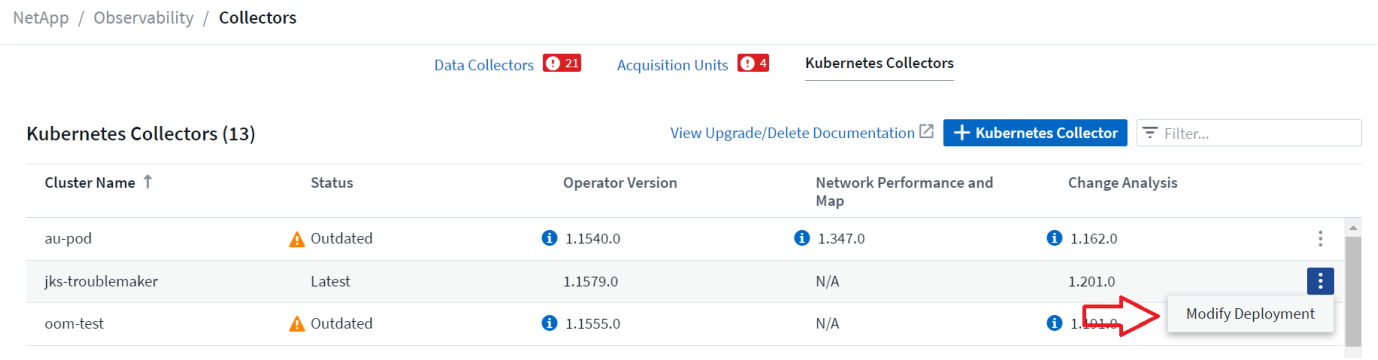
personnalisé/privé.

Composants de surveillance Kubernetes

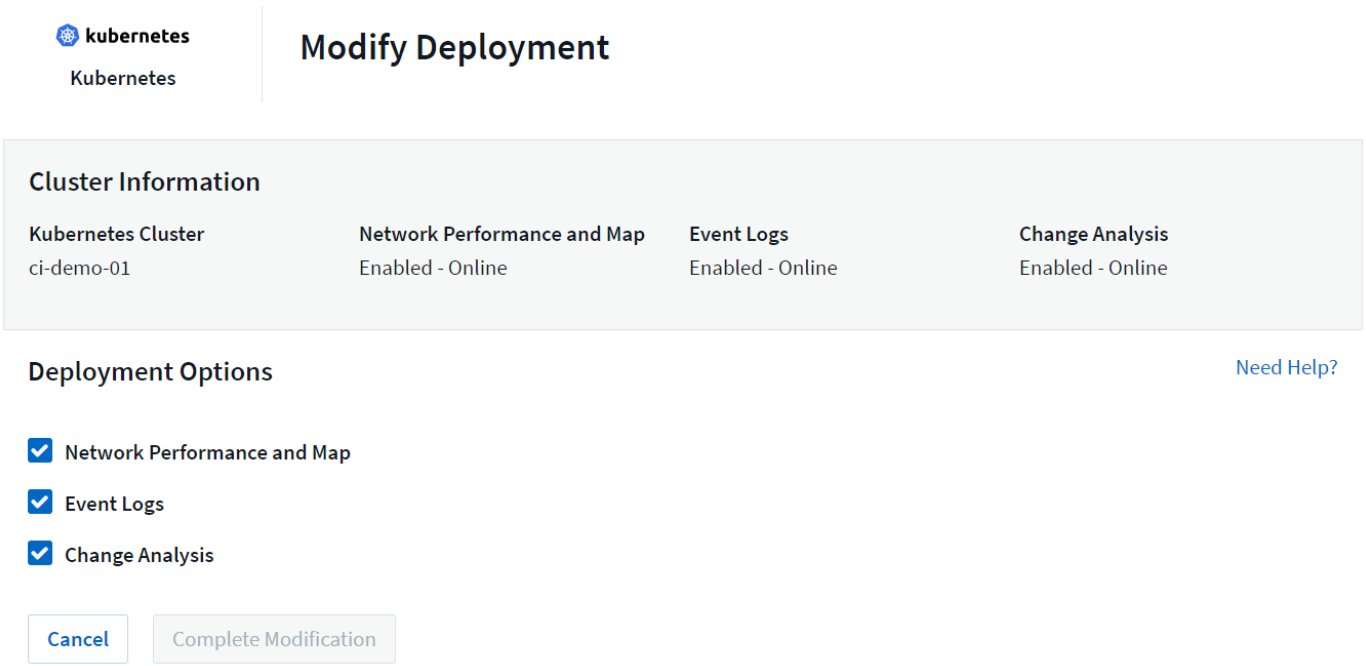
La surveillance Kubernetes de Data Infrastructure Insights comprend quatre composants de surveillance :

- Metrics du cluster
- Carte et performances réseau (en option)
- Journaux d'événements (facultatif)
- Analyse des modifications (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 > Collectors** et en sélectionnant *Modify Deployment* 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 pour ce collecteur selon vos besoins.



Mise à niveau vers le dernier opérateur de surveillance Kubernetes

Mises à niveau DII à bouton-poussoir

Vous pouvez mettre à niveau l'opérateur de surveillance Kubernetes à partir de la page collecteurs Kubernetes DII. Cliquez sur le menu en regard du cluster que vous souhaitez mettre à niveau et sélectionnez *Upgrade*. L'opérateur vérifie les signatures d'image, effectue un instantané de votre installation actuelle et effectue la mise à niveau. Dans quelques minutes, vous devriez voir l'état de l'opérateur progression de la mise à niveau en cours vers la dernière. Si vous rencontrez une erreur, vous pouvez sélectionner l'état d'erreur pour plus de détails et vous reporter au tableau Dépannage des mises à niveau par bouton-poussoir ci-dessous.

Mises à niveau à l'aide de référentiels privés par simple pression

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 les images manquantes, ajoutez-les simplement à votre référentiel et réessayez la mise à niveau. Pour télécharger les signatures d'images dans votre référentiel, utilisez l'outil de cosignature comme suit, en vous assurant de télécharger les signatures pour toutes les images spécifiées sous 3 Facultatif : chargez 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>
```

Retour à une version précédente

Si vous avez effectué une mise à niveau à l'aide de la fonction de mise à niveau par bouton-poussoir et que vous rencontrez des difficultés avec la version actuelle de l'opérateur dans les sept jours suivant la mise à niveau, vous pouvez revenir à la version précédente en utilisant l'instantané créé pendant le processus de mise à niveau. Cliquez sur le menu en regard du cluster que vous souhaitez restaurer et sélectionnez *Retour arrière*.

Mises à niveau manuelles

Déterminez si une configuration d'agentConfiguration existe avec l'opérateur existant (si votre espace de noms n'est pas le *netapp-monitoring* par défaut, remplacez l'espace de noms approprié) :

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-ci-monitoring-
configuration
Si une configuration d'agentConfiguration existe :
```

- Installez Dernier opérateur par rapport à l'opérateur existant.
  - Assurez-vous que vous extraction des dernières images du conteneurutilisez un référentiel personnalisé.

Si AgentConfiguration n'existe pas :

- Notez le nom de votre cluster tel qu'il a été reconnu par les informations d'infrastructure de données (si votre namespace n'est pas le contrôle NetApp par défaut, remplacez l'espace de noms approprié) :

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* Créer une sauvegarde de l'opérateur existant (si votre namespace n'est
pas la surveillance netapp par défaut, remplacez le namespace 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,Installez>> Le dernier
opérateur.
```

  - Utilisez le même nom de cluster.
  - Après avoir téléchargé les derniers fichiers Operator YAML, porter toutes les personnalisations trouvées dans agent_backup.yaml à l'opérateur-config.yaml téléchargé avant le déploiement.
  - Assurez-vous que vous extraction des dernières images du conteneurutilisez 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 de l'opérateur de surveillance Kubernetes est « netapp-monitoring ». Si vous avez défini votre propre espace de noms, remplacez-le dans ces commandes et tous les fichiers suivants.

Les nouvelles versions de l'opérateur de surveillance peuvent être désinstallées à l'aide des 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, supprimer l'espace de noms :

```
 kubectl delete ns <NAMESPACE>
Remarque : si la première commande renvoie "aucune ressource trouvée",
suivez les instructions ci-dessous pour désinstaller les anciennes
versions de l'opérateur de surveillance.
```

Exécutez chacune des commandes suivantes dans l'ordre indiqué. Selon votre installation actuelle, certaines de ces commandes peuvent renvoyer des messages « objet introuvable ». 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 des indicateurs Kube-State

L'opérateur de surveillance NetApp Kubernetes installe ses propres metrics kube-State pour éviter les conflits avec d'autres instances.

Pour plus d'informations sur Kube-State-Metrics, reportez-vous à "cette page"la section .

Configuration/personnalisation de l'opérateur

Ces sections contiennent des informations sur la personnalisation de la configuration de votre opérateur, l'utilisation du 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 contient des exemples de paramètres commentés. Voir la liste des pour la version la plus récente de "paramètres disponibles"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 du support de proxy

Vous pouvez utiliser un proxy sur votre locataire à deux endroits pour installer l'opérateur Kubernetes Monitoring. Il peut s'agir de systèmes proxy identiques ou distincts :

- Proxy nécessaire lors de l'exécution de l'extrait de code d'installation (à l'aide de « curl ») pour connecter le système sur lequel l'extrait de code 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'une ou l'autre de ces opérations, ou pour les deux, 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 que vous 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 le moniteur d'exploitation Kubernetes, avant d'installer l'opérateur, définissez les variables d'environnement *http_proxy/https_proxy*. Pour certains environnements proxy, il peut être nécessaire de définir la variable *no_proxy Environment*.

Pour définir la ou les variable(s), effectuez les opérations suivantes sur votre système **avant** installation de l'opérateur de surveillance Kubernetes :

1. Définissez les variables d'environnement *https_proxy* et/ou *http_proxy* pour l'utilisateur actuel :
    a. Si le proxy en cours de configuration n'a 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 la
commande suivante :
```

```
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 l'opérateur de surveillance Kubernetes après avoir lu toutes ces instructions.

Configurez la section proxy d'AgentConfiguration dans Operator-config.yaml avant de déployer l'opérateur de surveillance 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
  ...
...
```

À l'aide d'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 utilisez un cluster Kubernetes comme cible pour la surveillance et que ce cluster est configuré pour extraire uniquement les 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 requis par l'opérateur de surveillance Kubernetes.

Exécutez l'extrait de code image dans la mosaïque d'installation de NetApp Monitoring Operator. Cette commande permet de se connecter au référentiel Data Infrastructure Insights, d'extraire toutes les dépendances d'image pour l'opérateur et de se déconnecter du référentiel Data Infrastructure Insights. Lorsque vous y êtes invité, saisissez le mot de passe temporaire du référentiel fourni. Cette commande permet de télécharger toutes les images utilisées par l'opérateur, y compris pour les fonctions facultatives. Voir ci-dessous pour connaître les caractéristiques auxquelles ces images sont utilisées.

Fonctionnalités centrales de l'opérateur et surveillance Kubernetes

- surveillance netapp
- proxy ci-kube-rbac
- ci-ksm
- ci-telegraf
- utilisateur-root-distroless

Journal des événements

- bit fluide ci
- ci-kubernetes-exportateur-événements

Performances et carte réseau

- ci-net-observateur

Envoyez l'image de docker de l'opérateur à votre référentiel docker privé, local ou d'entreprise, conformément aux règles de votre entreprise. Assurez-vous que les balises d'image et les chemins de répertoire vers 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 la configuration d'agentConfiguration dans Operator-config.yaml pour refléter le nouvel emplacement docker repo. Créez une nouvelle imagePullSecret pour votre référentiel privé. Pour plus de détails, voir *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
```

Instructions OpenShift

Si vous exécutez sur OpenShift 4.6 ou une version ultérieure, vous devez modifier la configuration d'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 tainations

Les *netapp-ci-telegraf-ds*, *netapp-ci-Fluent-bit-ds* et *netapp-ci-net-observateur-l4-ds* Demonsets 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 certains **taints** bien connus. Si vous avez configuré des fichiers d'accès personnalisés sur vos nœuds, empêchant ainsi les modules de s'exécuter sur chaque nœud, vous pouvez créer une **tolérance** pour ces fichiers d'accès "Dans *AgentConfiguration*". Si vous avez appliqué des rejets personnalisés 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 opérateur.

En savoir plus sur Kubernetes "Teintes et tolérances".

Revenir au **"Page installation de l'opérateur de surveillance NetApp Kubernetes"**

Remarque sur les secrets

Pour supprimer l'autorisation pour l'opérateur de surveillance Kubernetes d'afficher les secrets à l'échelle du cluster, supprimez les ressources suivantes du fichier *Operator-setup.yaml* avant d'installer :

```
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'option analyse des modifications est activée, modifiez *AgentConfiguration* ou *Operator-config.yaml* pour annuler le commentaire de la section de gestion des modifications et incluez *kindsToIgnoreFromWatch: '"secrets"'* dans la section de gestion des modifications. 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'images 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 co-signer 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 : télécharger les images de l'opérateur dans votre référentiel privé > clé publique de signature d'image*

Pour vérifier manuellement une signature d'image, effectuez les opérations suivantes :

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 du cosigne. Reportez-vous à l'exemple suivant d'utilisation des coenseignes

```
$ 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

Voici quelques points à essayer en cas de problème lors de la configuration de l'opérateur de surveillance Kubernetes :

Problème :	Essayer :
Je ne vois pas de lien hypertexte/connexion entre mon volume persistant Kubernetes et le périphérique de stockage back-end correspondant. Mon volume persistant Kubernetes est configuré en utilisant le nom d'hôte du serveur de stockage.	Procédez comme suit pour désinstaller l'agent Telegraf existant, puis réinstaller l'agent Telegraf le plus récent. Vous devez utiliser Telegraf version 2.0 ou ultérieure et le stockage de votre cluster Kubernetes doit être activement surveillé par Data Infrastructure Insights.
Je vois des messages dans les journaux qui ressemblent à ce qui suit : E0901 15 352:21:39.962145 178 1 Reflector.Go:178] k8s.io/kube-state-metrics/Internal/store/Builder.Go:43.168161 : échec de la liste *v1.MutatingWebhookio Configuration : le serveur n'a pas pu trouver la ressource demandée E0901 15:21/352/Reflector.s.Go.so	Ces messages peuvent se produire si vous exécutez des metrics d'état kube version 2.0.0 ou supérieure avec les versions Kubernetes inférieures à 1.20. Pour obtenir la version Kubernetes : *kubectl version* pour obtenir la version kube-state-metrics : *kubectl get deployment/kube-state-metrics -o jsonpath='{..image}'* pour éviter que ces messages se produisent, les utilisateurs peuvent modifier leur déploiement de metrics kube-state-metrics pour désactiver les baux suivants : *hookingwebconfigurations*. Ressources=certificats,demandes persistantes,configmaps,cronjobs,demonets, déploiements,noeuds finaux,horizontalepodpodscalers,ingresources,details, resuts,undats,depositionsstatees,depositigmats,defiees,resottes,depositionssecuts,defiees,dees,depositionunedats,delimantees,delimantees,deficedats,dees,delimantees,delimantees,delimantees,deficedats,delimantees,deficedats,delimantees,deficedats,deficedats,dees,delimantees,delimantees,dees,delimantees,deficedats,dees,delimantees,delimantees,delimantees,delimantees,de vaillewebconfiguration,v'

Problème :	Essayer :
Je vois des messages d'erreur de Telegraf ressemblant aux messages suivants, mais Telegraf démarre et s'exécute : oct 11 14:23:41 ip-172-31-39-47 systemd[1] : lancé l'agent serveur piloté par des plug-ins pour signaler des mesures dans InfluxDB. Oct 11 14:23:41 ip-172-31-39-47 telegraf[1827] : heure="2021-10-11T14:23:41Z" level=erreur msg="Impossible de créer le répertoire de cache. /Etc/telegraf/.cache/flocon de neige, err : mkdir /etc/telegraf/.ca che : permission refusée. Ignored\n » func="nowgosflake.(*defaultLogger).Errorf" file="log.Go:10" Oct 1827 23:2021:39-47 ip-172-31-41 telegraf[11 14] : échec de l'ouverture:23:120. Ignoré. Ouvrir /etc/telegraf/.cache/flocon/ocsp_Response_cache.jso n : pas de fichier ou répertoire\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.Go:120 10" Oct 23:2021:39-47 ip-1827-31 telegraf[172]: 23-41-11 14:11Z! Démarrage de Telegraf 1.19.3	Il s'agit d'un problème connu. Voir "Article GitHub"pour plus de détails. Tant que Telegraf est opérationnel, les utilisateurs peuvent ignorer ces messages d'erreur.
Sur Kubernetes, mes coffee pad(s) Telegraf ont signalé l'erreur suivante : "erreur lors du traitement des informations de mountstats : échec de l'ouverture du fichier mountstats: /Hostfs/proc/1/mountstats, erreur: Ouvrir /hostfs/proc/1/mountstats: Permission refusée"	Si SELinux est activé et applique, il empêche probablement le ou les pod(s) Telegraf d'accéder au fichier /proc/1/mountstats sur le nœud Kubernetes. Pour contourner cette restriction, modifiez la configuration d'agentconfiguration 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 plug-in : impossible de charger keypair /etc/kubernetes/pki/ETcd/Server.crt:/etc/kubernetes/pki/ETcd/Server.key : ouvrir /etc/kubernetes/pki/ETcd/Server.crt : aucun fichier ni répertoire	Le pod Télégraf ReplicaSet est conçu pour 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 obtenez ces erreurs. Vérifiez si vos nœuds maître/ETCD ont des astuces sur eux. S'ils le font, ajoutez les tolérances nécessaires à Telegraf ReplicaSet, telegraf-RS. Par exemple, modifiez le ReplicaSet… kubectl edit RS telegraf-RS …et ajoutez les tolérances appropriées à la spécification. Redémarrez ensuite le pod ReplicaSet.

Problème :	Essayer :
J'ai un environnement PSP/PSA. Cela affecte-t-il mon opérateur de surveillance ?	Si votre cluster Kubernetes s'exécute avec la règle de sécurité Pod (PSP) ou l'admission de sécurité Pod (PSA) sur place, vous devez effectuer la mise à niveau vers l'opérateur de surveillance Kubernetes le plus récent. Procédez comme suit pour mettre à niveau vers l'opérateur actuel avec la prise en charge de PSP/PSA : 1. Désinstaller le précédent opérateur de surveillance : kubectl delete 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-cluster-agent-roleadmin-binding-cluster-2-agent-binding. Installez dernière version de l'opérateur de surveillance.
J'ai rencontré des problèmes lors de la tentative de déploiement de l'opérateur, et j'ai utilisé PSP/PSA.	1. Modifiez l'agent à l'aide de la commande suivante : kubectl -n <name-space> edit agent 2. Marquez « Security-policy-enabled » comme « false ». Ceci désactivera les stratégies de sécurité du Pod et l'admission de sécurité du Pod et permettra à l'opérateur de déployer. Confirmez en utilisant les commandes suivantes : kubectl get psp (devrait afficher Pod Security Policy supprimé) kubectl get all -n <namespace>
grep -i psp (doit montrer que rien n'a été trouvé)	Erreurs « ImagePullBackoff » détectées
Ces erreurs peuvent se produire si vous disposez d'un référentiel docker personnalisé ou privé et que vous n'avez pas encore configuré l'opérateur de surveillance Kubernetes pour qu'il le reconnaisse correctement. En savoir plus a propos de la configuration pour 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.

Capturer ou noter le résultat des commandes suivantes et contacter 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-observateur (Workload Map) de l'espace de noms de l'opérateur se trouvent dans CrashLoopBackOff

Problème :	Essayer :
Ces pods correspondent au collecteur de données Workload Map pour l'observabilité réseau. Essayez : • Vérifiez les journaux de l'un des modules pour confirmer la version minimale du noyau. Par exemple : --- {"ci-tenant-ID":"votre-tenant-ID","collectionneur-cluster":"votre-k8s-cluster-name","Environment":"prod","level":"error","msg":"échec de la validation. Raison : la version 3.10.0 du noyau est inférieure à la version minimale du noyau de 4.18.0","Time":"2022-11-09T08:23:08Z"} ---- • les pods Net-observateur requièrent 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'ils sont >= 4.18.0	Les pods s'exécutent dans l'espace de noms Operator (par défaut : surveillance netapp), mais aucune donnée n'est affichée dans l'interface pour la carte des workloads ou les metrics Kubernetes dans les requêtes
Vérifiez le réglage de l'heure sur les nœuds du cluster K8S. Pour un audit et un reporting précis des données, il est vivement recommandé de synchroniser l'heure sur l'ordinateur de l'agent à l'aide du protocole NTP (Network Time Protocol) ou SNTP (simple Network Time Protocol).	Certains des pods net-observateur dans l'espace de noms de l'opérateur sont à l'état en attente
Net-observateur est un DemonSet et exécute un pod dans chaque nœud du cluster k8s. • Notez le pod qui est à l'état en attente et vérifiez s'il rencontre un problème de ressource 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 l'opérateur de surveillance Kubernetes : [inputs.prometheus] erreur dans le plug-in : erreur lors de la demande HTTP vers http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics : get http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics : Dial tcp: kube-state-metrics.<namespace>.svc.cluster.local : pas de recherche d'hôte
Ce message n'apparaît généralement que lorsqu'un nouvel opérateur est installé et que le module *telegraf-RS* est en marche avant que le module *ksm* ne soit en marche. Ces messages doivent s'arrêter une fois que tous les modules sont en cours d'exécution.	Je ne vois aucun indicateur collecté pour les cronjobs Kubernetes qui existent dans mon cluster.
Vérifiez votre version de Kubernetes (c'est-à-dire `kubectl version`). S'il est v1.20.x ou inférieur, il s'agit d'une limitation attendue. La version de kube-state-metrics déployée avec l'opérateur de surveillance Kubernetes ne prend en charge que v1.cronjob. Avec Kubernetes 1.20.x et versions antérieures, la ressource cronjob est à v1beta.cronjob. Par conséquent, les indicateurs d'état kube ne peuvent pas trouver la ressource cronjob.	Après l'installation de l'opérateur, les modules telegraf-ds entrent dans CrashLoopBackOff et les journaux du pod indiquent « su: Authentication failure ».

Problème :	Essayer :
Modifiez la section telegraf dans *AgentConfiguration* et définissez *dockerMetricCollectionEnabled* sur FALSE. Pour plus de détails, reportez-vous au "options de configuration"manuel de l'opérateur . … spec: … telegraf: … - Nom: docker run-mode : - DemonSet substitutions: - Key: DOCKER_UNIX_SOCK_PLACEHOLDER valeur: unix:///run/docker.sock … …	Je vois des messages d'erreur récurrents ressemblant à ce qui suit dans mes journaux Telegraf: E! [Agent] erreur d'écriture dans outputs.http: Post "https://<tenant_url>/REST/v1/Lake/iningt/influxdb": Délai de contexte dépassé (client. Dépassement du délai d'attente des en-têtes)
Modifiez la section telegraf dans *AgentConfiguration* et augmentez *outputTimeout* à 10 s. Pour plus de détails, reportez-vous au "options de configuration"manuel de l'opérateur .	Il me manque des données *involvedobject* pour certains journaux d'événements.
Assurez-vous d'avoir suivi les étapes de la "Autorisations" section ci-dessus.	Pourquoi deux modules d'opérateurs de surveillance s'exécutent, l'un nommé netapp-ci-monitoring-Operator-<pod> et l'autre Monitoring-Operator-<pod> ?
Depuis le 12 octobre 2023, Data Infrastructure Insights a été décidé de réorganiser l'opérateur pour mieux répondre aux besoins de nos utilisateurs. Pour que ces changements soient entièrement adoptés, vous devez retirez l'ancien opérateur et installez le nouveau.	Mes événements kubernetes ont cessé de générer des rapports à Data Infrastructure Insights de manière inattendue.
Récupérer le nom du pod Event-exportateur : `kubectl -n netapp-monitoring get pods`	grep event-exporter

Problème :	Essayer :
awk '{print $1}'	sed 's/event-exporter./event-exporter/'` Il doit être « netapp-ci-event-exportatrice » ou « event-exportatrice ». Ensuite, modifiez l'agent de surveillance `kubectl -n netapp-monitoring edit agent` et définissez la valeur de LOG_FILE pour qu'elle reflète 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-exportatrice.log » ou «/var/log/containers/event-exportatrice*.log ». …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. Sinon, on peut aussi désinstaller et réinstallez l'agent.
J'constate que le ou les pods déployés par l'opérateur de surveillance Kubernetes sont en panne en raison de ressources insuffisantes.	Reportez-vous à l'opérateur de surveillance Kubernetes "options de configuration"pour augmenter les limites de processeur et/ou de mémoire selon les besoins.
Si une image manquante ou une configuration non valide a entraîné l'échec du démarrage ou de la préparation des pods de metrics d'état de netapp-ci-kube. L'état StatefulSet est bloqué et les modifications de configuration ne sont pas appliquées aux pods de metrics netapp-ci-kube-state.	StatefulSet est dans un "cassé" état. Après avoir résolu tout problème de configuration, utilisez les pods de metrics netapp-ci-kube-état.
les pods de metrics d'état-ci-kube-netapp ne parviennent pas à démarrer après l'exécution d'une mise à niveau d'opérateur Kubernetes, et lancent ErrImagePull (échec de l'extraction de l'image).	Essayez de réinitialiser les modules manuellement.
Des messages « événement ignoré comme étant plus ancien que maxEventAgeSeconds » sont observés pour mon cluster Kubernetes sous analyse du journal.	Modifiez l'opérateur *agentconfiguration* et augmentez les valeurs *event-exportatrice-maxEventAgeSeconds* (c.-à-d. à 60 s), *event-exportatrice-kubeQPS* (c.-à-d. à 100) et *event-exportatrice-kubeBurst* (c.-à-d. à 500). Pour plus de détails sur ces options de configuration, reportez-vous à la "options de configuration" page.

Problème :	Essayer :
Telegraf avertit ou se bloque en raison 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'agentNKMO et définissez *Unprotected* sur *true*. Cela indique 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 disque, il permet une exécution dans des environnements où il est impossible de réserver de la mémoire verrouillée. Pour plus de détails sur les options de configuration *Unprotected*, 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 lors de la lecture de /dev/vdc : pas de fichier ou de répertoire	Pour l'opérateur de surveillance Kubernetes, ces messages d'avertissement sont bénins et peuvent être ignorés en toute sécurité. Vous pouvez également modifier la section telegraf dans AgentConfiguration et définir *runDsPrivileged* sur TRUE. Pour plus de détails, reportez-vous au "options de configuration de l'opérateur".

Problème :	Essayer :

Mon pod Fluent-bit échoue avec les erreurs suivantes : [2024/10/16 14 23:16:23] [erreur] [/src/fluent-bit/plugins/In_tail/tail_fs_inotify.c:360 errno=10/16 14] trop de fichiers ouverts [2024/10/16 14:16:23] [erreur] échec de l'initialisation de l'entrée tail.0 [2024/24:16] [erreur d'initialisation du moteur]	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 lors des redémarrages de 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 :	Essayer :
Les pods telegraf DS signalent des erreurs liées au plug-in d’entrée kubernetes qui ne parviennent pas à faire de requêtes HTTP en raison de l’incapacité à valider le certificat TLS. Par exemple : E! [Inputs.kubernetes] erreur dans le plug-in : erreur lors de la demande HTTP pour "<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 la vérification du certificat : x509 : impossible de valider le certificat pour <kubelet_IP> car il ne contient pas de 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 des certificats *Subject alternative Name*. Pour résoudre ce problème, l'utilisateur peut modifier le "configuration de l'agent", et définir *telegraf:insecureK8sSkipVerify* sur *true*. Cela va configurer le plug-in d'entrée telegraf pour ignorer la vérification. Sinon, l'utilisateur peut configurer le kubelet pour "ServerTLSBootstrap", qui déclenchera une demande de certificat à partir de l'API 'certificates.k8s.io'.

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

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.

Le tableau ci-dessous répertorie les options possibles pour le fichier *AgentConfiguration* :

Composant	Option	Description
agent		Options de configuration communes à tous les composants que l'opérateur peut installer. Ces options peuvent être considérées comme des options « globales ».
	DockerRepo	Une substitution DockerRepo permet d'extraire les images des référentiels Docker privés du client plutôt que du référentiel Docker Data Infrastructure Insights . Le référentiel Docker Data Infrastructure Insights est utilisé par défaut.
	DockerImagePullSecret	Facultatif : un secret pour le référentiel privé du client.

Composant	Option	Description
	Nom du cluster	Champ de texte libre identifiant de manière unique un cluster parmi tous les clusters clients. Ce champ doit être unique pour un locataire Data Infrastructure Insights . La valeur par défaut correspond au champ « Nom du cluster » saisi par le client dans l'interface utilisateur.
	Proxy format: Proxy: Server: Port: Nom d'utilisateur: Mot de passe: NoProxy: IsTelegrafProxyEnabled: IsAuProxyEnabled: IsFluentbitProxyEnabled: IsCollectorProxyEnabled:	Facultatif pour définir le proxy. Il s'agit généralement du proxy d'entreprise du client.
telegraf		Options de configuration qui peuvent personnaliser l'installation de telegraf de l'opérateur
	Intervalle de collection	Intervalle de collecte des metrics, en secondes (max=60 s)
	DsCpuLimit	Limite CPU pour les telegraf ds
	DsMemLimit	Limite de mémoire pour les télégraf
	DsCpuRequest	Demande CPU pour les telegraf ds
	DsMemRequest	Demande de mémoire pour les télégraf
	RsCpuLimit	Limite CPU pour les RS telegraf
	RsMemLimit	Limite de mémoire pour les RS telegraf
	RsCpuRequest	Demande CPU pour les RS telegraf
	RsMemRequest	Demande de mémoire pour les RS telegraf
	Avec privilèges d'exécution	Exécutez le conteneur *telegraf-mountstats-poller* de telegraf DemonSet en mode privilégié. Définissez cette valeur sur true si SELinux est activé sur vos nœuds Kubernetes.
	RunDsPrivileged	Définissez runDsPrivileged sur true pour exécuter le conteneur telegraf de telegraf DemonSet en mode privilégié.
	Taille de la batchSize	Voir "Documentation de configuration de Telegraf"
	BufferLimit	Voir "Documentation de configuration de Telegraf"
	Interval	Voir "Documentation de configuration de Telegraf"
	CollectionJitter	Voir "Documentation de configuration de Telegraf"
	précision	Voir "Documentation de configuration de Telegraf"
	Intervalle de rinçage	Voir "Documentation de configuration de Telegraf"
	Scintillement	Voir "Documentation de configuration de Telegraf"

Composant	Option	Description
	OutputTimeout	Voir "Documentation de configuration de Telegraf"
	Tolérances de type dsTolerations	télégraf-ds tolérances supplémentaires.
	RsTolerations	tolérances supplémentaires de telegraf-rs.
	SkipProcessorsAfterAggregators	Voir "Documentation de configuration de Telegraf"
	non protégé	Voir ceci "Problème connu de Telegraf" . Le paramètre *non protégé* demandera à l'opérateur de surveillance Kubernetes d'exécuter Telegraf avec le `--unprotected` drapeau.
	insecureK8sSkipVerify	Si telegraf ne parvient pas à vérifier le certificat en raison de l'absence de SAN IP, essayez d'activer le saut de vérification
metrics-état-kube		Options de configuration permettant de personnaliser l'installation des mesures d'état kube de l'opérateur
	CpuLimit	Limite CPU pour le déploiement des indicateurs d'état kube
	MemLimit	Limite MEM pour le déploiement de mesures kube-state
	CpuRequest	Demande de processeur pour le déploiement de metrics d'état kube
	MemRequest	Demande MEM pour le déploiement de mesures d'état kube
	ressources	une liste de ressources séparées par des virgules à capturer. exemple : cronjobs,demonsets,déploiements,ingresses,travaux, espaces de noms,nœuds,perstentvolumeclaims, perstentvolumes,pods,réplicasets,resourcetas,services,statefulsets
	tolérances	tolérances supplémentaires des indicateurs d'état kube.
	étiquettes	une liste séparée par des virgules de ressources pour lesquelles kube-state-metrics doit capturer les étiquettes exemple : cronjobs=[*],daemonsets=[*],deployments=[*],ingresses=[*],jobs=[*],namespaces=[*],nodes=[*], persistentvolumeclaims=[*],persistentvolumes=[*],pods=[*],replicasets=[*],resourcequotas=[*],services=[*],statefulsets=[*]
journaux		Options de configuration permettant de personnaliser la collecte des journaux et l'installation de l'opérateur
	ReadFromHead	vrai/faux, doit couramment lire le journal à partir de la tête

Composant	Option	Description
	délai dépassé	délai, en secondes
	DnsMode	TCP/UDP, mode pour DNS
	tolérances fluentes-bit	fluent-bit-ds tolérances supplémentaires.
	tolérance-exportateur-événement	tolérances supplémentaires de l'exportateur d'événements.
	Event-exportateur-maxEventAgeSeconds	âge max. de l'événement de l'exportateur d'événement. Voir https://github.com/jkroepke/resmoio-kubernetes-event-exporter
	chemin du journal du conteneur de bits fluides	Par défaut, le DaemonSet Fluentbit monte les chemins d'accès /var/log et /var/lib/docker/containers pour accéder aux journaux des conteneurs Kubernetes et les lire. Si Kubernetes a été configuré pour placer les journaux des conteneurs dans un emplacement autre que celui par défaut, utilisez cette option pour modifier le DaemonSet Fluentbit afin de monter ce chemin.
mappe des charges de travail		Options de configuration permettant de personnaliser la collection de cartes de charge de travail et l'installation de l'opérateur.
	CpuLimit	Limite CPU pour net observateur ds
	MemLimit	limite mem pour les observateurs nets
	CpuRequest	Demande CPU pour net observateur ds
	MemRequest	demande mem pour net observateur ds
	Intervalle d'Aggregationde métadonnées	intervalle d'agrégation des mesures, en secondes
	BpfPollInterval	Intervalle d'interrogation BPF, en secondes
	EnableDNSLookup	Vrai/faux, activer la recherche DNS
	tolérances l4	net-observateur-l4-ds tolérances supplémentaires.
	Avec privilèges d'exécution	True/FALSE : définissez runPrivileged sur TRUE si SELinux est activé sur vos nœuds Kubernetes.
gestion des modifications		Options de configuration de Kubernetes change Management and Analysis
	CpuLimit	Limite CPU pour change-observateur-Watch-RS
	MemLimit	Limite MEM pour change-observateur-Watch-RS
	CpuRequest	Demande CPU pour change-observateur-Watch-RS
	MemRequest	demande mem pour changement-observateur-watch-rs
	workloadFailureDeclarationIntervalSeconds	Intervalle après lequel un déploiement infructueux d'une charge de travail sera marqué comme ayant échoué, en secondes

Composant	Option	Description
	charge de travailDeployAggrIntervalSeconds	Fréquence à laquelle les déploiements de charges de travail sont combinés et envoyés, en secondes
	nonWorkloadDeployAggrIntervalSeconds	Fréquence à laquelle les déploiements hors charge de travail sont combinés et envoyés, en secondes
	TermsToRedact	Un ensemble d'expressions régulières utilisées dans les noms env et les cartes de données dont la valeur sera bifftée. Exemples de termes : « pwd », « mot de passe », « jeton », « apikey », « api-key », « jwt »
	AdditionalKindsToWatch	Liste séparée par des virgules de types supplémentaires à surveiller par rapport à l'ensemble de types par défaut surveillés par le collecteur
	KindsToIgnoreFromWatch	Liste de types séparés par une virgule à ignorer de l'ensemble de types par défaut surveillés par le collecteur
	LogRecordAggrIntervalSeconds	Fréquence à laquelle les enregistrements de journal sont envoyés à l'EC à partir du collecteur
	tolérances de surveillance	change-observateur-watch-ds tolérances supplémentaires. Format abrégé à une seule ligne uniquement. Exemple : '{key: Taint1, operator: Exists, effect: NoSchedule},{key: Taint2, operator: Exists, effect: NoExecute}'

Exemple de fichier AgentConfiguration

Vous trouverez ci-dessous un exemple de fichier *AgentConfiguration*.

```
apiVersion: monitoring.netapp.com/v1alpha1
kind: AgentConfiguration
metadata:
  name: netapp-ci-monitoring-configuration
  namespace: "netapp-monitoring"
  labels:
    installed-by: nkmo-netapp-monitoring

spec:
  # # You can modify the following fields to configure the operator.
  # # Optional settings are commented out and include 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
clustername.
    # # clusterName must be unique across all clusters in your Data
```

```
Infrastructure Insights environment.
    clusterName: "my_cluster"

    # # Proxy settings. The proxy that the operator should use to send
metrics to Data Infrastructure Insights.
    # # Please see 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] By default, the operator uses the CI repository.
    # # To use a private repository, change this field to your repository
name.
    # # Please see 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] The name of the imagePullSecret for dockerRepo.
    # # If you are using a private repository, change this field from
'netapp-ci-docker' to the name of your secret.
    dockerImagePullSecret: 'netapp-ci-docker'

    # # Allow the operator to automatically rotate its ApiKey before
expiration.
    # tokenRotationEnabled: 'true'
    # # Number of days before expiration that the ApiKey should be
rotated. This must be less than the total ApiKey duration.
    # tokenRotationThresholdDays: '30'

  telegraf:
    # # Settings to fine-tune metrics data collection. Telegraf config
names are included in parenthesis.
    # # See
https://github.com/influxdata/telegraf/blob/master/docs/CONFIGURATION.md#a
gent

    # # The default time telegraf will wait between inputs for all plugins
(interval). Max=60
```

```
    # collectionInterval: '60s'
    # # Maximum number of records per output that telegraf will write in
one batch (metric_batch_size).
    # batchSize: '10000'
    # # Maximum number of records per output that telegraf will cache
pending a successful write (metric_buffer_limit).
    # bufferLimit: '150000'
    # # Collect metrics on multiples of interval (round_interval).
    # roundInterval: 'true'
    # # Each plugin waits a random amount of time between the scheduled
collection time and that time + collection_jitter before collecting inputs
(collection_jitter).
    # collectionJitter: '0s'
    # # Collected metrics are rounded to the precision specified. When set
to "0s" precision will be set by the units specified by interval
(precision).
    # precision: '0s'
    # # Time telegraf will wait between writing outputs (flush_interval).
Max=collectionInterval
    # flushInterval: '60s'
    # # Each output waits a random amount of time between the scheduled
write time and that time + flush_jitter before writing outputs
(flush_jitter).
    # flushJitter: '0s'
    # # Timeout for writing to outputs (timeout).
    # outputTimeout: '5s'

    # # telegraf-ds CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # dsCpuLimit: '750m'
    # dsMemLimit: '800Mi'
    # dsCpuRequest: '100m'
    # dsMemRequest: '500Mi'

    # # telegraf-rs CPU/Mem limits and requests.
    # rsCpuLimit: '3'
    # rsMemLimit: '4Gi'
    # rsCpuRequest: '100m'
    # rsMemRequest: '500Mi'

    # # Skip second run of processors after aggregators
    # skipProcessorsAfterAggregators: 'true'

    # # telegraf additional tolerations. Use the following abbreviated
single line format only.
```

```
    # # Inspect telegraf-rs/-ds to view tolerations which are always
present.
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # dsTolerations: ''
    # rsTolerations: ''


    # If telegraf warns of insufficient lockable memory, try increasing
the limit of lockable memory for Telegraf in the underlying operating
system/node.  If increasing the limit is not an option, set this to true
to instruct Telegraf to not attempt to reserve locked memory pages.  While
this might pose a security risk as decrypted secrets might be swapped out
to disk, it allows for execution in environments where reserving locked
memory is not possible.
    # unprotected: 'false'

    # # Run the telegraf DaemonSet's telegraf-mountstats-poller container
in privileged mode.  Set runPrivileged to true if SELinux is enabled on
your Kubernetes nodes.
    # runPrivileged: '{{
.Values.telegraf_installer.kubernetes.privileged_mode }}'

    # # Set runDsPrivileged to true to run the telegraf DaemonSet's
telegraf container in privileged mode
    # runDsPrivileged: '{{
.Values.telegraf_installer.kubernetes.ds.privileged_mode }}'

    # # Collect container Block IO metrics.
    # dsBlockIOEnabled: 'true'

    # # Collect NFS IO metrics.
    # dsNfsIOEnabled: 'true'

    # # Collect kubernetes.system_container metrics and objects in the
kube-system|cattle-system namespaces for managed kubernetes clusters (EKS,
AKS, GKE, managed Rancher).  Set this to true if you want collect these
metrics.
    # managedK8sSystemMetricCollectionEnabled: 'false'

    # # Collect kubernetes.pod_volume (pod ephemeral storage) metrics.
Set this to true if you want to collect these metrics.
    # podVolumeMetricCollectionEnabled: 'false'

    # # Declare Rancher cluster as managed.  Set this to true if your
Rancher cluster is managed as opposed to on-premise.
    # isManagedRancher: 'false'
```

```
    # # If telegraf-rs fails to start due to being unable to find the etcd
crt and key, manually specify the appropriate path here.
    # rsHostEtcdCrt: ''
    # rsHostEtcdKey: ''

  # kube-state-metrics:
    # # kube-state-metrics CPU/Mem limits and requests.
    # cpuLimit: '500m'
    # memLimit: '1Gi'
    # cpuRequest: '100m'
    # memRequest: '500Mi'

    # # Comma-separated list of resources to enable.
    # # See resources in https://github.com/kubernetes/kube-state-
metrics/blob/main/docs/cli-arguments.md
    # resources:
'cronjobs,daemonsets,deployments,ingresses,jobs,namespaces,nodes,persisten
tvolumeclaims,persistentvolumes,pods,replicasets,resourcequotas,services,s
tatefulsets'

    # # Comma-separated list of metrics to enable.
    # # See metric-allowlist in https://github.com/kubernetes/kube-state-
metrics/blob/main/docs/cli-arguments.md
    # 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'

    # # Comma-separated list of Kubernetes label keys that will be used in
the resources' labels metric.
    # # See metric-labels-allowlist in https://github.com/kubernetes/kube-
```

```
state-metrics/blob/main/docs/cli-arguments.md
    # labels:
'cronjobs=[*],daemonsets=[*],deployments=[*],ingresses=[*],jobs=[*],namesp
aces=[*],nodes=[*],persistentvolumeclaims=[*],persistentvolumes=[*],pods=[
*],replicasets=[*],resourcequotas=[*],services=[*],statefulsets=[*]'

    # # kube-state-metrics additional tolerations. Use the following
abbreviated single line format only.
    # # No tolerations are applied by default
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # tolerations: ''

    # # kube-state-metrics shards.  Increase the number of shards for
larger clusters if telegraf RS pod(s) experience collection timeouts
    # shards: '2'

  # # Settings for the Events Log feature.
  # logs:
    # # Set runPrivileged to true if Fluent Bit fails to start, trying to
open/create its database.
    # runPrivileged: 'false'

    # # If Fluent Bit should read new files from the head, not tail.
    # # See Read_from_Head in
https://docs.fluentbit.io/manual/pipeline/inputs/tail
    # readFromHead: "true"

    # # Network protocol that Fluent Bit should use for DNS: "UDP" or
"TCP".
    # dnsMode: "UDP"

    # # DNS resolver that Fluent Bit should use: "LEGACY" or "ASYNC"
    # fluentBitDNSResolver: "LEGACY"

    # # Logs additional tolerations. Use the following abbreviated single
line format only.
    # # Inspect fluent-bit-ds to view tolerations which are always
present. No tolerations are applied by default for event-exporter.
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # fluent-bit-tolerations: ''
    # event-exporter-tolerations: ''

    # # event-exporter CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
```

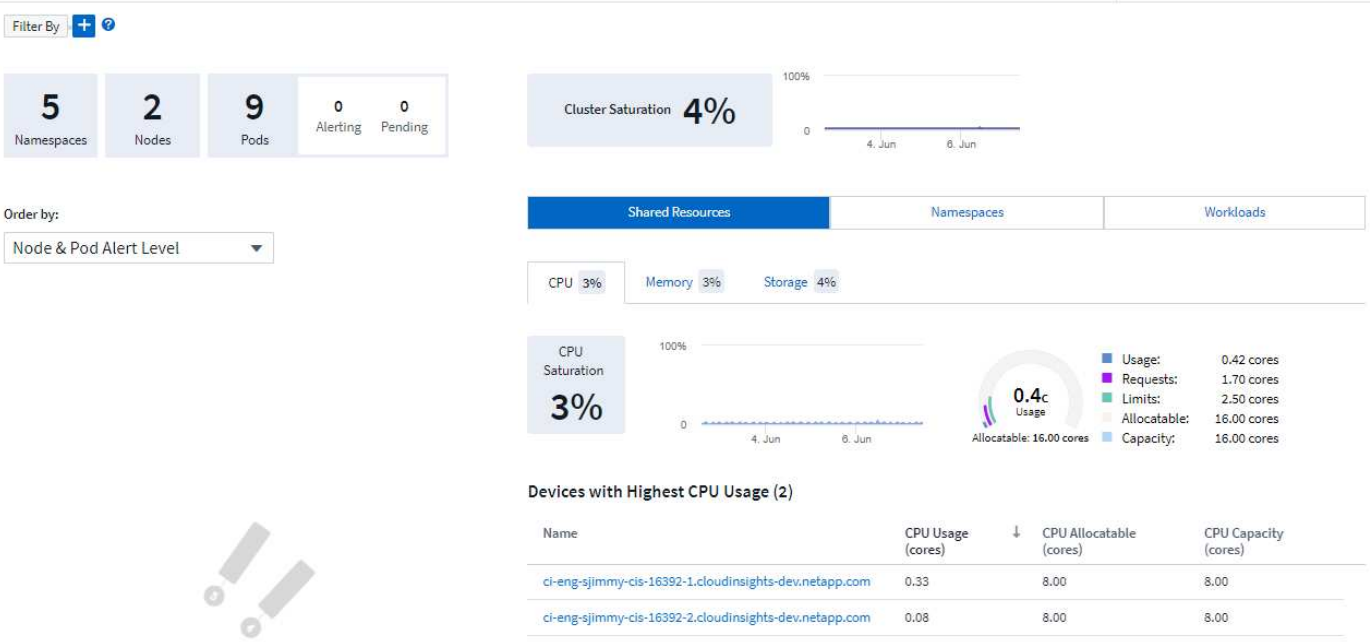
```
resources-containers/
    # event-exporter-cpuLimit: '500m'
    # event-exporter-memLimit: '1Gi'
    # event-exporter-cpuRequest: '50m'
    # event-exporter-memRequest: '100Mi'

    # # event-exporter max event age.
    # # See https://github.com/jkroepke/resmoio-kubernetes-event-exporter
    # event-exporter-maxEventAgeSeconds: '10'

    # # event-exporter client-side throttling
    # # Set kubeBurst to roughly match your events per minute and
kubeQPS=kubeBurst/5
    # # See https://github.com/resmoio/kubernetes-event-
exporter#troubleshoot-events-discarded-warning
    # event-exporter-kubeQPS: 20
    # event-exporter-kubeBurst: 100

    # # fluent-bit CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # fluent-bit-cpuLimit: '500m'
    # fluent-bit-memLimit: '1Gi'
    # fluent-bit-cpuRequest: '50m'
    # fluent-bit-memRequest: '100Mi'

    # By default, the Fluentbit DaemonSet will mount the /var/log and
/var/lib/docker/containers host paths to access/read the
    # Kubernetes container logs.  If Kubernetes has been configured to
place container logs in a non-default location, use
    # this option to modify the Fluentbit DaemonSet to mount the non-
default path.
    # fluent-bit-containerLogPath

  # # Settings for the Network Performance and Map feature.
  # workload-map:
    # # netapp-ci-net-observer-l4-ds CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # cpuLimit: '500m'
    # memLimit: '500Mi'
    # cpuRequest: '100m'
    # memRequest: '500Mi'

    # # Metric aggregation interval in seconds. Min=30, Max=120
    # metricAggregationInterval: '60'
```

```
    # # Interval for bpf polling. Min=3, Max=15
    # bpfPollInterval: '8'

    # # Enable performing reverse DNS lookups on observed IPs.
    # enableDNSLookup: 'true'

    # # netapp-ci-net-observer-l4-ds additional tolerations. Use the
following abbreviated single line format only.
    # # Inspect netapp-ci-net-observer-l4-ds to view tolerations which are
always present.
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # l4-tolerations: ''

    # # Set runPrivileged to true if SELinux is enabled on your Kubernetes
nodes.
    # # Note: In OpenShift environments, this is set to true
automatically.
    # runPrivileged: 'false'

  # change-management:
    # # change-observer-watch-rs CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # cpuLimit: '1'
    # memLimit: '1Gi'
    # cpuRequest: '500m'
    # memRequest: '500Mi'

    # # Interval after which a non-successful deployment of a workload
will be marked as failed, in seconds
    # workloadFailureDeclarationIntervalSeconds: '30'

    # # Frequency at which workload deployments are combined and sent, in
seconds
    # workloadDeployAggrIntervalSeconds: '300'

    # # Frequency at which non-workload deployments are combined and sent,
in seconds
    # nonWorkloadDeployAggrIntervalSeconds: '15'

    # # A 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"'

    # # A comma separated list of additional kinds to watch from the
default set of kinds watched by the collector
    # # Each kind will have to be prefixed by its apigroup
    # # Example: '"authorization.k8s.io.subjectaccessreviews"'
    # additionalKindsToWatch: ''

    # # A 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: ''

    # # 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: ''

    # # Frequency with which log records are sent to CI from the collector
    # logRecordAggrIntervalSeconds: '20'

    # # change-observer-watch-ds additional tolerations. Use the following
abbreviated single line format only.
    # # Inspect change-observer-watch-ds to view tolerations which are
always present.
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # watch-tolerations: ''
```

Page des détails du cluster Kubernetes

La page des détails du cluster Kubernetes affiche une présentation détaillée du cluster Kubernetes.



L’espace de noms, les nœuds et le Pod

Le nombre en haut de la page indique le nombre total d’espaces de noms, de nœuds et de pods dans le cluster, ainsi que le nombre de fenêtres d’alerte en cours et en attente.

Ressources partagées et saturation

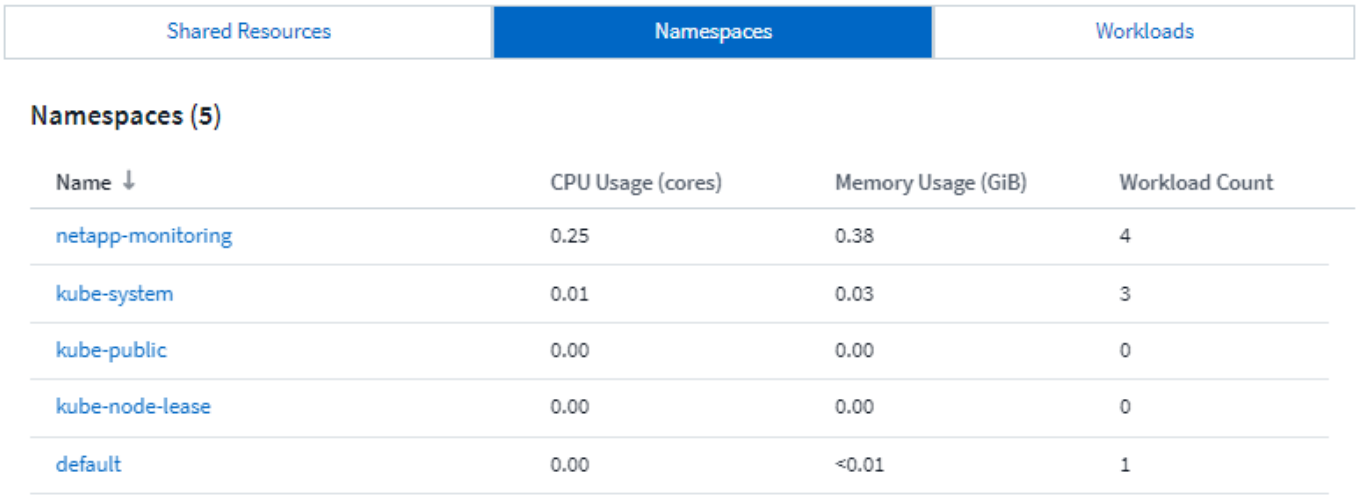
En haut à droite de la page de détails se trouve la saturation de votre cluster en tant que pourcentage actuel, ainsi qu’un graphique affichant la tendance récente dans le temps. La saturation du cluster est la plus élevée du CPU, de la mémoire ou du stockage à chaque point du temps.

Ci-dessous, la page affiche par défaut **Shared Resources**, avec des onglets pour CPU, mémoire et stockage. Chaque onglet affiche le pourcentage de saturation et la tendance dans le temps, avec des détails d’utilisation supplémentaires. Pour le stockage, la valeur indiquée est le plus grand nombre de saturation du système de fichiers back-end et du système de fichiers, qui sont calculés indépendamment.

Les périphériques les plus utilisés sont indiqués dans un tableau en bas. Cliquez sur n’importe quel lien pour explorer ces périphériques.

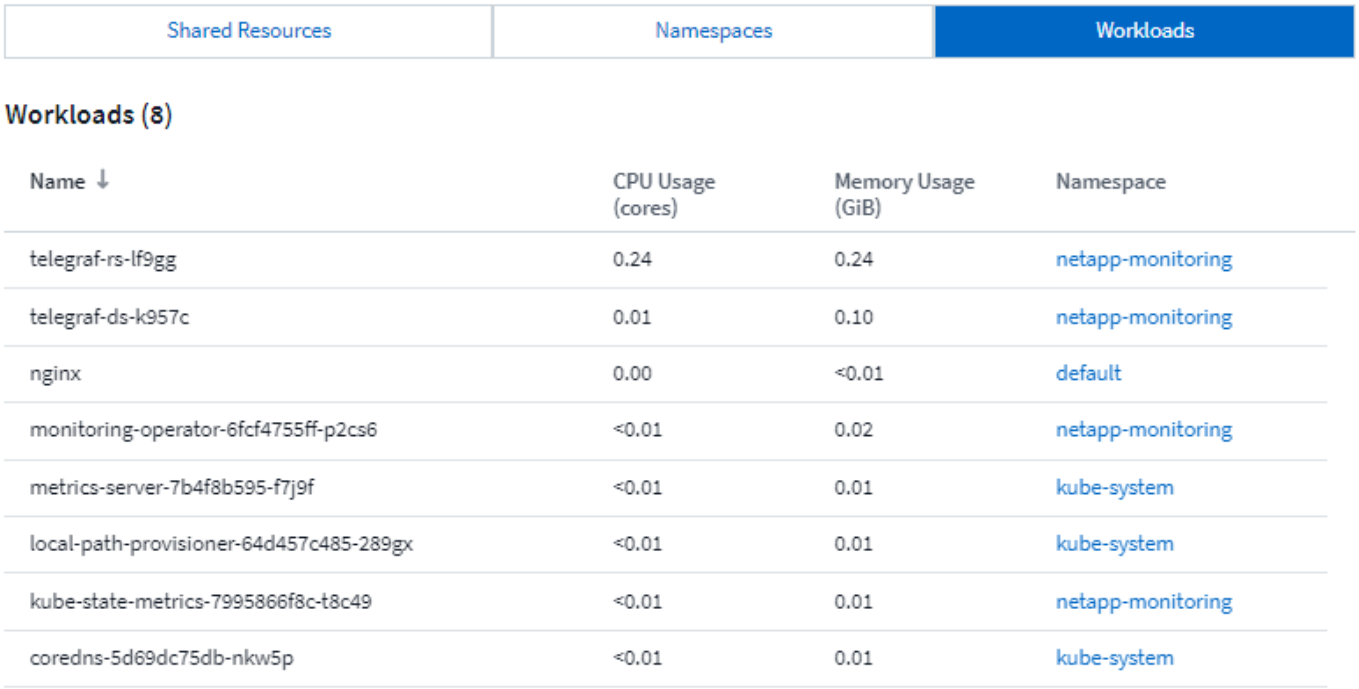
Espaces de noms

L’onglet espaces de noms affiche la liste de tous les espaces de noms de votre environnement Kubernetes, indiquant l’utilisation du CPU et de la mémoire, ainsi que le nombre de workloads dans chaque espace de noms. Cliquez sur les liens Nom pour explorer chaque espace de noms.



Charges de travail

De la même manière, l'onglet charges de travail affiche la liste des charges de travail de chaque namespace, avec pour nouveau l'affichage de l'utilisation du processeur et de la mémoire. Un clic sur les liens de l'espace de noms permet d'accéder à chacun d'eux



Le groupe d'instruments « roue »



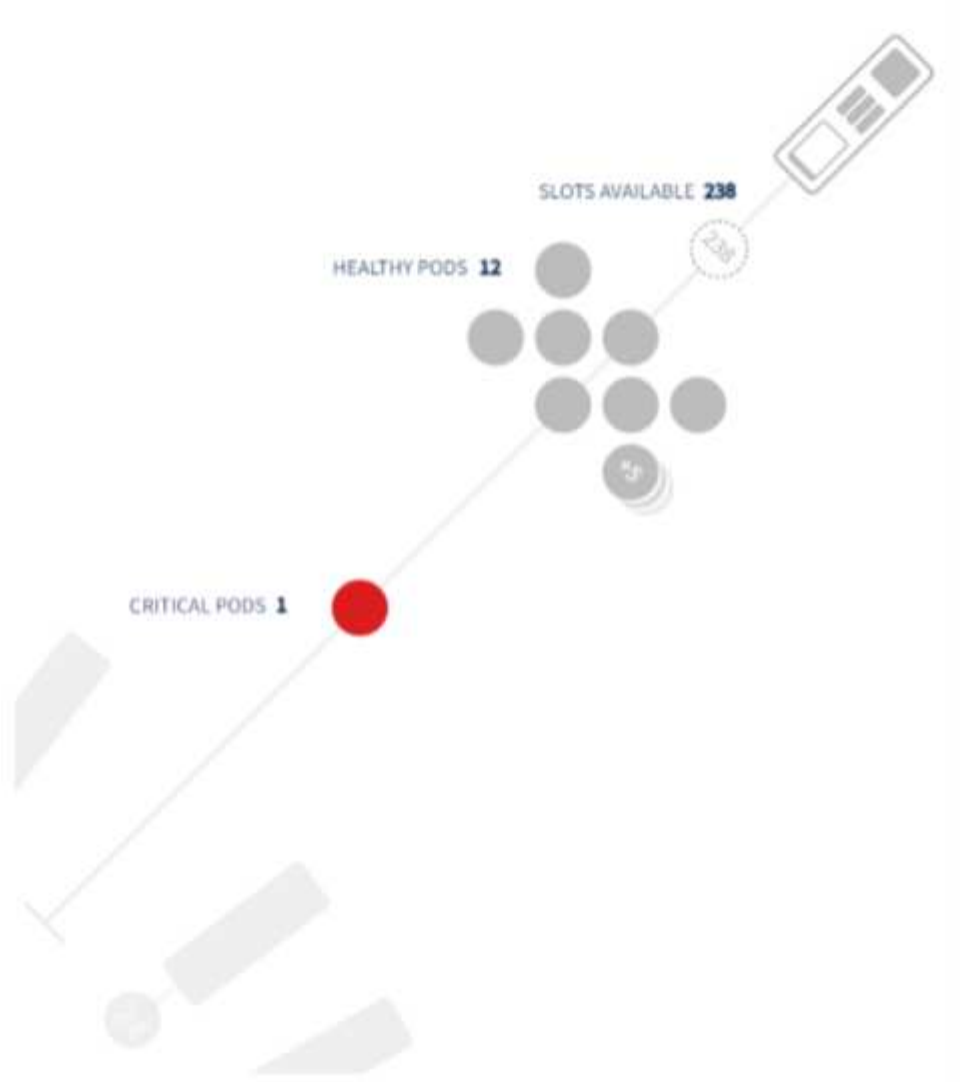
La section roue du cluster fournit un aperçu de l'état des nœuds et des pods pour en savoir plus. Si votre cluster contient plus de nœuds que ce qui peut être affiché dans cette zone de la page, vous pourrez tourner la roue à l'aide des boutons disponibles.

Les pods ou les nœuds d'alerte s'affichent en rouge. Les zones « Avertissement » s'affichent en orange. Les modules qui ne sont pas programmés (c'est-à-dire non connectés) s'affichent dans le coin inférieur du bloc d'instruments.

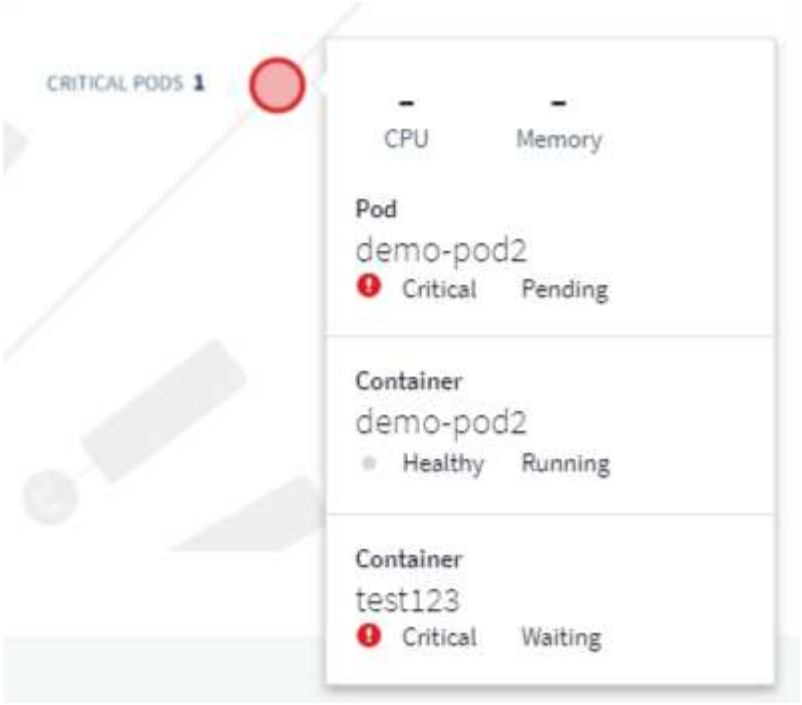
Le fait de passer la souris sur un pod (cercle) ou un nœud (barre) permet d'étendre la vue du nœud.



Cliquez sur le pod ou le nœud dans cette vue pour effectuer un zoom avant sur la vue développée du nœud.



À partir de là, vous pouvez passer le curseur sur un élément pour afficher des détails sur cet élément. Par exemple, passez la souris sur le pod critique dans cet exemple pour afficher des détails sur ce pod.



Vous pouvez afficher les informations relatives au système de fichiers, à la mémoire et à la CPU en passant le pointeur de la souris sur les éléments du nœud.



Une note sur les jauges

Les jauges mémoire et CPU affichent trois couleurs, puisqu'elles indiquent *used* par rapport à *allocatable Capacity* et *total Capacity*.

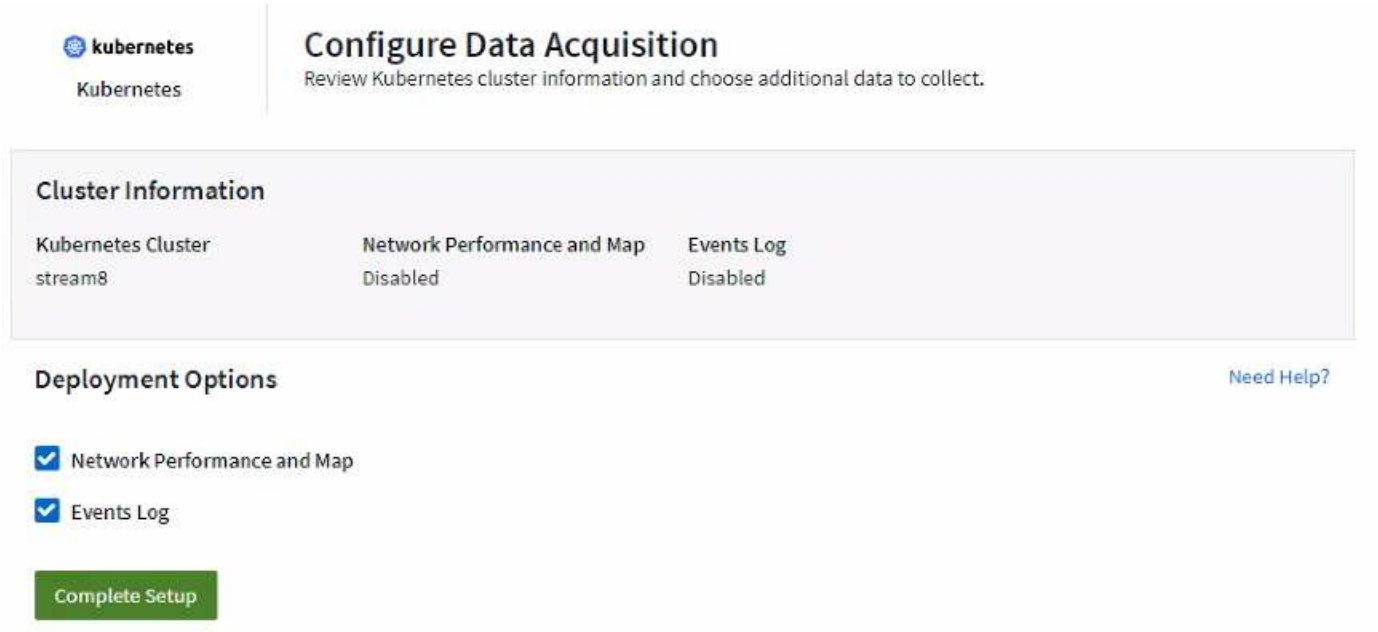
Surveillance et mappage des performances du réseau Kubernetes

La fonctionnalité de surveillance et de mappage des performances réseau Kubernetes simplifie la résolution de problèmes en mappant les dépendances entre les services (également appelés workloads). Elle fournit une visibilité en temps réel sur les latences des performances réseau et les anomalies pour identifier les problèmes de performance avant qu'ils n'affectent les utilisateurs. Cette fonctionnalité aide les entreprises à réduire les coûts globaux grâce à l'analyse et à l'audit des flux de trafic Kubernetes.

Principales fonctionnalités : • la carte des workloads présente les dépendances et les flux des workloads Kubernetes, et souligne les problèmes de réseau et de performance. • Surveiller le trafic réseau entre les pods Kubernetes, les workloads et les nœuds ; identifier la source des problèmes de trafic et de latence. • Réduire les coûts globaux en analysant les entrées, les sorties, le trafic interrégional et le trafic de réseau interzone.

Conditions préalables

Avant de pouvoir utiliser le contrôle et le mappage des performances du réseau Kubernetes, vous devez avoir configuré le "Opérateur de surveillance NetApp Kubernetes" pour activer cette option. Pendant le déploiement de l'opérateur, cochez la case « performances du réseau et carte » pour l'activer. Vous pouvez également activer cette option en accédant à une page d'accueil Kubernetes et en sélectionnant « Modifier le déploiement ».



Moniteurs

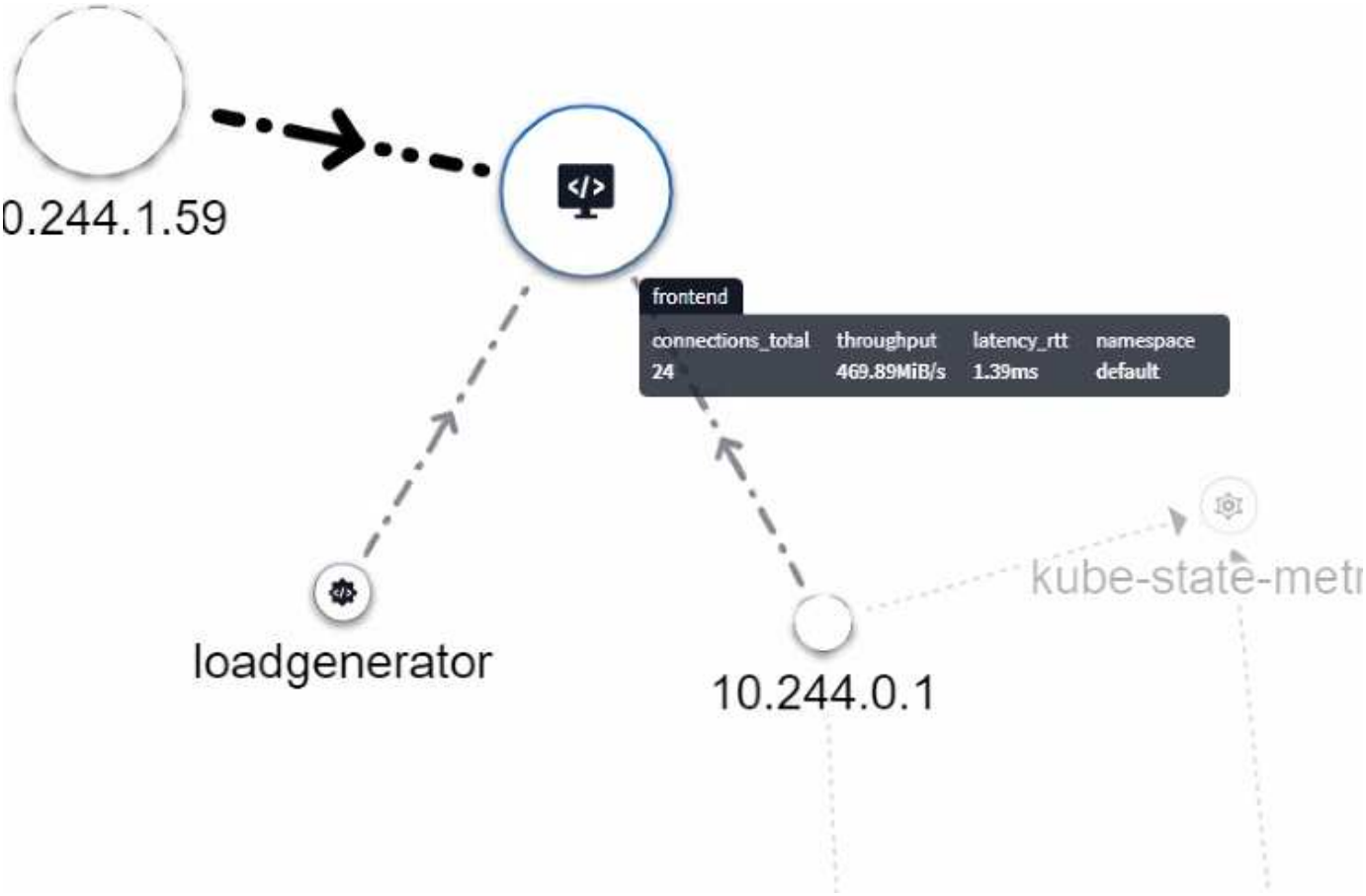
La carte des charges de travail utilise "moniteurs" pour dériver des informations. Data Infrastructure Insights fournit plusieurs moniteurs Kubernetes par défaut (ceux-ci peuvent être *utilisés* par défaut). Vous pouvez *reprendre* (c'est-à-dire activer) les moniteurs de votre choix), ou vous pouvez créer des moniteurs personnalisés pour les objets kubernetes que Workload Map utilisera également.

Vous pouvez créer des alertes de metric Data Infrastructure Insights sur l'un des types d'objet ci-dessous. Assurez-vous que les données sont regroupées par type d'objet par défaut.

- workloads kubernetes
- kubernetes.demonset
- kubernetes.deployment
- kubernetes.cronjob
- kubernetes.travail
- kubernetes.repliaset
- kubernetes.statefulset
- pod kubernetes
- kubernetes.network_traffic_l4

La carte

La carte montre les services/charges de travail et leurs relations les uns avec les autres. Les flèches indiquent l'itinéraire de la circulation. Le survol d'une charge de travail affiche un récapitulatif des informations relatives à cette charge, comme vous pouvez le voir dans cet exemple :



Les icônes situées dans les cercles représentent différents types de services. Notez que les icônes ne sont visibles que si les objets sous-jacents ont étiquettes.



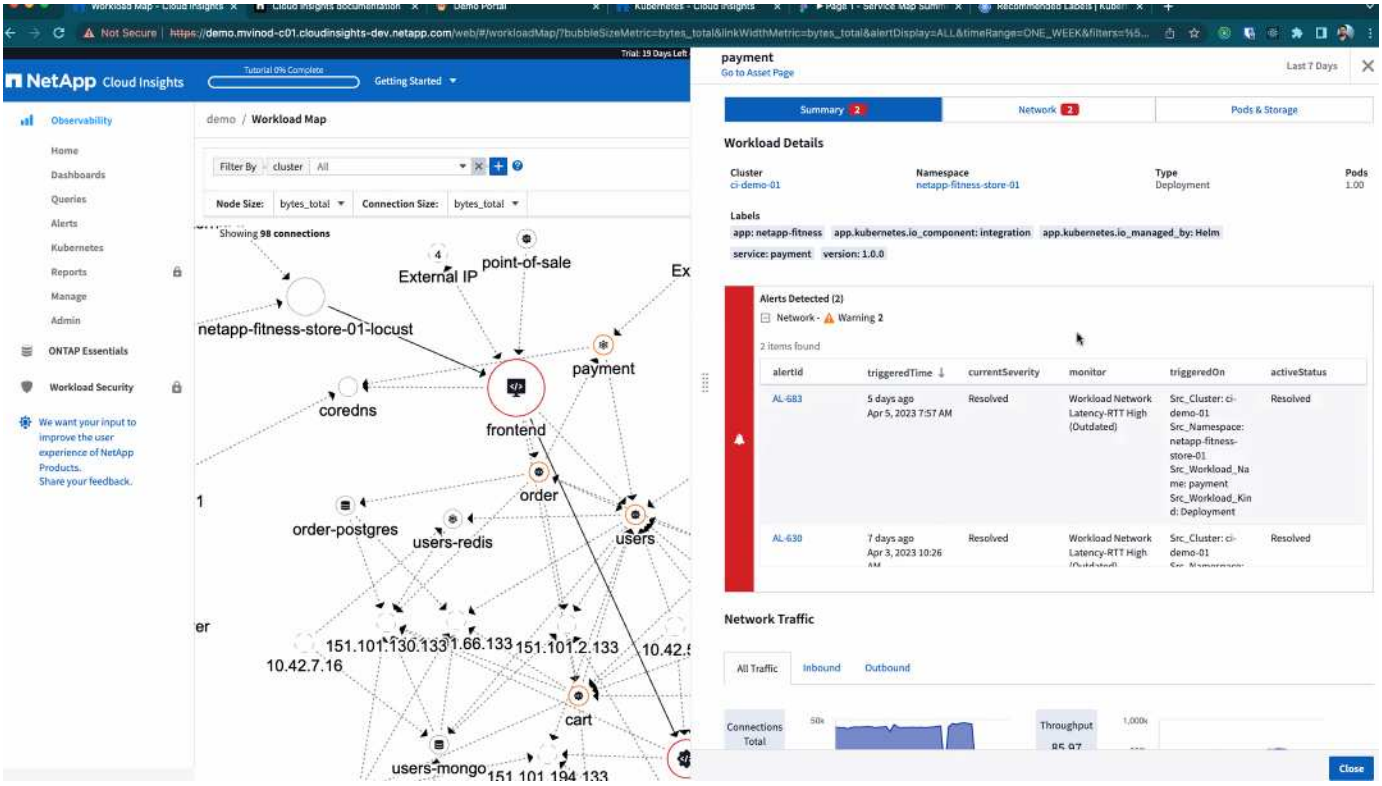
La taille de chaque cercle indique la taille du nœud. Notez que ces tailles sont relatives, le niveau de zoom ou la taille de l'écran de votre navigateur peut affecter la taille réelle des cercles. De la même manière, le style de ligne de trafic vous donne une vue d'un coup d'œil de la taille de la connexion ; les lignes en gras sont à fort trafic, tandis que les lignes en pointillés légers sont à faible trafic.

Les nombres à l'intérieur des cercles correspondent au nombre de connexions externes en cours de traitement par le service.



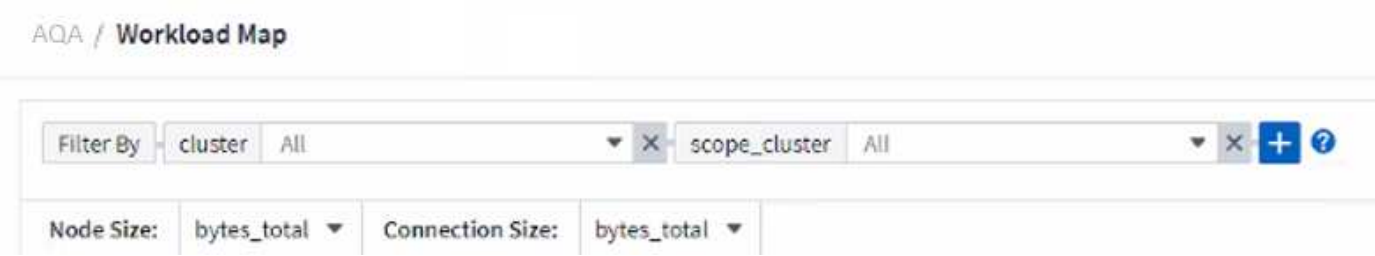
Détails de la charge de travail et alertes

Les cercles affichés en couleur indiquent une alerte de niveau critique ou d'avertissement pour la charge de travail. Passez le curseur sur le cercle pour obtenir un résumé du problème ou cliquez sur le cercle pour ouvrir un panneau coulissant avec plus de détails.

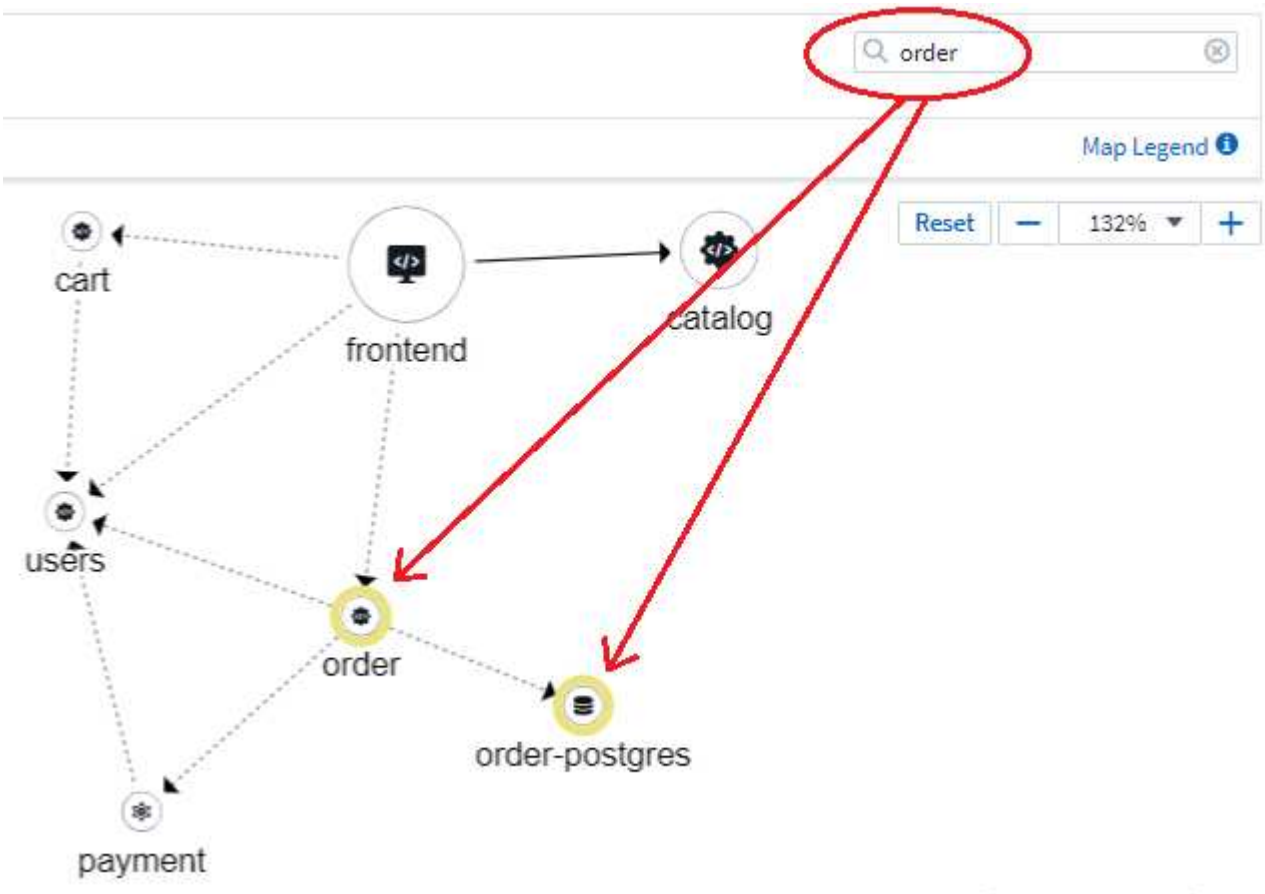


Recherche et filtrage

À l'instar des autres fonctionnalités Data Infrastructure Insights, vous pouvez facilement définir des filtres pour vous concentrer sur les objets ou les attributs de workload spécifiques que vous souhaitez.



De même, la saisie d'une chaîne dans le champ *find* met en surbrillance 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 cercle). Les étiquettes sont dérivées comme suit :

- Nom du service/de l'application s'exécutant en termes génériques
- Si la source est un pod :
  - L'étiquette est dérivée de l'étiquette de charge de travail du pod
  - Libellé attendu sur le workload : app.kubernetes.io/composant
  - Référence du nom de l'étiquette : https://kubernetes.io/docs/concepts/overview/working-with-objects/common-labels/
  - Étiquettes recommandées :
    - front-end

- back-end
- base de données
- cache
- file d'attente
- kafka

- Si la source est externe au cluster kubernetes :
  - Data Infrastructure Insights tente d'analyser le nom DNS résolu pour extraire le type de service.

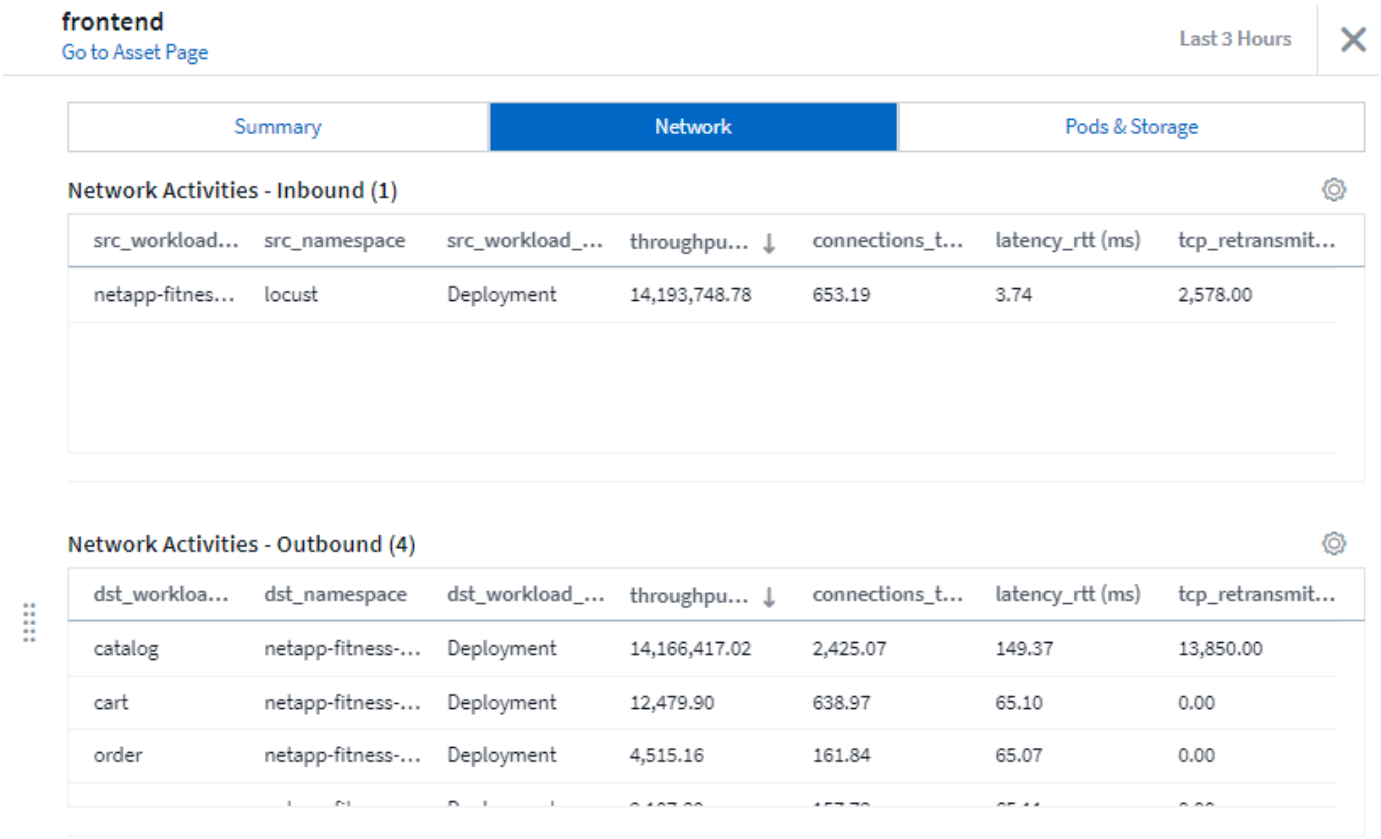
    Par exemple, avec un nom DNS résolu de *s3.eu-north-1.amazonaws.com*, le nom résolu est analysé pour obtenir *s3* comme type de service.

Plongez au cœur de l'aventure

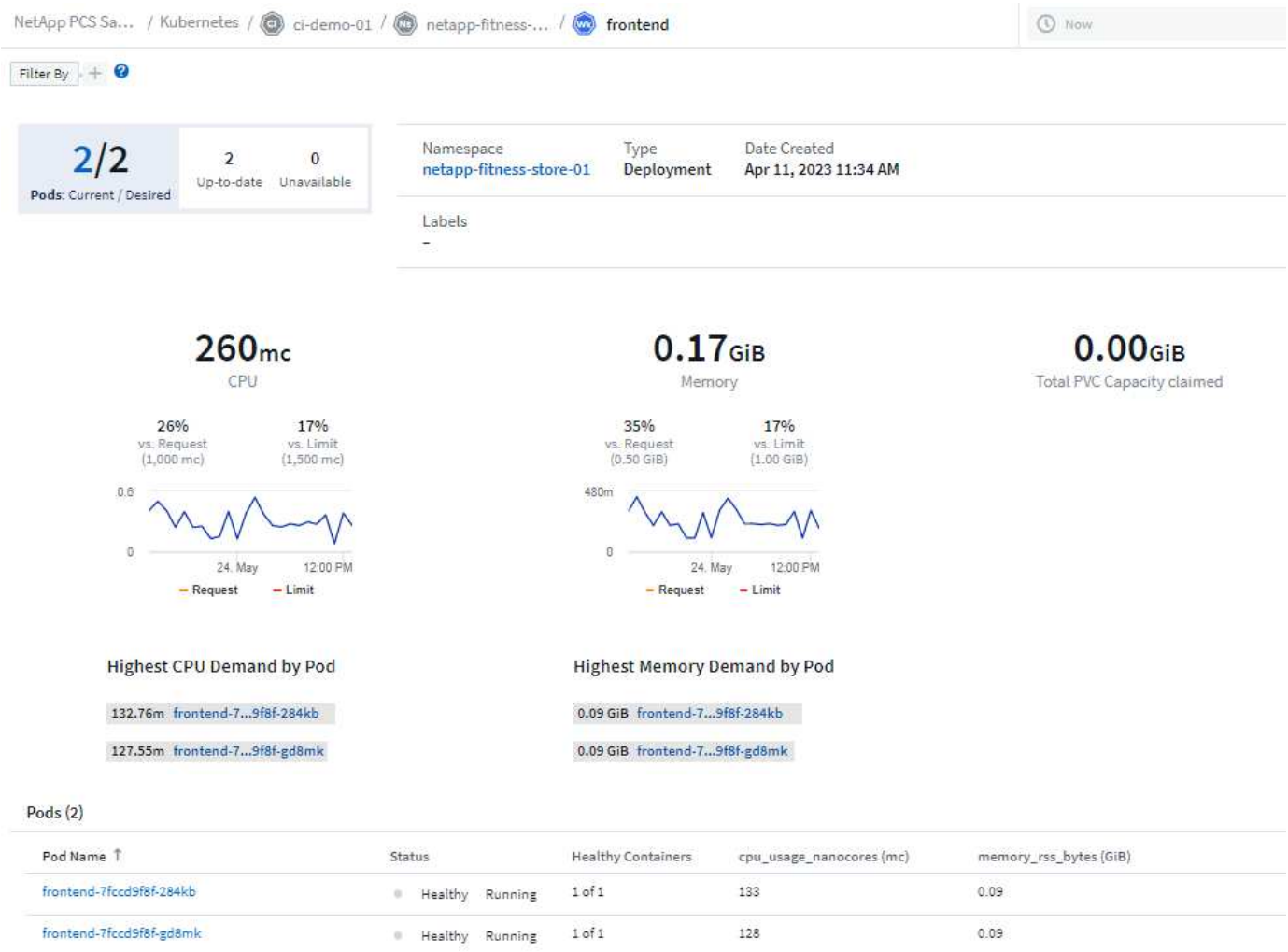
Cliquez avec le bouton droit de la souris sur une charge de travail pour afficher des options supplémentaires afin d'en savoir plus. Par exemple, vous pouvez effectuer un zoom avant pour afficher les connexions de cette charge de travail.



Vous pouvez également ouvrir le panneau détaillé pour afficher directement l'onglet *Summary*, *Network* ou *Pod & Storage*.



Enfin, en sélectionnant *aller à la page de ressources*, vous ouvrez la page d'accueil détaillée de la ressource pour la charge de travail.



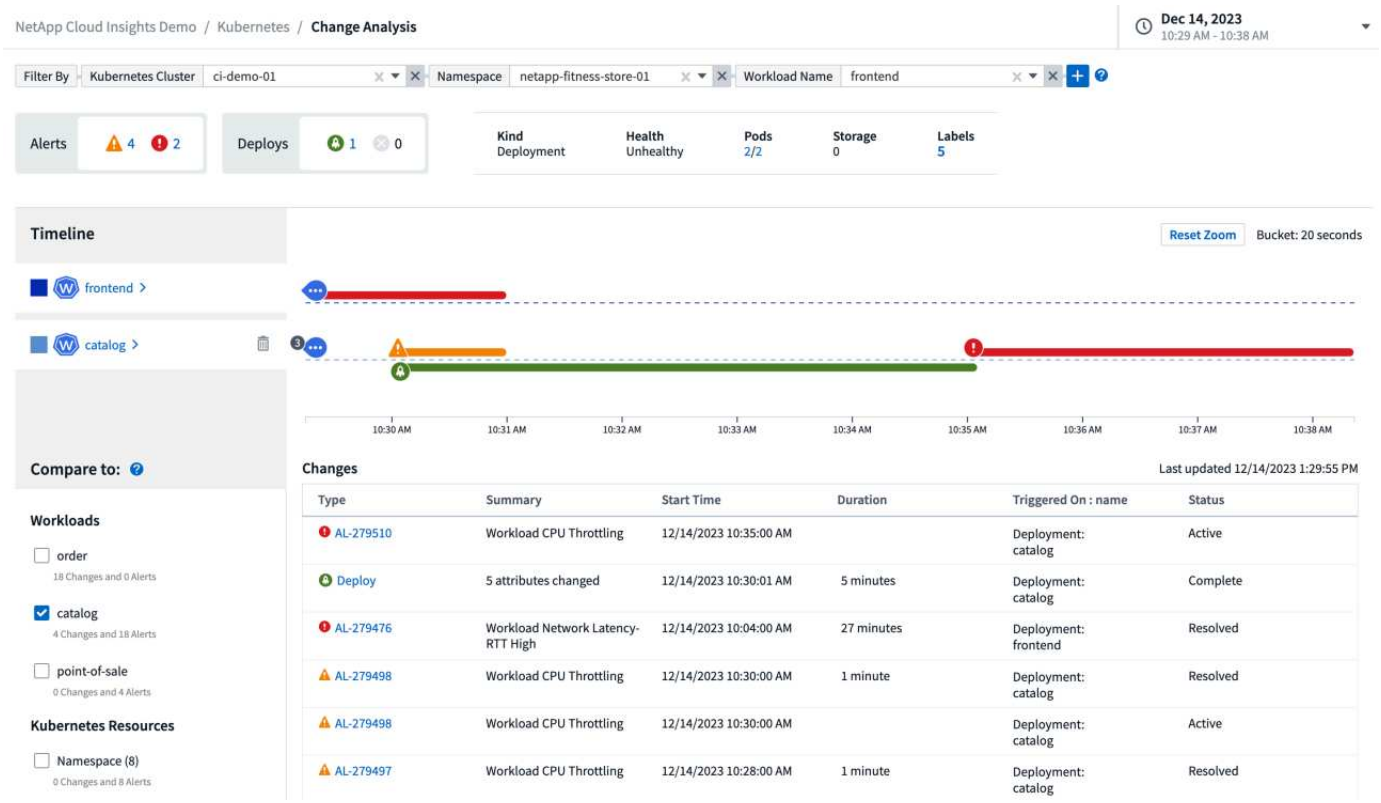
Analyse des changements Kubernetes

L'analytique des changements Kubernetes vous offre une vue complète des modifications récentes de 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 mettre en corrélation avec l'état et les performances des services, de l'infrastructure et des clusters K8s.

Comment l'analyse des changements peut-elle aider ?

- Dans les environnements Kubernetes mutualisés, les pannes peuvent se produire en raison de modifications mal configurées. L'analyse des changements permet d'y apporter une solution en fournissant une seule interface pour afficher et mettre en corrélation l'état des workloads et les modifications de configuration. Cela peut vous aider dans le dépannage des environnements Kubernetes dynamiques.

Pour afficher l'analyse des changements Kubernetes, accédez à **Kubernetes > analyse des changements**.



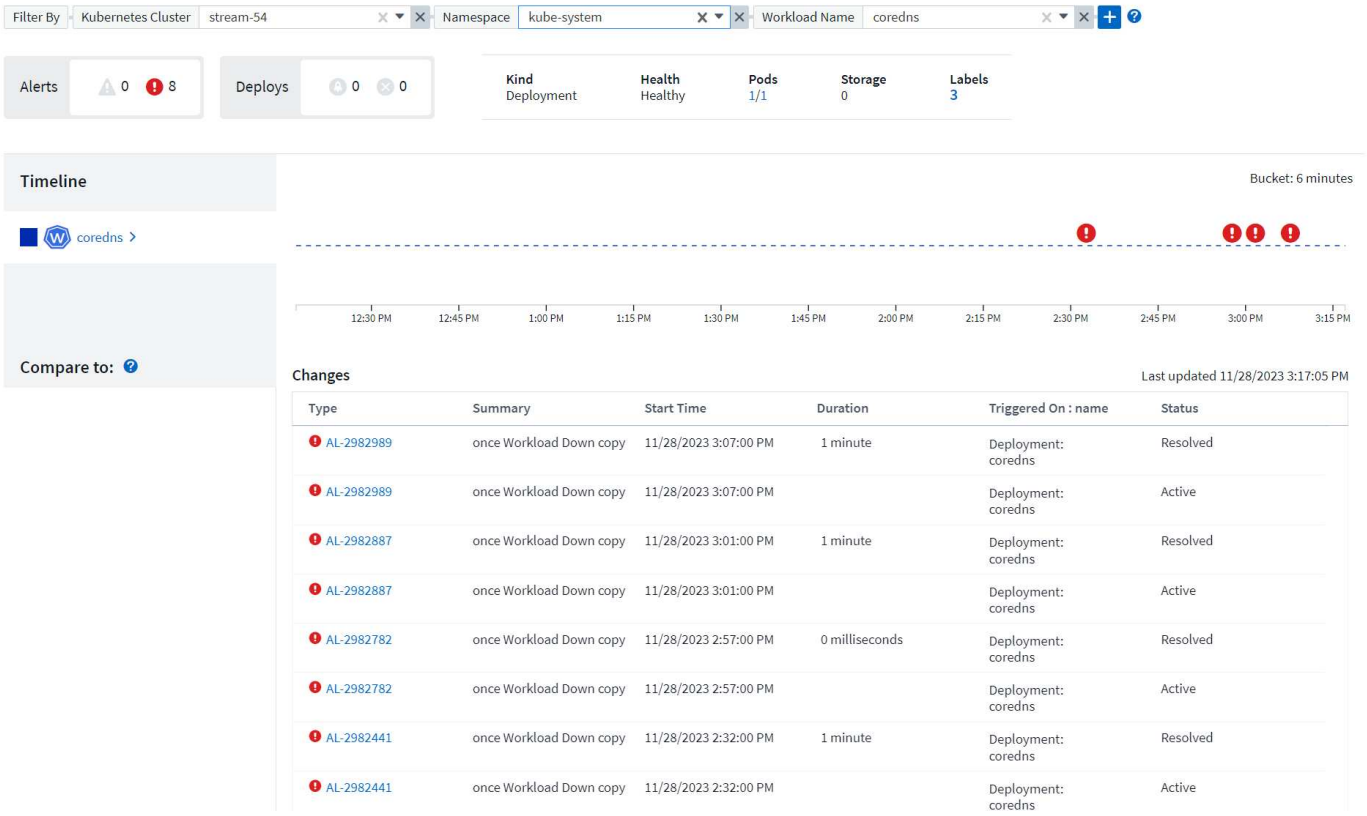
.

La page est automatiquement actualisée en fonction de la plage horaire Data Infrastructure Insights actuellement sélectionnée. Des plages de temps plus petites permettent un rafraîchissement plus fréquent de l'écran.

Filtrage

Comme toutes les fonctionnalités de Data Infrastructure Insights, il est intuitif de filtrer la liste de modifications : en haut de la page, entrez ou sélectionnez des valeurs pour votre cluster, espace de noms ou workload Kubernetes, ou ajoutez vos propres filtres en cliquant sur le bouton {+].

Lorsque vous filtrez vers un cluster, un espace de noms et une charge de travail spécifique (ainsi que tous les autres filtres que vous avez définis), la chronologie des déploiements et des alertes s'affiche pour cette charge de travail dans cet espace de noms sur ce cluster. Pour effectuer un zoom avant, cliquez sur le graphique et faites-le glisser pour vous concentrer sur une plage horaire plus spécifique.



Statut rapide

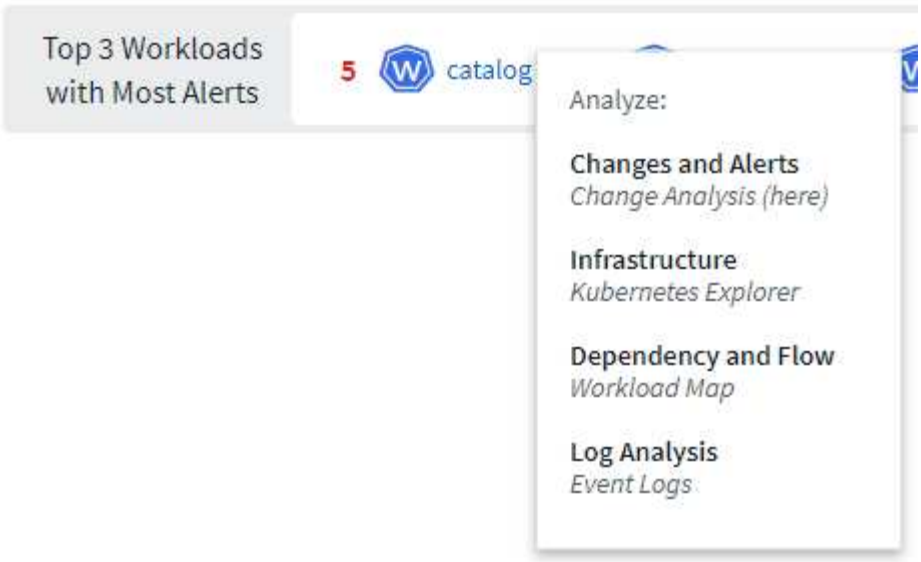
Sous la zone de filtrage se trouvent un certain nombre d'indicateurs de haut niveau. Le nombre d'alertes (Avertissement et critique) se trouve à gauche. Ce nombre inclut les alertes *Active* ainsi que les alertes *Resolved*. Pour afficher uniquement les alertes *Active*, définissez un filtre pour « Status » et choisissez « Active ».



L'état du déploiement est également indiqué ici. Encore une fois, la valeur par défaut est d'afficher le nombre de déploiements *démarrés*, *complets* et *échoués*. Pour afficher uniquement les déploiements *FAILED*, définissez un filtre pour « Status » et sélectionnez « FAILED ».

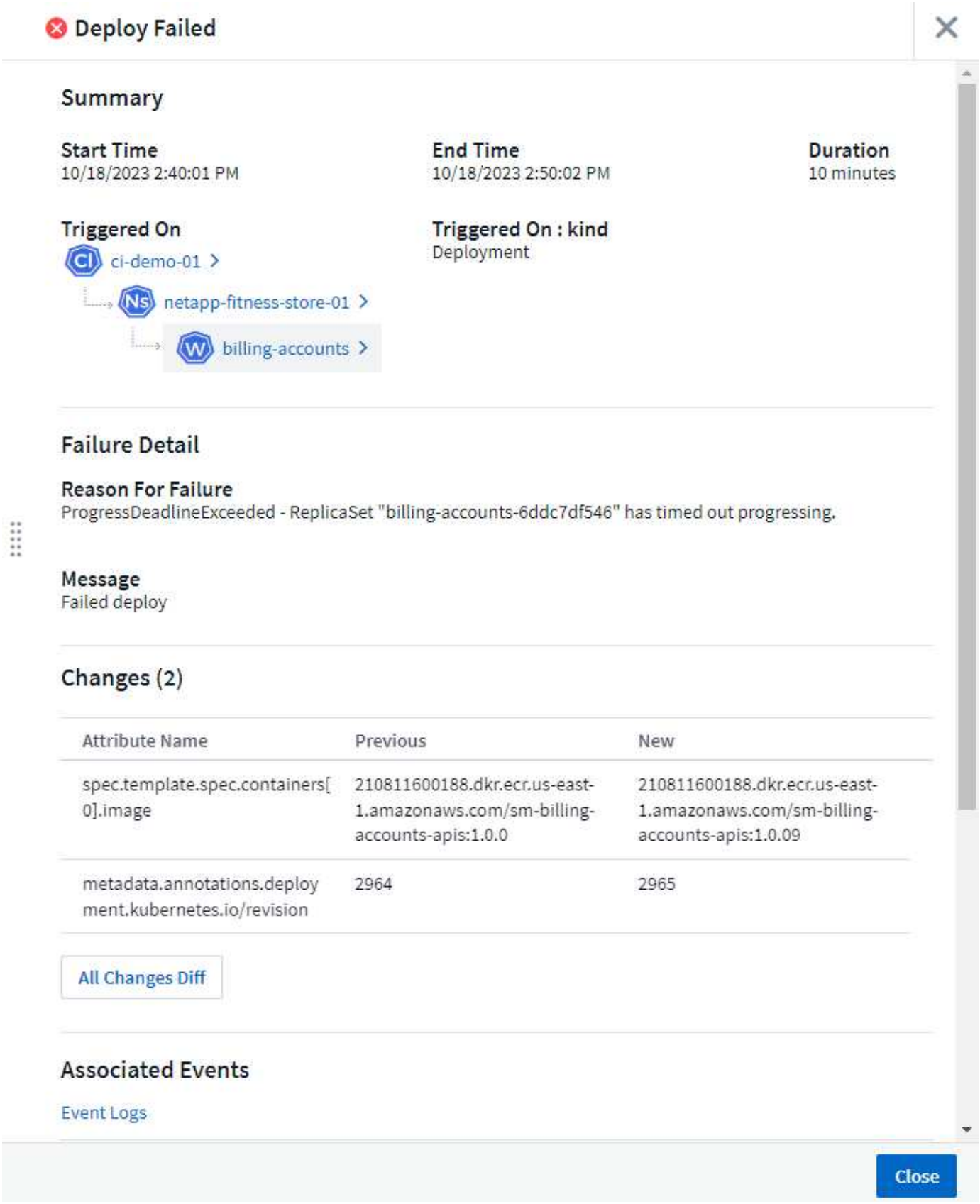


Les 3 principaux workloads avec le plus grand nombre d'alertes viennent ensuite. Le nombre en rouge en regard de chaque charge de travail indique le nombre d'alertes associées à cette charge de travail. Cliquez sur le lien correspondant aux workloads pour explorer votre infrastructure (Explorateur Kubernetes), les dépendances (carte des workloads) ou l'analyse des journaux (journaux d'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 en échec affiche un résumé du déploiement, avec les heures de début et de fin, la durée et l'endroit où le déploiement a été déclenché, avec des liens permettant d'explorer ces ressources. Il affiche également la raison de l'échec, les modifications associées et les événements associés.



La sélection d'une alerte de même type fournit des détails sur l'alerte, y compris le moniteur qui a déclenché l'alerte, ainsi qu'un graphique montrant un chronogramme visuel pour l'alerte.

ONTAP Essentials

ONTAP Essentials est un ensemble de tableaux de bord et de flux de production qui présentent en détail les inventaires et les charges de travail ONTAP. Les termes suivants peuvent être utilisés dans ONTAP Essentials :

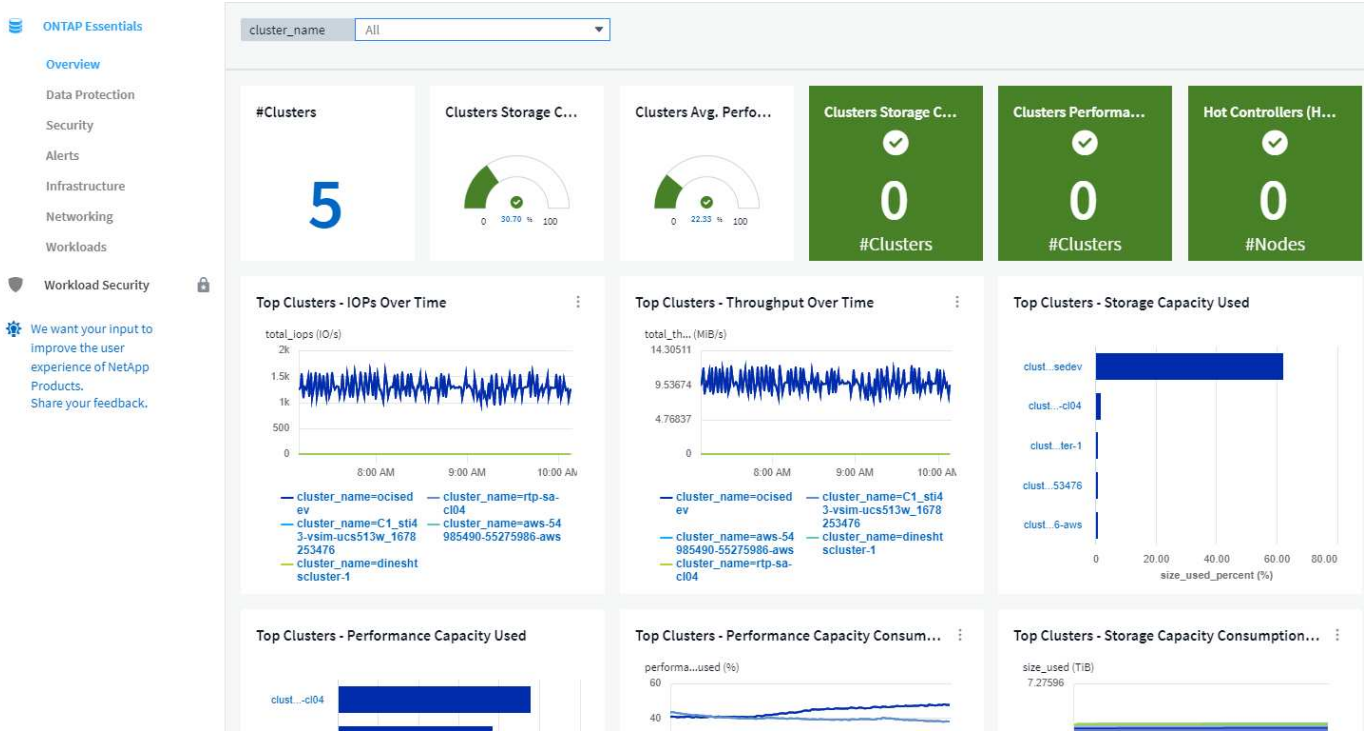
- Infrastructure/Inventaire : objets qui fournissent des services de stockage/réseau aux données utilisateur
- Workloads : objets offrant une interface pour les utilisateurs en matière de lecture/écriture des données.
- Protection des données : objets pouvant être protégés à l'aide des technologies de protection des données NetApp

Pour obtenir des termes et définitions supplémentaires relatifs à ONTAP, consultez la "Collecteur de données ONTAP" documentation.

ONTAP Essentials exige au moins un collecteur de données ONTAP opérationnel, avec les données collectées au cours des sept derniers jours.

Présentation

Pour commencer l'exploration, sélectionnez **ONTAP Essentials** dans le menu principal informations sur l'infrastructure de données.



Le tableau de bord **Overview** affiche des informations utiles telles que le nombre de clusters de votre locataire avec leurs pourcentages de capacité et de performances globaux. Des données prédictives concernant le nombre de jours prévus jusqu'à ce que la capacité de stockage ou les performances manque d'espace s'affichent. En outre, si des contrôleurs de votre infrastructure fonctionnent avec leur processeur à plus de 65 %, ce qui risque de compromettre votre cluster en cas de basculement, ONTAP Essentials les présente comme des contrôleurs actifs.

Des graphiques d'information vous permettent d'examiner les performances au fil du temps ainsi que les pannes d'utilisation de la capacité. Chacun de ces graphiques ou points de données peut être utilisé comme point de départ pour l'exploration ou l'enquête.

Remarque : un nombre « jours à plein » de « 0 » (zéro) indique que le nombre de jours à pleins est estimé à plus de 90 jours. En d'autres termes, vos systèmes ne risquent pas de manquer d'espace à tout moment.

Protection des données

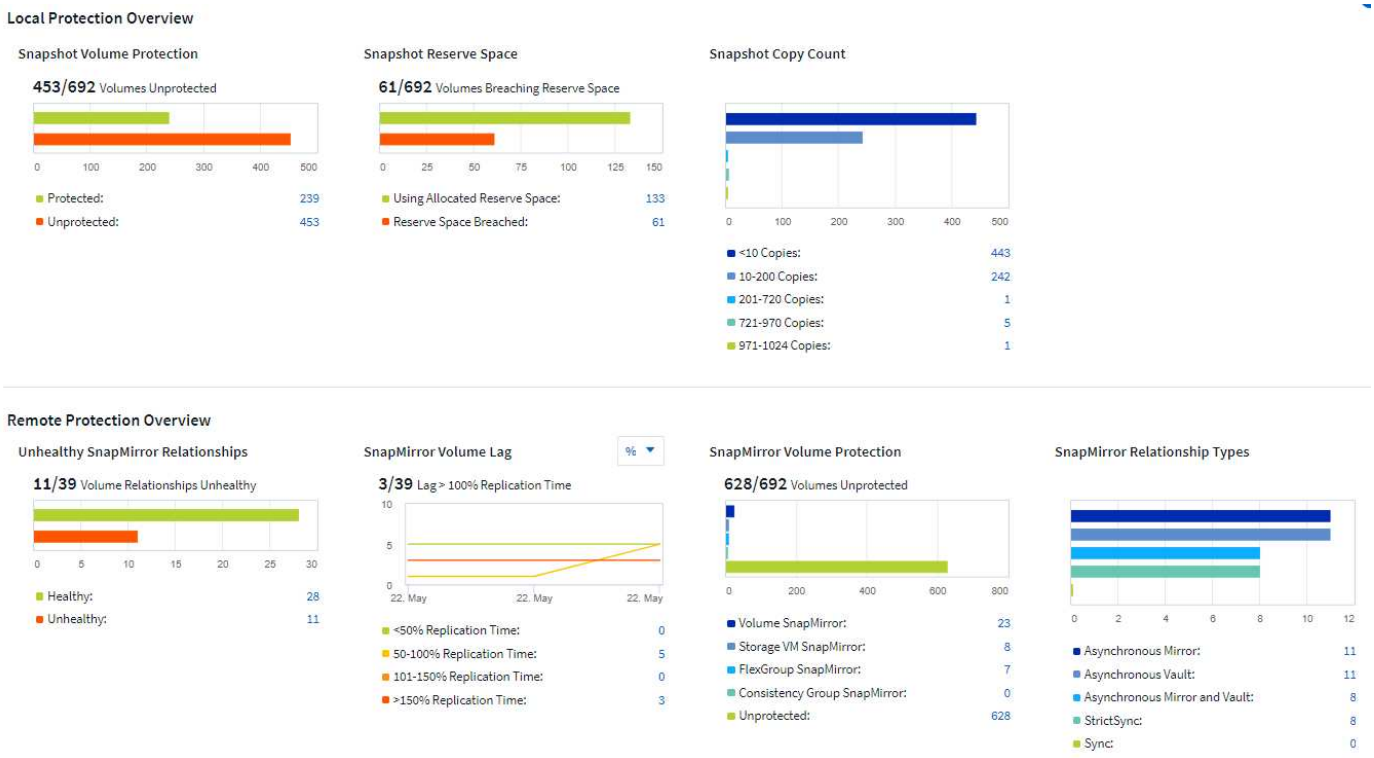
La page **Data protection** affiche l'état des volumes protégés par **Snapshot copies** ou **SnapMirror policies**.

Dans la section *vue d'ensemble de la protection locale*, les graphiques fournissent les informations suivantes pour les volumes protégés par des copies Snapshot :

- Le nombre de volumes protégés par les copies Snapshot, ainsi que les volumes non protégés.
- Nombre de volumes qui utilisent ou dépassent l'espace de réserve pour les copies Snapshot.
- 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 règles SnapMirror :

- Le nombre de relations SnapMirror saines et malsaines.
- Nombre de relations SnapMirror avec un décalage de l'objectif de point de récupération (RPO) basé sur le statut de décalage.
- Nombre de relations protégées par les types de protection de volume SnapMirror tels que SnapMirror volume, les relations SVMDR, les relations SnapMirror FlexGroup, les relations de groupe de cohérence SMBC (SnapMirror Business Continuity), ainsi que les volumes non protégés.
- Nombre de relations protégées par les types de relations SnapMirror tels que Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StrictSync et Sync.



La grille *clusters* au bas de la page fournit des détails sur les éléments suivants :

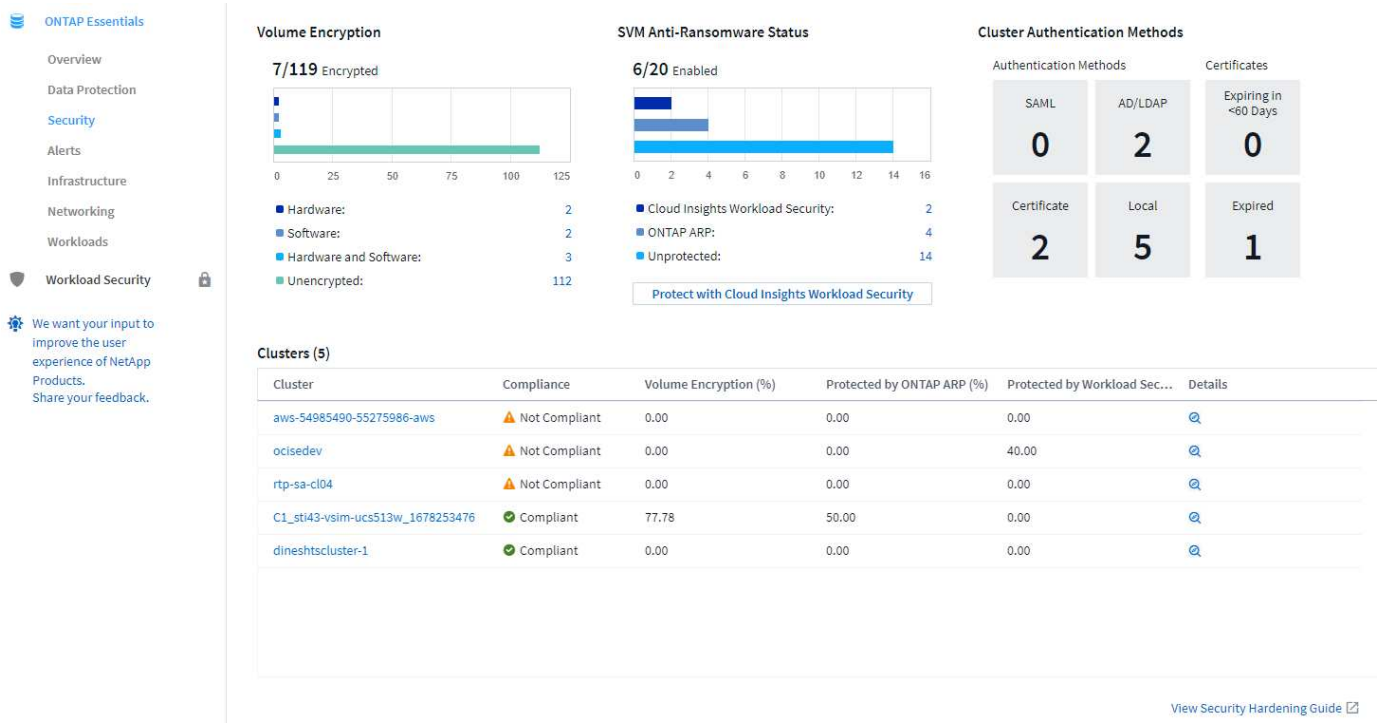
- Volumes non protégés par des snapshots.
- Les volumes ne correspondant pas à l'espace de réserve du snapshot.
- Les volumes non protégés par des règles snapmirror et les relations snapmirror sont en décalage.
- Relations SnapMirror défectueuses.



Sécurité

Le tableau de bord de sécurité vous offre une vue instantanée de votre situation en matière de sécurité et affiche des graphiques sur le chiffrement de volume matériel et logiciel, l'état anti-ransomware et les méthodes d'authentification du cluster. Les critères de sécurité sont évalués sur la base des recommandations définies dans le **"Guide NetApp de renforcement de la sécurité pour ONTAP 9"**.

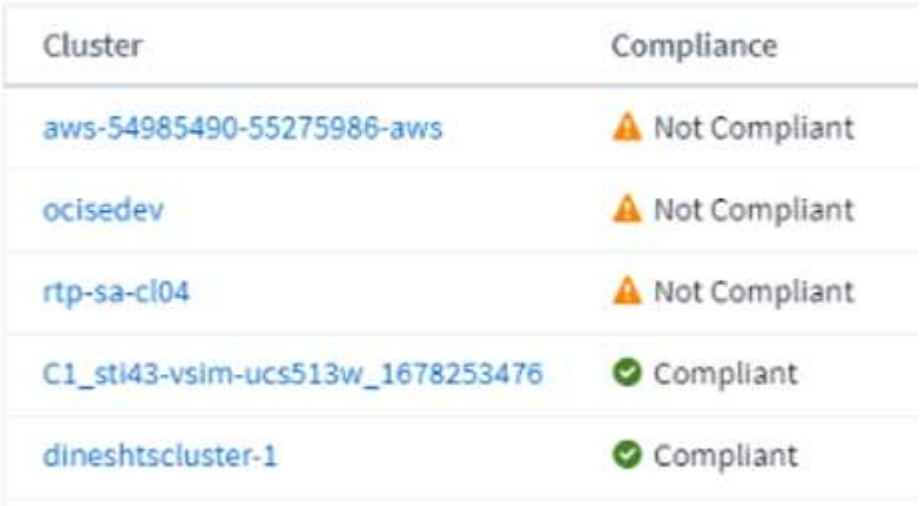
Sélectionnez l'un des chiffres de chiffrement ou de protection contre les ransomware pour accéder à votre environnement.



Le tableau de bord sécurité ONTAP Essentials surveille votre environnement pour déterminer l'état de conformité du cluster. Pour en savoir plus, reportez-vous au"Catégories de conformité du cluster". ONTAP Essentials utilise les moniteurs suivants pour déterminer la conformité :

Nom du moniteur	Nom de l'attribut (affiché dans les détails du cluster)	Valeur de conformité de l'attribut
Mode FIPS désactivé	Mode FIPS	Activé
Chiffrement de cluster non sécurisé pour SSH	Paramètres SSH sécurisés	Oui
Protocole Telnet activé	Telnet	Désactivé
Shell distant activé	Coque distante	Désactivé
Utilisateur Admin local par défaut activé	Utilisateur Admin par défaut	Désactivé
Mot de passe MD5 hachée	MD5 en cours d'utilisation	Non
Communication entre les pairs de cluster non chiffrée	Peering de clusters	Chiffré/sans homologue
Transport HTTPS AutoSupport désactivé	AutoSupport utilisant 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 journal non crypté	Transfert de journaux crypté	Oui

Notez que si un moniteur ci-dessus est désactivé, les détails du cluster indiquent que la valeur est « non cochée » pour l'attribut de conformité de sécurité correspondant.

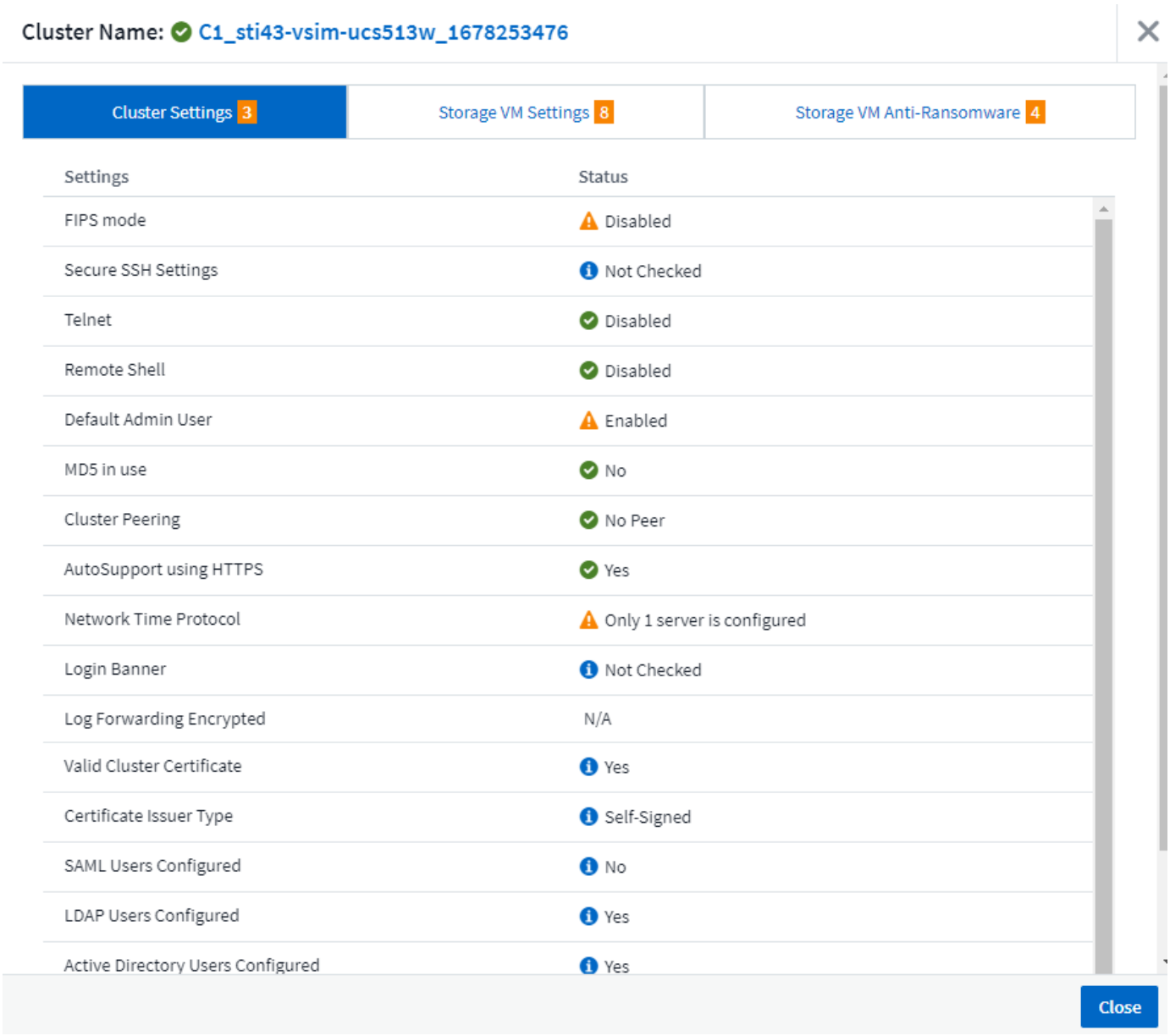


Pour les SVM, le tableau de bord de sécurité contrôle les moniteurs suivants :

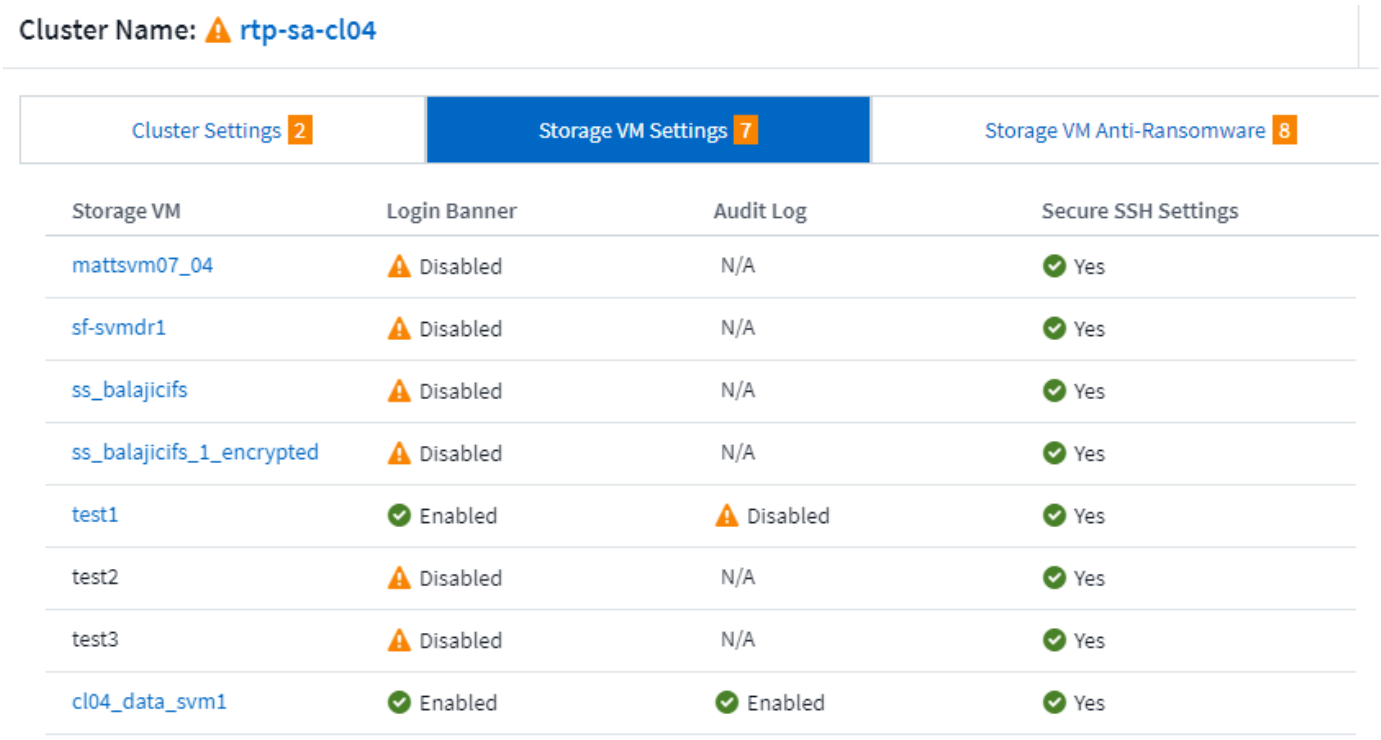
Nom du moniteur	Nom de l'attribut (affiché dans les paramètres de Storage VM)	Valeur de conformité de l'attribut
Chiffrement non sécurisé des machines virtuelles de stockage pour SSH	Paramètres SSH sécurisés	Oui
Bannière connexion VM de stockage désactivée	Bannière de connexion	Activé
Journal d'audit de VM de stockage désactivé	Journal d'audit	Activé

Dans la liste des clusters, sélectionnez *View Details* pour chaque cluster afin d'ouvrir un panneau coulissant affichant les paramètres actuels de *Cluster, Storage VM,* ou *anti-ransomware*.

Les détails du cluster incluent l'état de la connexion, des informations de certificat, etc. :



Les détails de la VM de stockage affichent des informations d'audit et SSH :

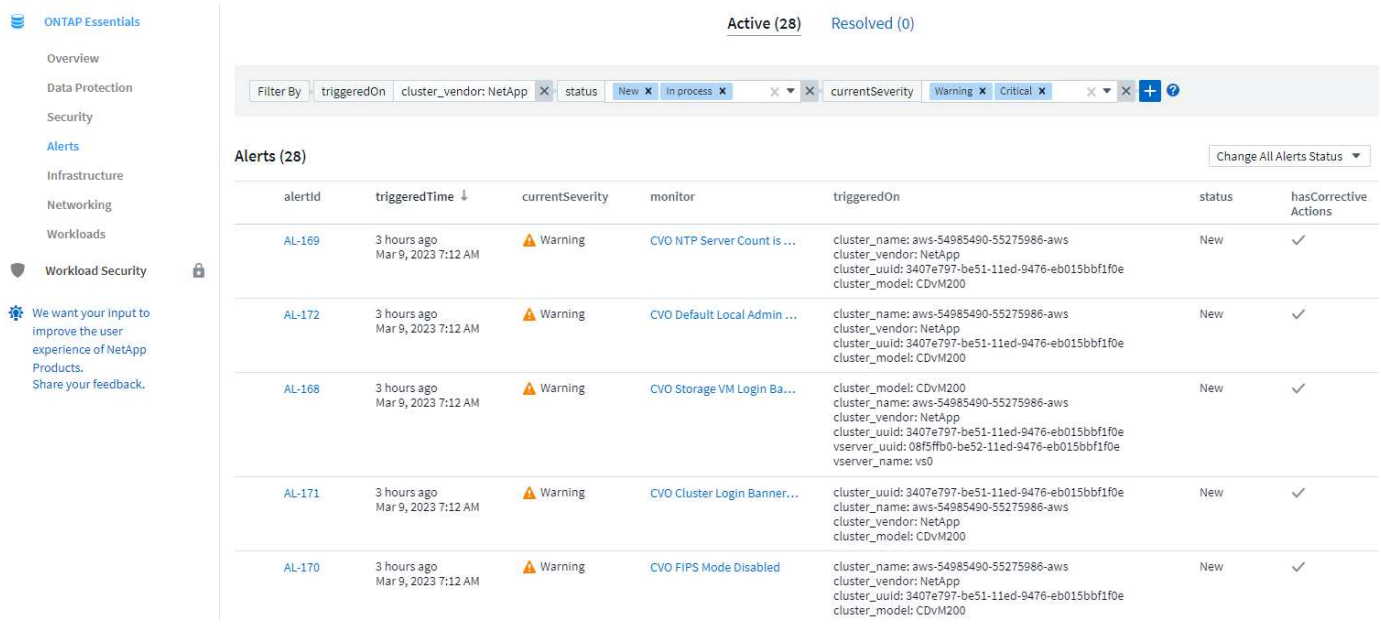


Les détails anti-ransomware indiquent si une machine virtuelle de stockage est protégée par la protection anti-ransomware de ONTAP ou les informations stratégiques sur l'infrastructure pour la sécurité des workloads. Notez que la colonne ARP de ONTAP affiche l'état actuel de la protection anti-ransomware intégrée d'ONTAP, qui est configurée sur le système ONTAP. Pour activer Data Infrastructure Insights Workload Security, sélectionnez « Protect » dans cette colonne.



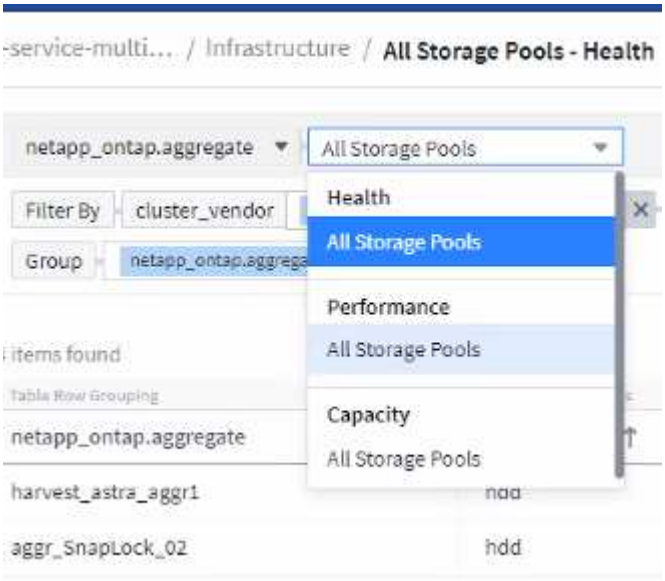
Alertes

Cette page vous permet de consulter les alertes actives sur votre locataire et d'explorer rapidement les problèmes potentiels. Sélectionnez l'onglet *Resolved* pour afficher les alertes qui ont été résolues.

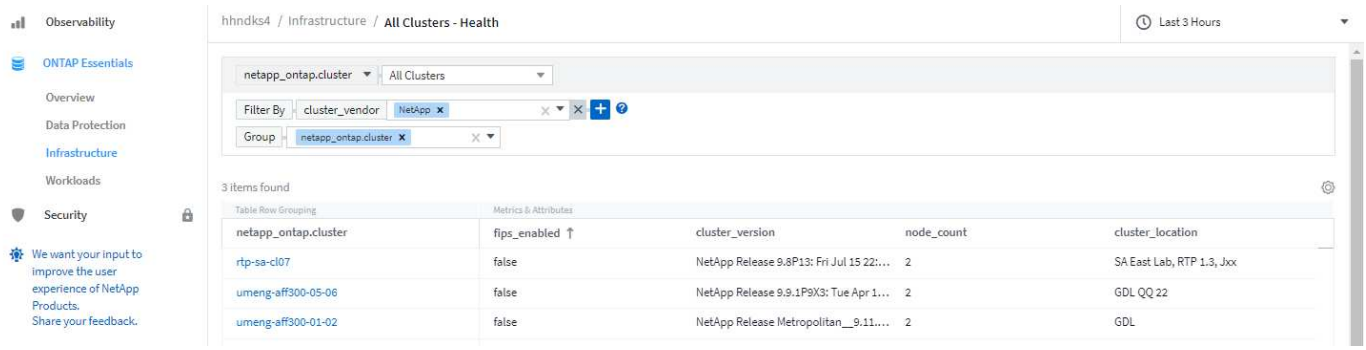


Infrastructures

La page ONTAP Essentials **Infrastructure** vous donne un aperçu de l'état et des performances du cluster à l'aide de requêtes pré-intégrées (mais encore personnalisables) sur tous les objets ONTAP de base. Sélectionnez le type d'objet à explorer (cluster, pool de stockage, etc.) et choisissez d'afficher les informations d'état ou de performance. Définissez des filtres pour approfondir chaque système.

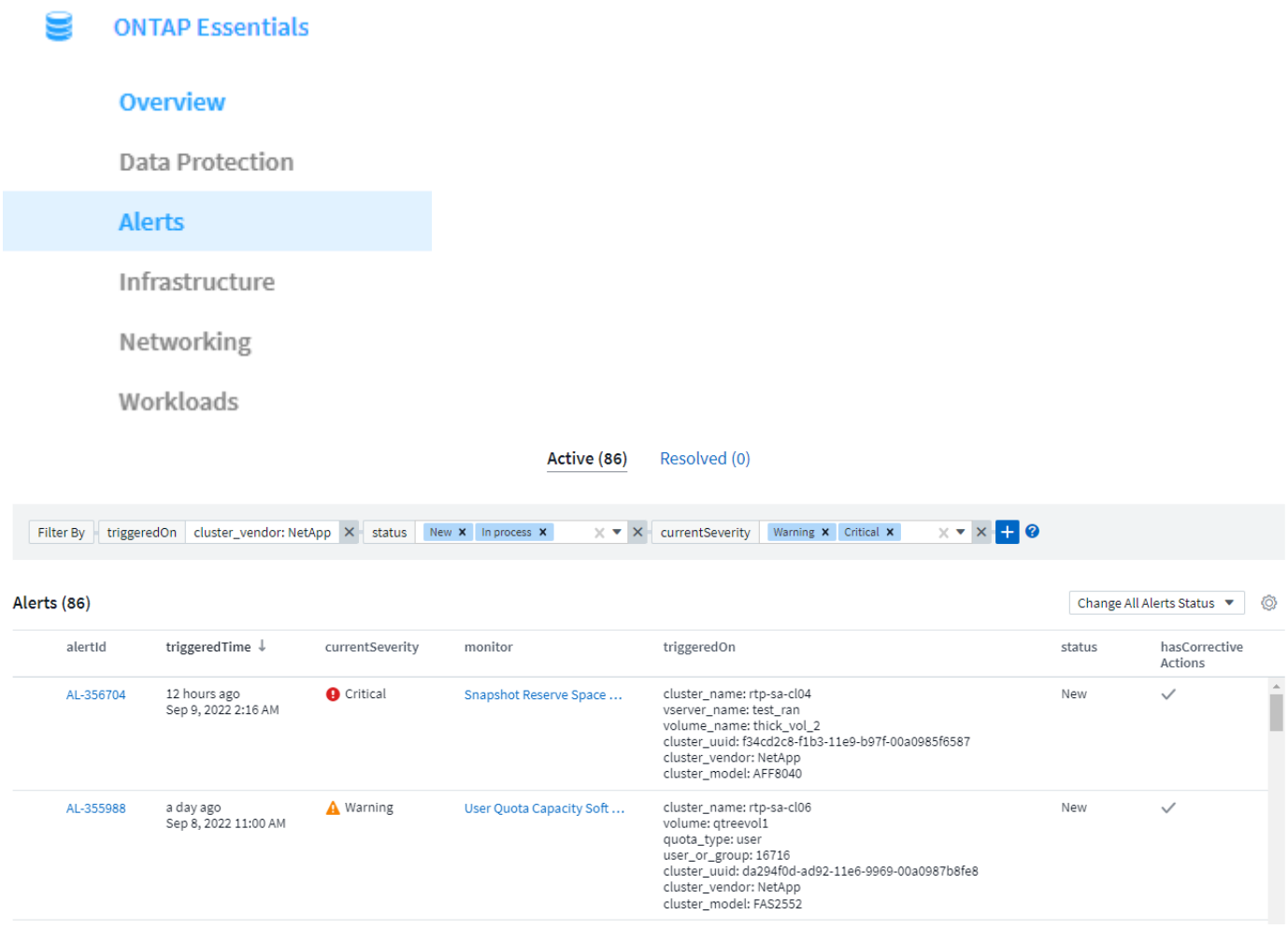


Page d'infrastructure affichant l'état du cluster :



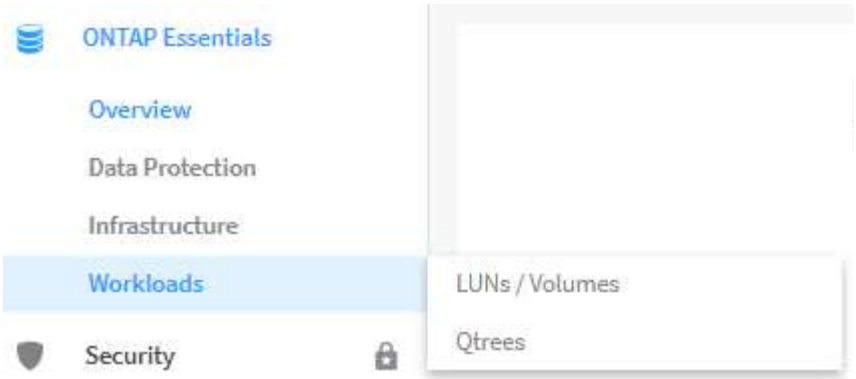
Mise en réseau

Le programme de mise en réseau ONTAP Essentials vous permet de visualiser votre infrastructure FC, NVMe FC, Ethernet et iSCSI. Sur ces pages, vous pouvez explorer des choses comme des ports dans vos clusters et leurs nœuds.



Charges de travail

Affichez et explorez les workloads sur des LUN/volumes, des partages NFS ou SMB ou des 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 d'intégrer des informations exploitables de l'infrastructure de données à d'autres applications, telles que des CMDB ou d'autres systèmes de gestion de tickets.

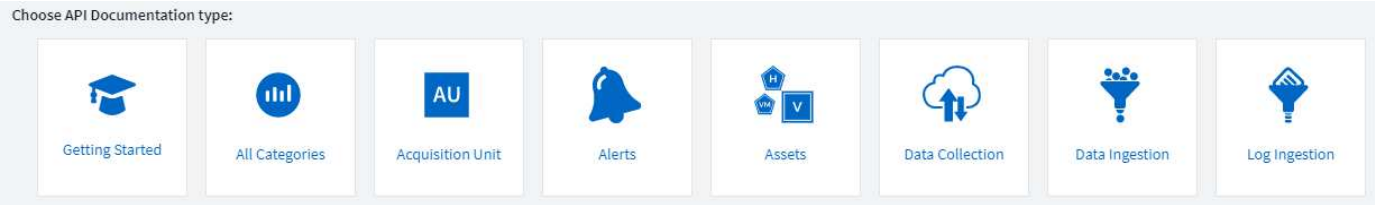
Vos informations stratégiques sur l'infrastructure de données "rôle du jeu de fonctions"déterminent les API auxquelles vous pouvez accéder. Les rôles utilisateur et invité disposent de privilèges moins nombreux que le rôle administrateur. Par exemple, si vous avez un rôle Administrateur dans Monitor and Optimize, mais que vous avez un rôle utilisateur dans Reporting, vous pouvez gérer tous les types d'API, à l'exception de Data Warehouse.

Conditions requises pour l'accès aux API

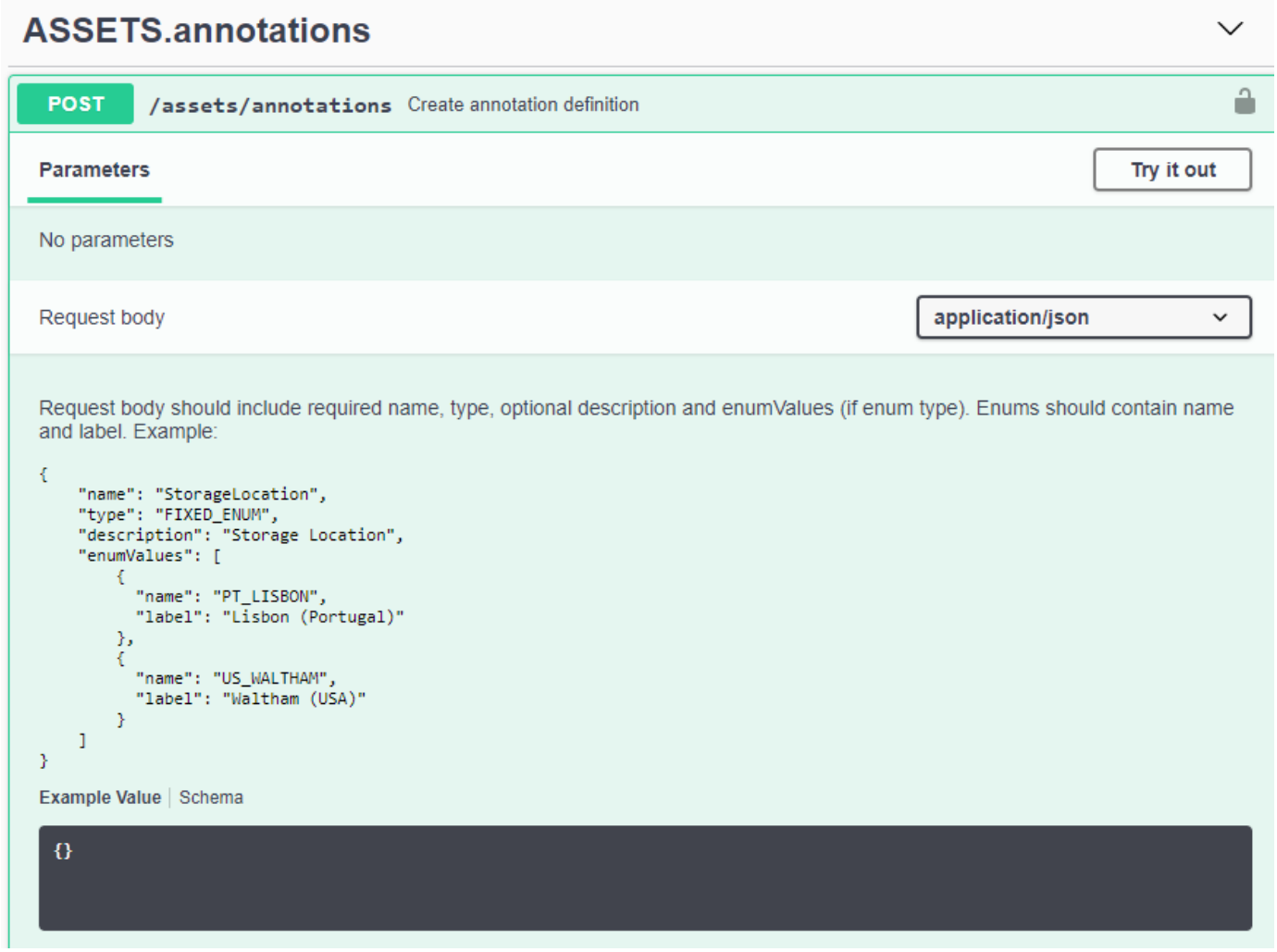
- Un modèle de token d'accès API est utilisé pour accorder l'accès.
- La gestion des tokens API est effectuée par les utilisateurs de Data Infrastructure Insights avec le rôle d'administrateur.

Documentation API (swagger)

Les informations les plus récentes sur l'API sont disponibles en se connectant à Data Infrastructure Insights et en accédant à **Admin > API Acccess**. Cliquez sur le lien **API Documentation**.



La documentation de l'API est basée sur swagger, qui fournit une brève description et des informations d'utilisation pour l'API, et vous permet de l'essayer dans votre locataire. Selon votre rôle d'utilisateur et/ou l'édition de Data Infrastructure Insights, les types d'API disponibles peuvent varier.



Jetons d'accès à l'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 vide d'un nom d'utilisateur ou d'un mot de passe.

Pour créer un token d'accès :

- Cliquez sur **Admin > accès API**
- Cliquez sur **+jeton d'accès API**
  - Entrez le nom du token
  - Sélectionnez les types d'API
  - Spécifiez les autorisations accordées pour cet accès API
  - Spécifiez l'expiration du token

Votre jeton ne sera disponible que pour la copie dans le presse-papiers et l'enregistrement pendant le processus de création. Les tokens ne peuvent pas être récupérés après leur création. Il est donc fortement recommandé de les copier et de les enregistrer dans un emplacement sécurisé. Vous serez invité à cliquer sur le bouton **Copier le token d'accès API** avant de pouvoir fermer l'écran de création de jeton.

Vous pouvez désactiver, activer et révoquer des jetons. Les tokens désactivés peuvent être activés.

Les jetons accordent un accès général aux API du point de vue du client, et gèrent l'accès aux API dans le cadre de leur propre locataire. Les administrateurs du client peuvent octroyer et révoquer ces tokens sans intervention directe du personnel back-end Data Infrastructure Insights.

L'application reçoit un token d'accès après l'authentification et l'autorisation de l'accès, puis transmet le token d'accès en tant qu'identifiant lorsqu'il appelle l'API cible. Le jeton transmis informe l'API que le porteur du token a été autorisé à accéder à l'API et à effectuer des actions spécifiques spécifiées par le périmètre qui a été accordé lors de l'autorisation.

L'en-tête HTTP où le token d'accès est transmis est **X-CloudInsights-ApiKey:**.

Par exemple, utilisez les éléments suivants pour récupérer des actifs 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 d'un accès à l'API.
```

Reportez-vous aux pages swagger pour obtenir des exemples spécifiques à l'API que vous souhaitez utiliser.

Type API

L'API Data Infrastructure Insights est basée sur des catégories et contient actuellement les types suivants :

- LE type DE RESSOURCES contient des API de ressource, de requête et de recherche.
  - Atouts : énumérer les objets de premier niveau et récupérer un objet spécifique ou une hiérarchie d'objets.
  - Requête : récupérez et gérez des requêtes Data Infrastructure Insights.
  - Importer : importez des annotations ou des applications et affectez-les à des objets
  - Recherche : recherchez un objet spécifique sans connaître son ID unique ou son nom complet.
- Le type DE COLLECTE DE DONNÉES est utilisé pour extraire 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 DU JOURNAL est utilisée pour récupérer et gérer les données des journaux

D'autres types et/ou API peuvent devenir disponibles au fil du temps. Vous trouverez les informations les plus récentes sur l'API dans le "Documentation de swagger API".

Notez que les types d'API auxquels un utilisateur a accès dépendent également de ceux "Rôle utilisateur" qu'ils possèdent dans chaque jeu de fonctionnalités Data Infrastructure Insights (surveillance, sécurité des workloads, reporting).

Traversée des stocks

Cette section décrit comment parcourir une hiérarchie d'objets Data Infrastructure Insights.

Objets de premier niveau

Les objets individuels sont identifiés dans les requêtes par une URL unique (appelée « self » dans JSON) et requièrent une connaissance du type d'objet et de l'ID interne pour certains objets de premier niveau (hôtes, systèmes de stockage, etc.). L'API REST permet d'accéder à la collection complète.

Le format général d'une URL 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 demande est :
```

```
https://mysite.c01.cloudinsights.netapp.com/rest/v1/assets/storages
```

Enfants et objets connexes

Les objets de premier niveau, tels que stockage, peuvent être utilisés pour circuler vers d'autres enfants et objets associés. Par exemple, pour récupérer tous les disques d'un stockage spécifique, concaténez l'URL de stockage « self » avec « /disks », par exemple :

```
https://<tenant>/rest/v1/assets/storages/4537/disks
```

Se développe

De nombreuses commandes API prennent en charge le paramètre **expansion**, qui fournit des détails supplémentaires sur l'objet ou les URL pour les objets associés.

Le paramètre de développement commun est *Expands*. La réponse contient une liste de tous les développement 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 versions 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 expansion contient des données, une URL ou les deux. Le paramètre développer prend en charge les attributs multiples et imbriqués, par exemple :

```
 https://<tenant>/rest/v1/assets/storages/2782?expand=performance,storageR
esources.storage
Développez vous permet de rassembler plusieurs données associées en une
seule réponse. NetApp vous conseille de ne pas demander trop
d'informations à la fois. Vous risquez alors d'endommager les
performances.
```

Pour décourager cela, les demandes de recouvrement de premier niveau ne peuvent pas être étendues. Par exemple, vous ne pouvez pas demander d'étendre simultanément les données de tous les objets de stockage. Les clients sont nécessaires pour récupérer la liste des objets, puis choisir des objets spécifiques à développer.

Données de performance

Les données de performances sont recueillies sur de nombreux appareils sous forme d'échantillons distincts. Toutes les heures (valeur par défaut), Data Infrastructure Insights agrège et récapitule les exemples de performances.

L'API permet d'accéder aux échantillons et aux données résumées. Pour un objet avec des données de performances, un résumé des performances est disponible sous la forme *développer=performance*. Les séries de temps d'historique des performances sont disponibles via *sexpansion=performance.historique* imbriqué.

Voici des exemples d'objets Performance Data :

- StoragePerformance
- Poolde stockage haute performance
- PortPerformance
- DiskPerformance

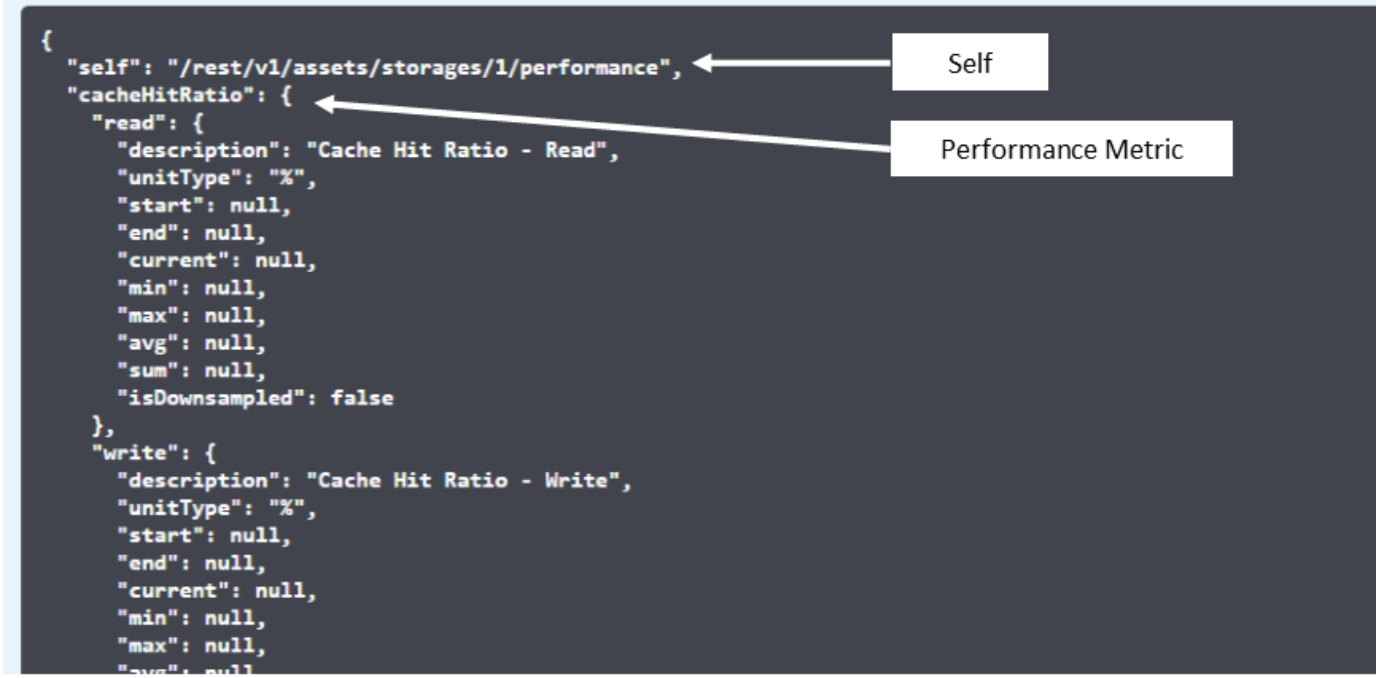
Une mesure de rendement a une description et un type et contient une collection de résumés de rendement. Par exemple, latence, trafic et débit.

Un résumé des performances comporte une description, une unité, l'heure de début de l'échantillon, l'heure de fin de l'échantillon et un ensemble de valeurs résumées (courant, min, max, moy, etc.) calculées à partir d'un seul compteur de performances sur une plage de temps (1 heure, 24 heures, 3 jours, etc.).

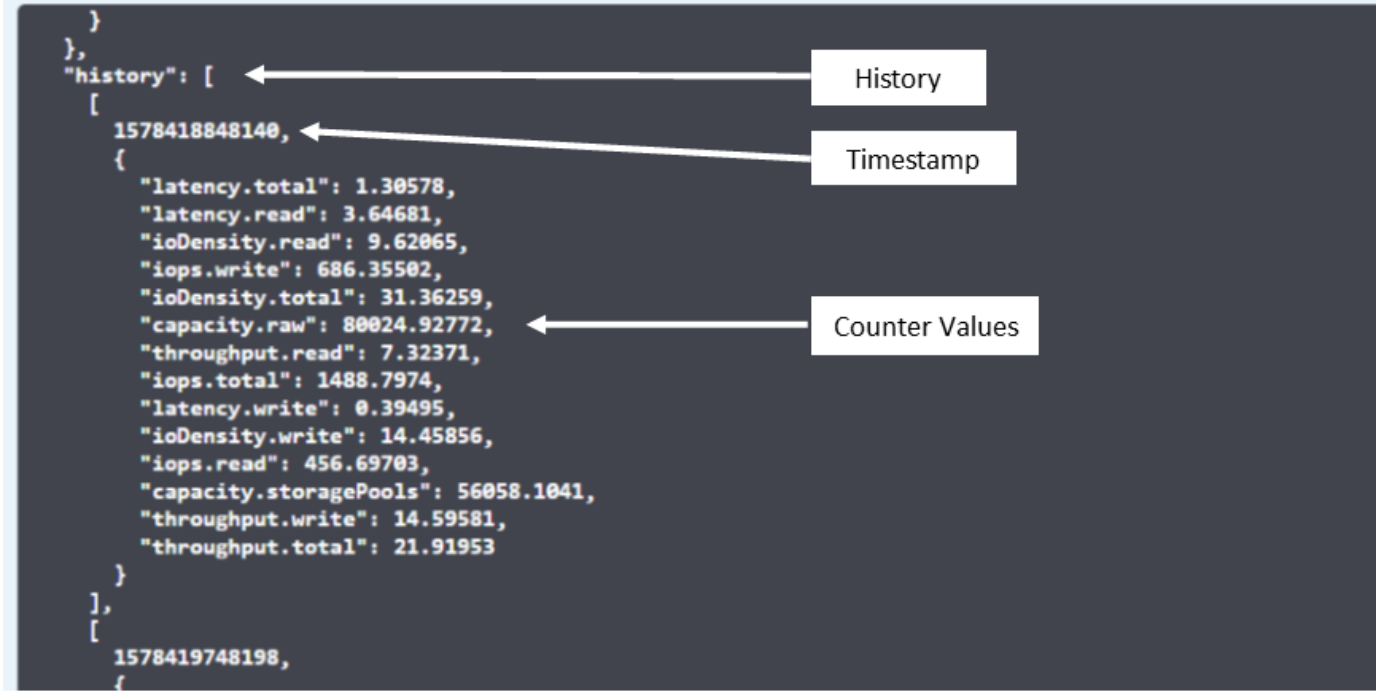
https://tenant.cloudinsights.netapp.com/rest/v1/assets/storages/1/performance?expand=history

Details

Response body



Response body



Le dictionnaire de données de performances obtenu possède les clés suivantes :

- « Self » est l'URL unique de l'objet

- “historique” est la liste des paires d’horodatage et de valeurs de compteurs
- Chaque autre clé de dictionnaire (« diskThroughput », etc.) est le nom d’une mesure de performance.

Chaque type d’objet de données de performance dispose d’un ensemble unique de metrics de performance. Par exemple, l’objet performances de la machine virtuelle prend en charge “diskThroughput” comme mesure de performances. Chaque mesure de performance prise en charge correspond à une certaine « catégorie de performance » présentée dans le dictionnaire de mesures. Data Infrastructure Insights prend en charge plusieurs types de metrics de performance répertoriés plus loin dans ce document. Chaque dictionnaire de mesures de performance aura 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 de synthèse des performances est le résumé des compteurs de performances. Il présente des valeurs agrégées typiques telles que min, max et avg pour un compteur ainsi que la dernière valeur observée, la plage de temps 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.

Les résumés de performance sont disponibles pour ces types de compteurs :

- Lire – Résumé des opérations de lecture
- Write – Résumé des opérations d’écriture
- Total : récapitulatif pour toutes les opérations. Elle peut être supérieure à la somme simple de lecture et d’écriture ; elle peut inclure d’autres opérations.
- Total max. : Récapitulatif pour toutes les opérations. Il s’agit de la valeur totale maximale dans la plage de temps spécifiée.

Mesures de performances de l’objet

L’API peut renvoyer des metrics détaillés pour les objets de votre locataire, par exemple :

- Mesures de performances du stockage telles que les IOPS (nombre de demandes d’entrée/sortie par seconde), la latence ou le débit.
- Mesures de performances de commutateur, telles que l’utilisation du trafic, les données de zéro crédit BB ou les erreurs de port.

Pour plus d’informations sur les metrics de chaque type d’objet, reportez-vous à la"Documentation de swagger API".

Données d’historique des performances

Les données historiques sont présentées dans les données de performance sous forme de liste de paires d’horodatage et de mappage de compteur.

Les compteurs historiques sont nommés en fonction du nom de l’objet de la mesure de performances. Par exemple, l’objet de performances de la machine virtuelle prend en charge “diskThroughput”, de sorte que la carte d’historique contient les clés nommées “diskThroughput.read”, “diskThroughput.write” et “diskThroughput.total”.

L’horodatage est au format d’heure UNIX.

Voici un exemple de données de performance 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 attributs de capacité utilisent des types de données de base et le CapacityItem pour la représentation.

Elément de capacité

CapacityItem est une unité logique unique de capacité. Il a “valeur” et “seuil” dans les unités définies par son objet parent. Il prend également en charge une carte de répartition facultative qui explique la construction de la valeur de capacité. Par exemple, la capacité totale d’un StoragePool de 100 To serait un CapacitéItem avec une valeur de 100. La répartition peut indiquer 60 To affectés aux « données » et 40 To pour les « instantanés ».

Remarque : « High Threshold » représente les seuils définis par le système pour les mesures correspondantes, qu’un client peut utiliser pour générer des alertes ou des signaux visuels sur des valeurs qui ne sont pas dans les plages configurées acceptables.

Voici la capacité du StoragePools avec plusieurs compteurs de capacité :



Utilisation de la fonction Rechercher 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 fichier JSON qui en résulte contient une liste classée des résultats. Les types de ressources sont différents des types d'inventaire, par exemple des stockages, des hôtes, des datastores, etc. Chaque type contiendra une liste d'objets du type correspondant aux critères de recherche.

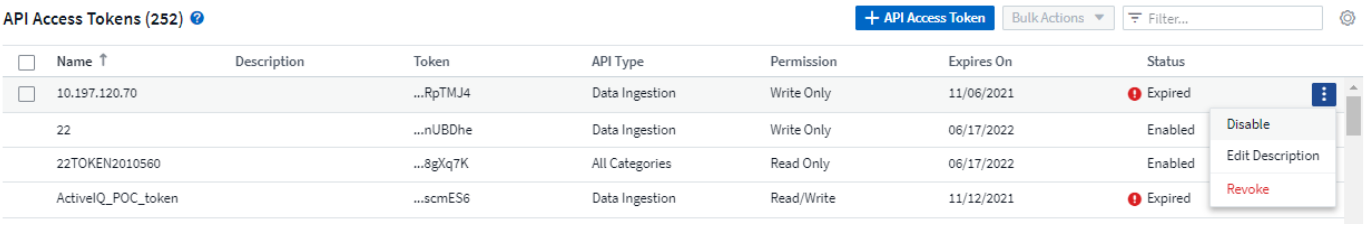
Data Infrastructure Insights est une solution extensible (large ouverture) qui permet des intégrations avec des systèmes tiers d'orchestration, de gestion des activités, de contrôle des changements et de gestion des tickets, ainsi que des intégrations CMDB personnalisées.

L'API RESTful de Cloud Insights 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 ces données.

Désactivation ou révocation d'un token API

Pour désactiver temporairement un jeton API, sur la page de la liste des jetons API, cliquez sur le menu "trois points" de l'API, puis sélectionnez *Disable*. Vous pouvez réactiver le token à tout moment à l'aide du même menu et sélectionner *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 tokens d'accès API expirés

Les jetons d'accès à l'API ont une date d'expiration. Lorsqu'un jeton d'accès à l'API expire, les utilisateurs doivent générer un nouveau jeton (de type *Data ingestion* avec les autorisations lecture/écriture) et reconfigurer Telegraf pour utiliser le jeton nouvellement généré au lieu du jeton expiré. Les étapes ci-dessous décrivent comment procéder.

Kubernetes

Notez que ces commandes utilisent le namespace par défaut « surveillance netapp ». Si vous avez défini votre propre espace de noms, remplacez-le dans ces commandes et tous les fichiers suivants.

Remarque : si la dernière version de NetApp Kubernetes Monitoring Operator est installée et que vous utilisez un jeton d'accès API renouvelable, les jetons arrivant à expiration seront automatiquement remplacés par des jetons d'accès à l'API nouveaux ou actualisés. Il n'est pas nécessaire d'effectuer les étapes manuelles indiquées ci-dessous.

- Modifiez l'opérateur de surveillance NetApp Kubernetes.

```
 kubectl -n netapp-monitoring edit agent netapp-ci-agent-monitoring-
netapp
* Modifiez la valeur _spec.output-sink.api-key_ en remplaçant l'ancien
jeton API par le nouveau jeton API.
```

```
spec:
…
  output-sink:
  - api-key:<NEW_API_TOKEN>
```

RHEL/CentOS et Debian/Ubuntu

- Modifiez les fichiers de configuration de 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
```

Fenêtres

- Pour chaque fichier de configuration de 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
```

Contrôle de 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 utilisateur 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, avec les détails suivants pour chaque entrée d'audit :

- **Heure** - Date et heure de l'événement ou de l'activité
- **Utilisateur** - l'utilisateur qui a lancé l'activité
- **Role** - rôle de l'utilisateur dans Data Infrastructure Insights (invité, utilisateur, administrateur)
- **IP** - adresse IP associée à l'événement
- **Action** - Type d'activité, par exemple connexion, création, mise à jour
- **Catégorie** - la catégorie d'activité
- **Détails** - Détails de l'activité

Affichage des entrées d'audit

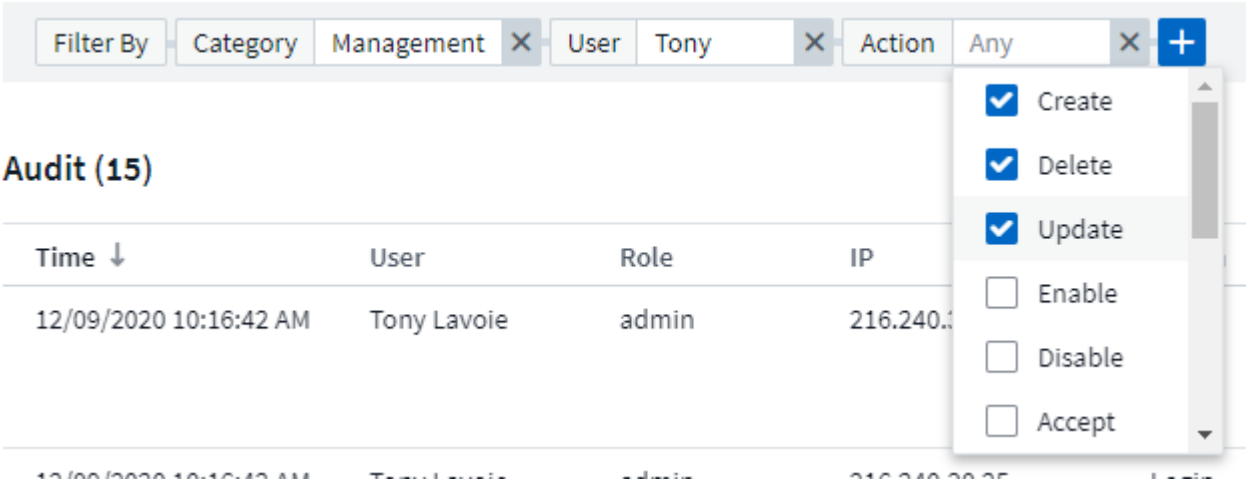
Il existe plusieurs façons d'afficher les entrées d'audit :

- Vous pouvez afficher les entrées d'audit en choisissant une période donnée (1 heure, 24 heures, 3 jours, etc.).

- Vous pouvez modifier l'ordre de tri des entrées en croissant (flèche vers le haut) ou en descendant (flèche vers le bas) en cliquant sur la flèche dans l'en-tête de colonne.

  Par défaut, le tableau affiche les entrées dans l'ordre décroissant.

- Vous pouvez utiliser les champs de filtre pour afficher uniquement les entrées souhaitées dans le tableau. Cliquez sur le bouton [+] pour ajouter des filtres supplémentaires.



Plus d'informations sur le filtrage

Vous pouvez utiliser l'une des méthodes suivantes pour affiner votre filtre :

Filtre	Ce qu'il fait	Exemple	Résultat
* (Astérisque)	permet de rechercher tout	vol*rhel	renvoie toutes les ressources commençant par « vol » et se terminant par « rhel ».
? (point d'interrogation)	permet de rechercher un nombre spécifique de caractères	BOS-PRD ??-S12	Renvoie BOS-PRD***12*** -S12, BOS-PRD***23***-S12, etc
OU	vous permet de spécifier plusieurs entités	FAS2240 OU CX600 OU FAS3270	Renvoie l'un des modèles FAS2440, CX600 ou FAS3270
PAS	permet d'exclure du texte des résultats de la recherche	PAS EMC*	Elle renvoie tous les éléments qui ne sont pas à l'avant par « EMC ».
Aucun	Recherche le champ vide/NULL/None 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 *text-only*	Pas *	renvoie les résultats lorsque le champ cible n'est pas vide.
« »	recherche une correspondance exacte	« NetApp* »	Renvoie les résultats contenant la chaîne littérale exacte *NetApp**

Si vous placez une chaîne de filtre entre deux guillemets, Insight traite tout entre le premier et le dernier devis comme une correspondance exacte. Tous les caractères spéciaux ou opérateurs situés dans les guillemets seront traités comme des littéraux. Par exemple, le filtrage pour "*" renvoie des résultats qui sont un astérisque littéral ; l'astérisque ne sera pas traité comme un caractère générique dans ce cas. Les opérateurs OU ET NON sont également traités comme des chaînes littérales lorsqu'ils sont entourés de guillemets doubles.

Événements et actions audités

Les événements et les actions audités par Data Infrastructure Insights peuvent être classés dans les domaines suivants :

- **Compte utilisateur** : connexion, déconnexion, changement de rôle, etc

  Exemple : *User **Tony Lavoie** connecté à partir de **10.1.120.15**, agent utilisateur **Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, comme Gecko) Chrome/85.0.4183.121 Safari/537.36**, méthode(s) de connexion **BlueXP Portal Login***

- **Unité d'acquisition** : créer, supprimer, etc

  Exemple : *unité d'acquisition **au-Boston-1** supprimé*.

- **Data Collector**: Ajouter, supprimer, modifier, différer/reprendre, changer l'unité d'acquisition, démarrage/arrêt, etc

  Exemple : *source de données **laboratoire FlexPod** supprimé, fournisseur **NetApp**, modèle **logiciel de gestion des données ONTAP**, ip **192.168.106.5***.

- **Application** : ajouter, attribuer à l'objet, supprimer, etc

  Exemple : *Volume interne **ocisedev:t1appSVM01:t1appFlexVol01** ajouté à l'application **Test App***.

- **Annotation** : ajouter, affecter, supprimer, actions de règle d'annotation, modifications de valeur d'annotation, etc

  Exemple : *valeur d'annotation **Boston** ajouté au type d'annotation **SalesOffice***.

- **Requête** : ajouter, supprimer, etc

  Exemple : *Query **TL Sales Query** est ajouté*.

- **Moniteur** : ajouter, supprimer, etc

  Exemple : Monitor *aggr Size - ci Alerts Notifications Dev* mis à jour

- **Notification** : changer d'e-mail, etc

  Exemple : destinataire *ci-alertes-notifications-dl* créé

Exportation d'événements d'audit

Vous pouvez exporter les résultats de votre affichage d'audit dans un fichier .CSV, qui vous permettra d'analyser les données ou de les importer dans une autre application.

Étapes

1. Sur la page Audit, définissez la plage de temps souhaitée et les filtres souhaités. Data Infrastructure Insights exporte uniquement les entrées d'audit correspondant au filtrage et à la plage de temps que vous avez définis.
2. Cliquez sur le bouton *Export* dans le coin supérieur droit de la table.

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 de conservation des données d'audit par Data Infrastructure est basée sur votre édition :

- Édition de base : les données d'audit sont conservées pendant 30 jours
- Éditions Standard et Premium : les données d'audit sont conservées pendant 1 an et 1 jour

Les entrées d'audit antérieures à la durée de conservation sont automatiquement supprimées. Aucune interaction de l'utilisateur n'est nécessaire.

Dépannage

Vous trouverez ici des suggestions pour résoudre les problèmes liés à l'audit.

Problème:	Essayez ceci:
Les messages d'audit me disent qu'un moniteur a été exporté.	Les ingénieurs NetApp peuvent généralement effectuer une exportation d'une configuration de moniteur personnalisée lors du développement et du test des nouvelles fonctionnalités. Si ce message ne s'affiche pas, envisagez d'explorer les actions de l'utilisateur nommé dans l'action vérifiée ou contactez l'assistance technique.

Conseiller digital Active IQ

NetApp "Conseiller digital Active IQ"(également connu sous le nom de conseiller digital) propose aux clients NetApp une série de visualisations, d'analyses et d'autres services de support pour leurs systèmes matériels et logiciels. Les données rapportées par Digital Advisor peuvent améliorer le dépannage des problèmes système et fournir des informations sur l'optimisation et l'analyse prédictive liées à vos appareils.

Data Infrastructure Insights collecte les **risques** pour tout système de stockage NetApp clustered Data ONTAP qui est surveillé et signalé par Digital Advisor. Les risques signalés pour les systèmes de stockage sont automatiquement collectés par Data Infrastructure Insights dans le cadre de leur collecte de données sur ces

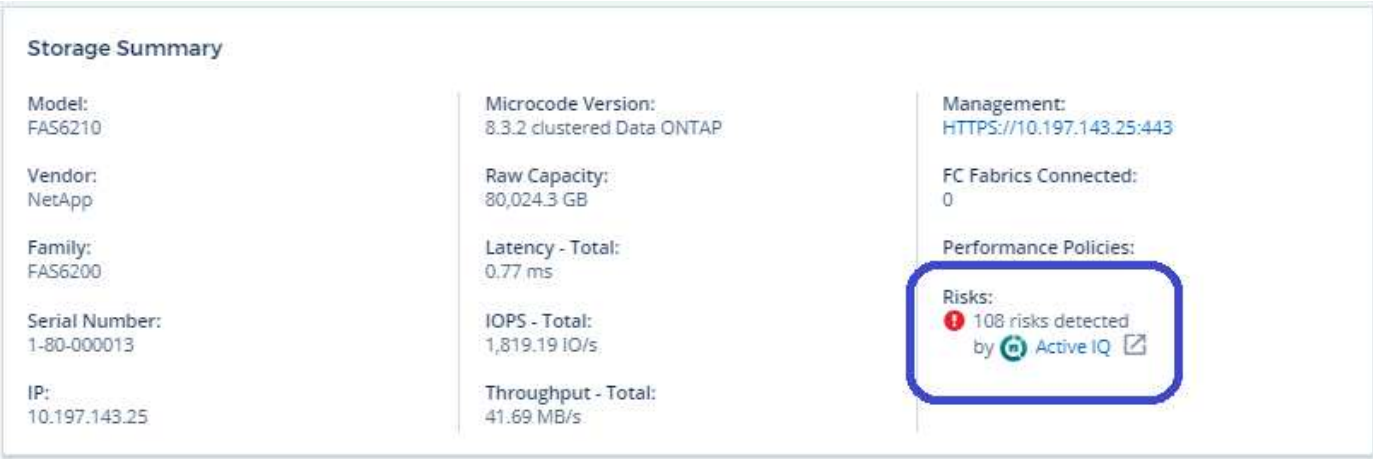
périphériques. Vous devez ajouter le collecteur de données approprié à Data Infrastructure Insights pour collecter les informations sur les risques de Digital Advisor.

Les informations sur l'infrastructure de données n'affichent pas les données de risques pour les systèmes ONTAP qui ne sont pas surveillés et signalés par Digital Advisor.

Les risques signalés sont présentés dans les informations sur l'infrastructure de données sur les pages d'accueil *Storage* and *Storage node* Asset, dans le tableau des risques. Le tableau présente les détails des risques, la catégorie de risque et l'impact potentiel du risque. Il fournit également un lien vers la page Digital Advisor résumant tous les risques pour le nœud de stockage (identifiant de compte de support NetApp requis).



Le nombre de risques signalés est également indiqué dans le widget Summary de la page d'accueil, avec un lien vers la page Digital Advisor appropriée. Sur une page *Storage* Landing, le nombre est une somme des risques pour tous les nœuds de stockage sous-jacents.



Ouverture de la page 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 Data Infrastructure Insights Summary ou le tableau Risks, cliquez sur le lien Digital Advisor.
2. Connectez-vous à votre compte sur le site de support NetApp. Vous accédez directement à la page du nœud de stockage dans Digital Advisor.

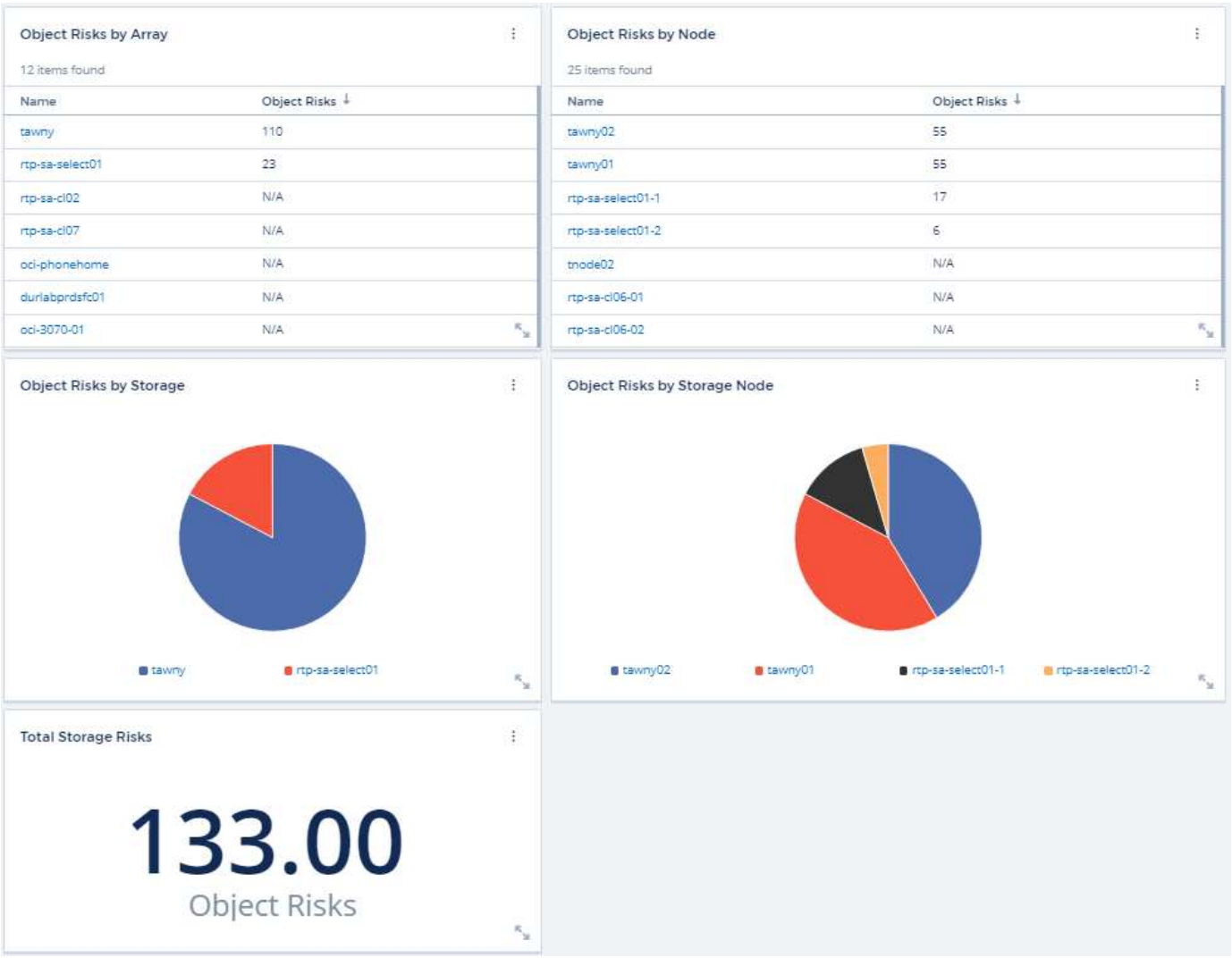
Recherche de risques

Dans Data Infrastructure Insights, vous pouvez ajouter la colonne **monitoring.count** à une requête de noeud

de stockage ou de noeud de stockage. Si le résultat renvoyé inclut des systèmes de stockage surveillés par Digital Advisor, la colonne monitoring.count affiche le nombre de risques pour le système ou le nœud de stockage.

Tableaux de bord

Vous pouvez créer des widgets (par exemple, un graphique à secteurs, un widget de tableau, une barre, une colonne, un graphique de dispersion et des widgets à valeur unique) afin de visualiser les risques liés aux objets pour les nœuds de stockage et de stockage pour les systèmes NetApp clustered Data ONTAP surveillés par Digital Advisor. Les « risques d'objet » peuvent être sélectionnés comme colonne ou mesure dans ces widgets où le stockage ou le nœud de stockage est l'objet de focalisation.



Sécurité des workloads

À propos de la sécurité des charges de travail du stockage

Informations exploitables sur les menaces internes avec le système de stockage Workload Security (anciennement Cloud Secure), vous protégez vos données. Elle assure la visibilité et le contrôle centralisés sur tous les accès aux données de l'entreprise à l'échelle des environnements de cloud hybride, afin de garantir l'atteinte des objectifs de sécurité et de conformité.

Visibilité

Bénéficiez d'une visibilité et d'un contrôle centralisés sur l'accès des utilisateurs aux données stratégiques de l'entreprise stockées sur site ou dans le cloud.

Remplacez les outils et les processus manuels qui n'offrent pas de visibilité opportune et exacte sur l'accès aux données et leur contrôle. La sécurité des charges de travail fonctionne de façon unique sur les systèmes de stockage cloud et sur site pour vous avertir en temps réel des comportements malveillants des utilisateurs.

La protection

Protégez les données de l'entreprise contre les activités abusives ou les usurpations d'identité à l'aide de fonctionnalités avancées de machine learning et de détection des anomalies.

Vous alerte en cas d'accès anormal aux données au moyen du machine learning avancé et de la détection des anomalies du comportement des utilisateurs.

La conformité

Assurez la conformité aux règles de l'entreprise en vérifiant l'accès des utilisateurs aux données critiques stockées dans des infrastructures sur site ou dans le cloud.

Mise en route

Mise en route de la sécurité des charges de travail

Certaines tâches de configuration doivent être effectuées avant de pouvoir utiliser la sécurité de la charge de travail pour surveiller l'activité des utilisateurs.

Le système Workload Security utilise un agent pour collecter les données d'accès des systèmes de stockage et des informations utilisateur à partir des serveurs Directory Services.

Vous devez configurer les éléments suivants avant de pouvoir commencer à collecter les données :

Tâche	Informations associées

Configurer un agent	"Exigences de l'agent" "Ajouter un agent" "**Vidéo** : déploiement de l'agent"
Configurer un connecteur de répertoire utilisateur	"Ajouter un connecteur de répertoire utilisateur" "**Vidéo** : connexion Active Directory"
Configurer des collecteurs de données	Cliquez sur **sécurité de la charge de travail > collecteurs** cliquez sur le collecteur de données que vous souhaitez configurer. Reportez-vous à la section Data Collector Vendor Reference de la documentation. "**Vidéo** : connexion SVM ONTAP"
Créer des comptes d'utilisateurs	"Gérer les comptes d'utilisateurs"
Dépannage	"**Vidéo** : dépannage"

La sécurité des charges de travail peut également s'intégrer à d'autres outils. Par exemple, "voir ce guide" lors de l'intégration avec Splunk.

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

Vous devez pour "Installez un agent"obtenir des informations de vos collecteurs de données. Avant d'installer l'agent, vous devez vous assurer que votre environnement répond aux exigences relatives au système d'exploitation, au processeur, à la mémoire et à l'espace disque.

Composant	Configuration Linux requise
Système d'exploitation	Un ordinateur exécutant une version sous licence de l'un des systèmes d'exploitation suivants : * AlmaLinux 9.4 et 9.5 (64 bits), y compris SELinux * CentOS 9 Stream (64 bits) * Debian 11 (64 bits) et 12 (64 bits), y compris SELinux * OpenSUSE Leap 15.3 (64 bits) à 15.6 (64 bits) * Oracle Linux 8.10 (64 bits) et 9.1 (64 bits) à 9.6 (64 bits), y compris SELinux * Red Hat Enterprise Linux 8.10 (64 bits) et 9.1 (64 bits) à 9.6 (64 bits), y compris SELinux * Rocky 9.4 (64 bits) et 9.5 (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) et 24.04 LTS (64 bits) Cet ordinateur ne doit exécuter aucun autre logiciel de niveau application. Un serveur dédié est recommandé.
Commandes	le dézipper est requis pour l'installation. En outre, la commande « udo su – » est requise pour l'installation, l'exécution de scripts et la désinstallation.
CPU	4 cœurs de processeurs
Mémoire	16 GO DE RAM

Composant	Configuration Linux requise
Espace disque disponible	L'espace disque doit être alloué de la manière suivante : /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 n'ont pas l'autorisation de ce dossier. Reportez-vous à la section pour plus de détails."dépannage"
Le réseau	Connexion Ethernet de 100 Mbit/s à 1 Gbit/s, adresse IP statique, connectivité IP à tous les périphériques et port requis à l'instance de sécurité de la charge de travail (80 ou 443).

Remarque : l'agent Workload Security peut être installé sur la même machine qu'un agent et/ou une unité d'acquisition Data Infrastructure Insights. Toutefois, il est recommandé de les installer sur des machines distinctes. Si ces derniers 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 à la fois sur le système ONTAP et sur l'ordinateur Agent à l'aide de **NTP (Network Time Protocol)** ou **SNTP (simple Network Time Protocol)**.

Règles d'accès au réseau cloud

Pour les environnements de sécurité de la charge de travail **basés aux États-Unis** :

Protocole	Port	Source	Destination	Description
TCP	443	Agent de sécurité des charges de travail	<site_name> .cs01.cloudinsights.netapp.com <site_name> .c01.cloudinsights.netapp.com <site_name> .c02.cloudinsights.netapp.com	Accès aux informations exploitables de l'infrastructure de données
TCP	443	Agent de sécurité des charges 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 des charges de travail	<site_name> .cs01-eu-1.cloudinsights.netapp.com <site_name> .c01-eu-1.cloudinsights.netapp.com <site_name> .c02-eu-1.cloudinsights.netapp.com	Accès aux informations exploitables de l'infrastructure de données
TCP	443	Agent de sécurité des charges de travail	agentlogin.cs01-eu-1.cloudinsights.netapp.com	Accès aux services d'authentification

Pour les environnements de sécurité de la charge de travail **APAC** :

Protocole	Port	Source	Destination	Description
TCP	443	Agent de sécurité des charges de travail	<site_name> .cs01-ap-1.cloudinsights.netapp.com <site_name> .c01-ap-1.cloudinsights.netapp.com <site_name> .c02-ap-1.cloudinsights.netapp.com	Accès aux informations exploitables de l'infrastructure de données
TCP	443	Agent de sécurité des charges de travail	agentlogin.cs01-ap-1.cloudinsights.netapp.com	Accès aux services d'authentification

Règles dans le réseau

Protocole	Port	Source	Destination	Description
TCP	389 (LDAP) 636 (LDAPS/Start-tls)	Agent de sécurité des charges de travail	URL du serveur LDAP	Connectez-vous à LDAP
TCP	443	Agent de sécurité des charges de travail	Adresse IP de gestion du cluster ou du SVM (selon la configuration du collecteur SVM)	Communication de l'API avec ONTAP

Protocole	Port	Source	Destination	Description
TCP	35000 - 55000	Adresses IP des LIF de données des SVM	Agent de sécurité des charges de travail	Communication de 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 que ONTAP lui envoie 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** de ces ports, mais que les ports que vous réservez pour ce port doivent être compris dans cette plage. Il est recommandé de commencer par réserver ~100 ports et d'augmenter si nécessaire.

Protocole	Port	Source	Destination	Description
TCP	35000-55000	IP de gestion de cluster	Agent de sécurité des charges de travail	Communication entre l'adresse IP de gestion du cluster ONTAP et l'agent Workload Security Agent pour les événements EMS. Ces ports doivent être ouverts vers l'agent Workload Security Agent pour qu'ONTAP puisse lui envoyer des événements EMS, y compris tout pare-feu de l'agent Workload Security Agent (le cas échéant). NOTEZ que vous n'avez pas besoin de réserver **tous** de ces ports, mais que les ports que vous réservez pour ce port doivent être compris dans cette plage. Il est recommandé de commencer par réserver ~100 ports et d'augmenter si nécessaire.
SSH	22	Agent de sécurité des charges de travail	Gestion du cluster	Nécessaire pour le blocage des utilisateurs CIFS/SMB.

Dimensionnement du système

Pour plus d'informations sur le dimensionnement, reportez-vous à la "Vérificateur de taux d'événement"documentation.

Installation de l'agent de sécurité de charge de travail

La sécurité des charges de travail (anciennement Cloud Secure) collecte des données d'activité utilisateur en utilisant un ou plusieurs agents. Les agents se connectent aux périphériques de votre locataire et collectent les données qui sont envoyées à la couche SaaS de sécurité de la charge de travail pour analyse. Reportez-vous à la section "Exigences de l'agent" pour configurer une machine virtuelle d'agent.

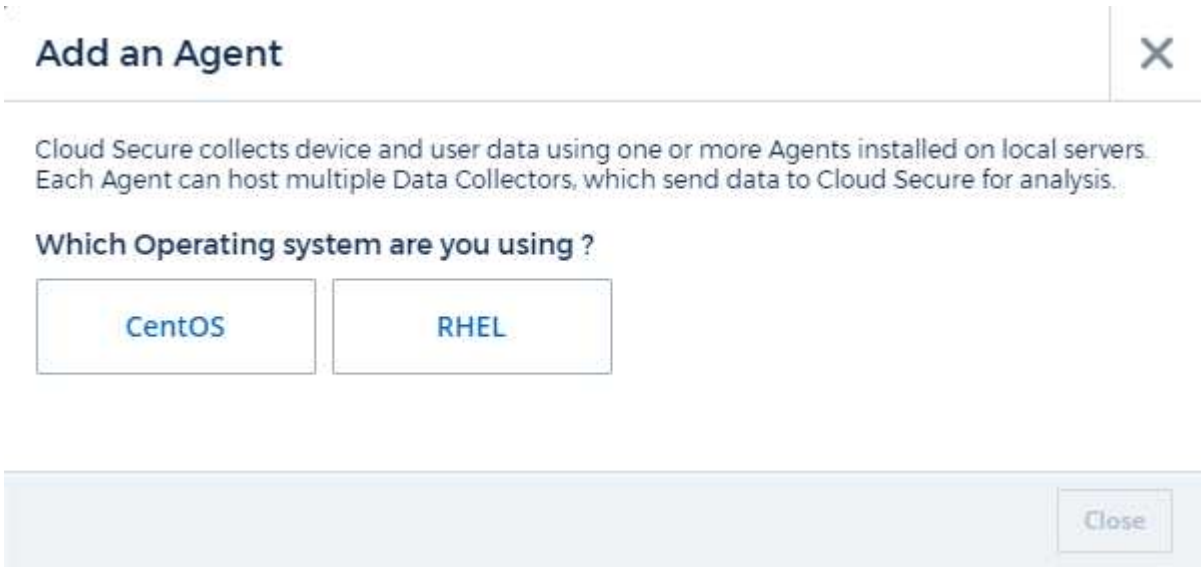
Avant de commencer

- 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 l'ordinateur. Si les paramètres d'autorisation n'autorisent pas la création d'un utilisateur local et nécessitent à la place Active Directory, un utilisateur avec le nom d'utilisateur *cssys* doit être créé dans le serveur Active Directory.
- Vous pouvez lire à propos de la sécurité Data Infrastructure Insights "ici".

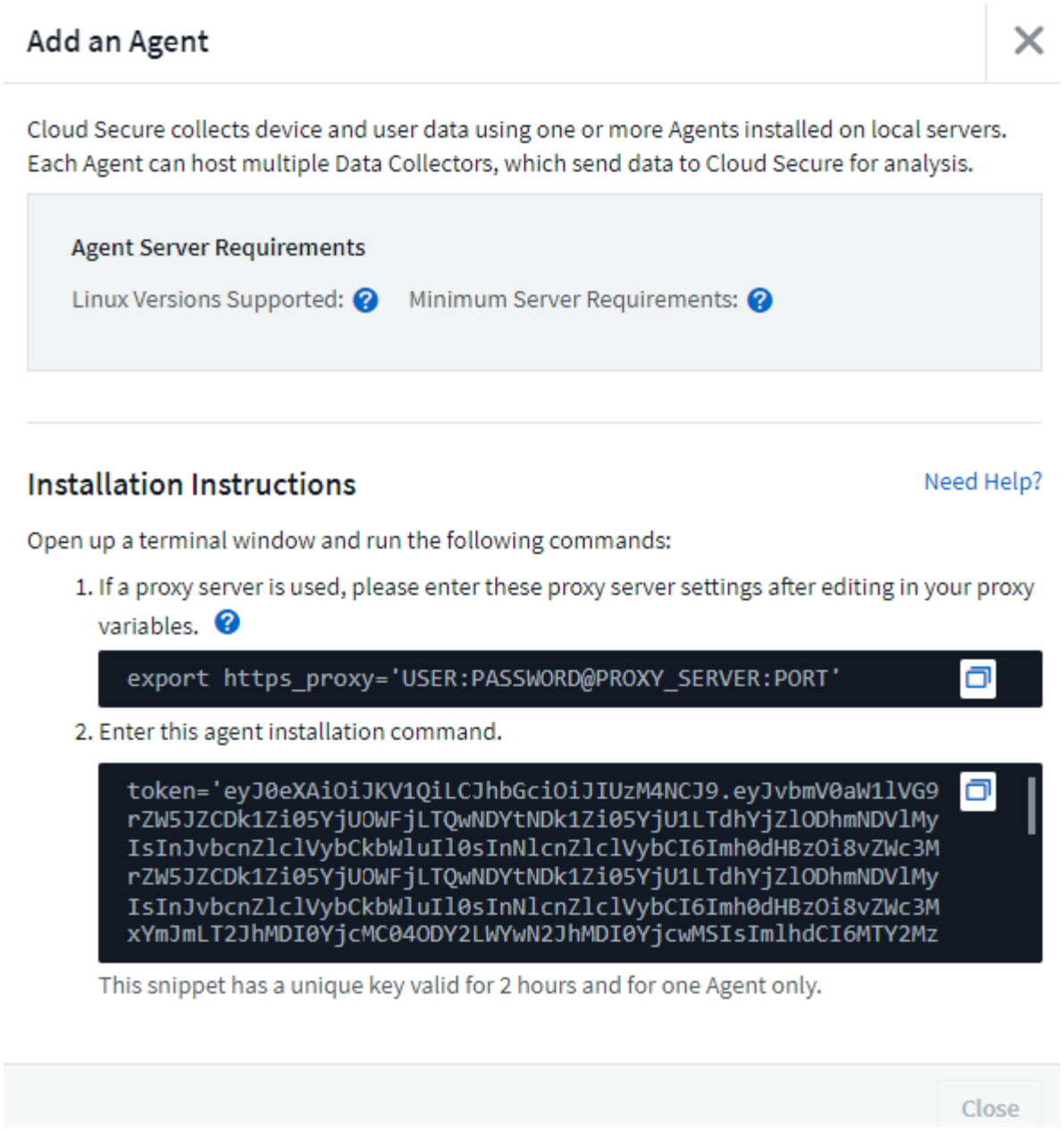
Procédure d'installation de l'agent

1. Connectez-vous en tant qu'administrateur ou responsable de compte à votre environnement de sécurité de la charge de travail.
2. Sélectionnez **collecteurs > agents > +Agent**

   Le système affiche la page Ajouter un agent :



3. Vérifiez que le serveur 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 supportées (i)*.
5. Si votre réseau utilise un serveur proxy, définissez 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. Une fois l'installation terminée, le système affiche le message suivant :



Et pour finir

1. Vous devez configurer un "Collecteur d'annuaire d'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. En cas de problème de sécurité concernant la plage de ports, vous pouvez utiliser une plage de ports inférieure, 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 plate-forme :

CentOS 7.x/RHEL 7.x :

1. `sudo iptables-save | grep 35000`

Sortie d'échantillon :

```
 -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)

Sortie d'échantillon :

```
35000-55000/tcp
```

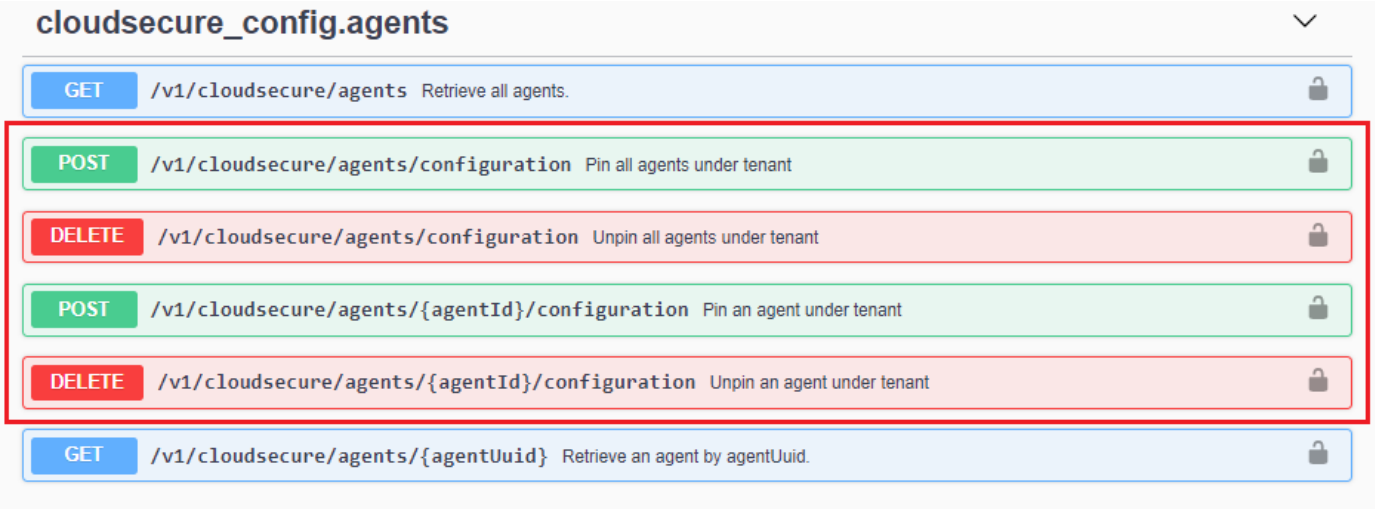
« Épingler » un agent à la version actuelle

Par défaut, Data Infrastructure Insights Workload Security met à jour les agents automatiquement. Certains clients peuvent souhaiter suspendre la mise à jour automatique, ce qui laisse un agent à sa version actuelle jusqu'à ce que l'une des situations suivantes se produise :

- Le client reprend les mises à jour automatiques de l'agent.
- 30 jours se sont écoulés. Notez que les 30 jours commencent le jour de la mise à jour la plus récente de l'agent, et non le jour de la mise en pause de l'agent.

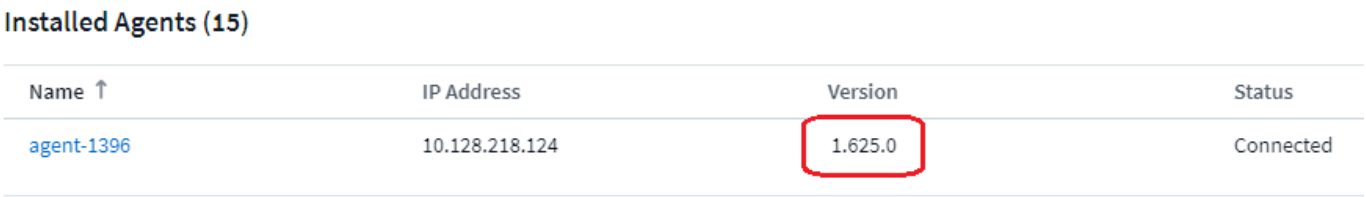
Dans chacun de ces cas, l'agent sera mis à jour lors de la prochaine actualisation de la sécurité de la charge de travail.

Pour interrompre ou reprendre les mises à jour automatiques des agents, utilisez les API *cloudsecure_config.agents* :



Notez qu'il peut prendre jusqu'à cinq minutes pour que l'action de pause ou de reprise prenne effet.

Vous pouvez afficher les versions actuelles de vos agents sur la page **Workload Security > Collectors**, 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 contient aucune information pertinente.	Cette erreur se produit lors du démarrage de l'agent. L'erreur n'est pas consignée 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 la `journalctl -u cloudsecure-agent.service` commande. Cette commande peut être utilisée pour résoudre le problème. est
L'installation de l'agent échoue avec 'cette distribution linux n'est pas prise en charge. Fermeture de l'installation».	Cette erreur apparaît lorsque vous tentez d'installer l'agent sur un système non pris en charge. Voir "Exigences de l'agent".
L'installation de l'agent a échoué avec l'erreur : "-bash : unzip : commande introuvable"	Installez unzip, puis exécutez de nouveau la commande d'installation. Si Yum est installé sur la machine, essayez "yum install unzip" pour installer le logiciel dézip. Ensuite, copiez à nouveau la commande à partir de 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. Toutefois, l'agent s'est arrêté soudainement.	SSH vers l'ordinateur Agent. Vérifiez l'état du service de l'agent via `sudo systemctl status cloudsecure-agent.service`. 1. Vérifiez si les journaux affichent un message « Impossible de démarrer le service démon Workload Security » . 2. Vérifiez si l'utilisateur cssys existe dans la machine Agent ou non. 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 stratégie de surveillance centralisée peut avoir supprimé l'utilisateur cssys. 4. Créez manuellement un utilisateur et un groupe cssys en exécutant les commandes suivantes. `sudo useradd cssys` `sudo groupadd cssys` 5. Redémarrez ensuite le service d'agent en exécutant la commande suivante : `sudo systemctl restart cloudsecure-agent.service` 6. S'il n'est toujours pas en cours d'exécution, vérifiez 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 autres collecteurs.
L'interface utilisateur indique que l'agent est à l'état NON CONNECTÉ.	Étapes de redémarrage de l'agent. 1. SSH vers l'ordinateur Agent. 2. Redémarrez ensuite le service d'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.
La machine virtuelle de l'agent 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 signé 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 procède à l'inspection SSL et remplace les certificats, la sécurité de la charge de travail ne fonctionnera pas.

Problème :	Résolution :
Lors de l'installation de l'agent, l'installation se bloque après le décompression.	La commande chmod 755 -RF est défectueuse. La commande échoue lorsque la commande d'installation de l'agent est exécutée par un utilisateur non-root sudo qui a des fichiers dans le répertoire de travail, appartenant à un autre utilisateur et que 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. Accédez à ce répertoire. 3. Copiez et collez la commande d'installation complète "token=…… ./cloudsecure-agent-install.sh" et appuyez sur entrée. 4. L'installation doit pouvoir continuer.
Si l'agent n'est toujours pas en mesure de se connecter à Saas, veuillez ouvrir un dossier auprès du support NetApp. Fournir le numéro de série Data Infrastructure Insights pour ouvrir un dossier de demande de support et joindre les journaux au dossier comme indiqué.	Pour joindre des journaux au cas : 1. Exécutez le script suivant avec l'autorisation root et partagez le fichier de sortie (cloudsecure-agent-symptomes.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. groupes 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 de l'état de service instantané prise de l'instantané de la structure d'annuaire de l'agent …… . …… . /Opt/netapp/cloudSecure/agent/bin/cloudSecure-agent-symptôme-Collector.sh: Ligne 52: Zip: Commande introuvable ERREUR: Échec de la création /tmp/cloudsecure-agent-symptoms.zip	L'outil de fermeture à glissière n'est pas installé. Installer l'outil zip en exécutant la commande "yum install zip". Puis exécutez à nouveau le 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 du manque d'autorisations. La solution serait de créer l'utilisateur cssys et d'ajouter son répertoire de connexion manuellement à l'aide de la commande suivante : *sudo useradd nom_utilisateur -m -d HOME_DIR* -m :Créez le répertoire de base de l'utilisateur s'il n'existe pas. -D : le nouvel utilisateur est créé en utilisant HOME_DIR comme valeur du 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 n'est pas en cours d'exécution après l'installation. *Systemctl status cloudsecure-agent.service* NetApp 126 26 affiche les éléments suivants : [root@demo ~]# systemctl status cloudsecure-agent.service agent.service 26 03 21 cloudsecure-agent.service – Workload Security Agent Daemon Service loaded: Loaded (/usr/lib/systemd/system/cloudsecure-agent.service; cloudsecure-agent.service: 12 Enabled; vendor preset: Disabled) Active: Activating (auto-restart) (result: Code-exit) depuis Mar 25889-126:126:26:03 21:12 PDT; 2s/basso. Démarrer/08-03 21:2021:25889:12(used). Aug 03 21:12:26 DEMO system[1]: cloudsecure-agent.service failed.	Ceci peut échouer car *cssys* l'utilisateur n'est peut-être pas autorisé à installer. Si /opt/netapp est un montage NFS et si l'utilisateur *cssys* n'a pas accès à ce dossier, l'installation échoue. *Cssys* est un utilisateur local créé par le programme d'installation de Workload Security qui n'a peut-être pas l'autorisation d'accéder au partage monté. Pour ce faire, essayez d'accéder à /opt/netapp/cloudSecure/agent/bin/cloudSecure-agent à l'aide de *cssys* user. S'il renvoie "permission refusée", l'autorisation d'installation n'est pas présente. Au lieu d'un dossier monté, installez-le sur un répertoire local de la machine.
L'agent était 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 modifier la configuration du proxy de l'agent ?	Vous pouvez modifier le fichier agent.properties pour ajouter les détails du proxy. Procédez comme suit : 1. Passez au dossier contenant le fichier de propriétés : cd /opt/netapp/cloudSecure/conf 2. À l'aide de votre éditeur de texte favori, 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 de sécurité de charge de travail, tous les collecteurs de données associés à l'agent doivent être supprimés en premier.

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 autre agent, vous devez créer une sauvegarde des configurations Data Collector 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 de sécurité de la charge de travail.

   Remarque : ignorez cette étape si tous les collecteurs associés sont à l'état ARRÊTÉ.

Procédure de suppression d'un agent :

1. SSH dans le VM agent 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'annuaire d'utilisateurs Active Directory (AD)

La sécurité des charges de travail peut être configurée pour collecter des attributs utilisateur à partir des serveurs Active Directory.

Avant de commencer

- Vous devez être un administrateur Data Infrastructure Insights ou un propriétaire de compte pour effectuer cette tâche.
- Vous devez avoir l'adresse IP du serveur hébergeant le serveur Active Directory.
- Un agent doit être configuré avant de configurer un connecteur de répertoire utilisateur.

Procédure de configuration d'un collecteur d'annuaire d'utilisateurs

1. Dans le menu sécurité de la charge de travail, cliquez sur **Collectors > User Directory Collectors > + User Directory Collector** et sélectionnez **Active Directory**

   Le système affiche l'écran Ajouter un répertoire d'utilisateurs.

Configurez le collecteur d'annuaire d'utilisateurs en entrant les données requises dans les tableaux suivants :

Nom	Description
Nom	Nom unique du répertoire utilisateur. Par exemple *GlobalADCollector*
Agent	Sélectionnez un agent configuré dans la liste
IP/Nom de domaine du serveur	Adresse IP ou nom de domaine complet (FQDN) du serveur hébergeant le répertoire actif

Nom de la forêt	Niveau forestier de la structure du répertoire. Le nom de forêt permet les deux formats suivants : *x. correct.z* ⇒ nom de domaine direct comme 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 les éléments suivants : *Ou=engineering,DC=hq,DC= companyname,DC=com* [to filter by Specific UO Engineering] *CN=username,ou=engineering,DC=companyname, DC=netapp, DC=com* [to get only user with <username> from ou <engineering>] _CN=Acrobat,CN=Users,CN=company=ID=DC=ID=ID=ID=ici=ID=ID=ID=ID=entreprise,DC=ID=ici=ID=s=ID=ID=s=s=s=s=ici=ID_a_a_a_c,c=ID=s=s=noms_a_a_c=noms_c=
Lier DN	L'utilisateur est autorisé à rechercher dans le répertoire. Par exemple : *username@companyname.com* ou *username@domainname.com* en outre, l'autorisation domaine en lecture seule est requise. L'utilisateur doit être membre du groupe de sécurité *contrôleurs de domaine en lecture seule*.
LIER le mot de passe	Mot de passe du serveur d'annuaire (c'est-à-dire mot de passe pour le nom d'utilisateur utilisé dans Bind DN)
Protocole	ldap, ldaps, ldap-start-tls
Ports	Sélectionnez le port

Entrez les attributs requis du serveur d'annuaire suivants si les noms d'attribut par défaut ont été modifiés dans Active Directory. Le plus souvent, ces noms d'attributs sont *non* modifiés dans Active Directory, auquel cas vous pouvez simplement continuer avec le nom d'attribut par défaut.

Attributs	Nom d'attribut dans le serveur d'annuaire
Afficher le nom	nom
SID	id d'objet
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 électronique	e-mail
Numéro de téléphone	téléphone
Rôle	titre
Pays	co
État	état

Service	service
Photo	miniature
Gestionnaire DN	gestionnaire
Groupes	Membre

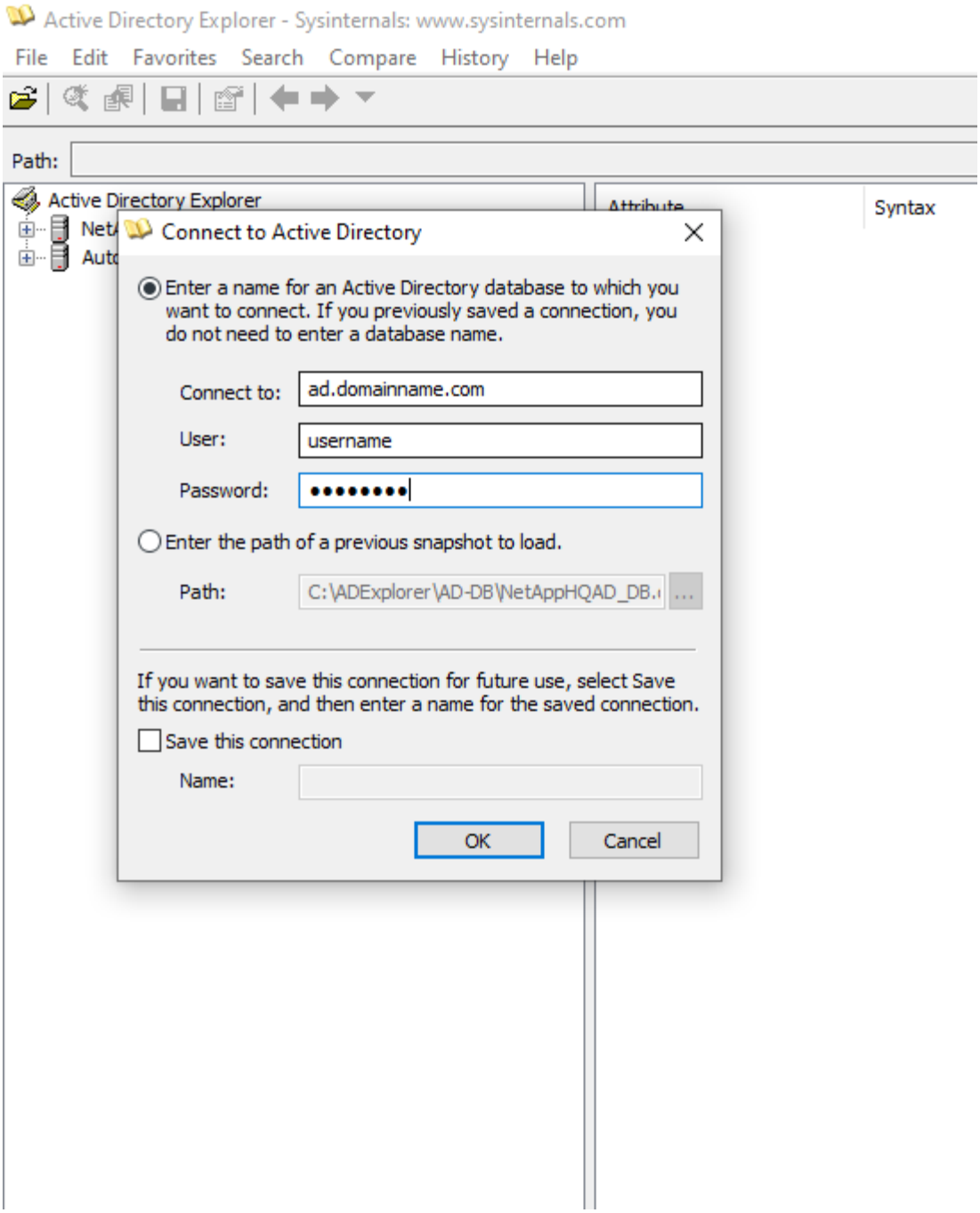
Test de la configuration du collecteur d'annuaire d'utilisateurs

Vous pouvez valider les autorisations utilisateur LDAP et les définitions d'attributs en suivant les procédures suivantes :

- Utilisez la commande suivante pour valider l'autorisation utilisateur LDAP de la sécurité de la charge de travail :

  ```
  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 l'Explorateur AD pour naviguer dans 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 exécuter à nouveau.
  - Installez "Explorateur D'ANNONCES" 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'annuaire utilisateur

Le tableau suivant décrit les problèmes connus et les solutions qui peuvent survenir pendant la configuration du collecteur :

Problème :	Résolution :
L'ajout d'un connecteur de répertoire utilisateur donne l'état "erreur". 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 de répertoire utilisateur donne 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 ne s'affichent pas dans la page profil utilisateur de sécurité de la charge de travail.	Ceci est probablement dû à une incohérence entre les noms des attributs facultatifs ajoutés dans CloudSecure et les noms réels des attributs dans Active Directory. Modifiez et fournissez le ou les noms d'attribut facultatifs appropriés.
Data Collector à l'état d'erreur avec « Impossible de récupérer les utilisateurs LDAP. Raison de l'échec : impossible de se connecter sur le serveur, la connexion est nulle »	Redémarrez le collecteur en cliquant sur le bouton *Restart*.
L'ajout d'un connecteur de répertoire utilisateur donne l'état "erreur".	Assurez-vous que vous avez fourni des valeurs valides pour les champs requis (serveur, nom-forêt, nom-bind, mot-de-passe-bind). Assurez-vous que l'entrée bind-DN est toujours fournie en tant que 'Administrateur@<nom_domaine_forêt>' ou en tant que compte d'utilisateur disposant de privilèges d'administrateur de domaine.
L'ajout d'un connecteur d'annuaire utilisateur a pour résultat l'état « RECOMMANDE ». Affiche l'erreur "Impossible de définir l'état du collecteur,raison de la commande TCP [Connect(localhost:35012,None,List(),About(,seconds),true)] a échoué en raison de java.net.ConnectionException:Connection refusé."	Adresse IP ou FQDN incorrecte fournie pour le serveur AD. Modifiez et fournissez l'adresse IP ou le nom de domaine complet approprié.
L'ajout d'un connecteur de répertoire utilisateur donne l'état "erreur". L'erreur indique "échec de l'établissement de la connexion LDAP".	Adresse IP ou FQDN incorrecte fournie pour le serveur AD. Modifiez et fournissez l'adresse IP ou le nom de domaine complet approprié.
L'ajout d'un connecteur de répertoire utilisateur donne l'état "erreur". L'erreur indique : « Impossible de charger les paramètres. Motif : la configuration de la source de données présente une erreur. Raison spécifique : /Connector/conf/application.conf: 70: ldap.ldap-port a une CHAÎNE de type plutôt QUE DU NOMBRE"	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 données facultatives, les données d'attributs facultatives ne sont pas extraites d'AD.	Ceci est probablement dû à une incohérence entre les attributs facultatifs ajoutés dans CloudSecure et les noms réels des attributs 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 se produira-t-elle ?	La synchronisation AD se produit immédiatement après le redémarrage du collecteur. La récupération des données utilisateur d'environ 300 000 utilisateurs prend environ 15 minutes. De plus, elle est mise à jour automatiquement toutes les 12 heures.
Les données utilisateur sont synchronisées de AD à CloudSecure. Quand les données seront-elles supprimées ?	Les données utilisateur sont conservées pendant 13 mois en cas d'actualisation non prévue. Si le locataire est supprimé, les données seront supprimées.
Le connecteur de répertoire utilisateur indique 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: AcceptSecurityContext error, data 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.	Ceci est probablement dû à un problème de mappage d'attribut avec Active Directory. 1. Modifiez le collecteur Active Directory qui extrait les informations de l'utilisateur depuis Active Directory. 2. Remarque sous attributs facultatifs, un nom de champ "Numéro de téléphone" est mappé à l'attribut Active Directory 'numéro de téléphone'. 4. Veuillez maintenant utiliser l'outil Explorateur Active Directory 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 a effectivement le numéro de téléphone de l'utilisateur. 5. Disons dans Active Directory qu'il a été modifié en 'phonenumber'. 6. Modifiez ensuite le collecteur de répertoire d'utilisateurs CloudSecure. Dans la section des attributs facultatifs, remplacer «téléphone» par «numéro de téléphone». 7. Enregistrez le collecteur Active Directory, le collecteur redémarre et obtient le numéro de téléphone de l'utilisateur et affiche le même numéro dans la page de profil utilisateur.
Si le certificat de cryptage (SSL) est activé sur le serveur Active Directory (AD), le collecteur d'annuaire de l'utilisateur de sécurité de charge de travail ne peut pas se connecter au serveur AD.	Désactivez le cryptage du serveur AD avant de configurer un collecteur d'annuaire utilisateur. Une fois les informations utilisateur extraites, elles seront disponibles pendant 13 mois. Si le serveur AD est déconnecté après avoir récupéré les détails de l'utilisateur, les nouveaux utilisateurs dans AD ne seront pas extraits. Pour récupérer à nouveau, le collecteur d'annuaire de l'utilisateur 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 d'Active Directory de CloudInsights Security. Pour supprimer l'utilisateur, le locataire complet doit être supprimé.

Configuration d'un collecteur de serveur d'annuaire LDAP

Vous configurez la sécurité de la charge de travail pour collecter les attributs utilisateur à partir des serveurs d'annuaire LDAP.

Avant de commencer

- Vous devez être un administrateur Data Infrastructure Insights ou un propriétaire de compte pour effectuer cette tâche.
- Vous devez avoir l'adresse IP du serveur hébergeant le serveur d'annuaire LDAP.
- Un agent doit être configuré avant de configurer un connecteur d'annuaire LDAP.

Procédure de configuration d'un collecteur d'annuaire d'utilisateurs

1. Dans le menu sécurité de la charge de travail, cliquez sur **Collectors > User Directory Collectors > + User Directory Collector** et sélectionnez **LDAP Directory Server**

   Le système affiche l'écran Ajouter un répertoire d'utilisateurs.

Configurez le collecteur d'annuaire d'utilisateurs en entrant les données requises dans les tableaux suivants :

Nom	Description
Nom	Nom unique du répertoire utilisateur. Par exemple *GlobalLDAPCollector*
Agent	Sélectionnez un agent configuré dans la liste
IP/Nom de domaine du serveur	Adresse IP ou nom de domaine complet (FQDN) du serveur hébergeant le serveur d'annuaire LDAP
Base de recherche	La base de recherche du serveur LDAP Search base permet les deux formats suivants : *x. correct.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 les éléments suivants : *Ou=engineering,DC=hq,DC=companyname,DC=com* [to filter by Specific UO Engineering] *CN=username,ou=engineering,DC=companyname, DC=netapp, DC=com* [to get only user with <username> from ou <Engineering>] _CN=Acrobat,CN=Users,CN=company=ID=Users,DC=Company=Company=Company=s==Company=Company=s=Company=Company=Company=s=s=Company=s=s=s=s=s=Company=Company=s=ID=s,DC=ID=s=ID=s=s=s=
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
--jean	--anna
LIER le mot de passe	Mot de passe du serveur d'annuaire (c'est-à-dire mot de passe pour le nom d'utilisateur utilisé dans Bind DN)
Protocole	ldap, ldaps, ldap-start-tls
Ports	Sélectionnez le port

Entrez les attributs requis du serveur d'annuaire suivants si les noms d'attribut par défaut ont été modifiés dans le serveur d'annuaire LDAP. Le plus souvent, ces noms d'attributs sont *NOT* modifiés dans LDAP Directory Server, auquel cas vous pouvez simplement continuer avec le nom d'attribut par défaut.

Attributs	Nom d'attribut dans le serveur d'annuaire
Afficher le nom	nom
NON-IXID	numéro uidnumber
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 électronique	e-mail
Numéro de téléphone	téléphone
Rôle	titre
Pays	co
État	état
Service	numéro du département
Photo	photo
Gestionnaire DN	gestionnaire
Groupes	Membre

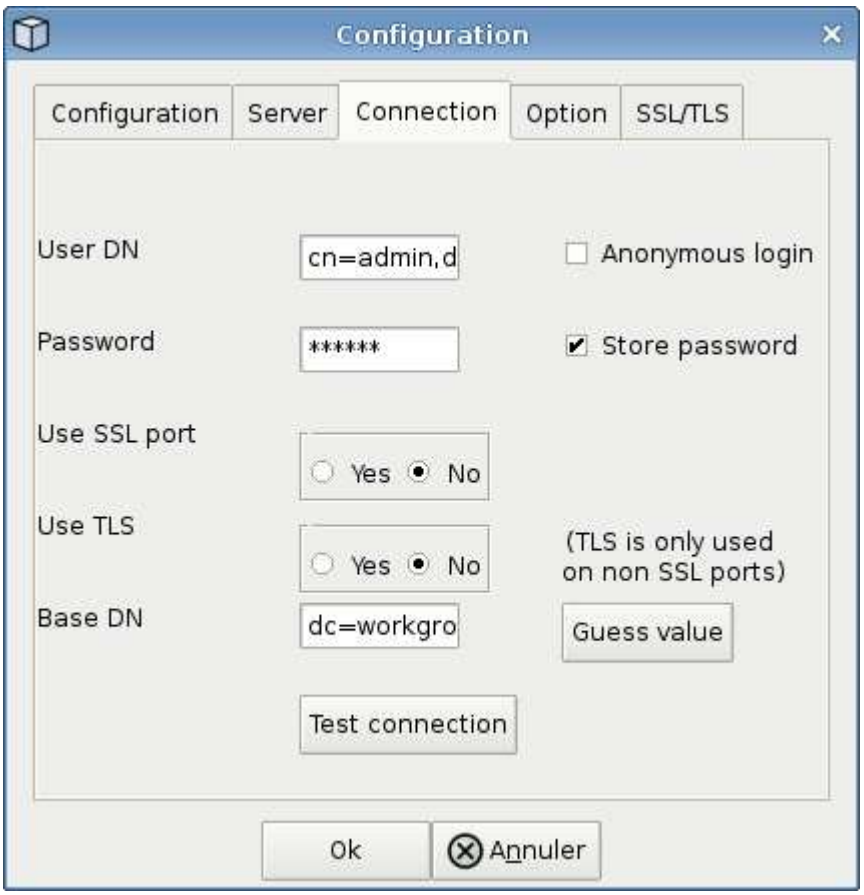
Test de la configuration du collecteur d'annuaire d'utilisateurs

Vous pouvez valider les autorisations utilisateur LDAP et les définitions d'attributs en suivant les procédures suivantes :

- Utilisez la commande suivante pour valider l'autorisation utilisateur LDAP de la sécurité de la charge de travail :

```
 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 l'Explorateur LDAP 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 exécuter à nouveau.
```

- Installez 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 à l'aide du nom d'utilisateur/mot de passe du serveur d'annuaire LDAP.



Dépannage des erreurs de configuration du collecteur d'annuaire LDAP

Le tableau suivant décrit les problèmes connus et les solutions qui peuvent survenir pendant la configuration du collecteur :

Problème :	Résolution :
L’ajout d’un connecteur d’annuaire LDAP entraîne l’état "erreur". Erreur indique : “informations d’identification non valides fournies pour le serveur LDAP”.	Nom unique de liaison ou mot de passe de liaison incorrect ou base de recherche fournie. Modifiez et fournissez les informations correctes.
L’ajout d’un connecteur d’annuaire LDAP entraîne 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 fournie incorrecte. Modifiez et fournissez le nom de forêt correct.
Les attributs facultatifs de l’utilisateur de domaine ne s’affichent pas dans la page profil utilisateur de sécurité de la charge de travail.	Ceci est probablement dû à une incohérence entre les noms des attributs facultatifs ajoutés dans CloudSecure et les noms réels des attributs dans Active Directory. Les champs sont sensibles à la casse. Modifiez et fournissez le ou les noms d’attribut facultatifs appropriés.
Data Collector à l’état d’erreur avec « Impossible de récupérer les utilisateurs LDAP. Raison de l’échec : impossible de se connecter sur le serveur, la connexion est nulle »	Redémarrez le collecteur en cliquant sur le bouton *Restart*.
L’ajout d’un connecteur d’annuaire LDAP entraîne l’état "erreur".	Assurez-vous que vous avez fourni des valeurs valides pour les champs requis (serveur, nom-forêt, nom-bind, mot-de-passe-bind). 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 « recommande ». Affiche l’erreur "Impossible de déterminer l’état de santé du collecteur d’où une nouvelle tentative"	Assurez-vous que l’adresse IP du serveur et la base de recherche sont correctes ///
Lors de l’ajout du répertoire LDAP, l’erreur suivante s’affiche : « Impossible de déterminer l’état du collecteur dans 2 tentatives, essayez de redémarrer le collecteur à nouveau (Code d’erreur : AGENT008) »	Assurez-vous que l’adresse IP du serveur et la base de recherche appropriées sont fournies
L’ajout d’un connecteur d’annuaire LDAP entraîne l’état « recommande ». Affiche l’erreur "Impossible de définir l’état du collecteur,raison de la commande TCP [Connect(localhost:35012,None,List(),About(,seconds),true)] a échoué en raison de java.net.ConnectionException:Connection refusé."	Adresse IP ou FQDN incorrecte fournie pour le serveur AD. Modifiez et fournissez l’adresse IP ou le nom de domaine complet approprié. ////
L’ajout d’un connecteur d’annuaire LDAP entraîne l’état "erreur". L’erreur indique "échec de l’établissement de la connexion LDAP".	Adresse IP ou FQDN incorrecte fournie pour le serveur LDAP. Modifiez et fournissez l’adresse IP ou le nom de domaine complet approprié. 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 entraîne l'état "erreur". L'erreur indique : « Impossible de charger les paramètres. Motif : la configuration de la source de données présente une erreur. Raison spécifique : /Connector/conf/application.conf: 70: ldap.ldap-port a une CHAÎNE de type plutôt QUE DU NOMBRE"	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 données facultatives, les données d'attributs facultatives ne sont pas extraites d'AD.	Ceci est probablement dû à une incohérence entre les attributs facultatifs ajoutés dans CloudSecure et les noms réels des attributs dans Active Directory. Modifiez et fournissez le nom d'attribut obligatoire ou facultatif correct.
Après le redémarrage du collecteur, quand la synchronisation LDAP se produira-t-elle ?	La synchronisation LDAP se produit immédiatement après le redémarrage du collecteur. La récupération des données utilisateur d'environ 300 000 utilisateurs prend environ 15 minutes. De plus, elle est mise à jour automatiquement toutes les 12 heures.
Les données utilisateur sont synchronisées de LDAP à CloudSecure. Quand les données seront-elles supprimées ?	Les données utilisateur sont conservées pendant 13 mois en cas d'actualisation non prévue. Si le locataire est supprimé, les données seront supprimées.
LDAP Directory Connector affiche 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: AcceptSecurityContext error, data 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.	Ceci est probablement dû à un problème de mappage d'attribut avec Active Directory. 1. Modifiez le collecteur Active Directory qui extrait les informations de l'utilisateur depuis Active Directory. 2. Remarque sous attributs facultatifs, un nom de champ "Numéro de téléphone" est mappé à l'attribut Active Directory 'numéro de téléphone'. 4. Veuillez maintenant utiliser l'outil Explorateur Active Directory 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 a effectivement le numéro de téléphone de l'utilisateur. 5. Disons dans l'annuaire LDAP qu'il a été modifié en "phonenumber". 6. Modifiez ensuite le collecteur de répertoire d'utilisateurs CloudSecure. Dans la section des attributs facultatifs, remplacer «téléphone» par «numéro de téléphone». 7. Enregistrez le collecteur Active Directory, le collecteur redémarre et obtient le numéro de téléphone de l'utilisateur et affiche le même numéro dans la page de profil utilisateur.

Problème :	Résolution :
Si le certificat de cryptage (SSL) est activé sur le serveur Active Directory (AD), le collecteur d'annuaire de l'utilisateur de sécurité de charge de travail ne peut pas se connecter au serveur AD.	Désactivez le cryptage du serveur AD avant de configurer un collecteur d'annuaire utilisateur. Une fois les informations utilisateur extraites, elles seront disponibles pendant 13 mois. Si le serveur AD est déconnecté après avoir récupéré les détails de l'utilisateur, les nouveaux utilisateurs dans AD ne seront pas extraits. Pour récupérer à nouveau, le collecteur d'annuaire de l'utilisateur doit être connecté à AD.

Configuration du SVM Data Collector de ONTAP

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 les prérequis, 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 des performances optimales, 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 de ONTAP 9.4 et versions ultérieures
  - ONTAP Select est pris en charge
- Seuls les SVM de type données sont pris en charge. Les SVM avec Infinite volumes ne sont pas pris en charge.
- SVM possède 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 des collecteurs de données.
- Assurez-vous que vous disposez d'un connecteur d'annuaire utilisateur correctement configuré. Dans le cas contraire, les événements affichent des noms d'utilisateur codés et non le nom réel de l'utilisateur (tel qu'il est stocké dans Active Directory) dans la page « activités approfondies ».
- • Le magasin permanent ONTAP est pris en charge à partir de 9.14.1.
- Pour des performances optimales, il est recommandé de configurer le serveur FPolicy sur le même sous-réseau que le système de stockage.
- Vous devez ajouter un SVM à l'aide de l'une des deux méthodes suivantes :
  - En utilisant l'IP du cluster, le nom du SVM et le nom d'utilisateur et mot de passe de Cluster Management. ***c'est la méthode recommandée.***
    - Le nom du SVM doit être exactement comme indiqué dans ONTAP et est sensible à la casse.

- En utilisant SVM Vserver Management IP, Nom d'utilisateur et Mot de passe
- Si vous ne pouvez pas utiliser le nom d'utilisateur et le mot de passe complets de gestion du cluster/SVM, vous pouvez créer un utilisateur personnalisé avec un Privileges inférieur, comme indiqué dans la "Une note sur les autorisations"section ci-dessous. Cet utilisateur personnalisé peut être créé pour l'accès au SVM ou au cluster.
  - o vous pouvez également utiliser un utilisateur AD avec un rôle qui possède au moins les autorisations de csrole, comme indiqué dans la section "Une note sur les autorisations" ci-dessous. Reportez-vous également à la "Documentation de l'ONTAP".

- S'assurer 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 résultat :

```
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.
```

- S'assurer que le SVM dispose d'un serveur CIFS configuré : clustershell:> `vserver cifs show`

  Le système renvoie le nom du Vserver, le nom du serveur CIFS et les champs supplémentaires.

- Définir un mot de passe pour l'utilisateur SVM vsadmin. Si vous utilisez un utilisateur personnalisé ou un utilisateur administrateur du cluster, ignorez cette étape. Clustershell:> `security login password -username vsadmin -vserver svmname`
- Déverouiller l'utilisateur SVM vsadmin pour l'accès externe Si vous utilisez un utilisateur personnalisé ou un utilisateur administrateur du cluster, ignorez cette étape. Clustershell:> `security login unlock -username vsadmin -vserver svmname`
- Assurez-vous que la politique de pare-feu de la LIF de données est définie sur « gmt » (et non « données »). Ignorez cette étape en cas d'utilisation d'une lif de gestion dédiée pour ajouter le SVM. Clustershell:> `network interface modify -lif <SVM_data_LIF_name> -firewall-policy mgmt`
- Lorsqu'un pare-feu est activé, une exception doit être définie pour autoriser le trafic TCP pour le port à l'aide du Data Collector Data ONTAP.

  Voir "Exigences de l'agent" pour plus d'informations sur la configuration. Cela s'applique aux agents et agents installés sur site dans le Cloud.

- Lorsqu'un agent est installé dans une instance EC2 AWS pour contrôler un SVM Cloud ONTAP, l'agent et le stockage doivent se trouver dans le même VPC. S'ils sont dans des VPC distincts, il doit y avoir une route valide entre les VPC.

Test Connectivity for Data Collectors

The test connectivity feature (introduced March 2025) aims to help end users identify the specific causes of failures when setting up data collectors in Data Infrastructure Insights (DII) Workload Security. This allows the users to self-correct issues related to network communication or missing roles.

This feature will help users determine if all network-related checks are in place before setting up a data collector. Additionally, it will inform users about the features they can access based on the ONTAP version, roles, and permissions assigned to them in ONTAP.

Test connectivity is not supported for User Directory collectors

Prerequisites for Connection Testing

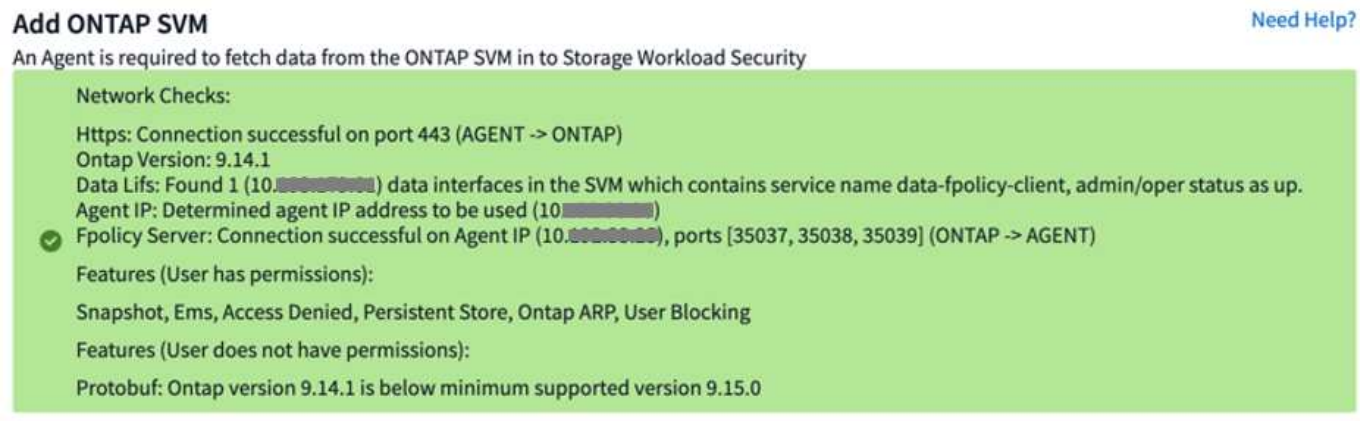
- Cluster level credentials are needed for this feature to work in full.
- Feature access check is not supported in SVM mode.
- Si vous utilisez les informations d'identification d'administration du cluster, aucune nouvelle autorisation n'est nécessaire.
- If you are using a custom user (e.g., *csuser*), provide the mandatory permissions and feature specific permissions for the features you want to use.



Be sure to review the Autorisations section below as well.

Test the Connection

The user can go to the add/edit collector page, enter the cluster level details (in Cluster Mode) or SVM level details (in SVM Mode), and click on the **Test Connection** button. Workload Security will then process the request and display an appropriate success or failure message.



Conditions préalables au blocage de l'accès utilisateur

Gardez à l'esprit les "Blocage de l'accès utilisateur"points suivants :

Des informations d'identification au niveau du cluster sont nécessaires pour que cette fonctionnalité fonctionne.

Si vous utilisez les informations d'identification d'administration du cluster, aucune nouvelle autorisation n'est nécessaire.

Si vous utilisez un utilisateur personnalisé (par exemple, *csuser*) avec des autorisations données à l'utilisateur, suivez les étapes de la section "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 du cluster pour permettre à Workload Security d'accéder au collecteur de données du SVM ONTAP, vous pouvez créer un nouvel utilisateur nommé « csuser » avec les rôles, comme indiqué dans les commandes ci-dessous. Utilisez le nom d'utilisateur "csuser" et le mot de passe pour "csuser" lors de la configuration du collecteur de données de la sécurité de la charge de travail pour utiliser l'adresse IP de gestion du cluster.

Remarque : vous pouvez créer un rôle unique à utiliser pour toutes les autorisations de fonction pour un utilisateur personnalisé. S'il existe un utilisateur existant, supprimez d'abord l'utilisateur et le rôle existants à l'aide des commandes suivantes :

```
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 à l'aide du nom d'utilisateur/mot de passe de l'administrateur de gestion des clusters 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 du cluster pour permettre à Workload Security d'accéder au collecteur de données du SVM ONTAP, vous pouvez créer un nouvel utilisateur nommé « csuser » avec les rôles, comme indiqué 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 de la sécurité Workload pour utiliser l'IP de gestion Vserver.

Remarque : vous pouvez créer un rôle unique à utiliser pour toutes les autorisations de fonction pour un utilisateur personnalisé. S'il existe un utilisateur existant, supprimez d'abord l'utilisateur et le rôle existants à l'aide des commandes suivantes :

```
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 à l'aide du nom d'utilisateur/mot de passe de l'administrateur de gestion des clusters et exécutez les commandes suivantes sur le serveur ONTAP. Pour faciliter la gestion, copiez ces commandes dans un éditeur de texte et remplacez <vservername> par votre nom de Vserver avant d'exécuter les commandes suivantes 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

La sécurité de la charge de travail configure le moteur FPolicy en mode protobuf lorsque cette option est activée dans les paramètres *Advanced Configuration* du collecteur. Le mode Protobuf est pris en charge dans ONTAP version 9.15 et ultérieure.

Vous trouverez plus de détails sur cette fonction dans le "Documentation de l'ONTAP".

Des autorisations spécifiques sont requises pour le protobuf (certaines ou toutes ces autorisations existent peut-être déjà) :

Mode cluster :

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
Mode SVM :
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
```

Autorisations pour la protection anti-ransomware autonome ONTAP et accès ONTAP refusées

Si vous utilisez les informations d'identification d'administration du cluster, aucune nouvelle autorisation n'est nécessaire.

Si vous utilisez un utilisateur personnalisé (par exemple, *csuser*) avec les autorisations accordées à l'utilisateur, suivez les étapes ci-dessous pour donner les autorisations à la sécurité de la charge de travail afin de collecter des informations relatives à ARP à partir de ONTAP.

Pour plus d'informations, consultez à propos de "Intégration avec l'accès ONTAP refusée"

et "Intégration avec la protection ONTAP autonome contre les ransomwares"

Configurer le collecteur de données

Étapes de configuration

1. Connectez-vous en tant qu'administrateur ou responsable 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. Placez le curseur de la souris sur la vignette **NetApp SVM et cliquez sur *+Monitor**.

   Le système affiche la page de configuration du SVM ONTAP. Entrez les données requises pour chaque champ.

Champ	Description
Nom	Nom unique pour le Data Collector
Agent	Sélectionnez un agent configuré dans la liste.
Se connecter via l'IP de gestion pour :	Sélectionnez IP de cluster ou IP de gestion SVM
Adresse IP de gestion cluster / SVM	L'adresse IP du cluster ou du SVM, en fonction de votre choix ci-dessus.
Nom de SVM	Le nom du SVM (ce champ est requis lors de la connexion via IP du cluster)
Nom d'utilisateur	Nom d'utilisateur pour accéder au SVM/Cluster lors de l'ajout via IP du cluster les options sont : 1. Cluster-admin 2. 'csuser' 3. UTILISATEUR AD ayant le rôle similaire à celui de csuser. Lors de l'ajout via SVM IP, les options sont les suivantes : 4. Vsadmin 5. 'csuser' 6. AD-username ayant le rôle similaire à csuser.
Mot de passe	Mot de passe du nom d'utilisateur ci-dessus
Filtrer les partages/volumes	Choisissez d'inclure ou d'exclure des partages/volumes de la collection d'événements
Entrez les noms de partage complets à exclure/inclure	Liste de partages séparés par des virgules à exclure ou inclure (le cas échéant) de la collection d'événements

Entrez les noms complets des volumes à exclure/inclure	Liste de volumes séparés par des virgules à exclure ou inclure (le cas échéant) de la collection d'événements
Surveiller l'accès au dossier	Lorsque cette case est cochée, active les événements pour la surveillance de l'accès aux dossiers. Notez que la création/le renommage et la suppression de dossiers seront contrôlés même si cette option n'est pas sélectionnée. L'activation de cette option augmente le nombre d'événements surveillés.
Définir la taille de la mémoire tampon d'envoi ONTAP	Définit la taille du tampon d'envoi de la Fpolicy ONTAP. Si une version antérieure à ONTAP 9.8p7 est utilisée et qu'un problème de performances est détecté, la taille de la mémoire tampon d'envoi ONTAP peut être modifiée pour améliorer les performances de ONTAP. Contactez le support NetApp si vous ne voyez pas cette option et souhaitez l'explorer.

Une fois que vous avez 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

Les recommandations suivantes sont recommandées pour MetroCluster :

1. Connectez deux collecteurs de données, un sur le SVM source et un autre sur le 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 une stratégie de service avec ONTAP **version 9.9.1 ou ultérieure**, pour vous connecter au Data Source Collector, 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 ONTAP antérieures à 9.9.1, *data-fpolicy-client* n'a pas besoin d'être défini.

Collecteur de données Play-Pause

Si le Data Collector est à l'état *running*, vous pouvez suspendre la collection. Ouvrez le menu « trois points » du collecteur et sélectionnez PAUSE. Lorsque le collecteur est en pause, aucune donnée n'est collectée à partir de ONTAP et aucune donnée n'est envoyée du collecteur vers ONTAP. Cela signifie qu'aucun événement Fpolicy ne circule de ONTAP vers le collecteur de données, et de là vers les informations d'infrastructure de données.

Notez que si de nouveaux volumes, etc. Sont créés sur ONTAP alors que le collecteur est en pause, Workload Security ne recueillera pas les données et ces volumes, etc. Ne sera pas reflété dans les tableaux de bord ou les tableaux.

Un collecteur ne peut pas être mis en pause s'il a des utilisateurs restreints. Restaurez l'accès utilisateur avant de mettre le collecteur en pause.

Gardez à l'esprit les éléments suivants :

- La purge des snapshots ne se produira pas conformément aux paramètres configurés sur un collecteur en pause.
- Les événements EMS (comme ONTAP ARP) ne seront pas traités sur un collecteur en pause. En d'autres termes, si ONTAP identifie une attaque par ransomware, il ne sera pas possible d'acquérir les connaissances nécessaires sur l'infrastructure de données avec Workload Security.
- Les e-mails de notification de santé NE seront PAS envoyés pour un collecteur en pause.
- Les actions manuelles ou automatiques (telles que instantané ou blocage utilisateur) ne sont pas prises en charge sur un collecteur en pause.
- Lors des mises à niveau d'agent ou de collecteur, des redémarrages/redémarrages de machine virtuelle d'agent ou du redémarrage du service d'agent, un collecteur en pause restera à l'état *Pause*.
- Si le collecteur de données est à l'état *Error*, le collecteur ne peut pas être remplacé par l'état *Papersed*. Le bouton Pause est activé uniquement si l'état du collecteur est *running*.
- Si l'agent est déconnecté, le collecteur ne peut pas être remplacé par l'état *Papersed*. Le collecteur passe à l'état *stopped* et le bouton Pause est désactivé.

Stockage persistant

Le stockage persistant est pris en charge avec ONTAP 9.14.1 et les versions ultérieures. Notez que les instructions relatives au nom du volume varient de ONTAP 9.14 à 9.15.

Le stockage persistant peut être activé en cochant la case dans la page de modification/ajout du collecteur. Une fois la case cochée, un champ de texte permettant d'accepter le nom du volume s'affiche. Le nom du volume est un champ obligatoire pour activer le stockage permanent.

- Pour ONTAP 9.14.1, vous devez créer le volume avant d'activer la fonction 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 stockage permanent (certaines ou toutes ces autorisations existent peut-être déjà) :

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 SVM :

```
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, ce qui permet un équilibrage de charge efficace des collecteurs entre les agents.

Prérequis

- L'agent source doit être à l'état *Connected*.
- Le collecteur à migrer doit être à l'état *running*.

Remarque :

- La migration est prise en charge pour les collecteurs de données et de répertoire d'utilisateurs.
- La migration d'un collecteur n'est pas prise en charge pour les locataires gérés manuellement.

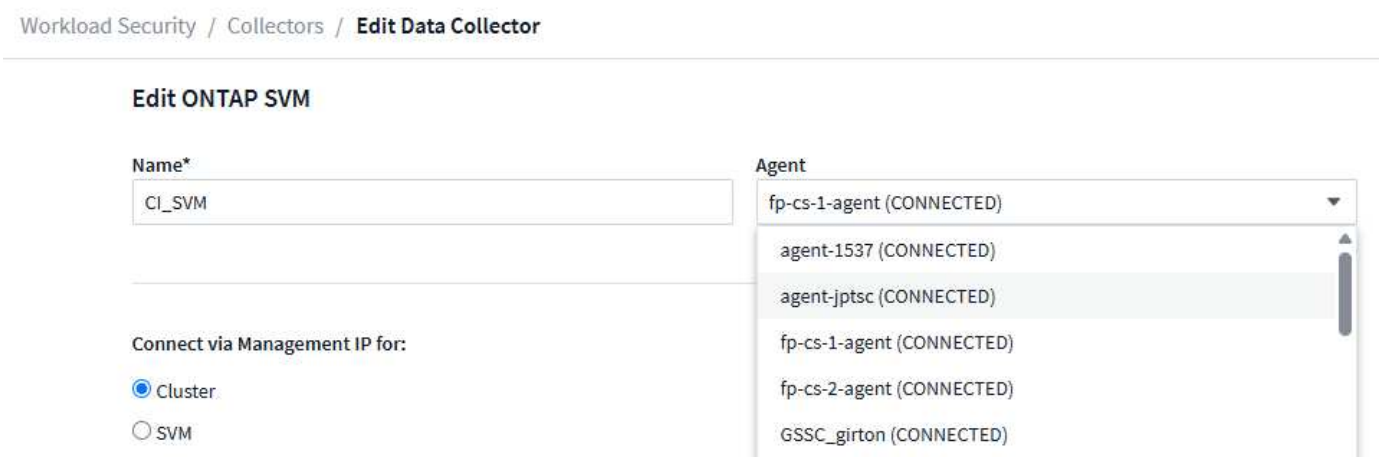
Migration du collecteur

Pour migrer un collecteur, procédez comme suit :

1. Accédez à la page « Modifier le collecteur ».
2. Sélectionnez un agent de destination dans la liste déroulante agent.
3. Cliquez sur le bouton Save Collector.

Workload Security traite la demande. Une fois la migration réussie, l'utilisateur sera redirigé vers la page de liste des collecteurs. En cas d'échec, un message approprié s'affiche sur la page d'édition.

Remarque : toute modification de configuration effectuée précédemment sur la page « Modifier le collecteur » reste appliquée lorsque le collecteur est migré avec succès vers l'agent de destination.



Dépannage

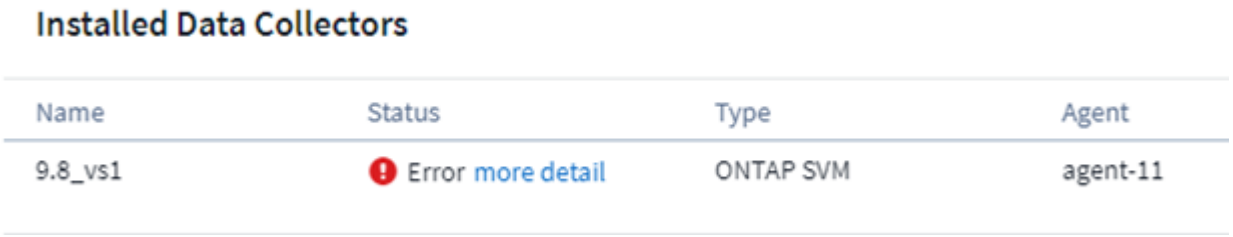
Reportez-vous "Dépannage du collecteur SVM"à la page pour obtenir des conseils de dépannage.

Dépannage du Data Collector SVM ONTAP

La sécurité de la charge de travail utilise des collecteurs de données pour collecter les données d'accès des fichiers et des utilisateurs à partir de terminaux. Vous trouverez ici des conseils pour résoudre les problèmes liés à ce collecteur.

Reportez-vous "Configuration du SVM Collector"à la 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 *Etat* de la page collecteurs de données installés pour plus de détails sur l'erreur.



Les problèmes connus et leurs résolutions sont décrits ci-dessous.

Problème: Data Collector 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. Cause de la panne : serveur fpolicy externe surchargé. »

Essayez ceci: le taux d'événement de ONTAP était beaucoup plus élevé que ce que la boîte agent peut gérer. Par conséquent, la connexion a été interrompue.

Vérifiez le trafic maximal dans CloudSecure lorsque la déconnexion s'est produite. Vous pouvez effectuer cette vérification à partir de la page **CloudSecure > activités approfondies > toutes les activités**.

Si le pic de trafic agrégé est supérieur à ce que l'Agent Box peut traiter, reportez-vous à la page Event Rate Checker sur la taille du déploiement collecteur dans une boîte d'agent.

Si l'agent a été installé dans la zone Agent avant le 4 mars 2021, exécutez les commandes suivantes dans la zone 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.

Problème: le Collector signale un message d'erreur: "Aucune adresse IP locale trouvée sur le connecteur qui peut atteindre les interfaces de données du SVM". **Essayez ceci:** Ceci est probablement dû à un problème de mise en réseau côté ONTAP. Procédez comme suit :

1. S'assurer qu'il n'y a aucun pare-feu sur la lif de données du SVM ou la lif de gestion qui bloquent la connexion de la SVM.
2. Lors de l'ajout d'un SVM via une IP de gestion de cluster, veillez à ce que la lif de données et la lif de gestion du SVM soient pingables depuis la VM Agent. En cas de problème, vérifier la passerelle, le masque de réseau et les routes de la lif.

   Vous pouvez également essayer de vous connecter au cluster via ssh à l'aide de l'IP de gestion de cluster et envoyer une requête ping à l'IP de l'agent. Assurez-vous que l'adresse IP de l'agent peut faire l'objet d'un ping :

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif
   <Lif Name> -show-detail
   ```

   Si vous ne pouvez pas effectuer de ping, assurez-vous que les paramètres réseau dans ONTAP sont corrects, de sorte que l'ordinateur de l'agent puisse effectuer des requêtes ping.
3. Si vous avez essayé de vous connecter via Cluster IP et qu'il ne fonctionne pas, essayez de vous connecter directement via SVM IP. Voir ci-dessus pour les étapes de connexion via SVM IP.
4. Lors de l'ajout du collecteur via les identifiants SVM IP et vsadmin, vérifier si le rôle Data plus Mgmt est activé dans la LIF du SVM. Dans ce cas, le ping vers la LIF du SVM va fonctionner, mais SSH vers la LIF du SVM ne fonctionnera pas. Si oui, créer une LIF SVM Mgmt uniquement et tenter de se connecter via cette LIF de management SVM uniquement.
5. Si cela ne fonctionne toujours pas, créer une nouvelle LIF du SVM et essayer de se connecter via cette LIF. Vérifiez que le masque de sous-réseau est correctement défini.
6. Débogage avancé :
   a. Démarrez une trace de paquet dans ONTAP.
   b. Essayez de connecter un collecteur de données au SVM à partir de l'interface utilisateur CloudSecure.
   c. Attendez que l'erreur s'affiche. Arrêtez la trace de paquet dans ONTAP.
   d. Ouvrez la trace de paquet à partir de ONTAP. Il est disponible à cet endroit

      ```
       https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_trac
      es/
      .. Assurez-vous qu'il y a un SYN de ONTAP dans la zone Agent.
      .. S'il n'y a pas de SYN dans ONTAP, il s'agit d'un problème
      avec le pare-feu dans ONTAP.
      .. Ouvrez le pare-feu dans ONTAP, afin que ONTAP puisse
      connecter le boîtier de l'agent.
      ```
7. S'il ne fonctionne toujours pas, veuillez consulter l'équipe réseau pour vous assurer qu'aucun pare-feu externe ne bloque la connexion entre ONTAP et le boîtier Agent.

8. Si aucune des solutions ci-dessus ne résout le problème, ouvrez un dossier auprès de "Support NetApp" pour obtenir de l'aide.

Problème: message: "Impossible de déterminer le type de ONTAP pour [nom d'hôte: <IP Address>. Raison : erreur de connexion à l'<IP Address> du système de stockage : l'hôte est inaccessible (hôte inaccessible) » **essayez ceci :**

1. Vérifier que l'adresse IP de gestion du SVM ou l'adresse IP de gestion du cluster correcte a été fournie.
2. SSH vers le SVM ou le Cluster auquel vous prévoyez de vous connecter. Une fois connecté, assurez-vous que le SVM ou le nom du cluster est correct.

Problème: message d'erreur: "Le connecteur est en état d'erreur. service.name: Vérification. Cause de la panne : le serveur fpolicy externe est terminé. » **Essayez ceci:**

1. Il est très probable qu'un pare-feu bloque les ports nécessaires sur la machine agent. Vérifier que la plage de ports 35000-55000/tcp est ouverte pour que l'ordinateur agent se connecte à partir du SVM. Assurez-vous également qu'aucun pare-feu n'est activé à partir du blocage de la communication côté ONTAP vers l'agent.
2. Entrez la commande suivante dans la zone Agent et assurez-vous que la plage de ports est ouverte.

   ```
   sudo iptables-save | grep 3500*
   ```

   La sortie de l'échantillon doit ressembler à :

   ```
    -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack
   -ctstate NEW -j ACCEPT
   . Connectez-vous au SVM, entrez les commandes suivantes et vérifiez
   qu'aucun pare-feu n'est défini pour bloquer la communication avec
   ONTAP.
   ```

   ```
   system services firewall show
   system services firewall policy show
   ```

   "Vérifiez les commandes du pare-feu" Du côté ONTAP.

3. Connectez-vous au SVM/Cluster que vous souhaitez surveiller en SSH. Envoyer un ping au boîtier Agent depuis la lif de données du SVM (avec prise en charge des protocoles CIFS, NFS) et vérifier que le ping fonctionne :

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif
   <Lif Name> -show-detail
   ```

   Si vous ne pouvez pas effectuer de ping, assurez-vous que les paramètres réseau dans ONTAP sont corrects, de sorte que l'ordinateur de l'agent puisse effectuer des requêtes ping.

4. Si un seul SVM est ajouté deux fois à un locataire via 2 collecteurs de données, cette erreur s'affiche. 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 affiche l'état « EN COURS d'EXÉCUTION » et commence à recevoir des événements du SVM.

   En réalité, dans un locataire, 1 SVM ne doit être ajouté qu'une seule fois, via 1 Data Collector. 1 SVM ne doit pas être ajouté deux fois via 2 collecteurs de données.

5. Lorsque le même SVM a été ajouté dans deux environnements Workload Security (tenants) différents, le dernier réussira toujours. Le second collecteur configure fpolicy avec sa propre adresse IP et commence le lancement du premier. Ainsi, le collecteur du premier arrête de recevoir des

événements et son service d'audit passe en état d'erreur. Pour éviter cela, configurer 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 Data Source Collector, le service client Data-fpolicy est requis avec le service de données Data-nfs et/ou Data-cifs. De plus, le service data-fpolicy-client doit être associé aux lif de données pour le SVM surveillé.

Problème: aucun événement vu dans la page d'activité. **Essayez ceci:**

1. Vérifiez si le collecteur ONTAP est à l'état « EN COURS D'EXÉCUTION ». Si oui, assurez-vous alors que certains événements cifs sont générés sur les machines virtuelles client cifs en ouvrant certains fichiers.
2. Si aucune activité n'est visible, veuillez vous connecter au SVM et saisir la commande suivante.

   ```
   <SVM>event log show -source fpolicy
   ```

   Assurez-vous qu'il n'y a pas d'erreur liée à fpolicy.

3. Si aucune activité n'est constatée, veuillez vous connecter au SVM. Saisissez la commande suivante :

   ```
   <SVM>fpolicy show
   ```

   Vérifiez si la politique fpolicy nommée avec le préfixe « cloudsecure_ » a été définie et que le statut est « activé ». Si non défini, 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.

Problème: le Data Collector SVM est en état d'erreur et le message d'erreur est "l'agent n'a pas pu se connecter au collecteur" **essayez ceci:**

1. L'agent est probablement surchargé et ne peut pas se connecter aux collecteurs de la source de données.
2. Vérifiez le nombre de collecteurs de sources de données 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 très élevé, installez un autre agent et déplacez certains des collecteurs de sources de données vers le nouvel agent.

Problème: le Data Collector SVM affiche le message d'erreur comme "fpolicy.server.connectError: nœud n'a pas pu établir de connexion avec le serveur FPolicy "12.195.15.146" (motif: "Select Timed out")" **essayez ceci:** le pare-feu est activé dans SVM/Cluster. Le moteur fpolicy ne peut donc pas se connecter au serveur fpolicy. Les interfaces de ligne de commande de ONTAP qui peuvent être utilisées pour obtenir plus d'informations sont les suivantes :

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"Vérifiez les commandes du pare-feu" Du côté ONTAP.

Problème: message d'erreur: "Le connecteur est en 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 : up) trouvée sur le SVM ». **Essayez ceci:** Assurez-vous qu'il existe une interface opérationnelle (ayant le rôle de protocole de données et de données comme CIFS/NFS.

Problème: le collecteur de données passe à l'état d'erreur et passe ensuite 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 sont ajoutés.
2. Les collecteurs de données qui montrent ce type de comportement auront 1 SVM ajouté à ces collecteurs de données. Signification : 2 collecteurs de données ou plus sont connectés à 1 SVM.
3. Assurez-vous que 1 collecteur de données se connecte à 1 seul SVM.
4. Supprimer les autres collecteurs de données qui sont connectés au même SVM.

Problème : le connecteur est en état d'erreur. Nom du service : audit. Motif de l'échec : échec de la configuration (politique sur la SVM svmname. Raison : valeur non valide spécifiée pour l'élément « shares-to-include » dans « fpolicy.policy.scope-modify : « Federal » **essayez ceci :** *les noms de partage doivent être donnés sans guillemets. Modifiez la configuration du SVM DSC de ONTAP pour corriger les noms de partage.

Inclure et exclure des partages n'est pas destiné à une longue liste de noms de partage. Utilisez le filtrage par volume à la place si vous avez un grand nombre de partages à inclure ou exclure.

Problème : il existe dans le cluster des stratégies de gestion de polices qui ne sont pas utilisées. Que faut-il faire avant l'installation de la sécurité des charges de travail ? **Essayez ceci:** il est recommandé de supprimer tous les paramètres fpolicy inutilisés existants, même s'ils sont déconnectés. La sécurité des charges de travail crée fpolicy avec le préfixe « cloudSecure_ ». Toutes les autres configurations fpolicy non utilisées peuvent être supprimées.

Commande CLI pour afficher la liste fpolicy :

```
 fpolicy show
Étapes de suppression des 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>
```

|après l'activation de la sécurité des charges de travail, les performances de ONTAP sont affectées : la latence devient de façon sporadique, les IOPS sont réduites de façon sporadique. |lors de l'utilisation de ONTAP avec la sécurité des charges de travail, des problèmes de latence sont parfois visibles dans ONTAP. Il y a un certain nombre de raisons possibles pour cela, comme indiqué dans les points suivants : "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.

Problème: le collecteur de données est en erreur, affiche ce message d'erreur. "Erreur : le connecteur est en état d'erreur. Nom du service : audit. Motif de l'échec : échec de la configuration de la règle sur le SVM svm_test. Motif : valeur manquante pour le champ zapi : événements. " **Essayez ceci:**

1. Commencez par un nouveau SVM avec uniquement le service NFS configuré.
2. Ajoutez un collecteur de données SVM ONTAP dans la sécurité des charges de travail. CIFS est configuré en tant que protocole autorisé pour la SVM lors de l'ajout du SVM Data Collector de ONTAP dans Workload Security.
3. Attendez que le collecteur de données de la sécurité de la charge de travail affiche une erreur.
4. Étant donné que le serveur CIFS n'est PAS configuré sur le SVM, cette erreur comme indiquée sur la gauche est indiquée par Workload Security.
5. Modifiez le collecteur de données du SVM ONTAP et décochez la case CIFS en tant que protocole autorisé. Enregistrer le collecteur de données. Il démarre alors que seul le protocole NFS est activé.

Problème : Data Collector affiche le message d'erreur : "erreur : échec de la détermination de l'intégrité du collecteur dans les 2 tentatives, essayez de redémarrer le collecteur (Code d'erreur : AGENT008)". **Essayez ceci:**

1. Sur la page collecteurs de données, faites défiler l'écran vers la droite du collecteur de données donnant l'erreur et cliquez sur le menu 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 *Save*. Data Collector redémarre et l'erreur doit être résolue.
2. La machine Agent peut ne pas disposer de suffisamment de ressources CPU ou RAM, c'est pourquoi les DSC sont défaillants. Veuillez vérifier le nombre de collecteurs de données ajoutés à l'agent de la machine. Si elle est supérieure à 20, augmentez la capacité CPU et RAM de l'ordinateur Agent. Une fois l'UC et la RAM augmentées, les DSC sont en cours d'initialisation, puis s'exécutent automatiquement. Consultez le guide de dimensionnement sur "cette page".

Problème: le Data Collector est en erreur lorsque le mode SVM est sélectionné. **Essayer ceci:** lors de la connexion en mode SVM, si l'IP de gestion du cluster est utilisée pour se connecter à la place de l'IP de gestion du SVM, alors la connexion sera erronée. S'assurer que l'IP de SVM correct est utilisé.

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 : la configuration de fpolicy sur le svm test_svm a échoué. Raison : l'utilisateur n'est pas autorisé. » **Essayez ceci:** l'utilisateur manque peut-être les autorisations de REPOS nécessaires pour la fonction accès refusé. Veuillez suivre les instructions de la section "cette page" pour définir les autorisations.

Redémarrez le collecteur une fois les autorisations définies.

Si vous rencontrez toujours des problèmes, accédez aux liens d'assistance mentionnés dans la page **aide > support**.

Configuration de Cloud Volumes ONTAP et d'Amazon FSX pour NetApp ONTAP Collector

La sécurité de la charge de travail utilise des collecteurs de données pour collecter les données d'accès des fichiers et des utilisateurs à partir de terminaux.

Configuration du stockage Cloud Volumes ONTAP

Pour configurer une instance AWS HA à un seul nœud ou pour héberger l'agent Workload Security, reportez-vous à la documentation OnCommand Cloud Volumes ONTAP : https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html

Une fois la configuration terminée, suivre 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 dans tous les fournisseurs de services cloud disponibles, là où il est disponible. Par exemple : Amazon, Azure et Google Cloud.

- ONTAP, Amazon FSX

Configuration de l'ordinateur agent

La machine de l'agent doit être configurée dans les sous-réseaux respectifs des fournisseurs de services cloud. Pour en savoir plus sur l'accès au réseau, consultez le [exigences de l'agent].

Vous trouverez ci-dessous les étapes d'installation d'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 la charge de travail :

Procédez comme suit pour configurer la machine à utiliser en tant qu'agent de sécurité de la charge de travail :

Étapes

1. Connectez-vous à la console AWS, accédez à la page EC2-instances et sélectionnez *Launch instance*.
2. Sélectionnez un ami RHEL ou CentOS avec la version appropriée comme indiqué sur 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 de Cloud ONTAP.
4. Sélectionnez *t2.XLarge* (4 cpu virtuels 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 package YUM :
    a. Installez les packages Linux natifs *wget* et *unzip*.

Installez l'agent de sécurité de la charge de travail

1. Connectez-vous en tant qu'administrateur ou responsable 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 installation de l'agent.
5. Collez la commande installation de l'agent dans l'instance RHEL EC2 à laquelle vous êtes connecté. Ceci installe l'agent Workload Security, à condition que tous les "Conditions préalables de l'agent" soient satisfaits.

Pour des étapes détaillées, veuillez vous reporter au lien suivant : 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	Solution

L’erreur "sécurité de la charge de travail : échec de la détermination du type de ONTAP pour le collecteur de données Amazon FxSN" est indiquée par le Data Collector. Le client ne peut pas ajouter un nouveau collecteur de données Amazon FSxN à la sécurité de la charge de travail. La connexion au cluster FSxN sur le port 443 de l’agent est en cours de temporisation. Les règles requises sont activées pour permettre la communication entre le pare-feu et les groupes de sécurité AWS. Un agent est déjà déployé et se trouve également dans le même compte AWS. Ce même agent est utilisé pour connecter et surveiller les dispositifs NetApp restants (et tous fonctionnent).	Résoudre ce problème en ajoutant le segment réseau LIF fsxadmin à la règle de sécurité de l’agent. Autorisé tous les ports si vous n’êtes pas sûr des ports.

Gestion des utilisateurs

Les comptes utilisateur Workload Security sont gérés via les informations exploitables de l’infrastructure de données.

Data Infrastructure Insights offre quatre niveaux de compte utilisateur : propriétaire de compte, administrateur, utilisateur et invité. Chaque compte se voit attribuer 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 charge de travail suivants :

Rôle	Accès à la sécurité du workload
Administrateur	Peut exécuter toutes les fonctions de sécurité de la charge de travail, y compris celles pour les alertes, les analyses approfondies, les collecteurs de données, les stratégies de réponse automatisées et les API pour la sécurité de la charge de travail. Un administrateur peut également inviter d’autres utilisateurs, mais peut uniquement attribuer des rôles de sécurité de la charge de travail.
Utilisateur	Peut afficher et gérer des alertes et afficher des informations judiciaires. Le rôle de l’utilisateur peut modifier l’état des alertes, ajouter une note, effectuer des instantanés manuellement et limiter l’accès des utilisateurs.
Invité	Peut afficher les alertes et les analyses approfondies. Le rôle invité ne peut pas modifier le statut des alertes, ajouter une note, effectuer des instantanés manuellement ou restreindre l’accès des utilisateurs.

Étapes

1. Connectez-vous à la sécurité des charges de travail
2. Dans le menu, cliquez sur **Admin > gestion des utilisateurs**

   Vous serez transféré à la page gestion des utilisateurs de Data Infrastructure Insights.

3. Sélectionnez le rôle souhaité pour chaque utilisateur.

Lors de l'ajout d'un nouvel utilisateur, il suffit de sélectionner le rôle souhaité (généralement utilisateur ou invité).

Pour plus d'informations sur les comptes et les rôles utilisateur, reportez-vous à la documentation Data Infrastructure Insights"Rôle utilisateur".

Vérificateur de taux d'événements SVM (Guide de dimensionnement des agents)

Le vérificateur de taux d'événement est utilisé pour vérifier le taux d'événement combiné NFS/SMB au sein du SVM avant d'installer un collecteur de données SVM ONTAP, afin de voir le nombre de SVM qu'un ordinateur Agent peut surveiller. Utilisez le vérificateur de taux d'événements comme guide de dimensionnement pour vous aider à planifier votre environnement de sécurité.

Un agent peut prendre en charge jusqu'à 50 collecteurs de données.

Besoins :

- IP de cluster
- Nom d'utilisateur et mot de passe de l'administrateur du cluster

Lors de l'exécution de ce script, aucun SVM Data Collector de ONTAP ne doit s'exécuter pour le SVM pour lequel le taux d'événement est déterminé.

Étapes :

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 l'installation de _sshpass_ 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. Indiquez les valeurs correctes lorsque vous y êtes invité. Voir un exemple ci-dessous.
4. L'exécution du script prend environ 5 minutes.
5. Une fois l'exécution terminée, le script imprime le taux d'évènement à partir du SVM. Vous pouvez vérifier le taux d'événement par SVM dans la sortie de la console :

```
“Svm svm_rate is generating 100 events/sec”.
```

Chaque SVM Data Collector de ONTAP peut être associé à un seul SVM, ce qui signifie que chaque collecteur de données sera en mesure de recevoir le nombre d’événements qu’un seul SVM génère.

Gardez à l’esprit les éléments suivants :

A) utilisez ce tableau comme guide de dimensionnement général. 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 l’ordinateur agent	Nombre de collecteurs de données SVM	Taux d’événement maximal que l’Agent machine peut traiter
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 total de vos événements, ajoutez les événements générés pour tous les SVM pour 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 un tampon de taux d’événement de 30 %.

B + C doit être inférieur À A, sinon la machine Agent ne sera pas en mesure de surveiller.

En d’autres termes, le nombre de collecteurs de données pouvant 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
Reportez-vous
xref:{relative_path}concept_cs_agent_requirements.html["Exigences de
l'agent"]à la page pour connaître les conditions requises et les
conditions requises supplémentaires.
```

Exemple

Disons que nous avons trois SVM générant des taux d’événements de 100, 200 et 300 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_<nom du*

SVM>.log dans le répertoire de travail actuel.

Le script peut donner des résultats erronés dans les cas suivants :

- Des identifiants, IP ou nom de SVM incorrects sont fournis.
- un serveur fpolicy existant avec le même nom, numéro de séquence, etc. Fournit une erreur.
- Le script s'arrête brusquement en cours d'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
```

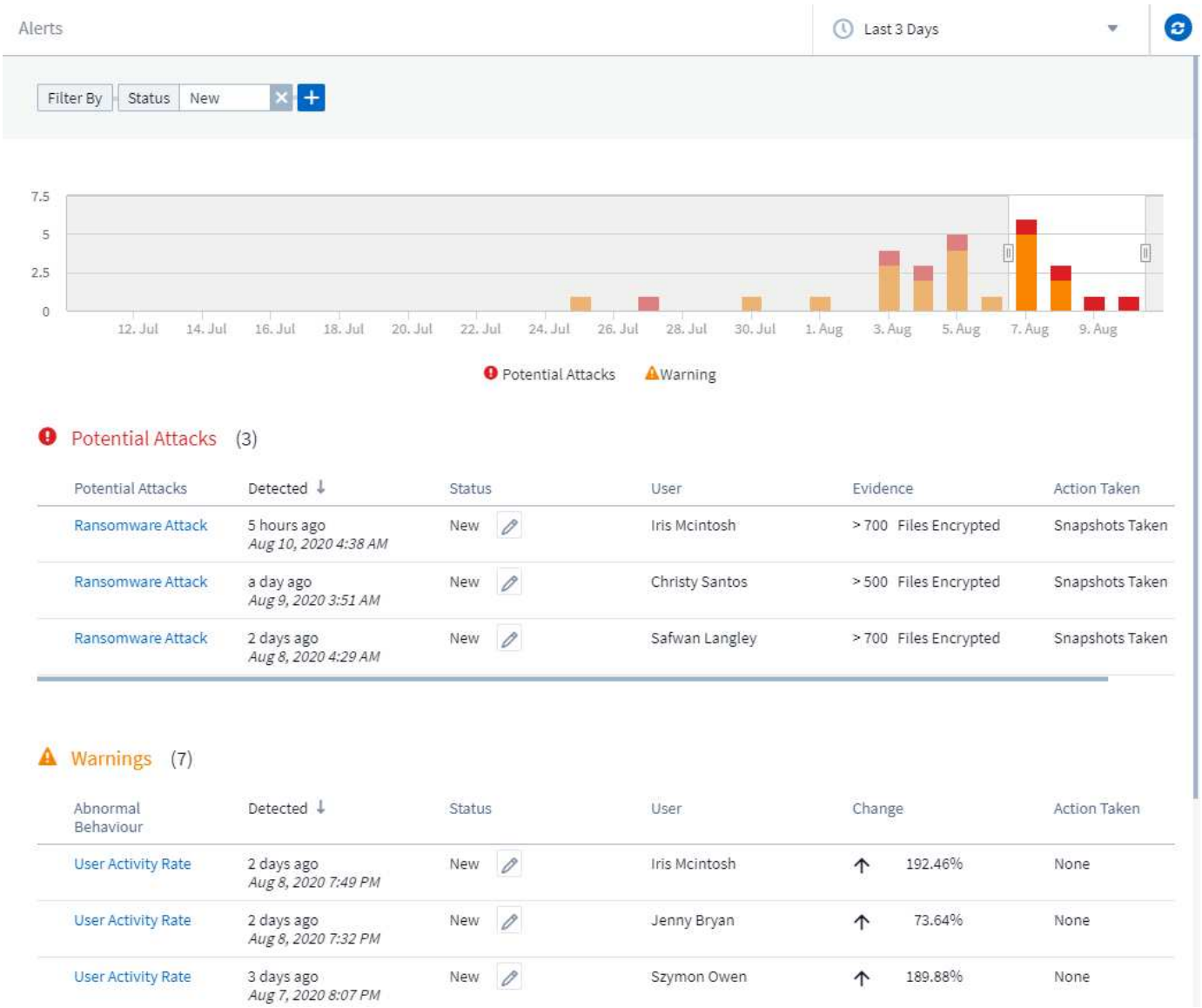
```
[root@ci-cs-data agent]#
```

Dépannage

Question	Réponse
Si je exécute ce script sur un SVM déjà configuré pour Workload Security, utilise-t-il simplement la configuration fpolicy existante sur le SVM ou configure-t-il une configuration temporaire et exécute-t-il le processus ?	L'Event Rate Checker peut s'exécuter correctement, même pour un SVM déjà configuré pour Workload Security. Il ne devrait y avoir aucun impact.
Puis-je augmenter le nombre de SVM sur lesquels le script peut être exécuté ?	Oui. Il vous suffit de modifier le script et de changer le nombre max de SVM de 5 à n'importe quel nombre souhaitable.
Si j'augmente le nombre de SVM, augmente-t-il le temps d'exécution du script ?	Non. Le script s'exécutera pendant 5 minutes maximum, même si le nombre de SVM sera augmenté.
Puis-je augmenter le nombre de SVM sur lesquels le script peut être exécuté ?	Oui. Vous devez modifier le script et changer le nombre max de SVM de 5 à n'importe quel nombre souhaitable.
Si j'augmente le nombre de SVM, augmente-t-il le temps d'exécution du script ?	Non. Le script s'exécutera pendant 5 min maximum, même si le nombre de SVM sera augmenté.
Que se passe-t-il si j'exécute Event Rate Checker avec un agent existant ?	L'exécution d'Event Rate Checker sur un agent existant peut entraîner une augmentation de la latence sur le SVM. Cette augmentation sera temporaire pendant l'exécution du vérificateur de taux d'événement.

Alertes

La page alertes de sécurité de la charge de travail affiche un calendrier des attaques et/ou avertissements récents et vous permet d'afficher les détails de chaque problème.



Alerte

La liste alerte affiche un graphique indiquant le nombre total d'attaques potentielles et/ou d'avertissements qui ont été soulevés dans la plage horaire sélectionnée, suivi d'une liste des attaques et/ou avertissements survenus dans cette plage de temps. Vous pouvez modifier la plage horaire en ajustant les curseurs heure de début et heure de fin dans le graphique.

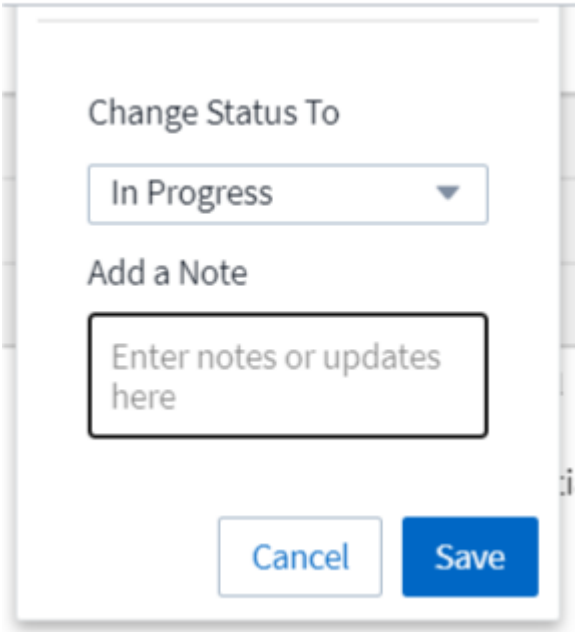
Pour chaque alerte, les éléments suivants s'affichent :

Attaques potentielles:

- Le type *attaque potentielle* (par exemple, ransomware ou sabotage)
- Date et heure de l'attaque potentielle *Detected*

- Le *Status* de l'alerte :
  - **Nouveau** : il s'agit de la valeur par défaut pour les nouvelles alertes.
  - **En cours** : l'alerte est en cours d'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 comme un comportement faux positif ou attendu.

    Un administrateur peut modifier l'état de l'alerte et ajouter une note pour faciliter l'enquête.



- Le *User* dont le comportement a déclenché l'alerte
- *Evidence* de l'attaque (par exemple, un grand nombre de fichiers ont été cryptés)
- La *action entreprise* (par exemple, un instantané a été créé)

Avertissements:

- Le *comportement anormal* qui a déclenché l'avertissement
- La date et l'heure auxquelles le comportement a été *détecté*
- Le *Status* de l'alerte (Nouveau, en cours, etc.)
- Le *User* dont le comportement a déclenché l'alerte
- Une description de *change* (par exemple, une augmentation anormale de l'accès aux fichiers)
- La *action entreprise*

Options de filtre

Vous pouvez filtrer les alertes en procédant comme suit :

- Le *Status* de l'alerte
- Texte spécifique dans la *Note*
- Type de *attaques/Avertissements*

- Le *User* 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 en fonction du type d'attaque ou d'alerte. Par exemple, une page de détails sur les attaques par ransomware peut afficher les informations suivantes :

Section Récapitulatif :

- Type d'attaque (ransomware, sabotage) et ID d'alerte (attribué par la sécurité de la charge de travail)
- Date et heure de détection de l'attaque
- Action entreprise (par exemple, un instantané automatique a été effectué. L'heure de l'instantané s'affiche immédiatement sous la section récapitulative)
- État (Nouveau, en cours, etc.)

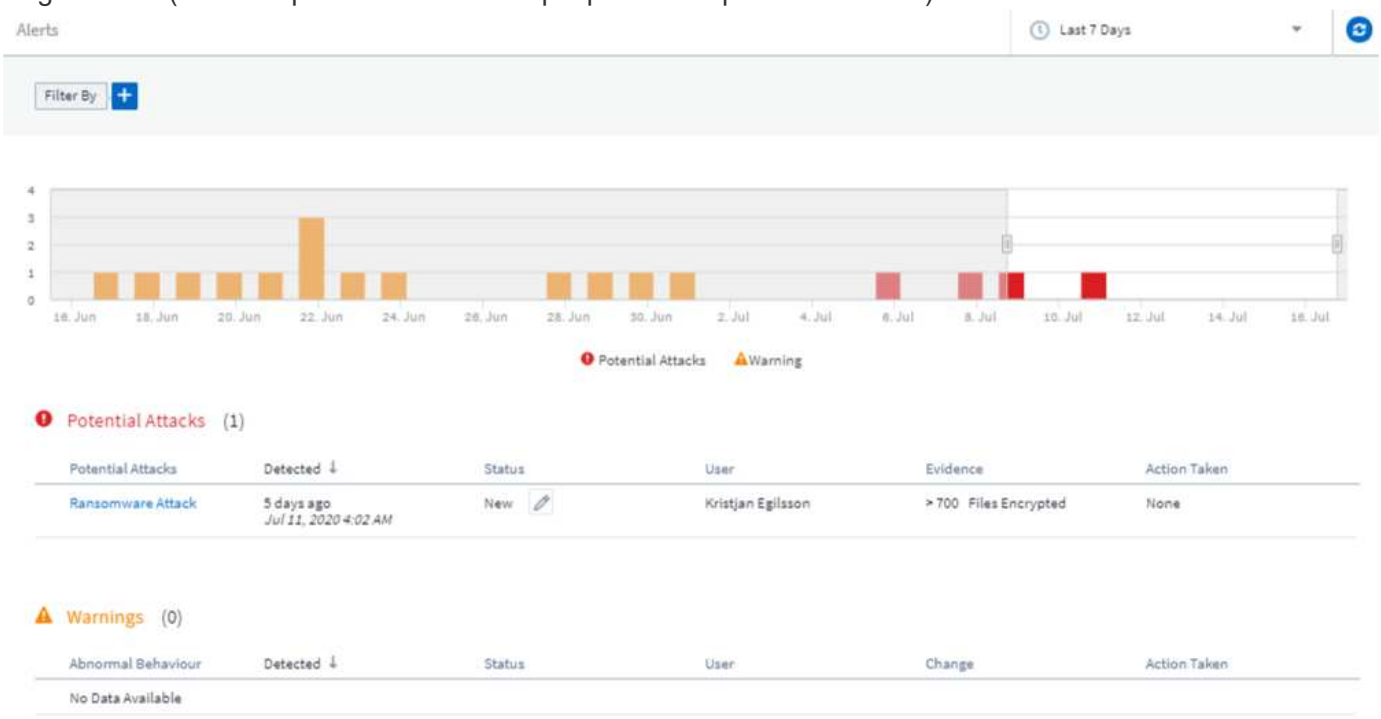
Section des résultats d'attaque :

- Nombre de volumes et de fichiers affectés
- Un résumé de la détection
- Graphique montrant l'activité du fichier pendant l'attaque

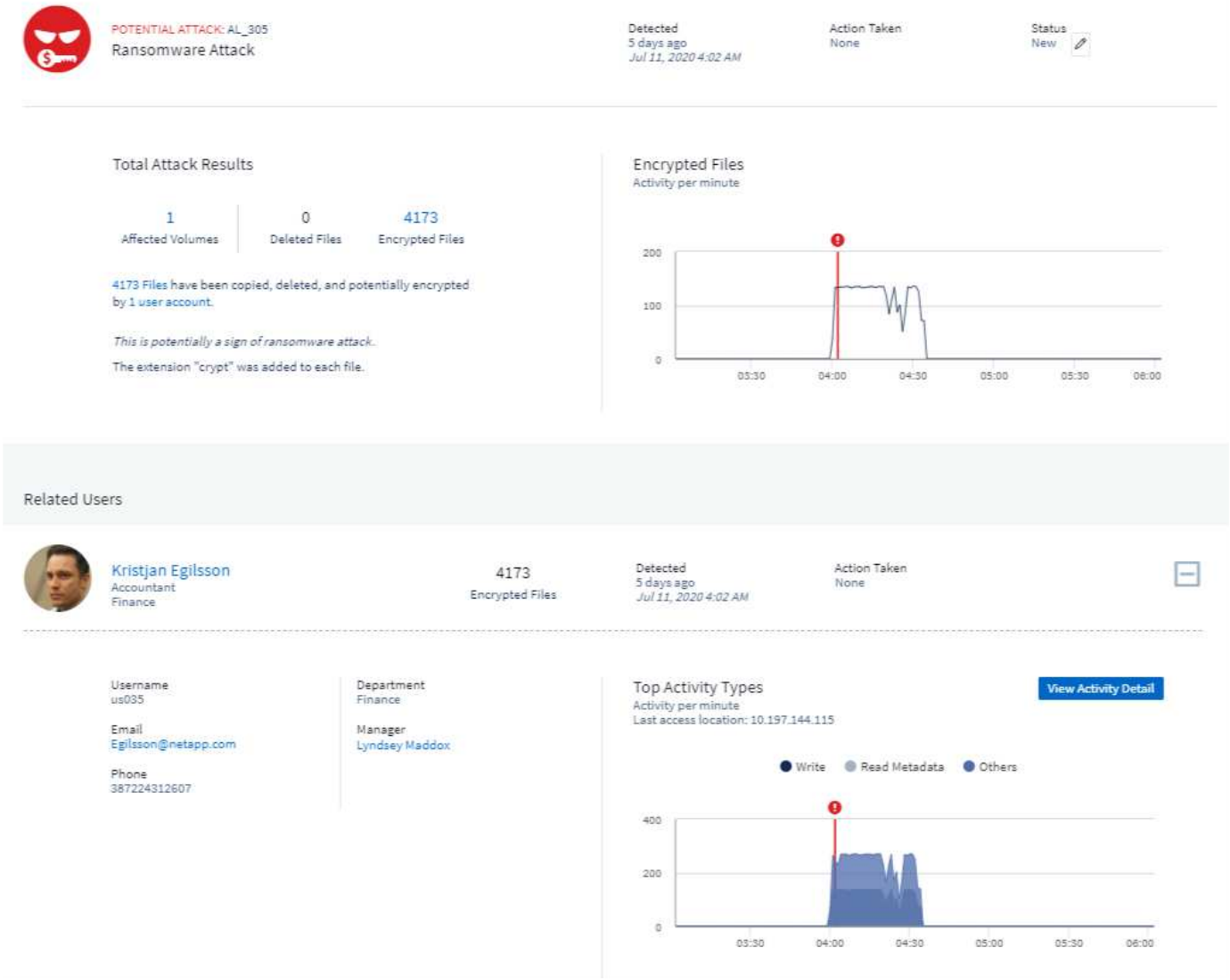
Section utilisateurs associés :

Cette section présente des détails sur l'utilisateur impliqué dans l'attaque potentielle, y compris un graphique de l'activité supérieure pour l'utilisateur.

Page alertes (cet exemple montre une attaque potentielle par ransomware) :



Page de détails (cet exemple montre une attaque potentielle par ransomware) :

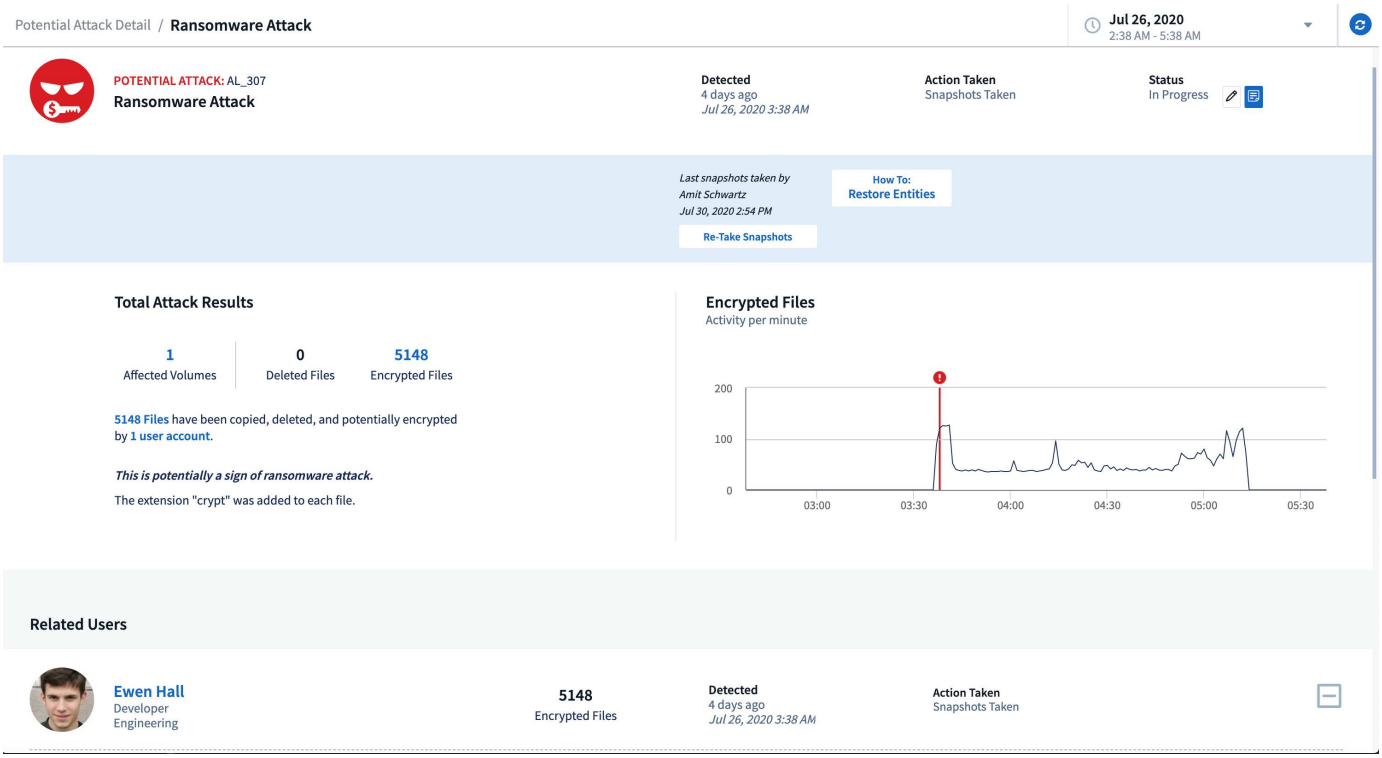


Prendre une action instantané

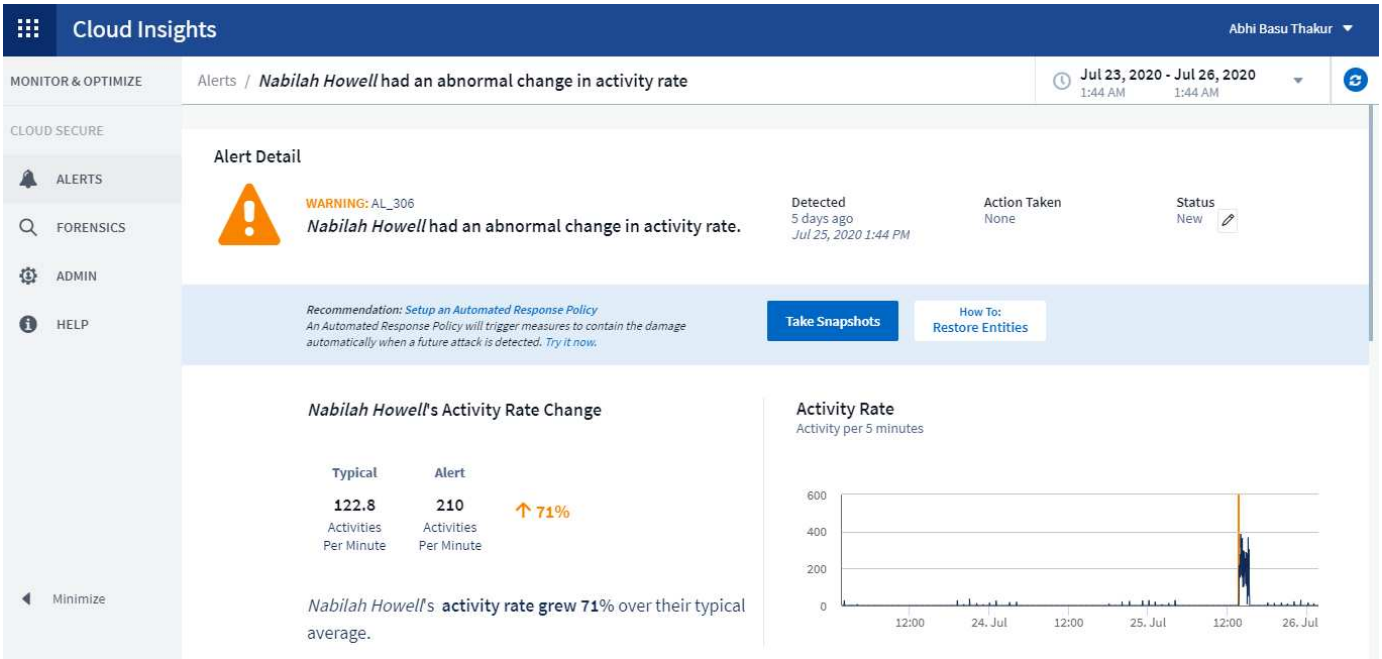
La sécurité des charges de travail protège vos données en prenant automatiquement un instantané en cas de détection d'une activité malveillante, ce qui garantit la sauvegarde sécurisée de vos données.

Vous pouvez définir "stratégies de réponse automatisées" qu'il faut une copie Snapshot lors de la détection d'une attaque par ransomware ou d'une autre activité anormale des utilisateurs. Vous pouvez également prendre un instantané manuellement à partir de la page d'alerte.

Instantané automatique pris :



Instantané manuel :



Notifications d’alerte

Les notifications par e-mail d’alertes sont envoyées à une liste de destinataires d’alertes pour chaque action de l’alerte. Pour configurer les destinataires d’alertes, cliquez sur **Admin > Notifications** et entrez une adresse e-mail pour chaque destinataire.

Stratégie de conservation

Les alertes et avertissements sont conservés pendant 13 mois. Les alertes et avertissements de plus de 13 mois seront supprimés. Si l’environnement de sécurité de la charge de travail est supprimé, toutes les données

associées à l'environnement sont également supprimées.

Dépannage

Problème :	Essayer :
Dans certains cas, ONTAP effectue des copies Snapshot par jour toutes les heures. Les snapshots de sécurité des workloads (WS) l'affecteront-ils ? Le snapshot de la station de travail prend-il la place du snapshot horaire ? Le snapshot horaire par défaut sera-t-il arrêté ?	Les snapshots de sécurité de la charge de travail n'affectent pas les snapshots horaires. Les instantanés WS ne prennent pas l'espace horaire de snapshot et doivent continuer comme précédemment. Le snapshot horaire par défaut n'est 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 échoue et la sécurité de la charge de travail affiche un message d'erreur signalant que le snapshot est plein. L'utilisateur doit définir des règles de snapshot pour supprimer les snapshots les plus anciens, sinon les snapshots ne seront pas effectués. Dans ONTAP 9.3 et versions antérieures, un volume peut contenir jusqu'à 255 copies Snapshot. Dans ONTAP 9.4 et versions ultérieures, un volume peut contenir jusqu'à 1023 copies Snapshot. Voir la documentation ONTAP pour plus d'informations sur "Définition de la règle de suppression Snapshot".
La sécurité de la charge de travail ne peut pas prendre de snapshots du tout.	Assurez-vous que le rôle utilisé pour créer des snapshots a le lien suivant : droits appropriés attribués. Assurez-vous que *csrole* est créé avec les droits d'accès appropriés pour la prise de snapshots : Security login role create -vserver <vservername> -role csrole -cmddirname « volume snapshot » -Access All
Les snapshots échouent pour les alertes plus anciennes sur les SVM qui ont été supprimées de la sécurité des charges de travail, puis rajoutées à nouveau. Pour les nouvelles alertes qui se produisent après l'ajout d'un SVM, des snapshots sont réalisés.	Ce scénario est rare. Si vous rencontrez ce problème, connectez-vous à ONTAP et prenez manuellement les snapshots pour les anciennes alertes.
Dans la page *Alert Details*, le message "Last tentative failed" (dernière tentative échouée) s'affiche sous le bouton *prendre snapshot*. Lorsque vous passez la souris sur l'erreur, "la commande Invoke API a expiré pour le collecteur de données avec ID" s'affiche.	Cela peut se produire lorsqu'un collecteur de données est ajouté à la sécurité de la charge de travail via SVM Management IP, si le LIF du SVM est dans *Disabled* state dans ONTAP. Activez la LIF particulière dans ONTAP et déclenchez *Take snapshot manuellement* à partir de la sécurité des charges de travail. L'action Snapshot va alors réussir.

Médecine légale

Analyse - toute l'activité

La page toutes les activités vous aide à comprendre les actions effectuées sur les entités

de l’environnement de sécurité de la charge de travail.

Examen de toutes les données d’activité

Cliquez sur **Forensics > activité Forensics** et cliquez sur l’onglet **toutes les activités** pour accéder à la page toutes les activités. Cette page présente les activités de votre locataire, en mettant en évidence les informations suivantes :

- Un graphique montrant *Historique des activités* (basé sur la plage de temps 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 de temps agrandie. Lorsque vous effectuez un zoom avant, un bouton s’affiche pour permettre à l’utilisateur d’effectuer un zoom arrière.

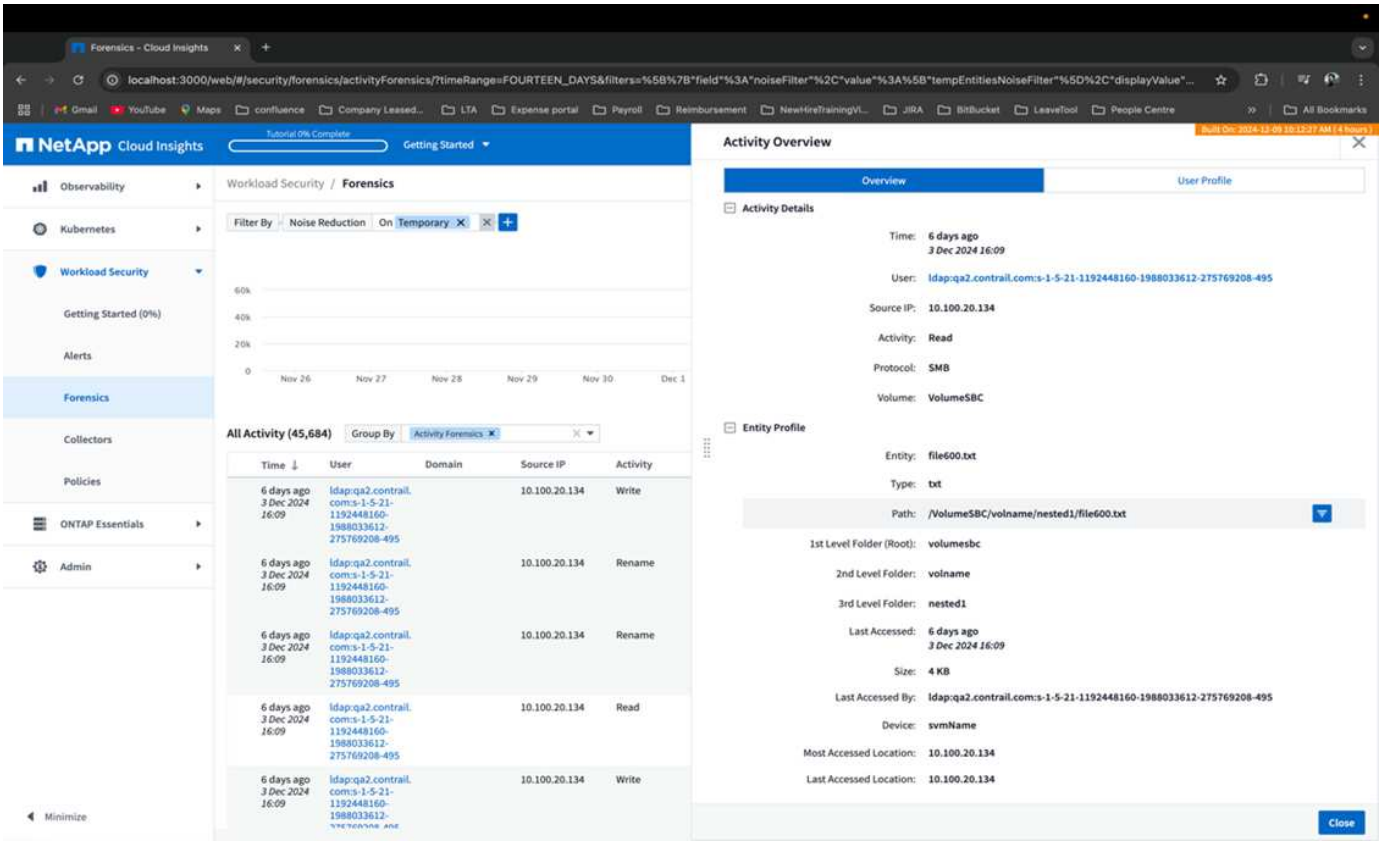
- Une liste des données *All Activity*.
- Un groupe par liste déroulante offrira la possibilité de regrouper l’activité par utilisateurs, type d’entité, etc.
- Un bouton de chemin d’accès commun sera disponible au-dessus du tableau en un clic, et nous pouvons obtenir un panneau coulissant avec les détails du chemin d’accès de l’entité.

Le tableau **All Activity** 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 ».

- Le **temps** où une entité a été consultée, y compris l’année, le mois, le jour et l’heure du dernier accès.
- **Utilisateur** qui a accédé à l’entité avec un lien vers le "Informations utilisateur" sous forme de panneau coulissant.
- L’activité * réalisée par l’utilisateur. Les types pris en charge sont les suivants :
  - **Changer la propriété du groupe** - la propriété du groupe est de fichier ou de dossier est modifiée. Pour plus d’informations sur la propriété du groupe, reportez-vous à la section "ce lien."
  - **Changer propriétaire** - la propriété du fichier ou du dossier est remplacée par un autre utilisateur.
  - **Modifier l’autorisation** - l’autorisation de fichier ou de dossier est modifiée.
  - **Créer** - Créer un fichier ou un dossier.
  - **Supprimer** - Supprimer le fichier ou le dossier. Si un dossier est supprimé, *delete* events sont obtenus pour tous les fichiers de ce dossier et de ces sous-dossiers.
  - **Lire** - le fichier est lu.
  - **Read Metadata** - uniquement sur l’activation de l’option de surveillance de dossier. 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.
  - **Ecrire** - les données sont écrites dans un fichier.
  - **Write Metadata** - les métadonnées de fichier sont écrites, par exemple, les autorisations modifiées.
  - **Autre changement** - tout autre événement qui n’est pas décrit ci-dessus. Tous les événements non mappés sont mappés sur le type d’activité « autre modification ». Applicable aux fichiers et dossiers.
- Le **chemin** est *chemin_entité. Il doit s’agir soit du chemin exact de l’entité (par exemple, "*/home/userX/nested1/nested2/abc.txt_"), SOIT de la partie répertoire du chemin pour la recherche récursive (par exemple, "*/home/userX/nested1/nested2/*"). REMARQUE : les motifs de chemin de regex (par exemple, *imbriqué*) NE sont PAS autorisés ici. Il est également possible de spécifier des filtres de niveau dossier de chemin d’accès individuels, comme indiqué ci-dessous, pour le filtrage de chemin d’accès.

- Le dossier **1er niveau (racine)** est le répertoire racine du chemin d'accès de l'entité en minuscules.
- Le dossier **2e niveau** est le répertoire de deuxième niveau du chemin d'entité en minuscules.
- Le dossier **3e niveau** est le répertoire de troisième niveau du chemin d'entité en minuscules.
- Le dossier **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.-à-d. fichier) (.doc, .docx, .tmp, etc.).
- **Périphérique** où résident les entités.
- Le **Protocole** utilisé pour récupérer des événements.
- Le **chemin d'origine** utilisé pour renommer les événements lorsque le fichier d'origine a été renommé. Par défaut, cette colonne n'est pas visible dans le tableau. Utilisez le sélecteur de colonne pour ajouter cette colonne à la table.
- Le **Volume** où résident les entités. Par défaut, cette colonne n'est pas visible dans le tableau. Utilisez le sélecteur de colonne pour ajouter cette colonne à la table.
- Le **Nom de l'entité** est le dernier composant du chemin d'accès de l'entité ; pour le Type d'entité en tant 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 la présentation 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 *regrouper par* différente—par exemple, Type d'entité—la table *regrouper par* de l'entité s'affiche. Si aucune sélection n'est effectuée, *regrouper par* **tout** s'affiche.

- Le nombre d'activités s'affiche sous forme de lien hypertexte. Si vous sélectionnez cette option, le regroupement sélectionné sera ajouté sous forme de filtre. Le tableau d'activité sera mis à jour en fonction de ce filtre.

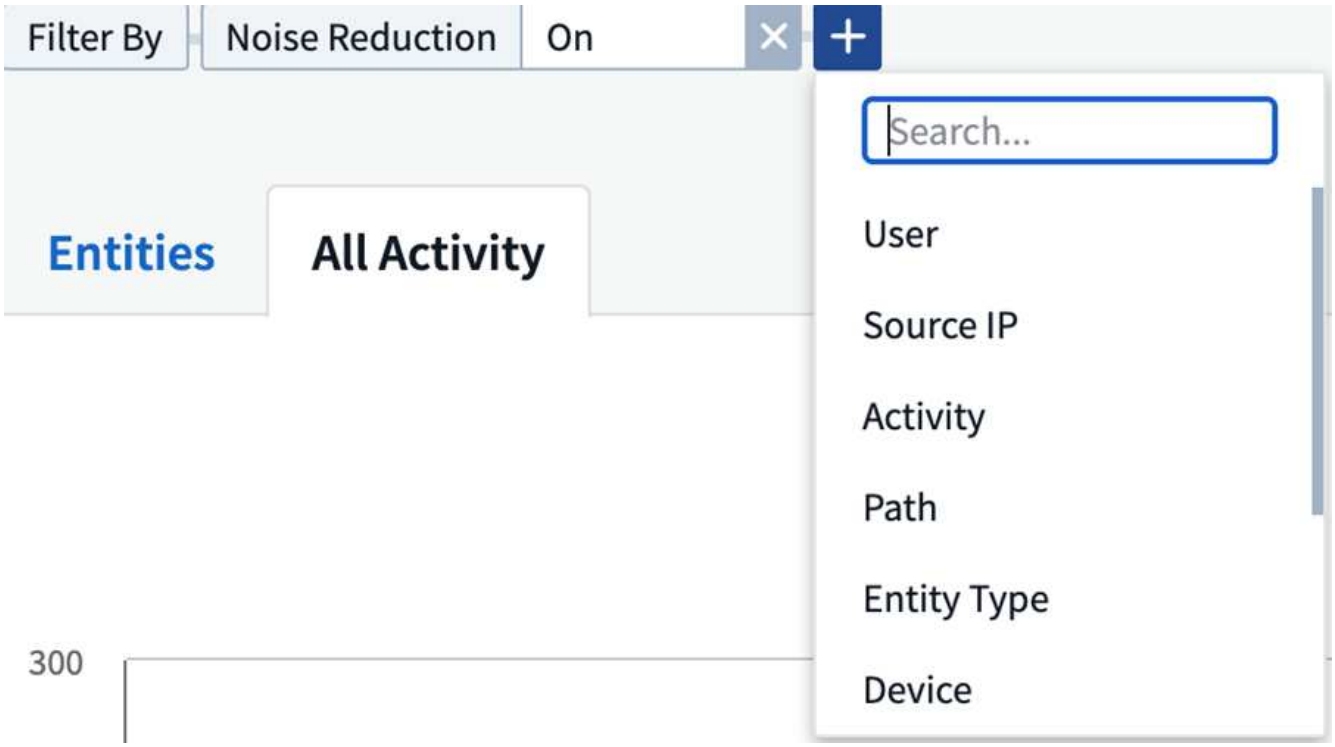
- Notez que si vous modifiez le filtre, modifiez la plage horaire ou actualisez l'écran, vous ne pourrez pas revenir aux résultats filtrés sans avoir à nouveau défini le filtre.
- Veuillez noter que lorsque Nom de l'entité est sélectionné comme filtre, la liste déroulante Grouper par est désactivée. De même, lorsque l'utilisateur est déjà sur l'écran regrouper par, le filtre Nom de l'entité en tant que est désactivé.

Filtrage des données d'historique d'activité Forensic

Vous pouvez utiliser deux méthodes pour filtrer les données.

- Le filtre peut être ajouté à partir du panneau coulissant. La valeur est ajoutée aux filtres appropriés dans la liste *Filter by* supérieure.
- Filtrez les données en entrant dans le champ *Filter by* :

  Sélectionnez le filtre approprié dans le widget « Filtrer par » supérieur 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 Forensic en utilisant les champs suivants :

- Le type **activité**.
- **Protocole** pour extraire des activités spécifiques au protocole.
- **Nom d'utilisateur** de l'utilisateur effectuant l'activité. Vous devez fournir le nom d'utilisateur exact pour filtrer. La recherche avec un nom d'utilisateur partiel ou un nom d'utilisateur partiel précédé ou suffixé de '*' ne fonctionnera pas.
- **Réduction du bruit** pour filtrer les fichiers créés par l'utilisateur au cours des 2 dernières heures. Il est également utilisé pour filtrer les fichiers temporaires (par exemple, les fichiers .tmp) auxquels l'utilisateur a

accès.

- **Domaine** de l'utilisateur exécutant l'activité. Vous devez fournir le **domaine exact** à filtrer. La recherche d'un domaine partiel, ou d'un domaine partiel préfixé ou suffixé avec le 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**, avec l'extension 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 du chemin exact de l'entité (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 motifs de chemin de regex (par exemple, *imbriqué*) NE sont PAS autorisés ici. Pour des résultats plus rapides, il est recommandé d'utiliser des filtres de chemin d'accès au répertoire (chaîne de chemin se terminant par /) jusqu'à 4 répertoires en profondeur. Par exemple, "*/home/userX/nested1/nested2/*". Voir le tableau ci-dessous pour plus de détails.
- Dossier de 1er niveau (racine) - répertoire racine de l'entité chemin d'accès en tant que filtres. Par exemple, si le chemin de l'entité est /home/userX/nested1/nested2/, Home OU Home peut être utilisé.
- Dossier de 2ème niveau - répertoire de 2ème niveau de l'entité filtres de chemin. Par exemple, si le chemin de l'entité est /home/userX/nested1/nested2/, alors userX OU "userX" peut être utilisé.
- Dossier de 3ème niveau – répertoire de 3ème niveau de l'entité filtres de chemin.
- Par exemple, si le chemin de l'entité est /home/userX/nested1/nested2/, alors nested1 OU « nested1 » peut être utilisé.
- Dossier de 4e niveau - répertoire répertoire de 4e niveau de l'entité filtres de chemin. Par exemple, si le chemin de l'entité est /home/userX/nested1/nested2/, alors nested2 OU "nested2" peut être utilisé.
- **Utilisateur** exécutant l'activité - il est préférable de spécifier l'utilisateur exact entre guillemets. Par exemple, *« Administrateur »*.
- **Périphérique** (SVM) où résident les entités
- **Volume** où résident les entités
- Le **chemin d'origine** utilisé pour renommer les événements lorsque le fichier d'origine a été renommé.
- **Source IP** à partir de laquelle l'entité a été accédée.
  - Vous pouvez utiliser des 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 guillemets doubles tels que "10.1.1.", "10.1..*", etc. Ne fonctionneront pas.
- **Nom de l'entité** - le nom de fichier du chemin de l'entité en tant que filtres. Par exemple, si le chemin d'accès 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 de fichier exact 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 des plages de temps plus courtes (jusqu'à 3 jours).

Les champs précédents sont soumis aux éléments suivants lors du filtrage :

- La valeur exacte doit se trouver dans les guillemets : exemple : « searchtext »
- Les chaînes de caractères génériques ne doivent pas contenir de guillemets : exemple : searchtext, *searchtext*, filtre les chaînes contenant 'searchtext'.
- Chaîne avec un préfixe, par exemple : searchtext* , recherche toutes les chaînes commençant par

'searchtext'.

Veuillez noter que tous les champs de filtre sont des recherches sensibles à la casse. Par exemple : si le filtre appliqué est Type d'entité avec la valeur 'texte', il renvoie les résultats avec Type d'entité comme 'texte', 'texte de référence', 'texte de référence', 'EARCHTEXT'

Exemples de filtres d'analyse des événements :

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 le répertoire donné	Rapides	Les recherches de répertoire jusqu'à 4 répertoires seront rapides.
Chemin = "/home/userX/nested1/"	Recherche récursive de tous les fichiers et dossiers sous le répertoire donné	Rapides	Les recherches de répertoire jusqu'à 4 répertoires seront rapides.
Chemin = "/home/userX/nested1/test"	Correspondance exacte où la valeur du chemin correspond à /home/userX/nested1/test	Plus lent	La recherche exacte sera plus lente que les recherches dans l'annuaire.
Chemin = "/home/userX/nested1/nested2/nested3/"	Recherche récursive de tous les fichiers et dossiers sous le répertoire donné	Plus lent	La recherche dans plus de 4 répertoires est plus lente.
Tout autre filtre sans chemin d'accès. Il est recommandé de placer les filtres utilisateur et Type d'entité entre guillemets, par exemple, utilisateur=« Administrateur » Type d'entité=« txt »		Rapides	
Nom de l'entité = « test.log »	Correspondance exacte où le nom du fichier est test.log	Rapides	Car il s'agit de la correspondance exacte
Nom de l'entité = *test.log	Noms de fichier se terminant par test.log	Lentes	En raison de caractères génériques, il peut être lent.
Nom de l'entité = test*.log	Les noms de fichiers commençant par test et se terminant par .log	Lentes	En raison de caractères génériques, il peut être lent.
Nom de l'entité = test.lo	Les noms de fichiers commençant par test.lo par exemple : ils correspondent à test.log, test.log.1, test.log1	Plus lent	En raison du caractère générique à la fin, il peut être lent.

Expression de filtre appliquée par l'utilisateur	Résultat attendu	Évaluation des performances	Commentaire
Nom de l'entité = test	Noms de fichiers commençant par test	Plus lente	En raison du caractère générique à la fin et d'une valeur générique plus utilisée, il peut être plus lent.

REMARQUE :

1. Le nombre d'activités affiché à côté de l'icône toutes les activités est arrondi à 30 minutes lorsque la plage de temps sélectionnée s'étend sur plus de 3 jours. Par exemple, une plage de temps de *1er sept 10:15 à 7 sept 10:15* affichera le nombre d'activités du 1er sept 10:00 au 7 sept 10:30.
2. De même, les mesures de comptage affichées dans le graphique Historique des activités sont arrondies à 30 minutes lorsque la plage horaire sélectionnée s'étend sur plus de 3 jours.

Tri des données d'historique d'activité Forensic

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, la table est triée par ordre décroissant *time*, ce qui signifie que les dernières données seront affichées en premier. Le tri est désactivé pour les champs *Device* et *Protocol*.

Guide de l'utilisateur pour les exportations asynchrones

Présentation

La fonction d'exportation asynchrone de Storage Workload Security est conçue pour gérer les exportations de données volumineuses.

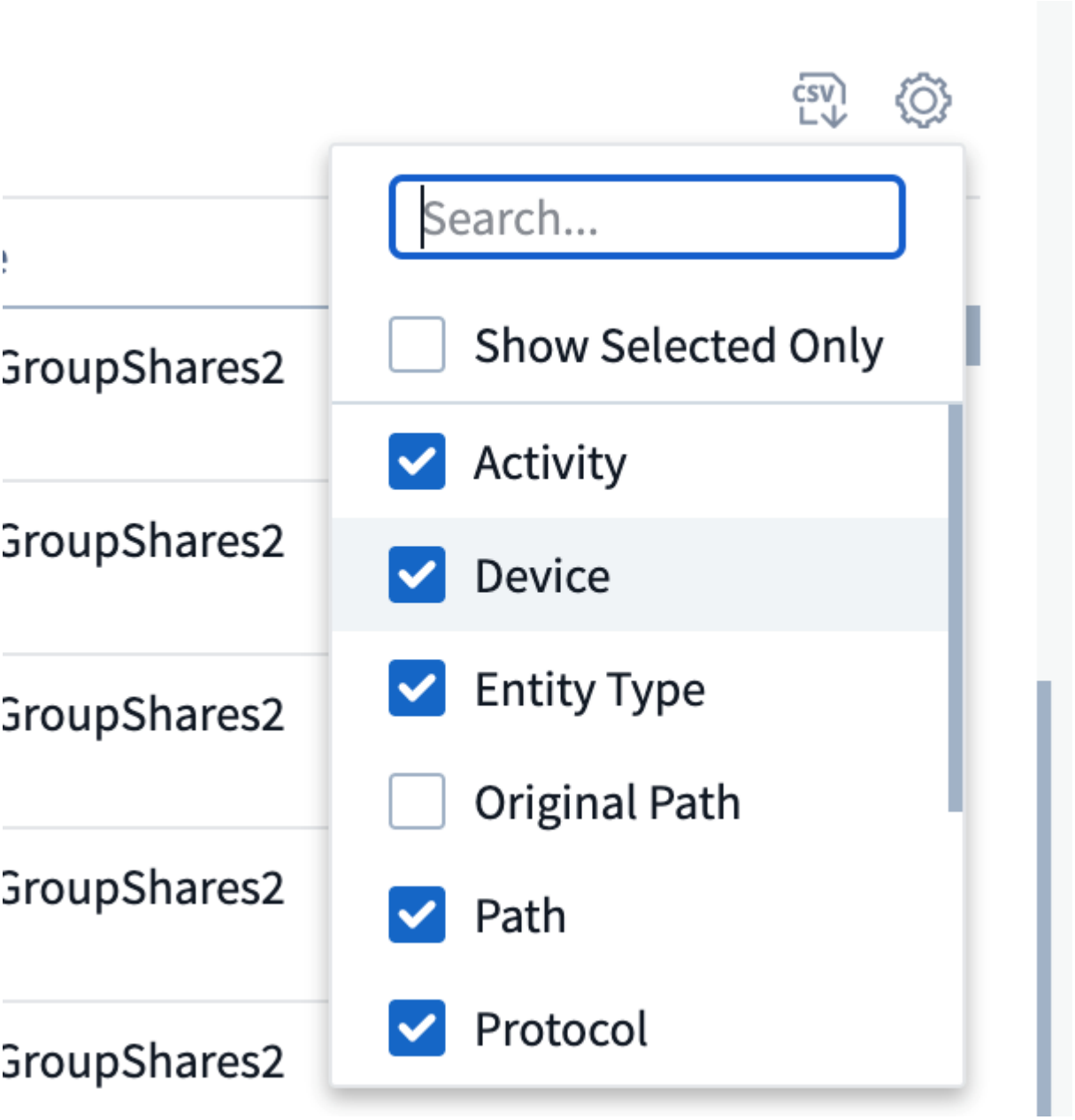
Guide étape par étape : exportation de données avec des exportations asynchrones

1. **Lancer l'exportation** : sélectionnez la durée et les filtres souhaités pour l'exportation et cliquez sur le bouton Exporter.
2. **Attendre la fin de l'exportation**: Le temps de traitement peut aller de quelques minutes à quelques heures. Vous devrez peut-être actualiser la page d'analyse plusieurs fois. Une fois le travail d'exportation terminé, le bouton « Télécharger le dernier fichier CSV d'exportation » est 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 reste activé jusqu'à ce qu'une autre exportation asynchrone soit lancée.
4. **Limitations** :
    - Le nombre de téléchargements asynchrones est actuellement limité à 1 par utilisateur pour chaque table d'analyse des activités et des activités et à 3 par locataire.
    - Les données exportées sont limitées à un maximum de 1 million d'enregistrements pour le tableau des activités, tandis que pour le groupe par, la limite est de 50 millions d'enregistrements.

Un exemple de script permettant d'extraire des données d'analyse via l'API est présent sur */opt/NetApp/cloudsecure/agent/export-script/* sur l'agent. Consultez le fichier readme à cet emplacement pour plus de détails sur le script.

Sélection de colonne pour toutes les activités

Le tableau *all Activity* affiche les colonnes sélectionnées par défaut. Pour ajouter, supprimer ou modifier les colonnes, cliquez sur l'icône engrenage située à droite du tableau et sélectionnez-la dans la liste des colonnes disponibles.



Conservation de l'historique des activités

L'historique des activités est conservé pendant 13 mois pour les environnements de sécurité active de la charge de travail.

Applicabilité des filtres dans la page Forensics

Filtre	Ce qu'il fait	Exemple	Applicable à ces filtres	Ne s'applique pas à ces filtres	Résultat
* (Astérisque)	permet de rechercher tout	Auto*03172022 si le texte de recherche contient un tiret ou un trait de soulignement, donner une expression entre parenthèses, par exemple (svm*) pour la recherche de svm-123	Utilisateur, Type d'entité, périphérique, Volume, chemin d'origine, dossier 1stLevel, dossier 2ndLevel, dossier 3rdLevel, dossier 4thLevel, Nom de l'entité, adresse IP source		Renvoie toutes les ressources commençant par « Auto » et se terminant par « 03172022 »
? (point d'interrogation)	permet de rechercher un nombre spécifique de caractères	AutoSabotageUser1_03172022 ?	Utilisateur, Type d'entité, périphérique, Volume, dossier 1stLevel, dossier 2ndLevel, dossier 3rdLevel, dossier 4thLevel, Nom de l'entité, adresse IP source		Renvoie AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022B, AutoSabotageUser1_031720225, etc
OU	vous permet de spécifier plusieurs entités	AutoSalotageUser1_03172022 OU AutoRansomUser4_03162022	Utilisateur, domaine, Type d'entité, chemin d'origine, Nom de l'entité, adresse IP source		Renvoie AutoSalotageUser1_03172022 OU AutoRansomUser4_03162022
PAS	permet d'exclure du texte des résultats de la recherche	NOT AutoRansomUser4_03162022	Utilisateur,domaine, Type d'entité, chemin d'origine, dossier 1stLevel, dossier 2ndLevel, dossier 3rdLevel, dossier 4thLevel, Nom de l'entité, adresse IP source	Périphérique	Renvoie tout ce qui ne démarre pas avec « AutoRansomiUser4_03162022 »
Aucune	Recherche les valeurs NULL dans tous les champs	Aucune	Domaine		renvoie les résultats où le champ cible est vide

Recherche de chemin

Les résultats de la recherche avec et sans / seront différents

"/AutoDir1/AutoFile03242022"	Seule la recherche exacte fonctionne ; renvoie toutes les activités avec le chemin exact /AutoDir1/AutoFile03242022 (cas non sensible)
« /AutoDir1/ »	Fonctionne ; renvoie toutes les activités avec un répertoire de premier niveau correspondant à AutoDir1 (cas non sensible)
"/AutoDir1/AutoFile03242022/"	Fonctionne ; renvoie toutes les activités avec un répertoire de premier niveau correspondant à AutoDir1 et un répertoire de 2e niveau correspondant à AutoFile03242022 (cas non sensible)
/AutoDir1/AutoFile03242022 OU /AutoDir1/AutoFile03242022	Ne fonctionne pas
NON /AutoDir1/AutoFile03242022	Ne fonctionne pas
NON /AutoDir1	Ne fonctionne pas
NON /AutoFile03242022	Ne fonctionne pas
*	Ne fonctionne pas

Modifications de l'activité des utilisateurs du SVM root local

Lorsqu'un utilisateur du SVM racine local réalise une activité, l'adresse IP du client sur lequel le partage NFS est monté est à présent prise en compte dans le nom d'utilisateur, qui sera affiché sous la forme root@<ip-address-of-the-client> sur les pages d'activité d'analyse et d'activité des utilisateurs.

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 indiqué sur la page d'activité d'analyse 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 sur la page d'activité d'analyse 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 *root* user, sans distinction IP.

Dépannage

Problème	Essayez

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 ».	Raisons possibles : 1. Aucun collectionneur de répertoires d'utilisateurs n'a encore été configuré. Pour en ajouter un, accédez à **Workload Security > Collectors > User Directory Collectors** et cliquez sur **+User Directory Collector**. Choisissez *Active Directory* ou *LDAP Directory Server*. 2. Un collecteur d'annuaire d'utilisateurs a été configuré, mais il s'est arrêté ou est en état d'erreur. Accédez à **collecteurs > collecteurs d'annuaire d'utilisateurs** et vérifiez l'état. Reportez-vous à la "Dépannage de l'utilisateur Directory Collector" section de la documentation pour obtenir des conseils de dépannage. Après la configuration correcte, le nom sera automatiquement résolu dans les 24 heures. Si elle n'est toujours pas résolue, vérifiez si vous avez ajouté le collecteur de données utilisateur approprié. Assurez-vous que l'utilisateur fait bien partie du serveur Active Directory/LDAP d'annuaire ajouté.
Certains événements NFS n'apparaissent pas dans l'interface utilisateur.	Vérifier ce qui suit : 1. Un collecteur d'annuaire utilisateur pour serveur AD avec un jeu d'attributs POSIX doit être exécuté avec l'attribut unixid activé à partir de l'interface utilisateur. 2. Tout utilisateur ayant accès au 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 par 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 moins. (Notez que NFS 4.1 est pris en charge par ONTAP 9.15 ou version ultérieure.)
Après avoir saisi des lettres contenant un caractère générique comme l'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 recherche tout. Cependant, les chaînes de caractères génériques comme *<*searchTerm*>* ou *<*searchTerm*>** entraînent 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 récursivement sous /path1/path2/path3. Vous pouvez également utiliser l'option « Ajouter au filtre » sous l'onglet toutes les activités. »
J'ai rencontré une erreur « Echec de la demande 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 d’analyse effectue un chargement lent des données lors de l’utilisation du filtre *PATH*.	Pour obtenir des 4 résultats plus rapides, il est recommandé d’utiliser des filtres de chemin d’accès au répertoire (chaîne se terminant par /). Par exemple, si le chemin d’accès au répertoire est /AAA/BBB/CCC/DDD, essayez de rechercher "/AAA/BBB/CCC/DDD/" pour charger les données plus rapidement.
L’interface utilisateur d’analyse charge les données lentement et rencontre des défaillances lors de l’utilisation du filtre de nom d’entité.	Essayez 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.

Vue d’ensemble de l’utilisateur judiciaire

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 électronique de l’utilisateur
- Responsable de l’utilisateur
- Contact téléphonique de l’utilisateur
- Emplacement 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.

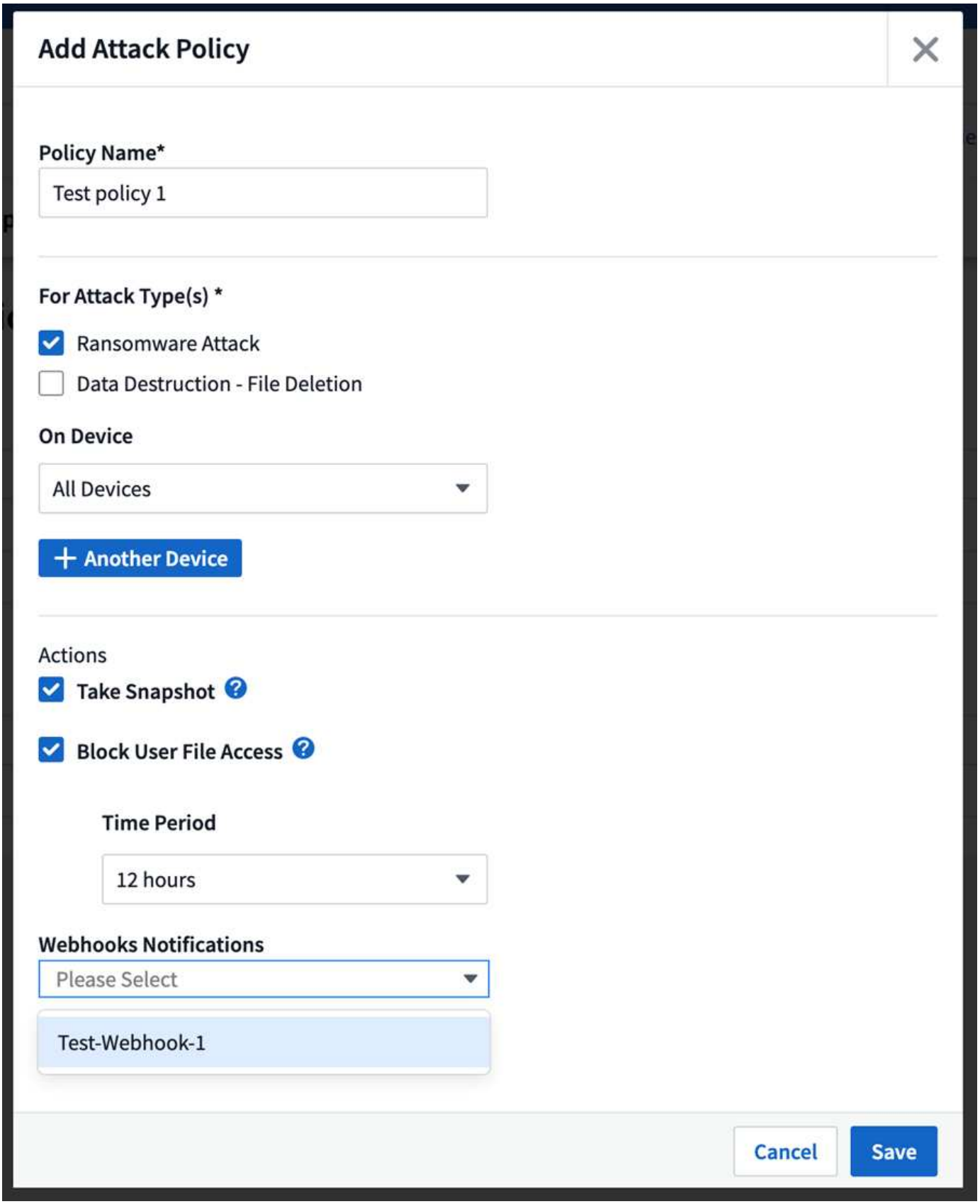
Stratégie de conservation

S'il n'est pas actualisé à nouveau, la liste des utilisateurs est conservée pendant 13 mois. Au bout de 13 mois, les données seront supprimées. Si votre environnement de sécurité des workloads est supprimé, toutes les données associées à l'environnement sont supprimées.

Stratégies de réponse automatisées

Les stratégies de réponse déclenchent des actions telles que la prise d'un instantané ou la restriction de l'accès de l'utilisateur en cas d'attaque ou de comportement anormal de l'utilisateur.

Vous pouvez définir des stratégies sur des périphériques spécifiques ou sur tous les périphériques. Pour définir une stratégie de réponse, sélectionnez **Admin > Automated Response Policies** et cliquez sur le bouton **+Policy** approprié. Vous pouvez créer des stratégies pour les attaques ou les avertissements.



Vous devez enregistrer la police avec un nom unique.

Pour désactiver une action de réponse automatisée (par exemple, prendre un instantané), il suffit d'annuler l'action et d'enregistrer la stratégie.

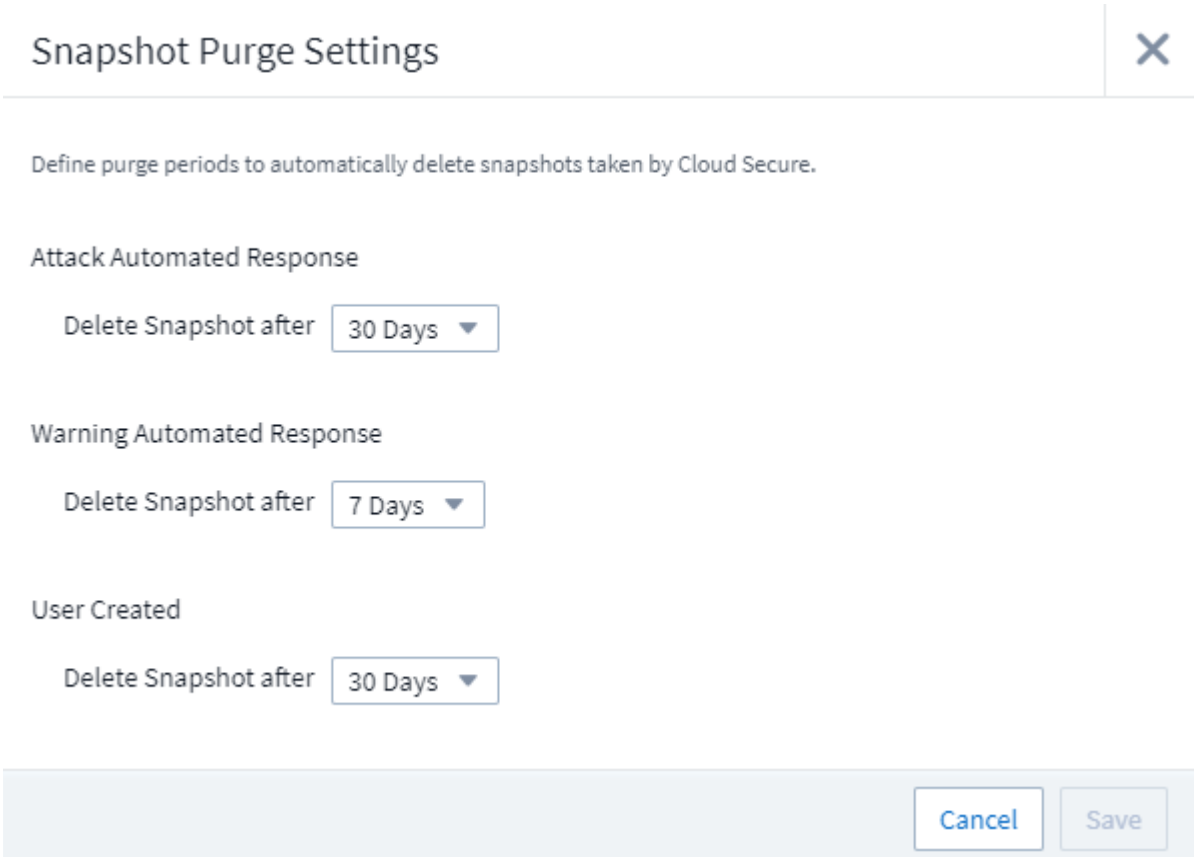
Lorsqu'une alerte est déclenchée par rapport aux périphériques spécifiés (ou à tous les périphériques, si elle est sélectionnée), la stratégie de réponse automatique prend un instantané de vos données. Vous pouvez voir l'état de l'instantané sur le "Page de détails de l'alerte".

Reportez-vous "Limiter l'accès des utilisateurs"à la page pour plus de détails sur la restriction de l'accès utilisateur par IP.

Vous pouvez joindre un ou plusieurs webhooks à une stratégie pour être averti lorsqu'une alerte est créée et que des mesures sont prises. Il est recommandé d'ajouter au plus 10 webhooks à une stratégie.n'oubliez pas que si une stratégie est suspendue, les notifications webhook ne seront pas déclenchées.

Vous pouvez modifier ou interrompre une stratégie de réponse automatique en sélectionnant l'option dans le menu déroulant de la stratégie.

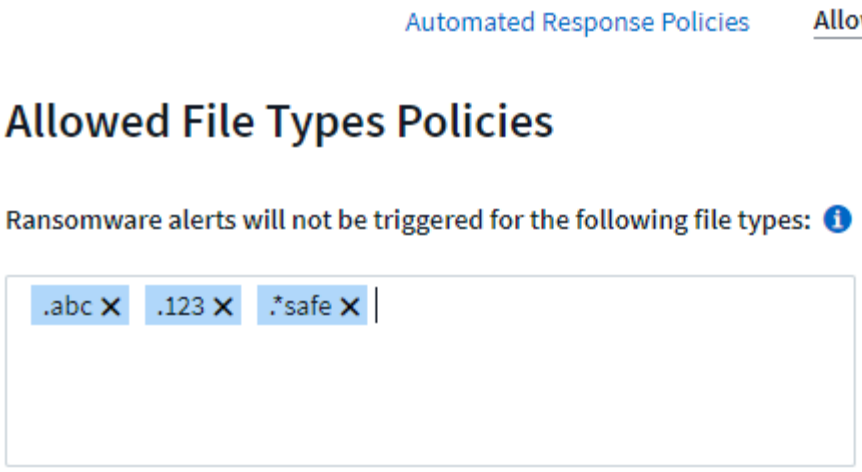
Le service de sécurité des charges de travail supprime automatiquement les snapshots une fois par jour en fonction des paramètres de suppression de Snapshot.



Stratégies de types de fichiers autorisées

Si une attaque par ransomware 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 *allowed file types* pour éviter des alertes inutiles.

Accédez à **Workload Security > Policies** et allez à l'onglet *Allowed File Type Policies*.



Une fois ajoutée à la liste *allowed file types* list, aucune alerte d'attaque par ransomware ne sera générée pour ce type de fichier autorisé. Notez que la règle *allowed File types* ne s'applique qu'à la détection des ransomware.

Par exemple, si un fichier nommé *test.txt* est renommé *test.txt.abc* et que Workload Security détecte une attaque par ransomware en raison de l'extension *.abc*, l'extension *.abc* peut être ajoutée à la liste *allowed file types* list. Après leur ajout à cette liste, les attaques par ransomware ne seront plus générées contre les fichiers portant 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 des types ".a*c", ".p*f" ne sont pas prises en charge.

Intégration avec la protection ONTAP autonome contre les ransomwares

La fonction ONTAP de protection autonome contre les ransomwares (Autonoman ransomware protection, ARP) utilise l'analyse des workloads dans les environnements NAS (NFS et SMB) pour détecter et avertir de manière proactive les anomalies d'activité dans les fichiers qui peuvent indiquer une attaque par ransomware.

Vous trouverez des détails supplémentaires et des exigences de licence concernant ARP "ici".

La sécurité des charges de travail s'intègre à ONTAP pour recevoir des événements ARP et fournir une couche d'analyse et de réponses automatiques supplémentaires.

La sécurité des charges de travail reçoit les événements ARP de ONTAP et effectue les opérations suivantes :

1. Met en corrélation les événements de cryptage des volumes avec l'activité des utilisateurs pour identifier qui est à l'origine des dommages.
2. Met en œuvre des politiques de réponse automatique (si définies)
3. Offre des fonctionnalités d'analyse :
    - Permettre aux clients de mener des enquêtes sur les violations de données.
    - Identifier les fichiers affectés, ce qui permet de les récupérer plus rapidement et de mener des enquêtes sur les violations de données.

Prérequis

1. Version minimale de 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. La sécurité des charges de travail ne peut pas activer ARP.
3. Le collecteur de sécurité de la charge de travail doit être ajouté via l'IP du cluster.
4. Des informations d'identification au niveau du cluster sont nécessaires pour que cette fonctionnalité fonctionne. En d'autres termes, les identifiants au niveau du cluster doivent être utilisés lors de l'ajout de la SVM.

Autorisations utilisateur requises

Si vous utilisez les informations d'identification d'administration du cluster, aucune nouvelle autorisation n'est nécessaire.

Si vous utilisez un utilisateur personnalisé (par exemple, *csuser*) avec les autorisations accordées à l'utilisateur, suivez les étapes ci-dessous pour donner les autorisations à la sécurité de la charge de travail afin de collecter des informations relatives à ARP à partir de ONTAP.

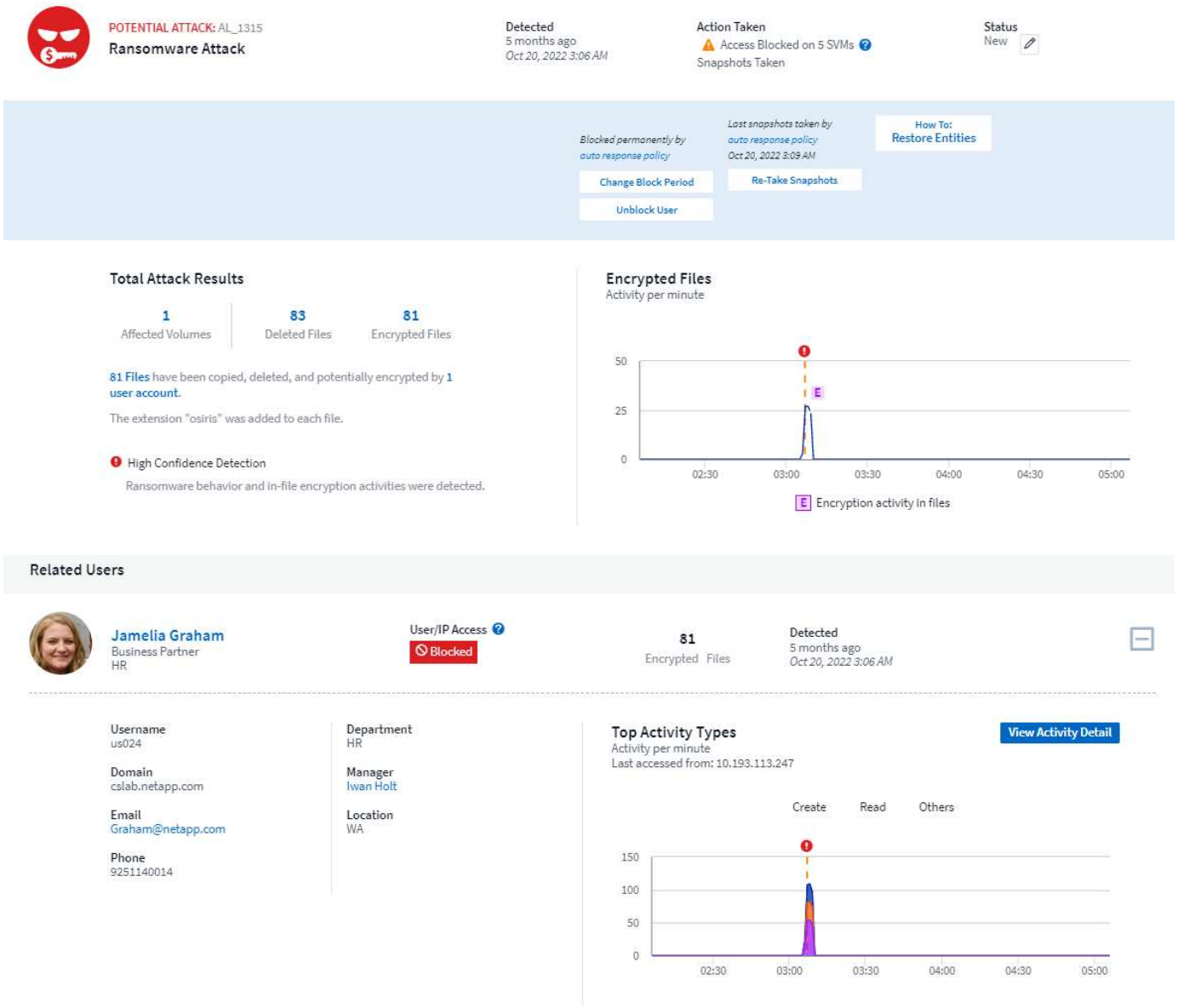
Pour *csuser* avec les informations d'identification du cluster, effectuez les opérations suivantes à partir de la ligne de commande ONTAP :

```
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".

Alerte exemple

Un exemple d'alerte générée en raison d'un événement ARP est illustré ci-dessous :



Une bannière de confiance élevée indique que l'attaque a montré un comportement par ransomware avec les activités de chiffrement de fichiers. Le graphique fichiers chiffrés indique l'horodatage auquel l'activité de chiffrement de volume a été détectée par la solution ARP.

Limites

Si un SVM n'est pas surveillé par la sécurité des charges de travail, mais que des événements ARP sont générés par ONTAP, les événements sont tout de même reçus et affichés par la sécurité des charges de travail. Cependant, les informations judiciaires liées à l'alerte, ainsi que le mappage des utilisateurs, ne seront pas capturées ni 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 s'affichent 24 heures avant que les e-mails soient reçus par Data Infrastructure Insights Workload Security.	Lorsque ONTAP envoie l'événement *ransomware Detected* à la sécurité de la charge de travail des informations de l'infrastructure de données (sécurité de la charge de travail), l'e-mail est envoyé. L'événement contient une liste d'attaques et de ses horodatages. L'interface utilisateur de la sécurité de la charge de travail affiche l'horodatage d'alerte du premier fichier attaqué. ONTAP envoie l'événement *ransomware détecté* aux informations de l'infrastructure de données lorsqu'un certain nombre de fichiers sont codés. Par conséquent, il peut y avoir une différence entre l'heure d'affichage de l'alerte dans l'interface utilisateur et l'heure d'envoi de l'e-mail.

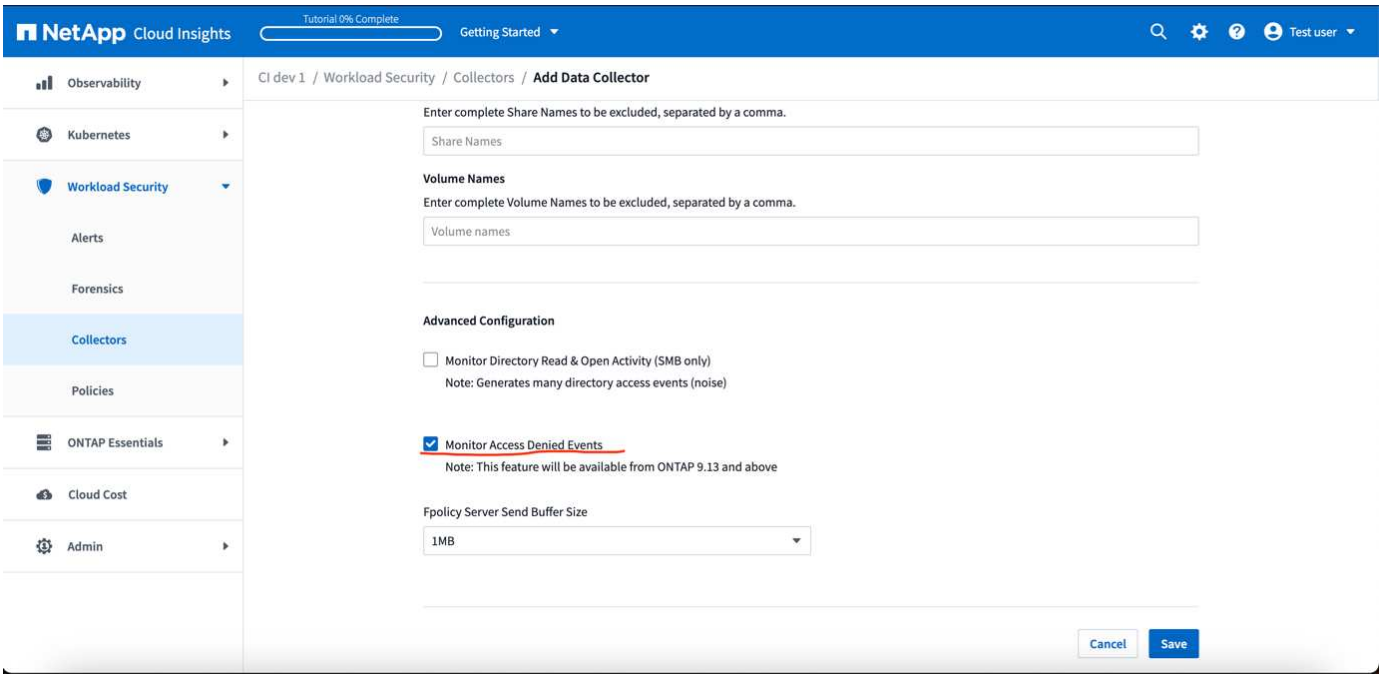
Intégration avec l'accès ONTAP refusée

La fonction ONTAP de refus d'accès utilise l'analyse de la charge de travail dans les environnements NAS (NFS et SMB) pour détecter de manière proactive les opérations de fichiers qui ont échoué et pour signaler ces échecs (c'est-à-dire qu'un utilisateur tente d'effectuer une opération pour laquelle il n'a pas l'autorisation nécessaire). Ces notifications d'échec d'opération de fichier, en particulier en cas de défaillances liées à la sécurité, aideront encore davantage à bloquer les attaques internes dès les premiers stades.

Informations sur l'infrastructure de données la sécurité des workloads s'intègre à ONTAP pour recevoir des événements de refus d'accès et fournir une couche supplémentaire d'analytique et de réponse automatique.

Prérequis

- Version minimale de ONTAP : 9.13.0.
- Un administrateur de Workload Security doit activer la fonctionnalité accès refusé lors de l'ajout d'un nouveau collecteur ou de la modification d'un collecteur existant, en cochant la case *Monitor Access Denied Events* sous Advanced Configuration.



Autorisations utilisateur requises

Si le Data Collector 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 les autorisations données 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.

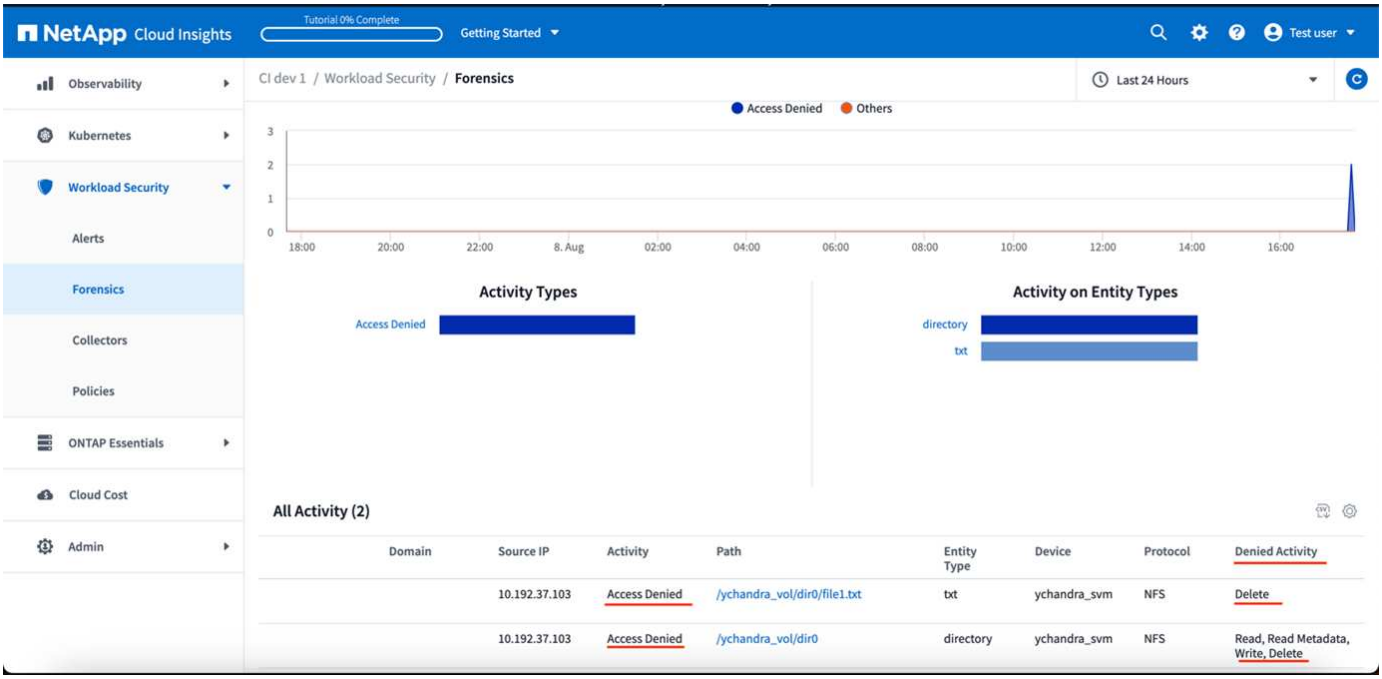
Pour les ccsuser avec des informations d'identification *cluster*, exécutez les commandes suivantes à partir de la ligne de commande ONTAP. Notez que cette autorisation existe peut-être déjà.

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
Pour les csuser avec _SVM_ credentials, executez les commandes suivantes
depuis 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'autres
xref:{relative_path}task_add_collector_svm.html["Autorisations ONTAP"].
```

Événements d'accès refusé

Une fois les événements acquis à partir du système ONTAP, la page analyse de sécurité de la charge de travail affiche les événements accès refusé. En plus des informations affichées, vous pouvez afficher les autorisations utilisateur manquantes pour une opération particulière en ajoutant la colonne *activité* souhaitée à la table à partir de l'icône en forme d'engrenage.



Blocage de l’accès utilisateur

Une fois qu’une attaque est détectée, Workload Security peut arrêter l’attaque en bloquant l’accès des utilisateurs au système de fichiers. L’accès peut être bloqué automatiquement à l’aide de politiques de réponse automatique ou manuellement à partir des pages d’alerte ou d’informations utilisateur.

Lorsque vous bloquez l’accès utilisateur, vous devez définir une période de blocage. Une fois la période sélectionnée terminée, l’accès utilisateur est automatiquement restauré. Le blocage des accès est pris en charge à la fois pour les protocoles SMB et NFS.

L’utilisateur est directement bloqué pour le protocole SMB et l’adresse IP des machines hôtes à l’origine de l’attaque sera bloquée pour NFS. Ces adresses IP de la machine seront bloquées lors de l’accès à l’un des SVM contrôlés par la sécurité des charges de travail.

Disons, par exemple, que la sécurité des charges de travail gère 10 SVM, et la stratégie de réponse automatique est configurée pour quatre de ces SVM. Si l’attaque provient de l’un des quatre SVM, l’accès de l’utilisateur sera bloqué dans les 10 SVM. Une copie Snapshot est toujours effectuée sur la SVM d’origine.

Si quatre SVM avec un SVM configuré pour SMB, un SVM pour NFS et les deux autres configurés pour NFS et SMB, tous les SVM seront bloqués si l’attaque provient de l’un des quatre SVM.

Conditions préalables au blocage de l’accès utilisateur

Des informations d’identification au niveau du cluster sont nécessaires pour que cette fonctionnalité fonctionne.

Si vous utilisez les informations d’identification d’administration du cluster, aucune nouvelle autorisation n’est nécessaire.

Si vous utilisez un utilisateur personnalisé (par exemple, *csuser*) avec les autorisations accordées à l’utilisateur, suivez les étapes ci-dessous pour donner des autorisations à Workload Security afin de bloquer

l'utilisateur.

Pour csuser avec les identifiants du cluster, effectuez la procédure suivante dans 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
```

Vérifiez également la section autorisations de la "Configuration du SVM Data Collector de ONTAP" page.

Comment activer la fonction ?

- Dans Workload Security, accédez à **Workload Security > Policies > Automated Response Policies**. Choisissez **+stratégie d'attaque**.
- Sélectionnez (cochez) *bloquer l'accès aux fichiers utilisateur*.

Comment configurer le blocage automatique des accès utilisateur ?

- Créez une nouvelle stratégie d'attaque ou modifiez une stratégie d'attaque existante.
- Sélectionnez les SVM sur lesquels la règle d'attaque doit être contrôlée.
- Cliquez sur la case à cocher "bloquer l'accès aux fichiers utilisateur". La fonction sera activée lorsque cette option est sélectionnée.
- Sous "time period", sélectionnez la durée jusqu'à laquelle le blocage doit être appliqué.
- Pour tester le blocage automatique de l'utilisateur, vous pouvez simuler une attaque via "script simulé".

Comment savoir s'il y a des utilisateurs bloqués dans le système ?

- Dans la page des listes d'alertes, une bannière s'affiche en haut de l'écran si un utilisateur est bloqué.
- Cliquez sur la bannière pour accéder à la page "utilisateurs", où la liste des utilisateurs bloqués peut être affichée.
- Dans la page "utilisateurs", il y a une colonne intitulée "accès utilisateur/IP". Dans cette colonne, l'état actuel du blocage de l'utilisateur s'affiche.

Limitez et gérez l'accès des utilisateurs manuellement

- Vous pouvez accéder à l'écran des détails de l'alerte ou des détails de l'utilisateur, puis bloquer ou restaurer manuellement un utilisateur à partir de ces écrans.

Historique des limitations d'accès utilisateur

Dans la page des détails de l'alerte et de l'utilisateur, dans le panneau utilisateur, vous pouvez afficher un audit de l'historique des limites d'accès de l'utilisateur : heure, action (Bloc, débloquer), durée, action effectuée par, Manuel/automatique et adresses IP concernées pour NFS.

Comment désactiver cette fonction ?

Vous pouvez à tout moment désactiver la fonction. Si le système contient des utilisateurs restreints, vous devez d'abord restaurer leur accès.

- Dans Workload Security, accédez à **Workload Security > Policies > Automated Response Policies**. Choisissez **+stratégie d'attaque**.
- Désélectionner (décocher) *bloquer l'accès aux fichiers utilisateur.*

La fonction sera masquée de toutes les pages.

Restaurez manuellement les adresses IP pour NFS

Procédez comme suit pour restaurer manuellement des adresses IP à partir de ONTAP si votre essai de sécurité de la charge de travail expire ou si l'agent/collecteur est arrêté.

1. Lister toutes les export policy 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 règles de la SVM qui ont "cloudSecure_rule" comme client Match en spécifiant son RuleIndex respectif. La règle de sécurité de la charge de travail est généralement de 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.
```

Restaurez manuellement les utilisateurs pour SMB

Procédez comme suit pour restaurer manuellement des utilisateurs à partir de ONTAP si votre version d'évaluation de la sécurité de la charge de travail expire ou si l'agent/collecteur est arrêté.

Vous pouvez obtenir la liste des utilisateurs bloqués dans la sécurité de la charge de travail à partir de la page liste des utilisateurs.

1. Connectez-vous au cluster ONTAP (où vous voulez débloquer des utilisateurs) avec les informations d'identification cluster *admin*. (Pour Amazon FSX, connectez-vous avec les informations d'identification FSX).
2. Exécutez la commande suivante pour lister 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 étaient 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>
. Vérifiez 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 bloqués précédemment.

Dépannage

Problème	Essayez
Certains utilisateurs ne sont pas limités, bien qu'il y ait une attaque.	1. Assurez-vous que le Data Collector et l'Agent des SVM sont à l'état *running*. La sécurité de charge de travail ne pourra pas envoyer de commandes si le Data Collector 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 adresse IP qui n'a pas été utilisée auparavant. La restriction s'effectue via l'adresse IP de l'hôte par l'intermédiaire de laquelle l'utilisateur accède au stockage. Vérifiez dans l'interface utilisateur (Détails de l'alerte > Historique des limitations d'accès pour cet utilisateur > adresses IP affectées) 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, alors l'utilisateur pourra toujours accéder au stockage via l'adresse IP non restreinte. Si l'utilisateur tente d'accéder aux hôtes dont les adresses IP sont restreintes, alors le stockage ne sera pas accessible.
Si vous cliquez manuellement sur restreindre l'accès, « les adresses IP de cet utilisateur ont déjà été restreintes » s'affiche.	L'adresse IP à restreindre est déjà restreinte par 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 indiqué ci-dessus.

Problème	Essayez
Le blocage de l'utilisateur (adresse IP) pour NFS fonctionne, mais pour SMB / CIFS, un message d'erreur s'affiche : « échec de la transformation entre SID et DomainName. Délai d'expiration du motif : le socket n'est pas établi »	Ceci peut se produire est *csuser* n'a pas l'autorisation d'exécuter ssh. (Vérifiez la connexion au niveau du cluster, puis assurez-vous que l'utilisateur peut effectuer ssh). le rôle *csuser* requiert 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, effectuez les opérations suivantes 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 -cmddirname set -Access all Security login role create -user name si le rôle ONTAP d'authentification est utilisé, ccsadmin user name -login name si le rôle de sécurité est un rôle d'authentification -login -user name -user name, user name est un rôle d'authentification -user name -user name.
J'obtiens le message d'erreur *SID Translate failed. Reason:255:Error: Command failed: Not authorized for this commandeError: "Access-check" n'est pas une commande reconnue*, quand un utilisateur aurait dû être bloqué.	Cela peut se produire lorsque *csuser* ne dispose pas des autorisations appropriées. 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 du répertoire utilisateur. Les commandes d'autorisation requises sont répertoriées ci-dessous. ---- sécurité 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 authentifiez" -all security login rôle create -role csrole -cmddirname "vserver name-mapping" -access all ----

Sécurité des charges de travail : simulation d'une attaque

Vous pouvez utiliser les instructions de cette page pour simuler une attaque à des fins de test ou de démonstration de la sécurité des charges de travail à l'aide du script inclus de simulation d'attaques par ransomware.

À noter avant de commencer

- Le script de simulation d'attaque par ransomware fonctionne uniquement sur Linux. Le script de simulation doit également générer des alertes de haute confiance dans le cas où l'utilisateur a 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 de sécurité de la charge de travail. Il est disponible sur n'importe quelle machine sur laquelle un agent de sécurité de la charge de travail est installé.
- Vous pouvez exécuter le script sur l'agent de sécurité de la charge de travail lui-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.
- Les utilisateurs peuvent opter pour le script Python ou Shell en fonction de leurs préférences et des exigences système.
- Le script Python nécessite des prérequis. Si vous ne souhaitez pas utiliser Python, utilisez le script shell.

Lignes directrices :

Ce script doit être exécuté sur une SVM contenant un dossier contenant un nombre important de fichiers à chiffrer, idéalement 100 ou plus, y compris les fichiers des sous-dossiers. Assurez-vous que les fichiers ne sont pas vides.

Pour générer l'alerte, suspendez temporairement le collecteur avant la création des données de test. Une fois les fichiers d'exemple générés, relancez le collecteur et lancez le processus de chiffrement.

Étapes :

Préparez le système :

Commencez par monter 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 NFS version 4.1 ; il n'est pas pris 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]
Configurez ensuite un Data Collector :
```

1. Configurez l'agent de sécurité de la charge de travail si ce n'est 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 des fichiers à chiffrer. Vous pouvez copier manuellement les fichiers à chiffrer dans le dossier cible ou utiliser l'un des scripts inclus pour les créer par programmation. Quelle que soit la méthode choisie, assurez-vous qu'au moins 100 fichiers sont présents à chiffrer.

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 dans le
dossier de montage sous un répertoire appelé « test_dataset »
```

Reprendre le collectionneur

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 Ransomware, vous pouvez exécuter le script inclus qui simulera une alerte ransomware 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'échantillons 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'échantillons 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.

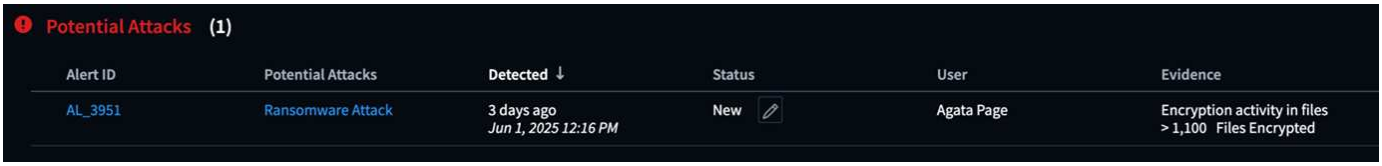
Remarque : si toutes les conditions suivantes sont remplies, une alerte de haute confiance sera générée.

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.

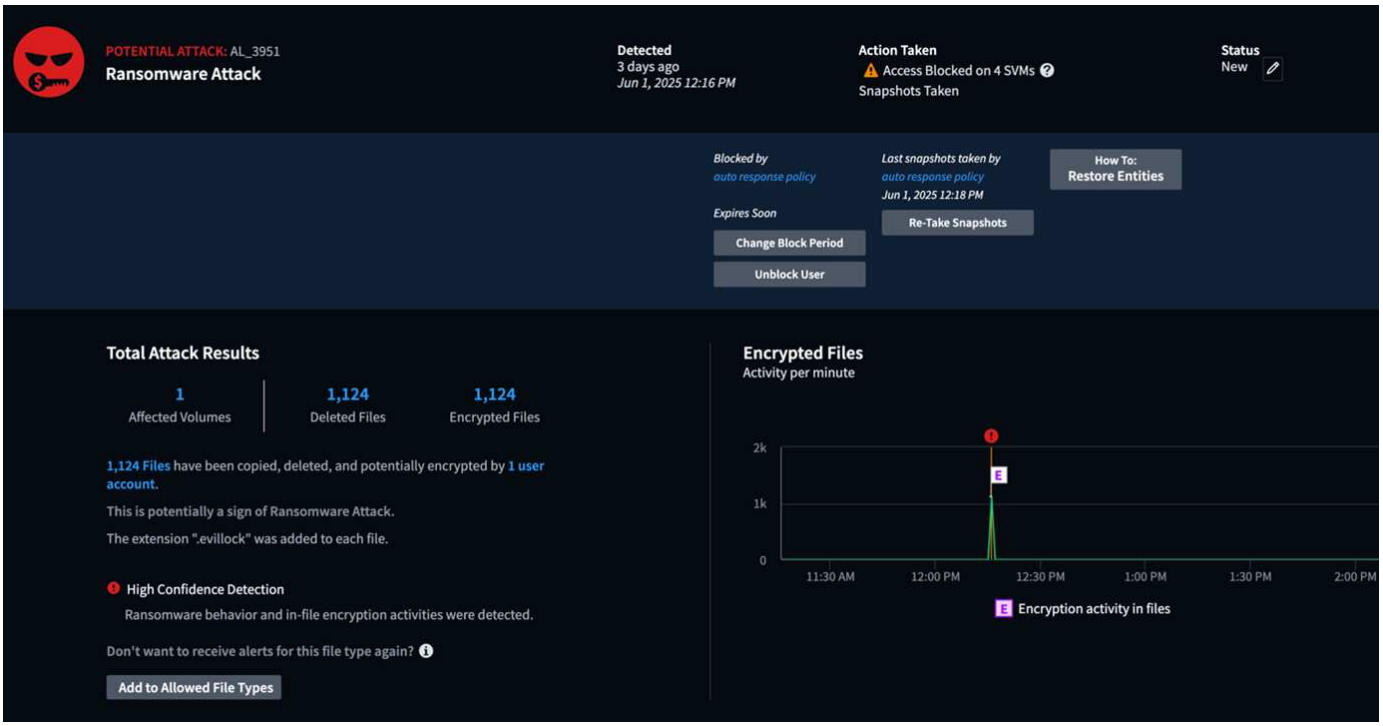
Workload Security détecte les modèles de ransomware en fonction du comportement de l'utilisateur tandis qu'ONTAP ARP détecte l'activité de ransomware en fonction des activités de chiffrement dans les fichiers.

Si les conditions sont remplies, Workload Security marque les alertes comme étant des alertes 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 apprend le comportement des utilisateurs et ne génère pas d’alertes sur les attaques répétées de ransomware dans les 24 heures pour le 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 du collecteur d’agents/de sources de données

Pour configurer les destinataires d’alertes de sécurité de la charge de travail, cliquez sur **Admin > Notifications** et entrez une ou plusieurs adresses électroniques dans les sections appropriées pour chaque destinataire.

Alertes et avertissements d’attaque potentielle

Pour envoyer des notifications *attaque potentielle* alerte, entrez les adresses e-mail des destinataires dans la section *Envoyer alertes d’attaque potentielles*. Les notifications par e-mail sont envoyées à la liste des destinataires des alertes pour chaque action de l’alerte.

Pour envoyer des notifications *Warning*, entrez les adresses e-mail des destinataires dans la section *Send Warning Alerts*.

Surveillance de l’état de santé des agents et des Data Collector

Vous pouvez surveiller l’état des agents et des sources de données grâce aux notifications.

Afin de recevoir des notifications si un agent ou un collecteur de source de données ne fonctionne pas, entrez

les adresses électroniques des destinataires dans la section *Data Collection Health Alerts*.

Gardez à l'esprit les éléments suivants :

- Les alertes d'intégrité ne seront envoyées qu'une fois que l'agent/le collecteur cesse de générer des rapports pendant au moins une heure.
- Une seule notification par e-mail est envoyée aux destinataires prévus dans une période donnée de 24 heures, même si l'agent ou le collecteur de données est déconnecté pendant une période plus longue.
- En cas de défaillance d'un agent, une alerte est envoyée (pas une par collecteur). Cet e-mail inclura une liste de tous les SVM affectés.
- L'échec de la collecte de répertoire actif est signalé comme un avertissement ; elle n'a aucun impact sur la détection de ransomware.
- La liste mise en route comprend maintenant une nouvelle phase *configurer les notifications par e-mail*.

Réception de notifications de mise à niveau d'agent et de Data Collector

- Entrez les ID d'e-mail dans le champ « Data Collection Health Alerts » (alertes d'état de la 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 Data Collector sont envoyées aux ID d'e-mail un jour avant la mise à niveau prévue.

Dépannage

Problème:	Essayez ceci:
Les ID d'e-mail sont présents dans les « alertes d'intégrité du Data Collector », mais je ne reçois pas de notifications.	Des e-mails de notification sont envoyés à partir du domaine NetApp Data Infrastructure Insights, c'est-à-dire à partir de_NetApp.com_. Certaines entreprises bloquent les e-mails entrants s'ils proviennent d'un domaine externe. Assurez-vous que les notifications externes provenant des domaines NetApp Data Infrastructure Insights sont placées sur liste blanche.

Notifications de Webhook

Notifications de sécurité des workloads 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 Web 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 un grand nombre de ces canaux de distribution. Vous trouverez des informations sur la configuration des webhooks sur les sites Web de l'application concernée. Par exemple, Slack fournit "ce guide utile".

Vous pouvez créer plusieurs canaux Webhook, chaque canal ciblé pour un usage différent, des applications séparées, des destinataires différents, etc

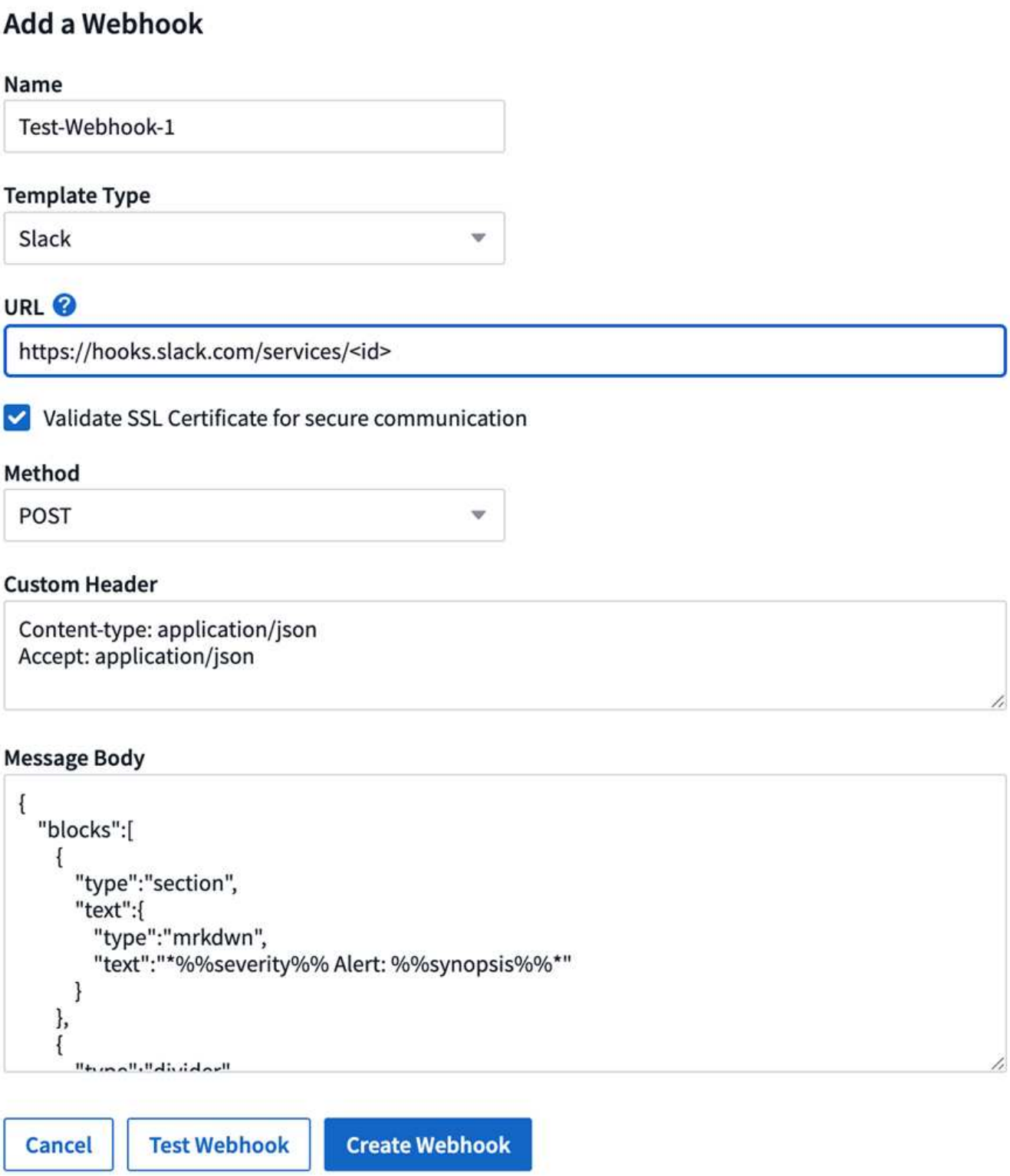
L’instance de canal webhook comprend les éléments suivants

Nom	Description
URL	URL cible Webhook, y compris le préfixe http:// ou https:// avec les paramètres url
Méthode	OBTENIR/PUBLIER - la valeur par défaut est POST
En-tête personnalisé	Spécifiez les en-têtes personnalisés ici
Corps du message	Mettez le corps de votre message ici
Paramètres d’alerte par défaut	Répertorie les paramètres par défaut du mousqueton
Paramètres et secrets personnalisés	Les paramètres personnalisés et les secrets vous permettent d’ajouter des paramètres uniques et des éléments sécurisés tels que des mots de passe

Création d’un mousqueton

Pour créer un composant Workload Security Webhook, accédez à Admin > Notifications et sélectionnez l’onglet Workload Security Webhooks. L’image suivante montre un exemple d’écran de création de webhook Slack.

Remarque : l’utilisateur doit être un *Admin* de Workload Security pour créer et gérer les Webhooks de Workload Security.



- Entrez les informations appropriées pour chacun des champs, puis cliquez sur « Enregistrer ».
- Vous pouvez également cliquer sur le bouton « Tester Webhook » pour tester la connexion. Notez que le « corps du message » (sans substitutions) est envoyé à l'URL définie selon la méthode sélectionnée.
- Les webhooks SWS comprennent un certain nombre de paramètres par défaut. En outre, vous pouvez créer vos propres paramètres ou secrets personnalisés.

Paramètres : quels sont-ils et comment les utiliser ?

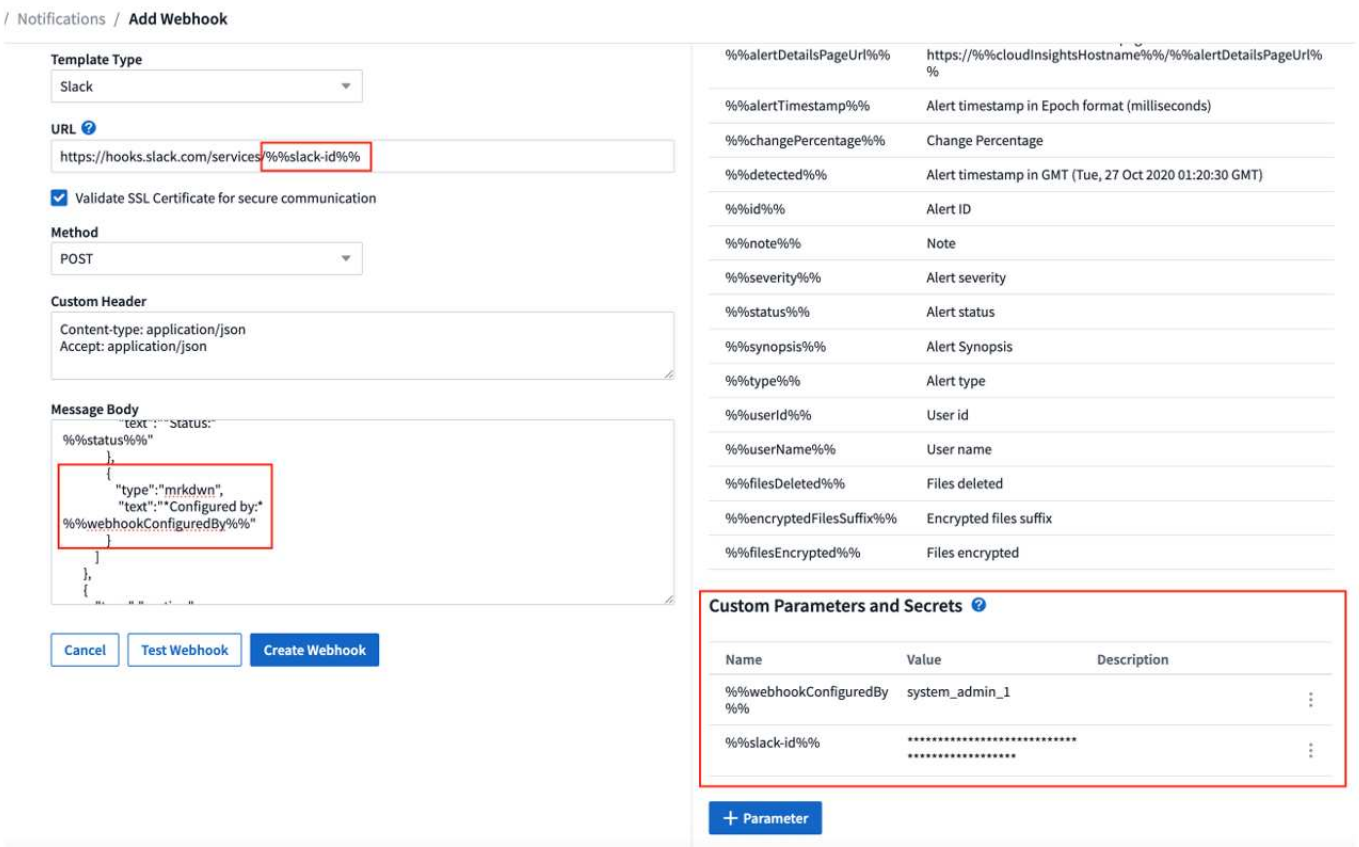
Les paramètres d'alerte sont des valeurs dynamiques remplies par alerte. Par exemple, le paramètre *%%Severity%%* sera remplacé par le type de gravité de l'alerte.

Notez que les substitutions ne sont pas effectuées lorsque vous cliquez sur le bouton « Tester le crochet » ; 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 des paramètres et/ou des secrets personnalisés. Un paramètre personnalisé ou un secret peut se trouver dans l'URL ou le corps du message. Les secrets permettent à l'utilisateur de configurer un paramètre personnalisé sécurisé tel que mot de passe, apiKey, etc

L'exemple d'image suivant montre comment les paramètres personnalisés sont utilisés dans la création de webhook.



Page de liste Webhooks pour la sécurité des charges de travail

Sur la page de liste Webhooks, sont affichés le Nom, créé par, créé le, État, sécurisé, et les champs dernier rapport. Remarque : la valeur de la colonne « Etat » ne cesse de changer en fonction du résultat du dernier déclenchement du webhook. Voici des exemples de résultats d'état.

État	Description
OK	Notification envoyée avec succès.
403	Interdit.

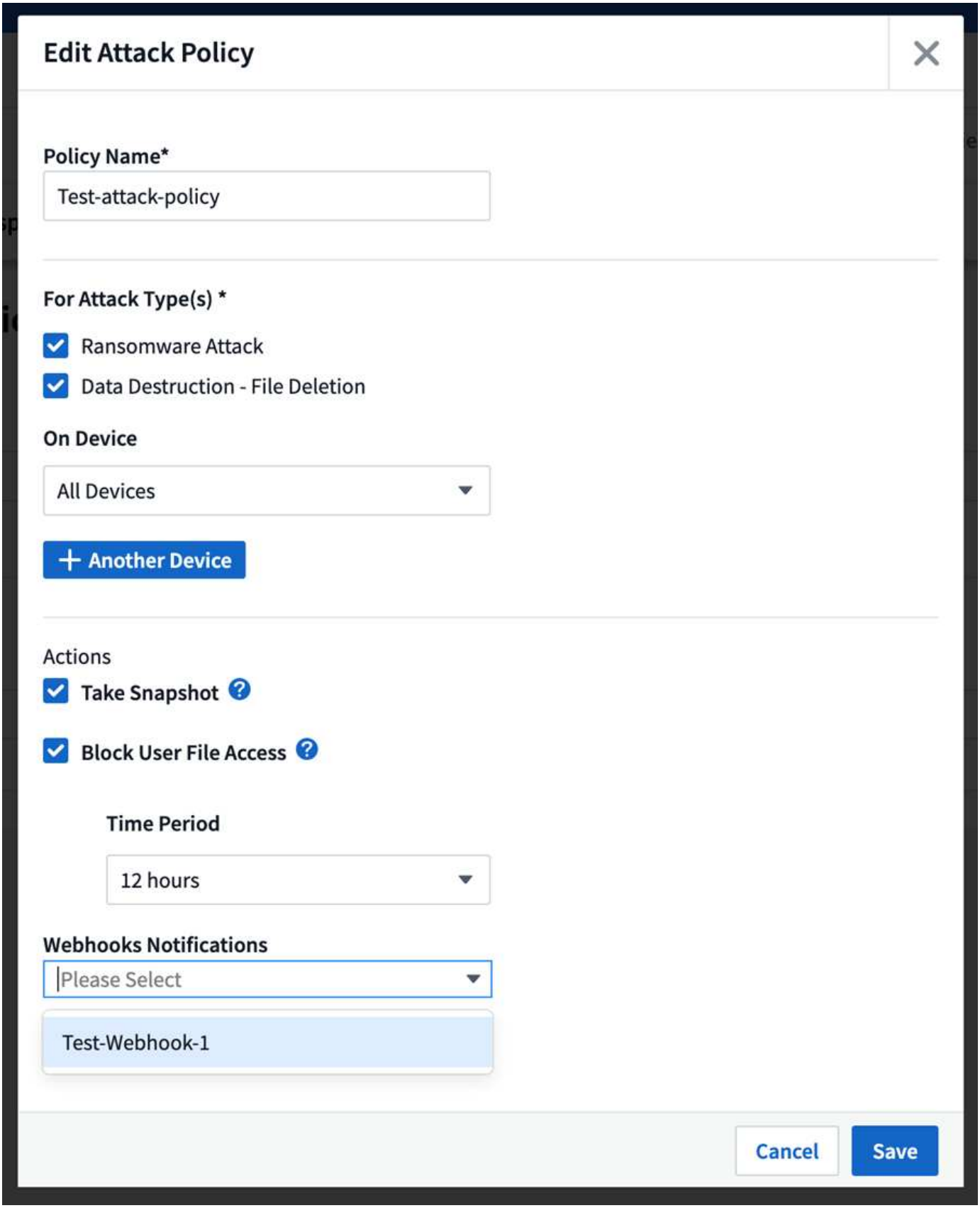
404	URL introuvable.
400	Demande incorrecte. Vous pouvez voir cet état en cas d'erreur dans le corps du message, par exemple : • Json mal formaté. • Valeur non valide pour les clés réservées. Par exemple, PagerDuty accepte uniquement critique/avertissement/erreur/info pour "gravité". Tout autre résultat peut donner un état 400. • Erreurs de validation spécifiques à l'application. Par exemple, Slack autorise un maximum de 10 champs dans une section. Si vous en inclure plus de 10, vous risquez d'obtenir un statut 400.
410	La ressource n'est plus disponible

La colonne "dernier rapport" indique l'heure à laquelle le webhook a été déclenché pour la dernière fois.

À partir de la page de liste webhooks, les utilisateurs peuvent également modifier/dupliquer/supprimer des webhooks.

Configurez la notification Webhook dans la stratégie d'alerte

Pour ajouter une notification webhook à une stratégie d'alerte, accédez à -Workload Security > Policies- et sélectionnez une stratégie existante ou ajoutez une nouvelle stratégie. Dans la section *actions* > *Webhook Notifications*, sélectionnez les webhooks requis.



Les notifications Webhook sont liées aux stratégies. Lorsque l'attaque (RW/DD/WARN) se produit, l'action configurée (prendre instantané / blocage utilisateur) est effectuée et la notification liée au webhook est déclenchée.

Remarque : les notifications par e-mail sont indépendantes des politiques. Elles seront déclenchées comme d'habitude.

- Si une stratégie est mise en pause, les notifications webhook ne seront pas déclenchées.
- Plusieurs webhooks peuvent être attachés à une seule stratégie, mais il est recommandé de ne pas attacher plus de 5 webhooks à une police.

Exemples de Webhook pour la sécurité des charges de travail

Webhooks pour "Mou"

Webhooks pour "Service de PagerDuty" Webhooks pour "Équipes""Déroulez"

Exemple de Webhook de sécurité des charges de travail pour la discorde

Les Webpatères permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal Web personnalisé. Cette page fournit un exemple de configuration des crochets pour le discorde.

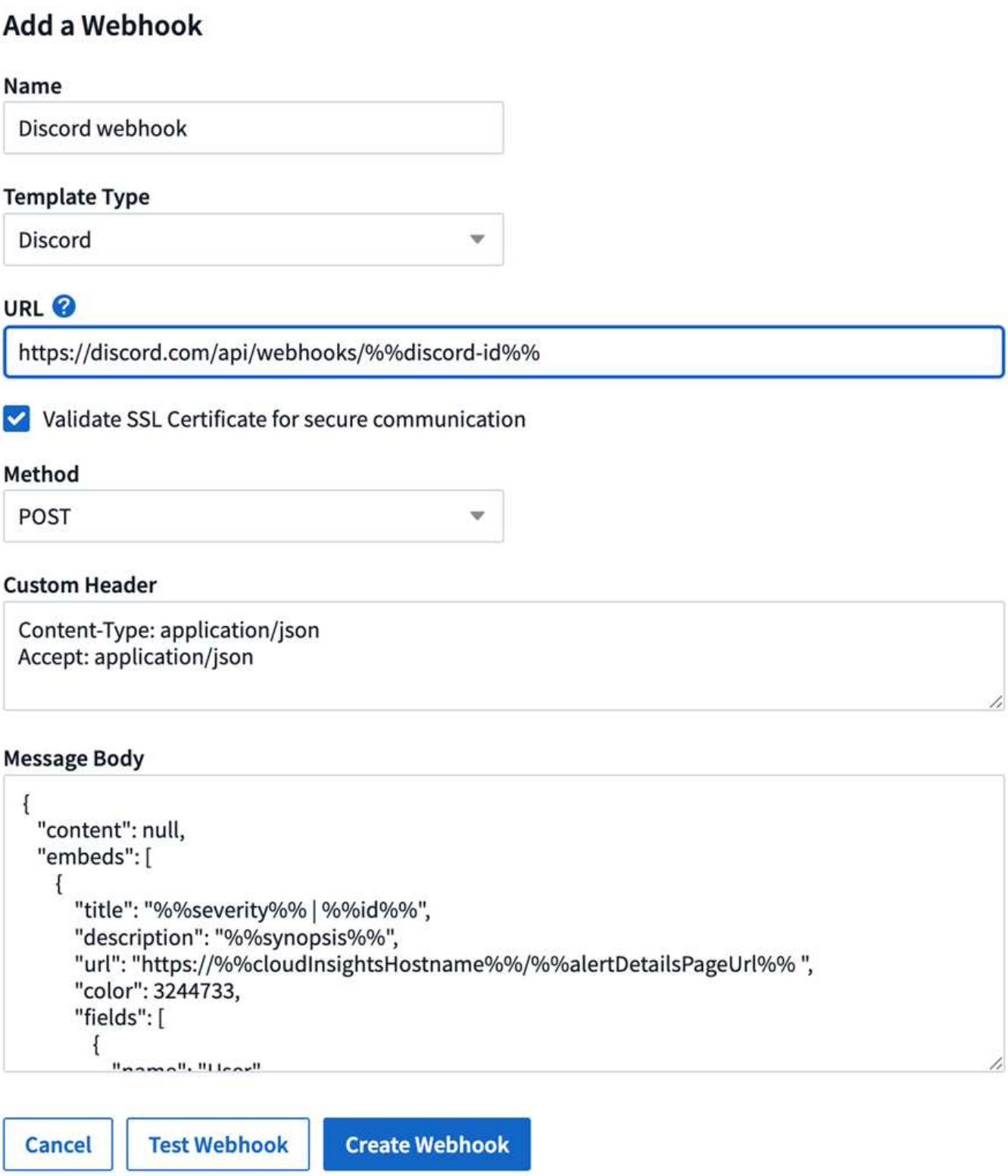
Cette page fait référence aux instructions de tiers, qui sont sujettes à modification. Reportez-vous au "Documentation de discorde" pour obtenir les informations les plus récentes.

Configuration de la discorde :

- Dans Discordon, sélectionnez le serveur, sous canaux de texte, sélectionnez Modifier le canal (icône d'engrenage)
- Sélectionnez **intégrations > Afficher Webpatères** et cliquez sur **Nouveau Webhook**
- Copiez l'URL du Webhook. Vous devez coller cette information dans la configuration du webhook de sécurité de la charge de travail.

Créer Workload Security Webhook :

1. Accédez à Admin > Notifications et sélectionnez l'onglet *Workload Security Webhooks*. Cliquez sur '+ Webhook' pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif.
3. Dans la liste déroulante *Template Type*, sélectionnez **discorde**.
4. Collez l'URL de discord ci-dessus dans le champ *URL*.



Pour tester le webhook, remplacez temporairement la valeur de l'URL dans le corps du message par une URL valide (telle que *https://netapp.com*), puis cliquez sur le bouton *Test Webhook*. Pour que la fonctionnalité Test Webhook fonctionne, il est nécessaire de fournir une URL valide.

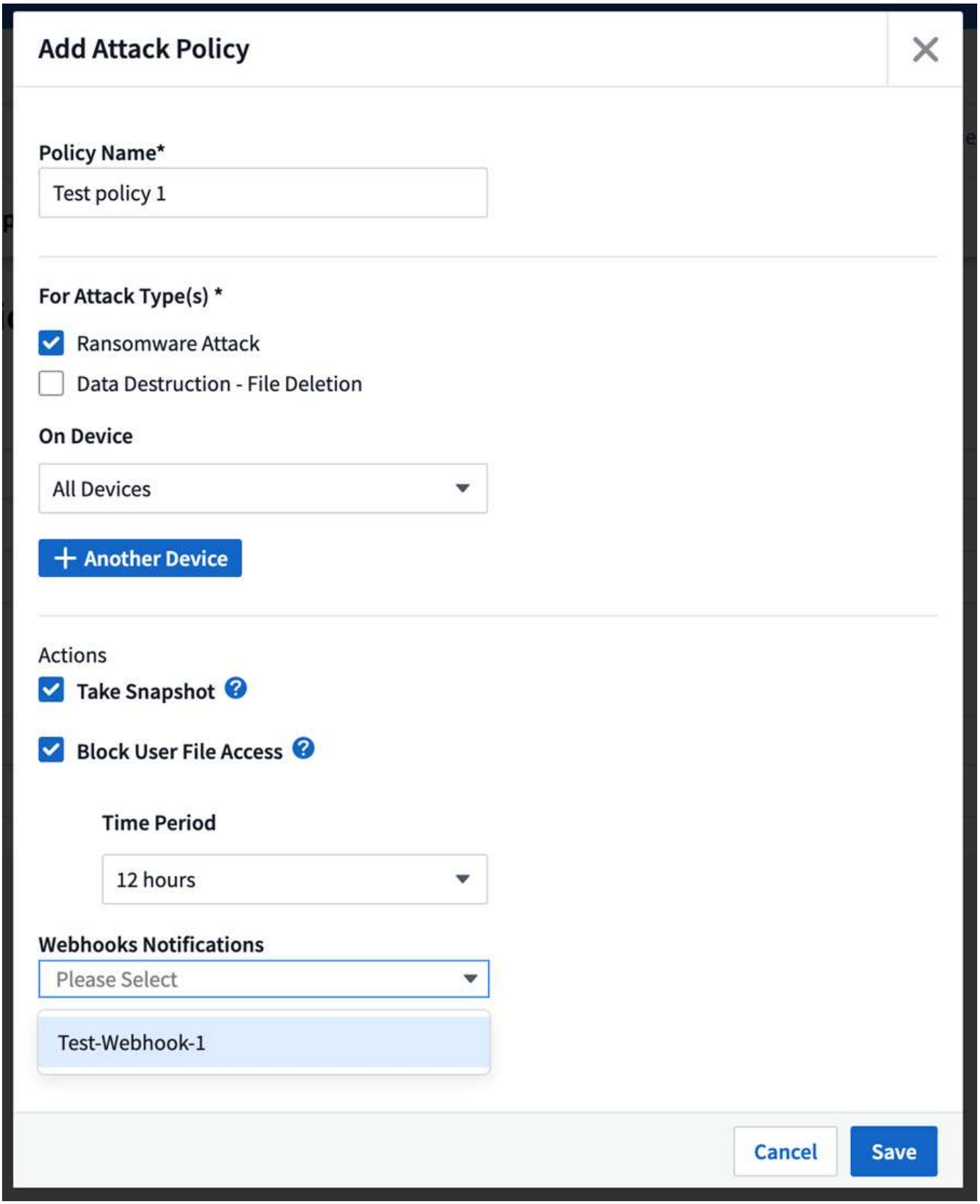
Une fois le test terminé, veillez à remettre le corps du message en place.

Notifications via Webhook

Pour signaler des événements via Webhook, accédez à *Workload Security* > *Policies*. Cliquez sur *+Stratégie d'attaque* ou *+politique d'avertissement*.

- Entrez un nom de règle significatif.
- Sélectionnez le(s) type(s) d'attaque requis, les périphériques auxquels la stratégie doit être associée et les actions requises.
- Dans la liste déroulante *Webhooks Notifications*, sélectionnez les webhooks requis et enregistrez.

Remarque : les Webhooks peuvent également être associés à des stratégies existantes en les modifiant.



Exemple de Webhook pour PagerDuty

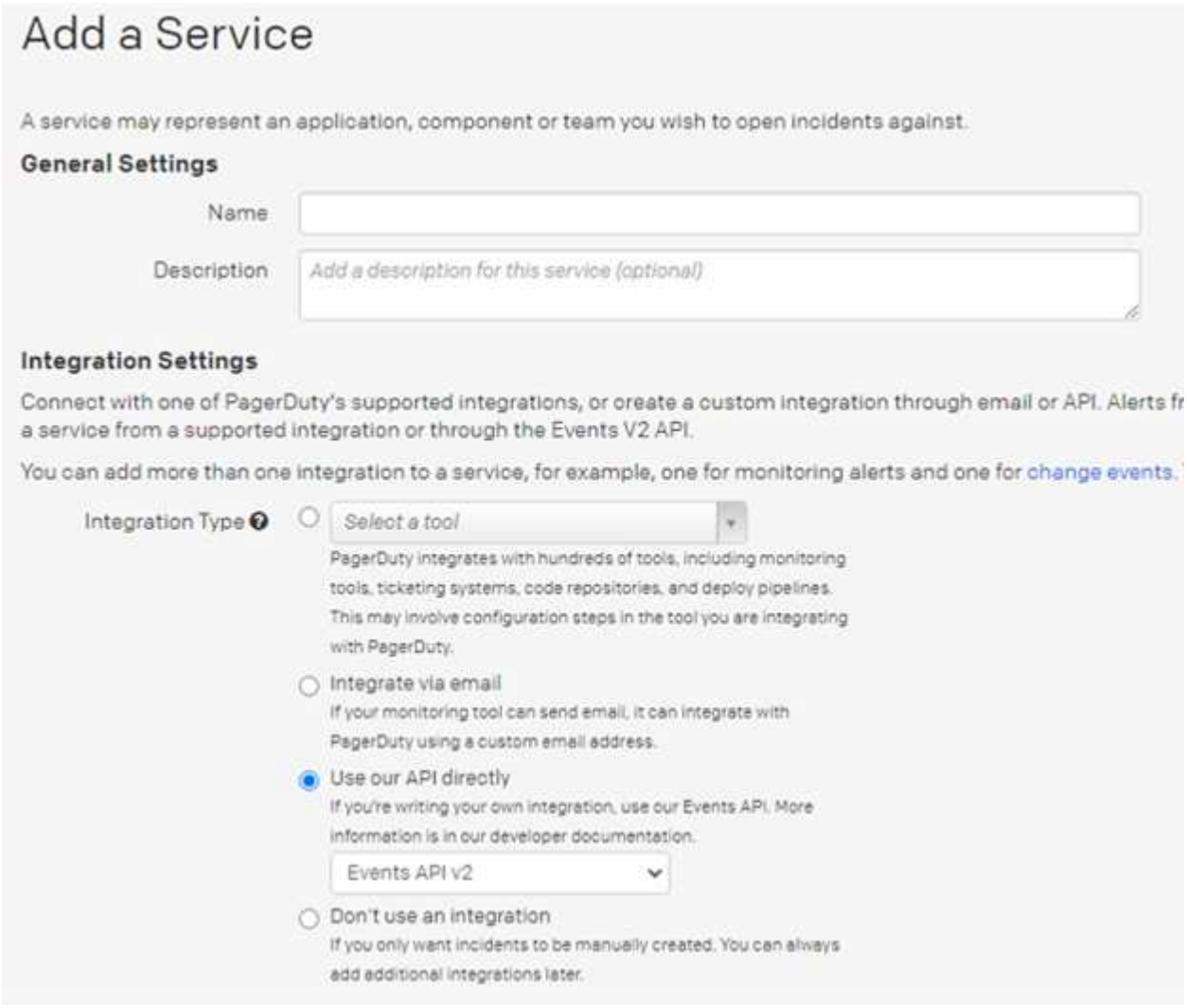
Les Webpatères permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal Web personnalisé. Cette page fournit un

exemple de configuration des crochets pour PagerDuty.

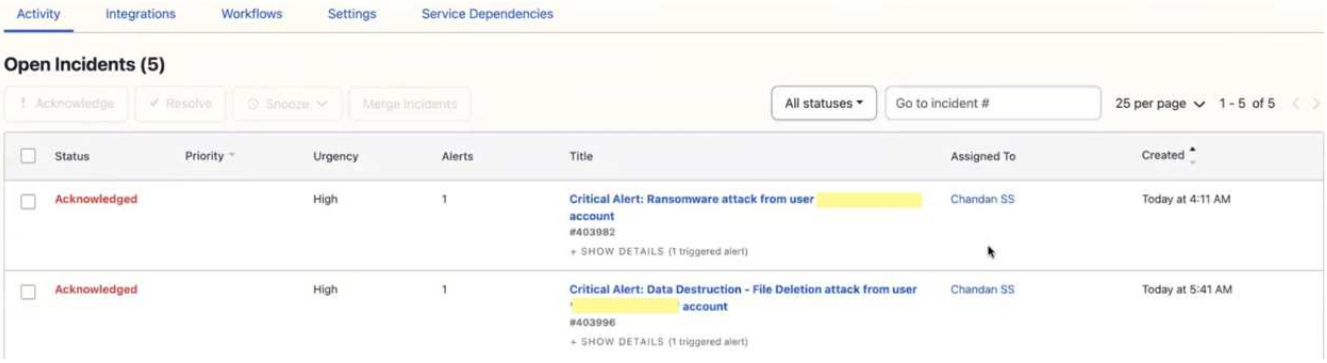
Cette page se réfère aux instructions de tiers, qui sont sujettes à modification. Reportez-vous au "Documentation PagerDuty" pour obtenir les informations les plus récentes.

Configuration de la fonction PagerDuty :

1. Dans PagerDuty, accédez à **Services > répertoire de services** et cliquez sur le bouton **+Nouveau service**.
2. Entrez un *Nom* et sélectionnez *utiliser directement notre API*. Sélectionnez *Ajouter un service*.

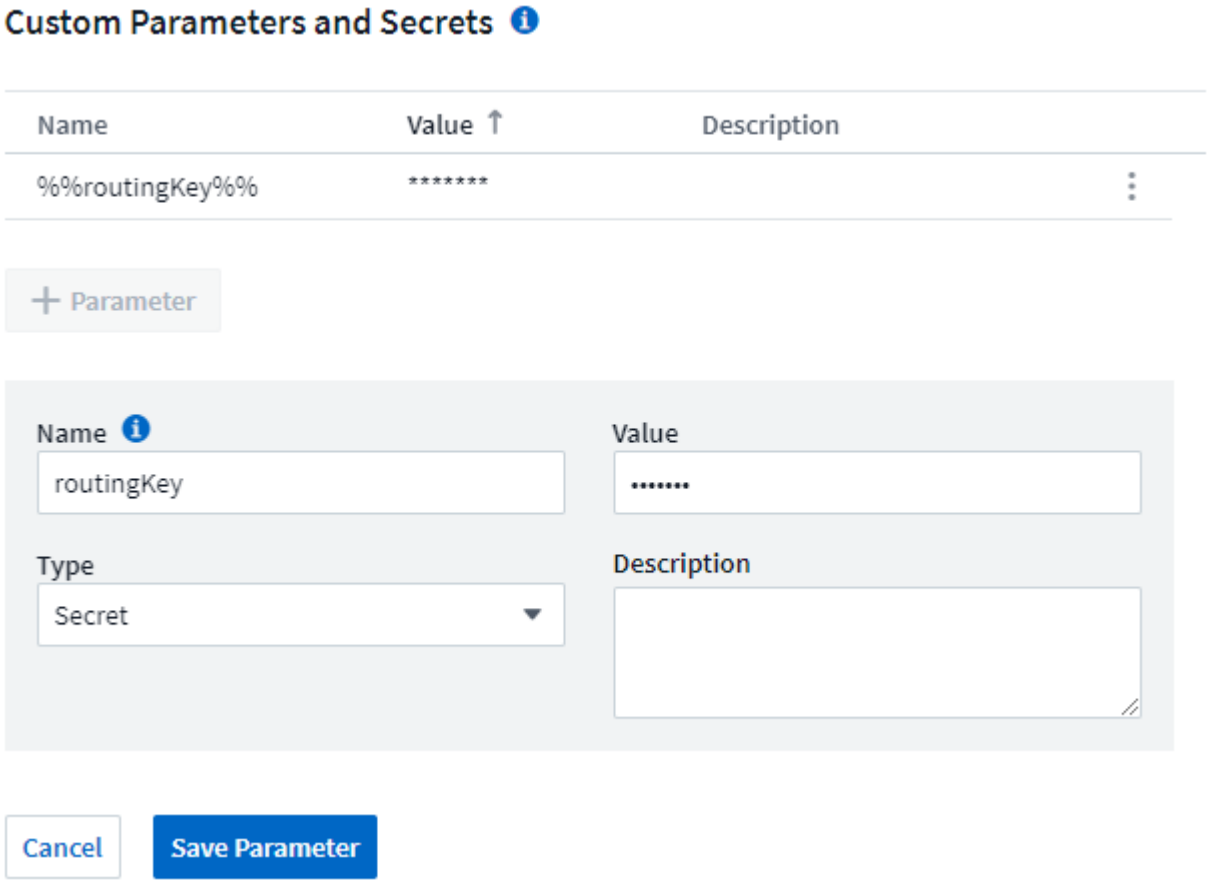


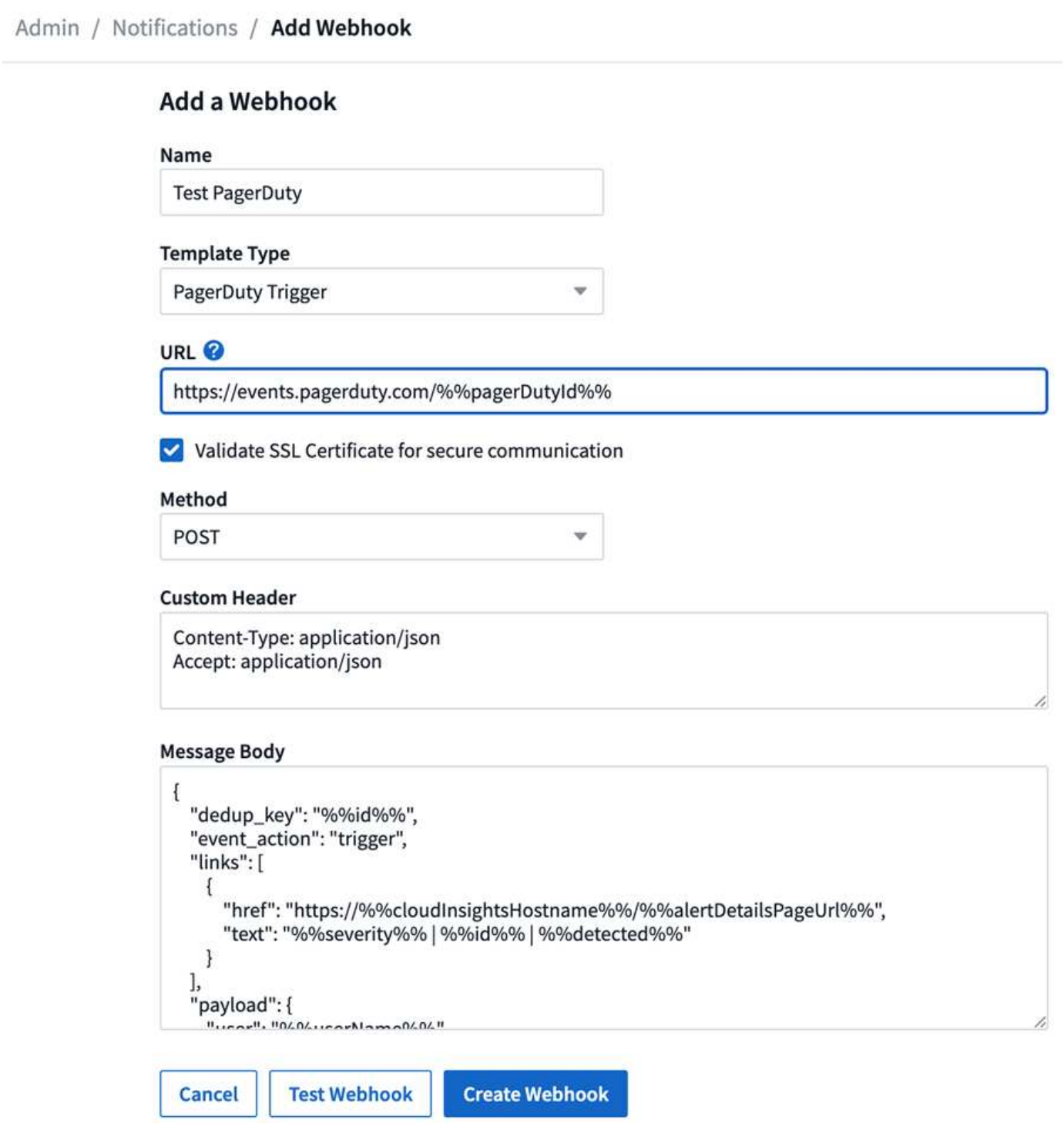
3. Sélectionnez l'onglet *Integrations* pour afficher la **clé d'intégration**. Vous aurez besoin de cette clé lorsque vous créez le webhook Workload Security ci-dessous.
4. Accédez à **incidents** ou **Services** pour afficher les alertes.



Créer Workload Security PagerDuty Webhook :

- Accédez à Admin > Notifications et sélectionnez l'onglet *Workload Security Webhooks*. Sélectionnez '+ Webhook' pour créer un nouveau webhook.
- Donnez un nom significatif au webhook.
- Dans la liste déroulante *Template Type*, sélectionnez *PagerDuty Trigger*.
- Créez un secret de paramètre personnalisé nommé *routingKey* et définissez la valeur sur PagerDuty *Integration Key* créée ci-dessus.

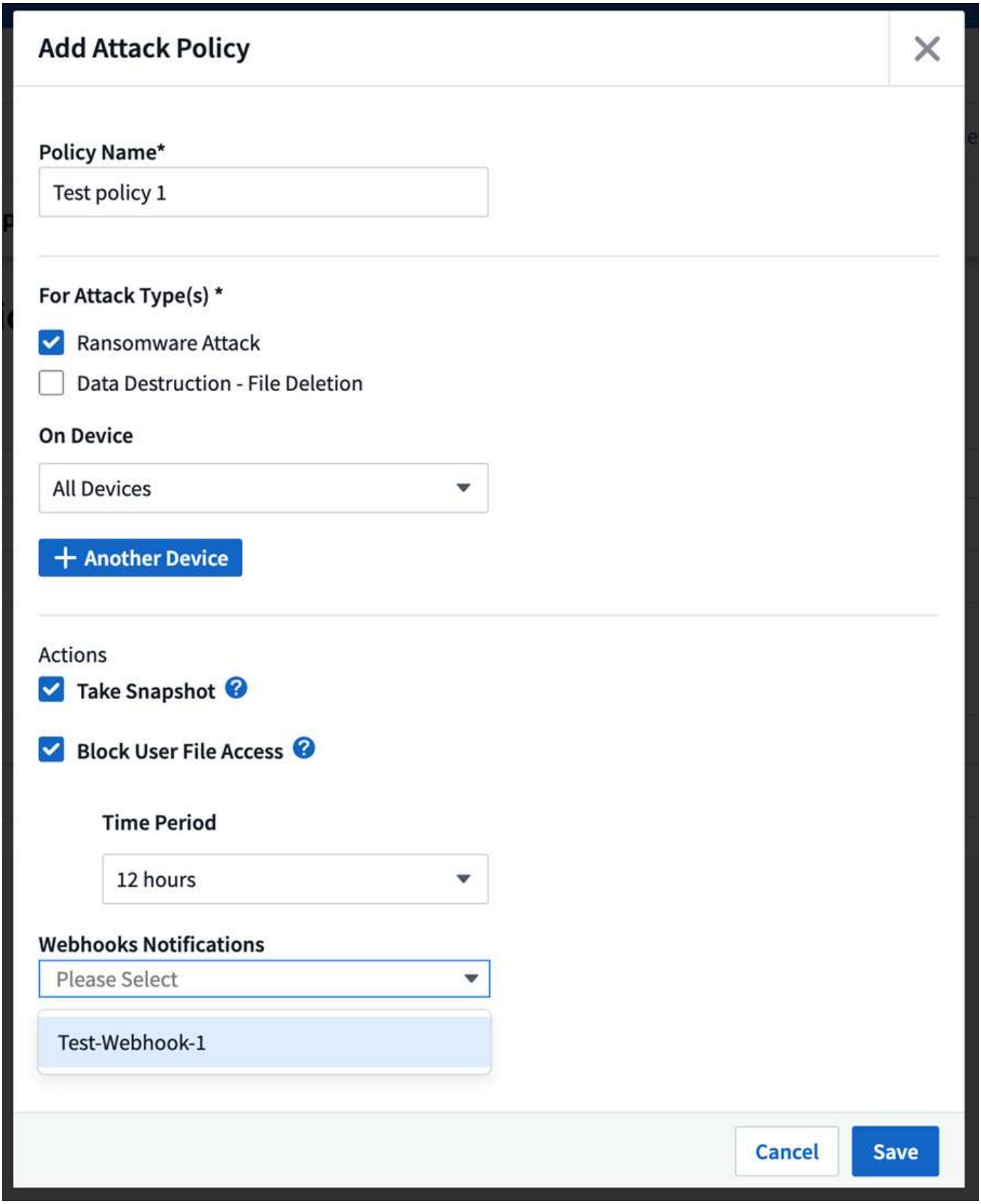




Notifications via Webhook

- Pour signaler des événements via Webhook, accédez à *Workload Security* > *Policies*. Sélectionnez *+Stratégie d'attaque* ou *+politique d'avertissement*.
- Entrez un nom de règle significatif.
- Sélectionnez le(s) type(s) d'attaque requis, les périphériques auxquels la stratégie doit être associée et les actions requises.
- Sous la liste déroulante *Webhooks Notifications*, sélectionnez les webhooks PagerDuty requis. Enregistrez la stratégie.

Remarque : les Webhooks peuvent également être associés à des stratégies existantes en les modifiant.



Exemple de Webhook pour Slack pour Workload Security

Les Webpatères permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal Web personnalisé. Cette page fournit un exemple de configuration des crochets pour le mou.

Cette page se réfère aux instructions de tiers, qui sont sujettes à modification. Reportez-vous à la documentation Slack pour obtenir les informations les plus récentes.

Exemple de mou

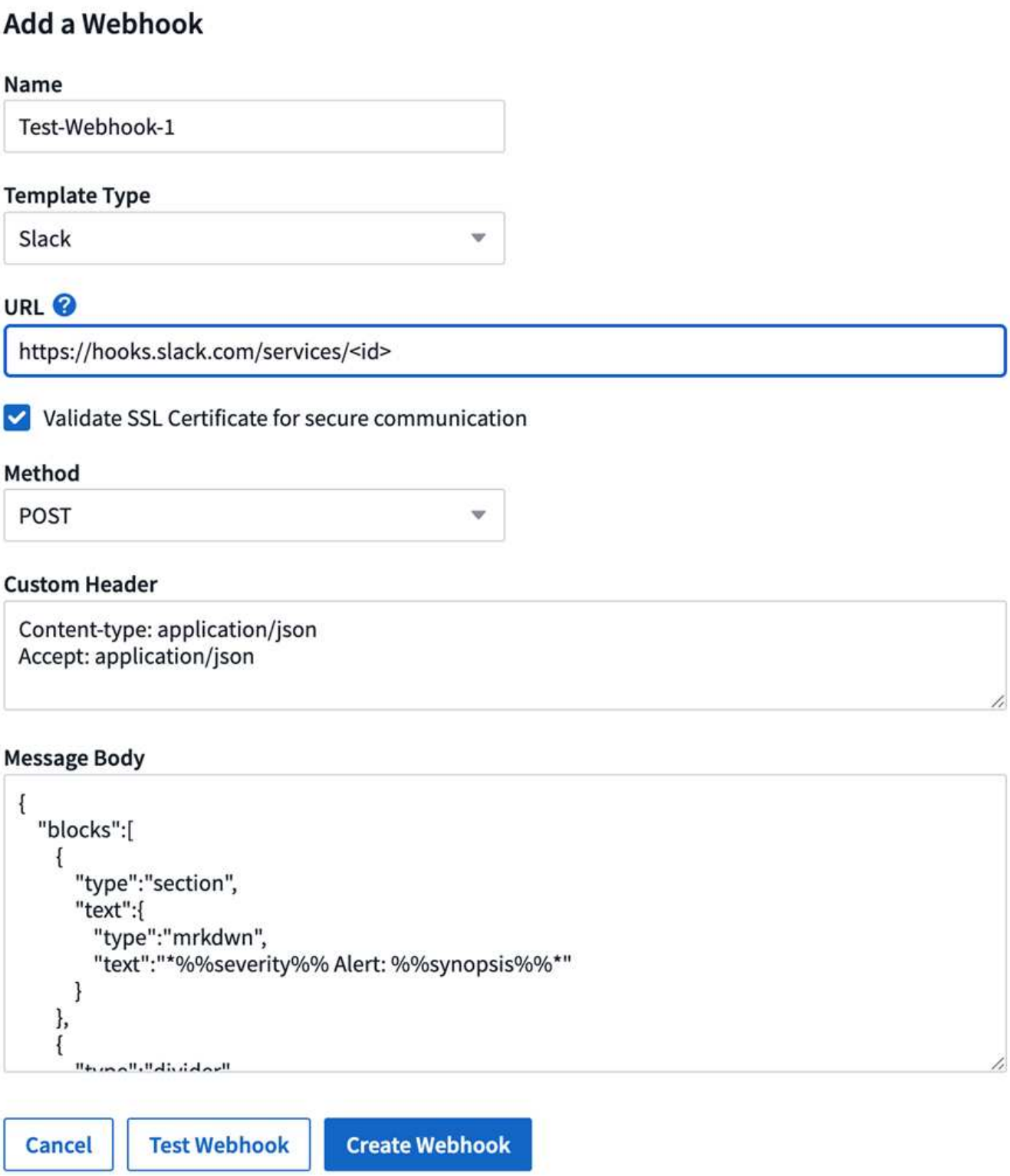
- Accédez à https://api.slack.com/apps et créez une nouvelle application Donnez-lui un nom significatif et sélectionnez un espace de travail.



- Allez dans les 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.

Créez Workload Security Slack Webhook

1. Accédez à Admin > Notifications et sélectionnez l'onglet *Workload Security Webhooks*. Sélectionnez + *Webhook* pour créer un nouveau webhook.
2. Donnez un nom significatif au webhook.
3. Dans la liste déroulante *Type de modèle*, sélectionnez *Slack*.
4. Collez l'URL copiée ci-dessus.

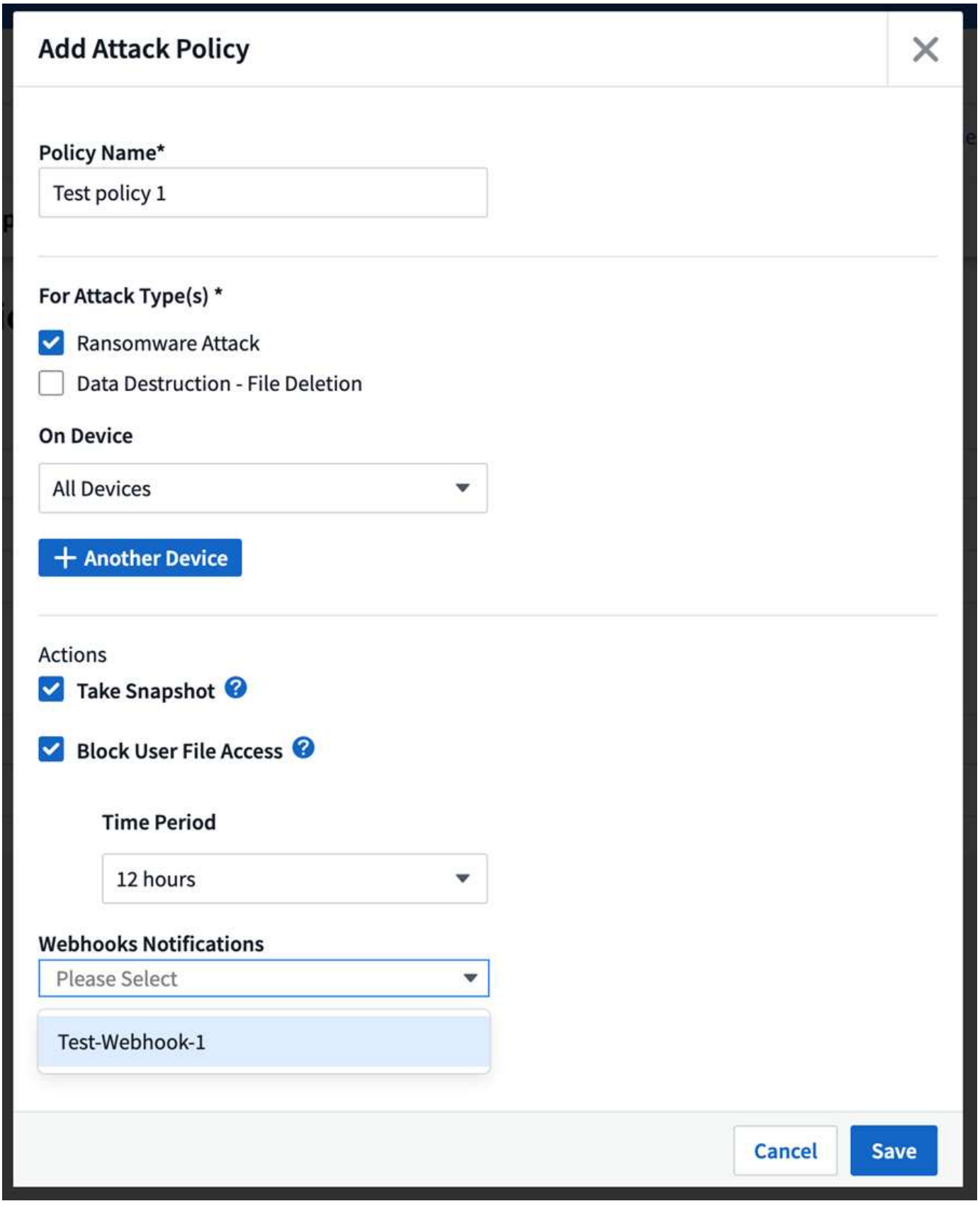


Notifications via webhook

- Pour signaler des événements via Webhook, accédez à *Workload Security* > *Policies*. Cliquez sur *+Stratégie d'attaque* ou *+politique d'avertissement*.
- Entrez un nom de règle significatif.
- Sélectionnez le(s) type(s) d'attaque requis, les périphériques auxquels la stratégie doit être associée et les actions requises.

- Dans la liste déroulante *Webhooks Notifications*, sélectionnez les webhooks requis. Enregistrez la stratégie.

Remarque : les Webhooks peuvent également être associés à des stratégies existantes en les modifiant.



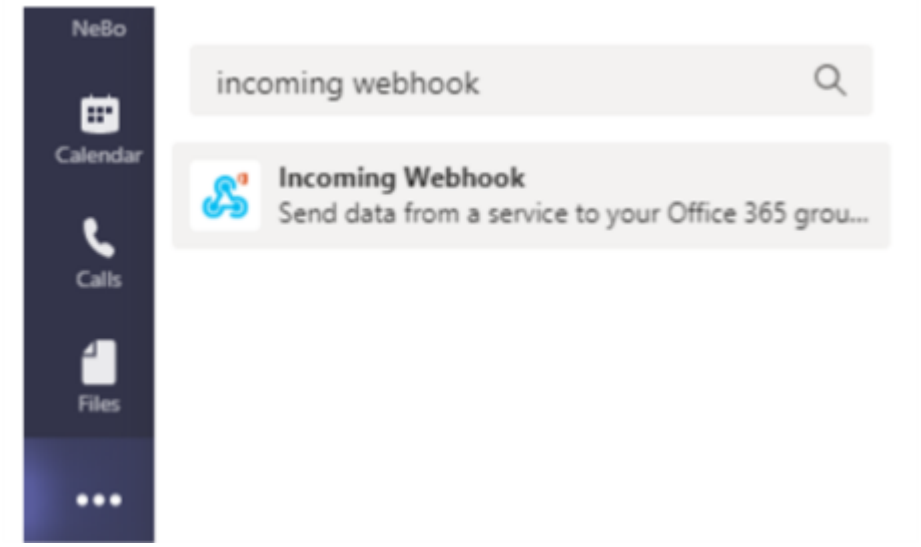
Exemple de Webhook de sécurité des charges de travail pour les équipes Microsoft

Les Webpatères permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal Web personnalisé. Cette page fournit un exemple de configuration des crochets pour les équipes.

Cette page se réfère aux instructions de tiers, qui sont sujettes à modification. Reportez-vous au "Documentation des équipes" pour obtenir les informations les plus récentes.

Configuration des équipes :

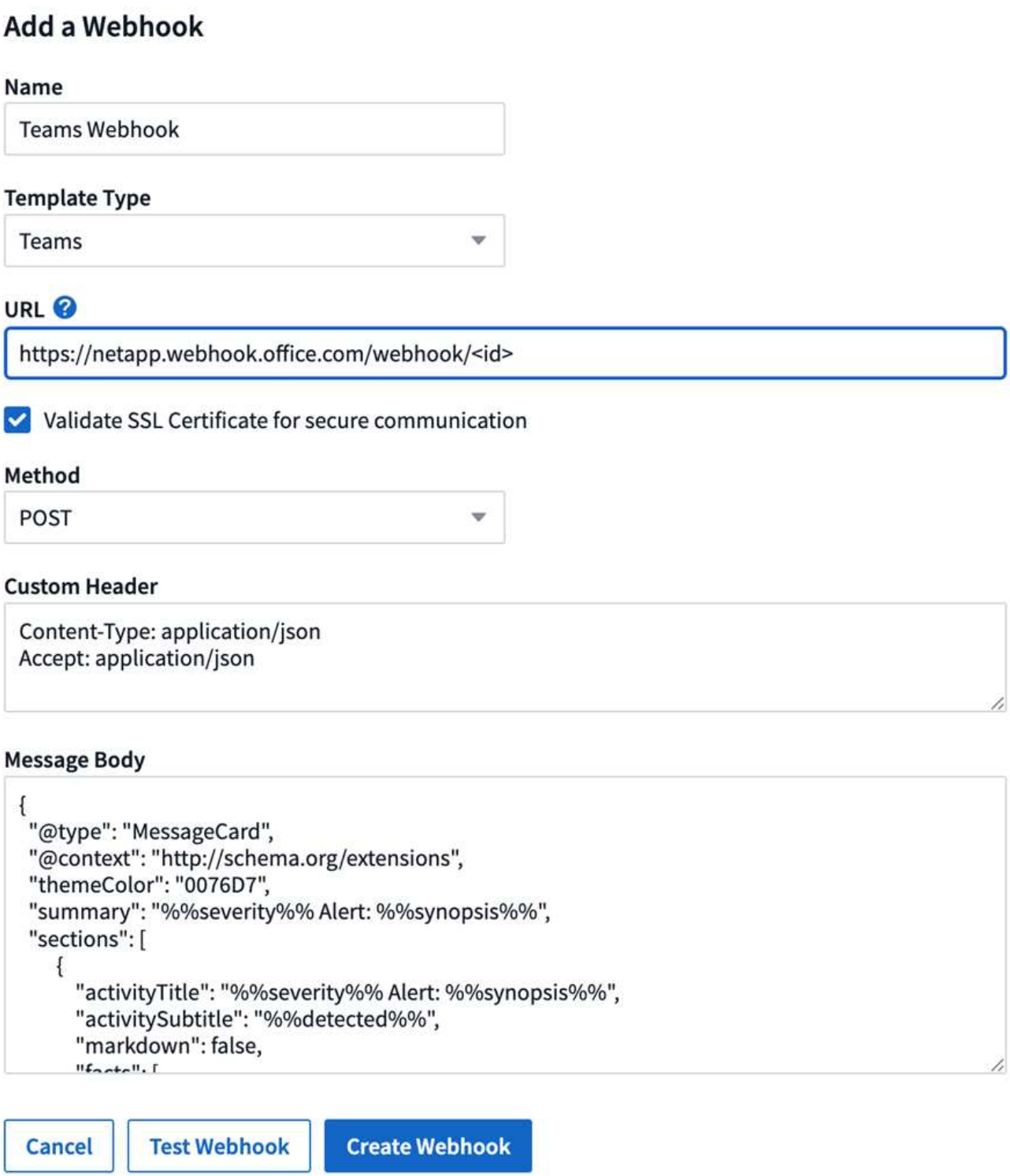
1. Dans Teams, sélectionnez le kebab et recherchez le Webhook entrant.



2. Sélectionnez **Ajouter à une association > Sélectionner une association > configurer un connecteur**.
3. Copiez l'URL du Webhook. Vous devez coller cette information dans la configuration du webhook de sécurité de la charge de travail.

Créer des équipes chargées de la sécurité des charges de travail Webhook :

1. Accédez à Admin > Notifications et sélectionnez l'onglet *« Workload Security Webhooks*. Sélectionnez *+ Webhook* pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif.
3. Dans la liste déroulante *Template Type*, sélectionnez **Teams**.



4. Collez l'URL ci-dessus dans le champ *URL*.

Notifications via Webhook

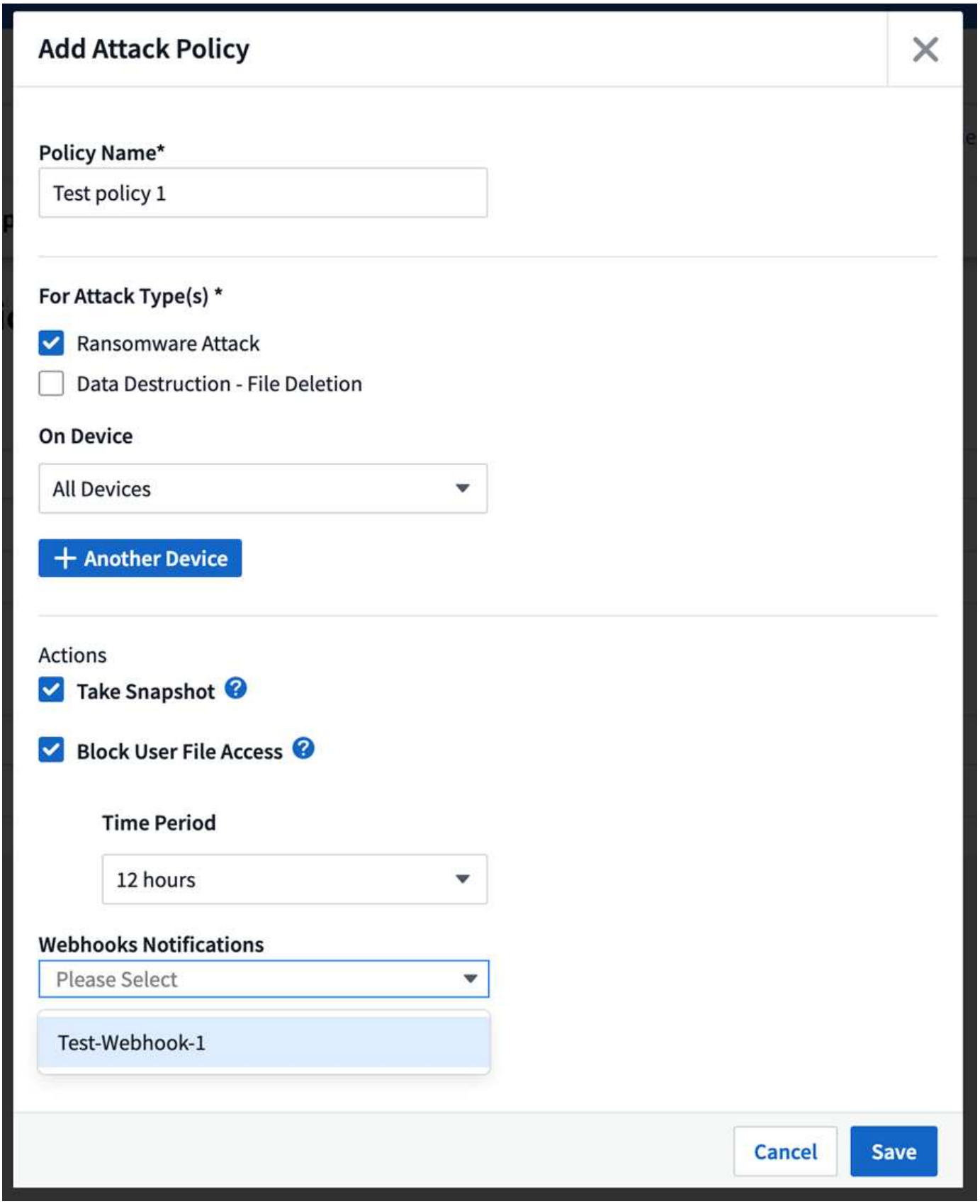
Pour signaler des événements via Webhook, accédez à *Workload Security > Policies*. Sélectionnez *+Stratégie d'attaque* ou *+politique d'avertissement*.

- Entrez un nom de règle significatif.
- Sélectionnez le(s) type(s) d'attaque requis, les périphériques auxquels la stratégie doit être associée et les

actions requises.

- Dans la liste déroulante *Webhooks Notifications*, sélectionnez les webhooks Teams requis. Enregistrez la stratégie.

Remarque : les Webhooks peuvent également être associés à des stratégies existantes en les modifiant.



API de sécurité du workload

L'API de sécurité des charges de travail permet aux clients NetApp et aux éditeurs de

logiciels indépendants d'intégrer la sécurité des charges de travail à d'autres applications, comme les CMDB ou d'autres systèmes de gestion des tickets.

Conditions requises pour l'accès à l'API :

- Un modèle de token d'accès API est utilisé pour accorder l'accès.
- La gestion des tokens API est effectuée par les utilisateurs de la sécurité de la charge de travail dotés du rôle d'administrateur.

Documentation API (swagger)

Pour obtenir les dernières informations sur l'API, connectez-vous à la sécurité de la charge de travail et accédez à **Admin > API Access**. Cliquez sur le lien **API Documentation**. La documentation de l'API est basée sur swagger, qui fournit une brève description et des informations d'utilisation pour 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 vers cette API, assurez-vous que les appels se produisent séquentiellement et non en parallèle. Plusieurs appels parallèles peuvent entraîner la temporisation de l'API.

Jetons d'accès à l'API

Avant d'utiliser l'API de sécurité de la charge de travail, 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 token d'accès :

- Cliquez sur **Admin > accès API**
- Cliquez sur **+jeton d'accès API**
- Saisissez **Nom de token**
- Spécifiez **expiration du token**

Votre jeton ne sera disponible que pour la copie dans le presse-papiers et l'enregistrement pendant le processus de création. Les tokens ne peuvent pas être récupérés après leur création. Il est donc fortement recommandé de les copier et de les enregistrer dans un emplacement sécurisé. Vous serez invité à cliquer sur le bouton Copier le token d'accès à l'API avant de pouvoir fermer l'écran de création du jeton.

Vous pouvez désactiver, activer et révoquer des jetons. Les tokens désactivés peuvent être activés.

Les tokens accordent un accès à usage général aux API du point de vue du client, ce qui permet de gérer l'accès aux API dans le cadre de leur propre locataire.

L'application reçoit un token d'accès après l'authentification et l'autorisation de l'accès, puis transmet le token d'accès en tant qu'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 l'étendue accordée lors de l'autorisation.

L'en-tête HTTP où le token d'accès est transmis est **X-CloudInsights-ApiKey:**

Par exemple, utilisez les éléments suivants pour récupérer des actifs 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.
```

Vous trouverez des informations détaillées dans le lien *API Documentation* sous **Admin > API Access**.

Script pour extraire les données via l'API

Les agents de sécurité de la charge de travail incluent un script d'exportation qui facilite les appels parallèles vers l'API v2 en divisant la plage de temps demandée en lots plus petits.

Le script se trouve à l'adresse */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
```

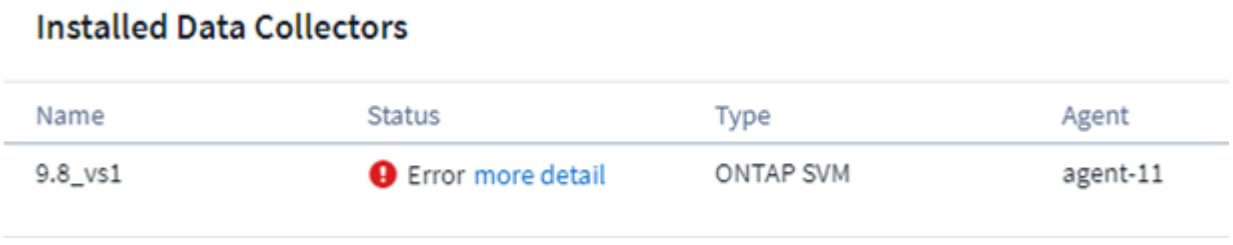
Paramètres clés `--iteration_interval 12` : -: fractionne la plage de temps demandée en intervalles de 12 heures. - `--num_workers 3`: Fetches ces intervalles en parallèle à l'aide de 3 threads.

Dépannage du Data Collector SVM ONTAP

La sécurité de la charge de travail utilise des collecteurs de données pour collecter les données d'accès des fichiers et des utilisateurs à partir de terminaux. Vous trouverez ici des conseils pour résoudre les problèmes liés à ce collecteur.

Reportez-vous "Configuration du SVM Collector"à la 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 *Etat* de la page collecteurs de données installés pour plus de détails sur l'erreur.



Les problèmes connus et leurs résolutions sont décrits ci-dessous.

Problème: Data Collector 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. Cause de la panne : serveur fpolicy externe surchargé. »

Essayez ceci: le taux d'événement de ONTAP était beaucoup plus élevé que ce que la boîte agent peut gérer. Par conséquent, la connexion a été interrompue.

Vérifiez le trafic maximal dans CloudSecure lorsque la déconnexion s'est produite. Vous pouvez effectuer cette vérification à partir de la page **CloudSecure > activités approfondies > toutes les activités**.

Si le pic de trafic agrégé est supérieur à ce que l'Agent Box peut traiter, reportez-vous à la page Event Rate Checker sur la taille du déploiement collecteur dans une boîte d'agent.

Si l'agent a été installé dans la zone Agent avant le 4 mars 2021, exécutez les commandes suivantes dans la zone 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.

Problème: le Collector signale un message d'erreur: "Aucune adresse IP locale trouvée sur le connecteur qui peut atteindre les interfaces de données du SVM". **Essayez ceci:** Ceci est probablement dû à un problème de mise en réseau côté ONTAP. Procédez comme suit :

1. S'assurer qu'il n'y a aucun pare-feu sur la lif de données du SVM ou la lif de gestion qui bloquent la connexion de la SVM.
2. Lors de l'ajout d'un SVM via une IP de gestion de cluster, veillez à ce que la lif de données et la lif de gestion du SVM soient pingables depuis la VM Agent. En cas de problème, vérifier la passerelle, le masque de réseau et les routes de la lif.

   Vous pouvez également essayer de vous connecter au cluster via ssh à l'aide de l'IP de gestion de cluster et envoyer une requête ping à l'IP de l'agent. Assurez-vous que l'adresse IP de l'agent peut faire l'objet d'un ping :

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif
   <Lif Name> -show-detail
   ```

   Si vous ne pouvez pas effectuer de ping, assurez-vous que les paramètres réseau dans ONTAP sont corrects, de sorte que l'ordinateur de l'agent puisse effectuer des requêtes ping.
3. Si vous avez essayé de vous connecter via Cluster IP et qu'il ne fonctionne pas, essayez de vous connecter directement via SVM IP. Voir ci-dessus pour les étapes de connexion via SVM IP.
4. Lors de l'ajout du collecteur via les identifiants SVM IP et vsadmin, vérifier si le rôle Data plus Mgmt est activé dans la LIF du SVM. Dans ce cas, le ping vers la LIF du SVM va fonctionner, mais SSH vers la LIF du SVM ne fonctionnera pas. Si oui, créer une LIF SVM Mgmt uniquement et tenter de se connecter via cette LIF de management SVM uniquement.
5. Si cela ne fonctionne toujours pas, créer une nouvelle LIF du SVM et essayer de se connecter via cette LIF. Vérifiez que le masque de sous-réseau est correctement défini.
6. Débogage avancé :
   a. Démarrez une trace de paquet dans ONTAP.
   b. Essayez de connecter un collecteur de données au SVM à partir de l'interface utilisateur CloudSecure.
   c. Attendez que l'erreur s'affiche. Arrêtez la trace de paquet dans ONTAP.
   d. Ouvrez la trace de paquet à partir de ONTAP. Il est disponible à cet endroit

      ```
       https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_trac
      es/
      .. Assurez-vous qu'il y a un SYN de ONTAP dans la zone Agent.
      .. S'il n'y a pas de SYN dans ONTAP, il s'agit d'un problème
      avec le pare-feu dans ONTAP.
      .. Ouvrez le pare-feu dans ONTAP, afin que ONTAP puisse
      connecter le boîtier de l'agent.
      ```
7. S'il ne fonctionne toujours pas, veuillez consulter l'équipe réseau pour vous assurer qu'aucun pare-feu externe ne bloque la connexion entre ONTAP et le boîtier Agent.

8. Si aucune des solutions ci-dessus ne résout le problème, ouvrez un dossier auprès de "Support NetApp" pour obtenir de l'aide.

Problème: message: "Impossible de déterminer le type de ONTAP pour [nom d'hôte: <IP Address>. Raison : erreur de connexion à l'<IP Address> du système de stockage : l'hôte est inaccessible (hôte inaccessible) » **essayez ceci :**

1. Vérifier que l'adresse IP de gestion du SVM ou l'adresse IP de gestion du cluster correcte a été fournie.
2. SSH vers le SVM ou le Cluster auquel vous prévoyez de vous connecter. Une fois connecté, assurez-vous que le SVM ou le nom du cluster est correct.

Problème: message d'erreur: "Le connecteur est en état d'erreur. service.name: Vérification. Cause de la panne : le serveur fpolicy externe est terminé. » **Essayez ceci:**

1. Il est très probable qu'un pare-feu bloque les ports nécessaires sur la machine agent. Vérifier que la plage de ports 35000-55000/tcp est ouverte pour que l'ordinateur agent se connecte à partir du SVM. Assurez-vous également qu'aucun pare-feu n'est activé à partir du blocage de la communication côté ONTAP vers l'agent.
2. Entrez la commande suivante dans la zone Agent et assurez-vous que la plage de ports est ouverte.

   ```
   sudo iptables-save | grep 3500*
   ```

   La sortie de l'échantillon doit ressembler à :

   ```
    -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack
   -ctstate NEW -j ACCEPT
   . Connectez-vous au SVM, entrez les commandes suivantes et vérifiez
   qu'aucun pare-feu n'est défini pour bloquer la communication avec
   ONTAP.
   ```

   ```
   system services firewall show
   system services firewall policy show
   ```

   "Vérifiez les commandes du pare-feu" Du côté ONTAP.

3. Connectez-vous au SVM/Cluster que vous souhaitez surveiller en SSH. Envoyer un ping au boîtier Agent depuis la lif de données du SVM (avec prise en charge des protocoles CIFS, NFS) et vérifier que le ping fonctionne :

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif
   <Lif Name> -show-detail
   ```

   Si vous ne pouvez pas effectuer de ping, assurez-vous que les paramètres réseau dans ONTAP sont corrects, de sorte que l'ordinateur de l'agent puisse effectuer des requêtes ping.

4. Si un seul SVM est ajouté deux fois à un locataire via 2 collecteurs de données, cette erreur s'affiche. 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 affiche l'état « EN COURS d'EXÉCUTION » et commence à recevoir des événements du SVM.

   En réalité, dans un locataire, 1 SVM ne doit être ajouté qu'une seule fois, via 1 Data Collector. 1 SVM ne doit pas être ajouté deux fois via 2 collecteurs de données.

5. Lorsque le même SVM a été ajouté dans deux environnements Workload Security (tenants) différents, le dernier réussira toujours. Le second collecteur configure fpolicy avec sa propre adresse IP et commence le lancement du premier. Ainsi, le collecteur du premier arrête de recevoir des

événements et son service d'audit passe en état d'erreur. Pour éviter cela, configurer 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 Data Source Collector, le service client Data-fpolicy est requis avec le service de données Data-nfs et/ou Data-cifs. De plus, le service data-fpolicy-client doit être associé aux lif de données pour le SVM surveillé.

Problème: aucun événement vu dans la page d'activité. **Essayez ceci:**

1. Vérifiez si le collecteur ONTAP est à l'état « EN COURS D'EXÉCUTION ». Si oui, assurez-vous alors que certains événements cifs sont générés sur les machines virtuelles client cifs en ouvrant certains fichiers.
2. Si aucune activité n'est visible, veuillez vous connecter au SVM et saisir la commande suivante.

   ```
   <SVM>event log show -source fpolicy
   ```

   Assurez-vous qu'il n'y a pas d'erreur liée à fpolicy.

3. Si aucune activité n'est constatée, veuillez vous connecter au SVM. Saisissez la commande suivante :

   ```
   <SVM>fpolicy show
   ```

   Vérifiez si la politique fpolicy nommée avec le préfixe « cloudsecure_ » a été définie et que le statut est « activé ». Si non défini, 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.

Problème: le Data Collector SVM est en état d'erreur et le message d'erreur est "l'agent n'a pas pu se connecter au collecteur" **essayez ceci:**

1. L'agent est probablement surchargé et ne peut pas se connecter aux collecteurs de la source de données.
2. Vérifiez le nombre de collecteurs de sources de données 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 très élevé, installez un autre agent et déplacez certains des collecteurs de sources de données vers le nouvel agent.

Problème: le Data Collector SVM affiche le message d'erreur comme "fpolicy.server.connectError: nœud n'a pas pu établir de connexion avec le serveur FPolicy "12.195.15.146" (motif: "Select Timed out")" **essayez ceci:** le pare-feu est activé dans SVM/Cluster. Le moteur fpolicy ne peut donc pas se connecter au serveur fpolicy. Les interfaces de ligne de commande de ONTAP qui peuvent être utilisées pour obtenir plus d'informations sont les suivantes :

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"Vérifiez les commandes du pare-feu" Du côté ONTAP.

Problème: message d'erreur: "Le connecteur est en 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 : up) trouvée sur le SVM ». **Essayez ceci:** Assurez-vous qu'il existe une interface opérationnelle (ayant le rôle de protocole de données et de données comme CIFS/NFS.

Problème: le collecteur de données passe à l'état d'erreur et passe ensuite 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 sont ajoutés.
2. Les collecteurs de données qui montrent ce type de comportement auront 1 SVM ajouté à ces collecteurs de données. Signification : 2 collecteurs de données ou plus sont connectés à 1 SVM.
3. Assurez-vous que 1 collecteur de données se connecte à 1 seul SVM.
4. Supprimer les autres collecteurs de données qui sont connectés au même SVM.

Problème : le connecteur est en état d'erreur. Nom du service : audit. Motif de l'échec : échec de la configuration (politique sur la SVM svmname. Raison : valeur non valide spécifiée pour l'élément « shares-to-include » dans « fpolicy.policy.scope-modify : « Federal » **essayez ceci :** *les noms de partage doivent être donnés sans guillemets. Modifiez la configuration du SVM DSC de ONTAP pour corriger les noms de partage.

Inclure et exclure des partages n'est pas destiné à une longue liste de noms de partage. Utilisez le filtrage par volume à la place si vous avez un grand nombre de partages à inclure ou exclure.

Problème : il existe dans le cluster des stratégies de gestion de polices qui ne sont pas utilisées. Que faut-il faire avant l'installation de la sécurité des charges de travail ? **Essayez ceci:** il est recommandé de supprimer tous les paramètres fpolicy inutilisés existants, même s'ils sont déconnectés. La sécurité des charges de travail crée fpolicy avec le préfixe « cloudSecure_ ». Toutes les autres configurations fpolicy non utilisées peuvent être supprimées.

Commande CLI pour afficher la liste fpolicy :

```
 fpolicy show
Étapes de suppression des 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>
```

|après l'activation de la sécurité des charges de travail, les performances de ONTAP sont affectées : la latence devient de façon sporadique, les IOPS sont réduites de façon sporadique. |lors de l'utilisation de ONTAP avec la sécurité des charges de travail, des problèmes de latence sont parfois visibles dans ONTAP. Il y a un certain nombre de raisons possibles pour cela, comme indiqué dans les points suivants : "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.

Problème: le collecteur de données est en erreur, affiche ce message d'erreur. "Erreur : le connecteur est en état d'erreur. Nom du service : audit. Motif de l'échec : échec de la configuration de la règle sur le SVM svm_test. Motif : valeur manquante pour le champ zapi : événements. " **Essayez ceci:**

1. Commencez par un nouveau SVM avec uniquement le service NFS configuré.
2. Ajoutez un collecteur de données SVM ONTAP dans la sécurité des charges de travail. CIFS est configuré en tant que protocole autorisé pour la SVM lors de l'ajout du SVM Data Collector de ONTAP dans Workload Security.
3. Attendez que le collecteur de données de la sécurité de la charge de travail affiche une erreur.
4. Étant donné que le serveur CIFS n'est PAS configuré sur le SVM, cette erreur comme indiquée sur la gauche est indiquée par Workload Security.
5. Modifiez le collecteur de données du SVM ONTAP et décochez la case CIFS en tant que protocole autorisé. Enregistrer le collecteur de données. Il démarre alors que seul le protocole NFS est activé.

Problème : Data Collector affiche le message d'erreur : "erreur : échec de la détermination de l'intégrité du collecteur dans les 2 tentatives, essayez de redémarrer le collecteur (Code d'erreur : AGENT008)". **Essayez ceci:**

1. Sur la page collecteurs de données, faites défiler l'écran vers la droite du collecteur de données donnant l'erreur et cliquez sur le menu 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 *Save*. Data Collector redémarre et l'erreur doit être résolue.
2. La machine Agent peut ne pas disposer de suffisamment de ressources CPU ou RAM, c'est pourquoi les DSC sont défaillants. Veuillez vérifier le nombre de collecteurs de données ajoutés à l'agent de la machine. Si elle est supérieure à 20, augmentez la capacité CPU et RAM de l'ordinateur Agent. Une fois l'UC et la RAM augmentées, les DSC sont en cours d'initialisation, puis s'exécutent automatiquement. Consultez le guide de dimensionnement sur "cette page".

Problème: le Data Collector est en erreur lorsque le mode SVM est sélectionné. **Essayer ceci:** lors de la connexion en mode SVM, si l'IP de gestion du cluster est utilisée pour se connecter à la place de l'IP de gestion du SVM, alors la connexion sera erronée. S'assurer que l'IP de SVM correct est utilisé.

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 : la configuration de fpolicy sur le svm test_svm a échoué. Raison : l'utilisateur n'est pas autorisé. » **Essayez ceci:** l'utilisateur manque peut-être les autorisations de REPOS nécessaires pour la fonction accès refusé. Veuillez suivre les instructions de la section "cette page" pour définir les autorisations.

Redémarrez le collecteur une fois les autorisations définies.

Si vous rencontrez toujours des problèmes, accédez aux liens d'assistance mentionnés dans la page **aide > support**.

Dépannage

Résolution des problèmes liés à l'analyse générale de l'infrastructure de données

Vous trouverez ici des suggestions de dépannage pour Data Infrastructure Insights.

Voir aussi "Dépannage des problèmes d'unité d'acquisition Linux" et "Dépannage des problèmes d'unité d'acquisition Windows".

Problèmes de connexion

Problème:	Essayez ceci:
Data Infrastructure Insights se déconnecte automatiquement toutes les 6 heures	Ceci est dû aux cookies tiers désactivés du navigateur. Les utilisateurs peuvent configurer leur navigateur pour activer tous les cookies tiers ou utiliser une liste d'exceptions plus étroite pour activer uniquement ceux de 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 se charge du même format pour les exceptions que Chrome. Dans Firefox, les exceptions relatives aux cookies sont désignées simplement par *auth0.com* et *netapp.com*.
Je dispose d'un compte BlueXP, mais je ne peux pas me connecter à BlueXP.	Ouvrez un ticket à partir de https://mysupport.netapp.com/site/help. Sélectionnez la catégorie « blueXP.netapp.com > problèmes de compte/connexion » ou « bluexp.netapp.com > problèmes de fédération ». Ces solutions répondent spécifiquement aux problèmes et aux questions concernant BlueXP. Pour tout autre problème de support technique concernant Data Infrastructure Insights, contactez "Support NetApp".
J'ai été invité à Data Infrastructure Insights, mais je reçois un message « non autorisé ».	Vérifiez que vous avez créé un compte BlueXP ou que votre entreprise utilise la connexion SSO avec BlueXP. Vérifiez que l'adresse e-mail de votre profil BlueXP correspond à celle indiquée dans l'e-mail de bienvenue informations sur votre infrastructure de données. Si l'e-mail ne correspond pas, demandez une nouvelle invitation avec l'adresse e-mail correcte.
Je me suis déconnecté de BlueXP et ai été automatiquement déconnecté de Data Infrastructure Insights.	L'authentification unique (SSO) pour tous les services cloud NetApp déconnecte toutes les sessions d'informations d'infrastructure de données. Si vous avez accès à plusieurs comptes Data Infrastructure Insights, la déconnexion de n'importe quel compte déconnecte toutes les sessions actives. Reconnectez-vous pour accéder à votre compte.

Problème:	Essayez ceci:
J'ai été automatiquement déconnecté après plusieurs jours.	Les comptes cloud NetApp requièrent une nouvelle authentification tous les deux ou trois jours (la configuration actuelle de BlueXP est de 7 jours). Reconnectez-vous pour accéder à votre compte.
Je reçois un message d'erreur "n'est plus autorisé à se connecter".	Contactez votre administrateur de compte pour vérifier l'accès à Data Infrastructure Insights. Vérifiez que l'adresse e-mail de votre profil BlueXP correspond à celle indiquée dans l'e-mail de bienvenue informations sur votre infrastructure de données
Autres erreurs de connexion	Essayez le mode incognito dans Chrome ou effacez l'historique du navigateur, les cookies et le cache. Essayez avec un autre profil de navigateur (c.-à-d. Chrome - ajouter personne).

Autres questions

Question:	Réponse:
Mes quotas matériels Qtree s'affichent correctement dans les requêtes, mais mes quotas souples s'affichent comme capacité totale du volume. Est-ce correct ?	Seuls les quotas matériels, définis manuellement ou définis via Trident, s'afficheront comme quotas définis ; si aucun quota matériel n'est spécifié, la capacité du volume interne sera la capacité du volume.
J'ai à la fois un quota souple et un quota matériel définis manuellement dans le même qtree, mais la capacité totale affichée est le quota dur ; est-ce correct ?	Oui, si un quota matériel est spécifié, il s'affichera comme la capacité totale.
Lors de la saisie d'un horaire de rapport Cognos, parfois, je me termine par un "m" supplémentaire dans l'horaire. Par exemple, si j'entre l'heure « 02:15 PM », il peut ajouter un caractère supplémentaire : « 02:15 PMM » (ou PMM). Lorsque je clique à l'extérieur, il passe à « 2:15 AM ». Je suis capable d'enregistrer le rapport, mais lorsque je rouvre le rapport enregistré, l'heure de planification apparaît comme AM (c'est-à-dire matin), que je saisis AM ou PM dans l'heure de planification.	Entrez à nouveau l'heure programmée en veillant à ne pas entrer les caractères « AM » ou « PM » ; il suffit de taper « A » pour « AM » ou « P » pour « PM ». Si le caractère supplémentaire n'est pas affiché, l'heure de programmation sera définie correctement.

Ressources

Vous trouverez d'autres conseils de dépannage dans le "Base de connaissances NetApp" (connexion à l'assistance requise).

Des informations de support supplémentaires sont disponibles sur la page Data Infrastructure Insights"Assistance".

Si vous disposez d'un abonnement actif à Data Infrastructure Insights, vous pouvez utiliser les options de support suivantes :

"Téléphone" "Ticket de support"

Pour plus d'informations, voir "Documentation de support des informations sur l'infrastructure de données".

Dépannage des problèmes d'unité d'acquisition sous Linux

Vous trouverez ici des suggestions de dépannage des problèmes liés aux unités d'acquisition sur un serveur Linux.

Problème:	**Essayez ceci:**
Le statut au sur la page **observabilité > collecteurs** de l'onglet **unités d'acquisition** affiche "certificat expiré" ou "certificat révoqué" .	Cliquez sur le menu à droite de l'UA et sélectionnez **Restaurer la connexion**. Suivez les instructions pour restaurer votre unité d'acquisition : 1. Arrêtez le service de l'unité d'acquisition (au). Vous pouvez cliquer sur le bouton *Copy Stop Command* pour copier rapidement la commande dans le presse-papiers, puis la coller dans une invite de commande sur la machine d'acquisition. 2. Créez un fichier nommé "token" dans le dossier */var/lib/NetApp/cloudInsights/acq/conf* de l'au. 3. Cliquez sur le bouton *Copier le token* et collez ce token dans le fichier que vous avez créé. 4. Redémarrez le service AU. Cliquez sur le bouton *Copy Restart Command* et collez la commande dans une invite de commande sur l'au.
Autorisation refusée lors du démarrage du service du serveur d'unité d'acquisition	Lorsque l'au est installé sur SELINUX, le se doit être réglé sur *permissive* mode. *Appliquer* mode n'est pas pris en charge. Après avoir défini SELINUX en mode permissif, redémarrez le service au. "En savoir plus >>".
Configuration serveur non respectée	Assurez-vous que votre serveur d'unité d'acquisition ou votre VM se rencontrent "de formation"
Configuration réseau non respectée	Assurez-vous que le serveur/la machine virtuelle de votre 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 depuis l'infrastructure de données sortantes.

Le serveur proxy n’est pas configuré correctement	Vérifiez les paramètres de votre proxy et désinstallez/réinstallez le logiciel de l’unité d’acquisition si nécessaire pour entrer les paramètres de proxy corrects. 1. Essayez de « boucler ». Reportez-vous aux informations/documentation sur "boucle homme" concernant les proxys : --préproxy, --proxy-* (c’est un caractère générique "*" car Curl prend en charge de nombreux paramètres proxy). 2. Essayez « wget ». Consultez la documentation pour connaître les options du proxy.
L’installation de l’unité d’acquisition a échoué dans Data Infrastructure Insights avec des erreurs 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/fichier manquant introuvable	Assurez-vous que votre serveur/VM Linux acquisition Unit dispose de toutes les bibliothèques nécessaires. Par exemple, la bibliothèque *unzip* doit être 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*
Acquisition non en cours d’exécution :	Collectez les acq.log de /opt/netapp/cloudInsights/acq/logs (Linux) redémarrez le service d’acquisition : sudo cloudinsights-service.sh redémarrez l’acquisition
Problèmes de collecte de données :	Envoyez un rapport d’erreur à partir de la page d’accueil du Data Collector en cliquant sur le bouton « Envoyer un rapport d’erreur »
État : échec du signal de détection	L’unité d’acquisition (au) envoie un signal de détection 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 si Data Infrastructure Insights ne répond pas, l’heure de bail de l’au n’est pas mise à jour. Lorsque la durée de bail de l’au expire, Data Infrastructure Insights affiche l’état « échec de Heartbeat ». Étapes de dépannage : vérifiez la connexion réseau entre l’unité d’acquisition et CloudInsights. Vérifiez si le service de l’unité d’acquisition est en cours d’exécution. Si le service n’est pas en cours d’exécution, démarrez-le. Consultez le journal des unités d’acquisition (/var/log/netapp/cloudInsights/acq/acq.log) pour vérifier s’il y a des erreurs.

Je vois un message « erreur Heartbeat : »	Cette erreur peut se produire en cas d'interruption du réseau entraînant l'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: File context for /opt/NetApp/cloudInsights(/.*)? Déjà défini".	Sur un système avec SELinux, ce message d'erreur peut apparaître après l' `cloudinsights-uninstall.sh -p`exécution de a et la réinstallation de l'unité d'acquisition. L'exécution de la commande `semanage fcontext -d -t usr_t "/opt/netapp/cloudinsights(/.*)?"` doit corriger le problème et supprimer le message.

Considérations sur Proxies et pare-feu

Si votre entreprise a besoin d'un proxy pour accéder à Internet, vous devrez peut-être comprendre le comportement du proxy de votre entreprise et rechercher certaines exceptions pour que Data Infrastructure Insights fonctionne. Gardez à l'esprit les éléments suivants :

- Tout d'abord, votre organisation bloque-t-elle l'accès par défaut et autorise-t-elle uniquement l'accès à des sites ou domaines Web spécifiques par exception ? Si c'est le cas, vous devrez ajouter le domaine suivant à la 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 effectuées sur les hôtes portant ce nom de domaine.

- Deuxièmement, certains proxys tentent d'effectuer une inspection TLS/SSL en usurpant l'identité 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, à l'exception de cette fonctionnalité, pour que l'unité d'acquisition Data Infrastructure Insights se connecte avec succès à Data Infrastructure Insights et facilite la découverte des données.

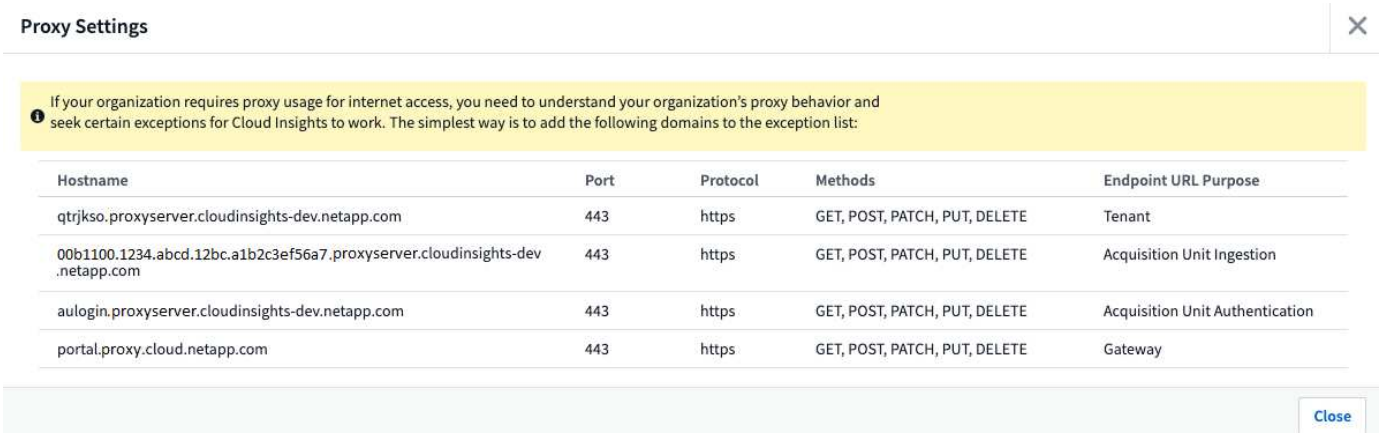
Si le proxy est configuré pour l'inspection du trafic, l'environnement Data Infrastructure Insights doit être ajouté à une liste d'exceptions dans la configuration du proxy. Le format et la configuration de cette liste d'exceptions varient en fonction de votre environnement proxy et de vos outils, mais 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 façon la plus simple d'y parvenir consiste à ajouter le domaine Data Infrastructure Insights lui-même à la liste d'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 nécessaire ou non. Si vous n'êtes pas sûr de savoir si vous avez besoin d'ajouter Data Infrastructure Insights à une liste d'exceptions, ou si vous rencontrez des difficultés à installer ou à exécuter Data Infrastructure Insights en raison de la configuration du proxy et/ou du pare-feu, contactez votre équipe d'administration proxy pour configurer la gestion de l'interception SSL par le proxy.
```

Affichage des noeuds finaux du proxy

Vous pouvez afficher vos noeuds finaux proxy en cliquant sur le lien **Paramètres proxy** lorsque vous choisissez un collecteur de données pendant l'intégration, ou sur le lien sous *Paramètres proxy* de la page **aide > support**. Un tableau comme celui ci-dessous s'affiche. Si vous avez la sécurité de la charge de travail dans votre environnement, les URL de point final configurées s'affichent également dans cette liste.



Ressources

Vous trouverez d'autres conseils de dépannage dans le "Base de connaissances NetApp" (connexion à l'assistance requise).

Des informations de support supplémentaires sont disponibles sur la page Data Infrastructure Insights"Assistance".

Dépannage des problèmes d'unité d'acquisition sous Windows

Vous trouverez ici des suggestions de dépannage des problèmes liés aux unités d'acquisition sur un serveur Windows.

Problème:	Essayez ceci:

Le statut au sur la page **observabilité > collecteurs** de l'onglet **unités d'acquisition** affiche "certificat expiré" ou "certificat révoqué" .	Cliquez sur le menu à droite de l'UA et sélectionnez **Restaurer la connexion**. Suivez les instructions pour restaurer votre unité d'acquisition : 1. Arrêtez le service de l'unité d'acquisition (au). Vous pouvez cliquer sur le bouton *Copy Stop Command* pour copier rapidement la commande dans le presse-papiers, puis la coller dans une invite de commande sur la machine d'acquisition. 2. Créez un fichier nommé « token » dans le dossier *c:\Program Files\Cloud Insights\acquisition Unit\conf* sur le dossier au. 3. Cliquez sur le bouton *Copier le token* et collez ce token dans le fichier que vous avez créé. 4. Redémarrez le service AU. Cliquez sur le bouton *Copy Restart Command* et collez la commande dans une invite de commande sur l'au.
Configuration serveur non respectée	Assurez-vous que votre serveur d'unité d'acquisition ou votre VM se rencontrent "de formation"
Configuration réseau non respectée	Assurez-vous que le serveur/la machine virtuelle de votre 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 depuis l'infrastructure de données sortantes.
Le serveur proxy n'est pas configuré correctement	Vérifiez les paramètres de votre proxy et désinstallez/réinstallez le logiciel de l'unité d'acquisition si nécessaire pour entrer les paramètres de proxy corrects. 1. Essayez de « boucler ». Reportez-vous aux informations/documentation sur "boucle homme" concernant les proxys : --préproxy, --proxy-* (c'est un caractère générique "*" car Curl prend en charge de nombreux paramètres proxy). 2. Essayez « wget ». Consultez la documentation pour connaître les options du proxy.
L'installation de l'unité d'acquisition a échoué dans Data Infrastructure Insights avec des erreurs 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

Acquisition non en cours d'exécution	Vous trouverez des informations dans le fichier acq.log dans le dossier *<répertoire d'installation>\Cloud Insights\acquisition Unit\log*. Redémarrez l'acquisition via les services Windows
Problèmes de collecte de données	Envoyez un rapport d'erreur à partir de la page d'accueil du Data Collector en cliquant sur le bouton « Envoyer un rapport d'erreur »
État : échec du signal de détection	L'unité d'acquisition (au) envoie un signal de détection 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 si Data Infrastructure Insights ne répond pas, l'heure de bail de l'au n'est pas mise à jour. Lorsque la durée de bail de l'au expire, Data Infrastructure Insights affiche l'état « échec de Heartbeat ». Étapes de dépannage : * Vérifiez la connexion réseau entre l'unité d'acquisition sever et CloudInsights. * Vérifiez si le service de l'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 (<dossier d'installation>:\Program Files\Cloud Insights\acquisition Unit\log\acq.log) pour voir s'il y a des erreurs.
Je vois un message « Heartbeat Error:	Cette erreur peut se produire en cas d'interruption du réseau entraînant l'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 Proxies et pare-feu

Si votre entreprise a besoin d'un proxy pour accéder à Internet, vous devrez peut-être comprendre le comportement du proxy de votre entreprise et rechercher certaines exceptions pour que Data Infrastructure Insights fonctionne. Gardez à l'esprit les éléments suivants :

- Tout d'abord, votre organisation bloque-t-elle l'accès par défaut et autorise-t-elle uniquement l'accès à des sites ou domaines Web spécifiques par exception ? Si c'est le cas, vous devrez ajouter le domaine suivant à votre liste d'exceptions :

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

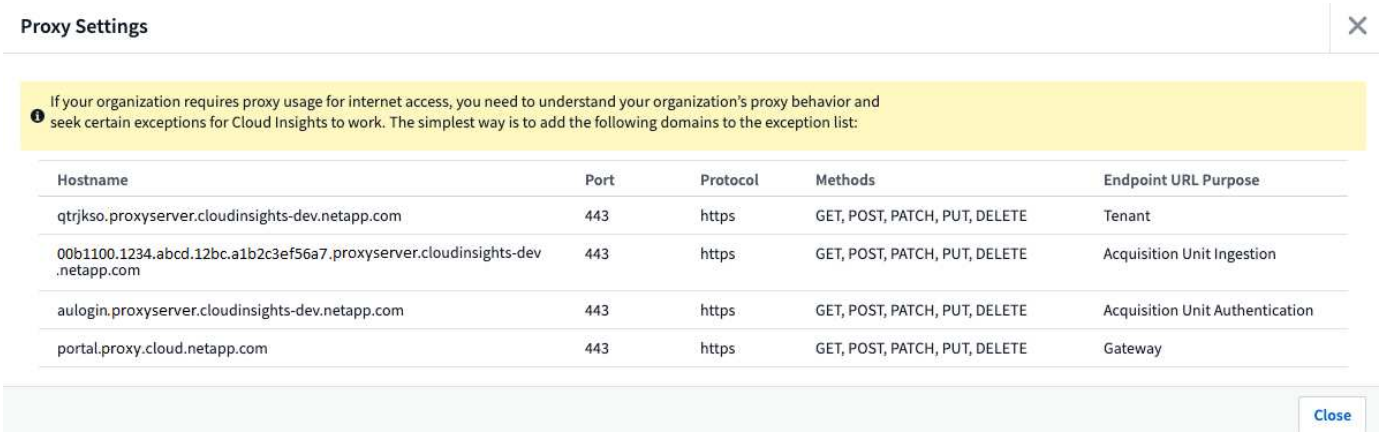
  Votre unité d'acquisition Data Infrastructure Insights, ainsi que vos interactions dans un navigateur Web avec Data Infrastructure Insights, seront toutes effectuées sur les hôtes portant ce nom de domaine.

- Deuxièmement, certains proxys tentent d'effectuer une inspection TLS/SSL en usurpant l'identité 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, à l'exception de cette fonctionnalité, pour que l'unité d'acquisition Data Infrastructure Insights se connecte avec succès à Data

Infrastructure Insights et facilite la découverte des données.

Affichage des noeuds finaux du proxy

Vous pouvez afficher vos noeuds finaux proxy en cliquant sur le lien **Paramètres proxy** lorsque vous choisissez un collecteur de données pendant l'intégration, ou sur le lien sous *Paramètres proxy* de la page **aide > support**. Un tableau comme celui ci-dessous s'affiche. Si vous avez la sécurité de la charge de travail dans votre environnement, les URL de point final configurées s'affichent également dans cette liste.



Ressources

Vous trouverez d'autres conseils de dépannage dans le "Base de connaissances NetApp" (connexion à l'assistance requise).

Des informations de support supplémentaires sont disponibles sur la page Data Infrastructure Insights"Assistance".

Recherche d'un collecteur de données défectueux

Si un collecteur de données a 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.

Procédez comme suit pour déterminer la cause de l'échec des collecteurs de données. Les messages d'échec du collecteur de données s'affichent dans le menu **Admin** et sur la page **Data Collectors installés**.

Étapes

1. Cliquez sur **Admin** > **Data Collectors** > **Data Collectors installés**.
2. Cliquez sur le nom lié du collecteur de données défaillant pour ouvrir la page Résumé.
3. Sur la page Summary, vérifiez dans la zone Comments les remarques qui auraient pu être laissées par un autre ingénieur pour compte.
4. Notez tous les messages de performance.
5. Déplacez le pointeur de la 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 affiché 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 en cours d'utilisation et les suggestions sur ce qui peut être tenté de corriger le problème.

7. Dans la zone périphériques signalés par ce Data Collector, vous pouvez filtrer la liste pour n'afficher que les périphériques qui vous intéressent et cliquer sur le **Nom** lié d'un périphérique pour afficher la page de ressources de ce périphérique.
8. Lorsque vous revenez à la page de résumé du collecteur de données, vérifiez la zone **Afficher les changements récents** en bas de la page pour voir si des modifications récentes pourraient avoir causé le problème.

Matrice de prise en charge du Data Collector Data Infrastructure Insights

La matrice de prise en charge des collecteurs de données fournit des références pour les collecteurs de données pris en charge par Data Infrastructure Insights , y compris des informations sur les fournisseurs et les modèles.

HP Enterprise 3PAR / Alletra 9000 / stockage Primera StoreServ

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
HPE ALLETRA 9080 7200 8400 HPE_3PAR 20450 7400 8440 HPE_3PAR 20800 20800 8200 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	3.1.1 4.5.24 9.5.15 (MU1) 3.1.2 4.5.7 9.5.8 (MU3) 3.1.3 4.5.21 4.6.1 9.6.1 (MU1) 3.3.1 (MU2) 3.3.2 (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) 3.1.3 (MU5) 3.2.1 (MU1) 4.3.1 4.3.3 4.4.1 Type de support standard Type de version 4.5.15 : version de support étendu : version 4.5.18 : version de support étendu

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

					stockage ?
		Capacité écrite	Mise en œuvre	SSH	Capacité totale
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
	Carte de volume	LUN	Mise en œuvre	SSH	Nom de la lun backend
		Contrôleur de protocole	Mise en œuvre	SSH	
		Port de stockage	Mise en œuvre	SSH	
		Type	Écart	SSH	
	Masque de volume	Initiateur	Mise en œuvre	SSH	
		Contrôleur de protocole	Mise en œuvre	SSH	
		Port de stockage	Mise en œuvre	SSH	
		Type	Écart	SSH	
	Réf. Volume	Nom	Mise en œuvre	SSH	
		IP de stockage	Mise en œuvre	SSH	
	Alias WWN	Alias de l’hôte	Mise en œuvre	SSH	
		Type d’objet	Mise en œuvre	SSH	
		Source	Mise en œuvre	SSH	
		WWN	Mise en œuvre	SSH	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Rapport de blocage partiel	Mise en œuvre	SMI-S	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		ID du serveur	Mise en œuvre	SMI-S	
		Débit de lecture	Mise en œuvre	SMI-S	
		Débit total	Mise en œuvre	SMI-S	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d’écriture	Mise en œuvre	SMI-S	
		Écriture en attente	Mise en œuvre	SMI-S	nombre total d’écritures en attente

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
3PAR SMI-S	SMI-S	HTTP/HTTPS	5988/5989		vrai	vrai	vrai	vrai
CLI 3PAR	SSH	SSH	22		vrai	faux	vrai	vrai

Amazon AWS EC2

Modèles et versions pris en charge par ce collecteur de données : versions API :

- 1 octobre 2014

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

	Disque de Virtualmachine	OID	Mise en œuvre	HTTPS	
		ID objet virtualDisk	Mise en œuvre	HTTPS	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		OID de Virtualmachine	Mise en œuvre	HTTPS	
	Hôte	Système d’exploitation hôte	Mise en œuvre	HTTPS	
		IPS	Mise en œuvre	HTTPS	
		Fabricant	Mise en œuvre	HTTPS	
		Nom	Mise en œuvre	HTTPS	
		OID	Mise en œuvre	HTTPS	
	Info	Description de l’API	Mise en œuvre	HTTPS	
		Nom de l’API	Mise en œuvre	HTTPS	
		Version de l’API	Mise en œuvre	HTTPS	
		Nom de la source de données	Mise en œuvre	HTTPS	Info
		Date	Mise en œuvre	HTTPS	
		ID émetteur	Mise en œuvre	HTTPS	
		Clé d’émetteur	Mise en œuvre	HTTPS	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
					des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre	HTTPS	
	vm	Utilisation totale du processeur	Mise en œuvre	HTTPS	
		Lecture IOPS	Mise en œuvre	HTTPS	Nombre d'IOPS de lecture sur le disque
		DiskIops.total	Mise en œuvre	HTTPS	
		Écriture d'IOPS du disque	Mise en œuvre	HTTPS	
		Latence lecture	Mise en œuvre	HTTPS	
		Latence Total	Mise en œuvre	HTTPS	
		Écriture de latence	Mise en œuvre	HTTPS	
		Débit de lecture du disque	Mise en œuvre	HTTPS	
		Débit de lecture	Mise en œuvre	HTTPS	débit total en lecture du disque
		Écriture du débit du disque	Mise en œuvre	HTTPS	
		Lecture du débit IP	Mise en œuvre	HTTPS	
		Débit total	Mise en œuvre	HTTPS	Débit IP total
		Écriture ipThroughput	Mise en œuvre	HTTPS	
	VM	Capacité totale	Mise en œuvre	HTTPS	
		Clé	Mise en œuvre	HTTPS	
		ID du serveur	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API EC2	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

Amazon AWS S3

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
S3	1 août 2010

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

					disques de spare)
		Virtualisation	Mise en œuvre	HTTPS	S'agit-il d'un

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
					stockage ?
	Pool de stockage	Inclure dans la capacité DWH	Mise en œuvre	HTTPS	Une façon de contrôler les pools de stockage intéressants dans DWH Capacity
		Nom	Mise en œuvre	HTTPS	
		Capacité sur disque physique (Mo)	Mise en œuvre	HTTPS	utilisé comme capacité brute pour le pool de stockage
		Groupe RAID	Mise en œuvre	HTTPS	Indique si StoragePool est un groupe raid
		Rapport brut/utilisable	Mise en œuvre	HTTPS	ratio pour la conversion de la capacité utilisable en capacité brute
		ID du pool de stockage	Mise en œuvre	HTTPS	
		Provisionnement fin pris en charge	Mise en œuvre	HTTPS	Si ce volume interne prend en charge le provisionnement fin pour la couche de volume en haut de celui-ci
		Capacité totale allouée	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	
		Virtualisation	Mise en œuvre	HTTPS	S'agit-il d'un dispositif de virtualisation du stockage ?

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances	Volume interne	Capacité totale	Mise en œuvre	HTTPS	
		Capacité utilisée	Mise en œuvre	HTTPS	
		Rapport de capacité utilisé	Mise en œuvre	HTTPS	
		Clé	Mise en œuvre	HTTPS	
		Nombre total d'objets	Mise en œuvre	HTTPS	
		ID du serveur	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API S3	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

Microsoft 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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					
750					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Capacité totale allouée	Mise en œuvre	HTTPS	
		Capacité totale utilisée	Mise en œuvre	HTTPS	Capacité totale en Mo
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Type	Écart	HTTPS	
		Virtualisation	Mise en œuvre	HTTPS	S’agit-il d’un dispositif de virtualisation du stockage ?
		Commentaire	Écart	HTTPS	état : commentaire libre décrivant le svm

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
					des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre		
	StoragePool	Lecture IOPS	Mise en œuvre		Nombre d'IOPS de lecture sur le disque
		Écriture d'IOPS	Mise en œuvre		
		Débit de lecture	Mise en œuvre		
		Débit d'écriture	Mise en œuvre		
		Débit total	Mise en œuvre		Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Total d'IOPS	Mise en œuvre		

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST Azure NetApp Files	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

Commutateurs Fibre Channel Brocade

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
Brocade Brocade Brocade 200E Brocade Brocade Brocade Brocade 300E Brocade Brocade Brocade 4024 8 intégré Brocade 5000 4 Brocade 5100 7840 4 8 Brocade 5300 Brocade 5480 intégré Brocade 6505 Brocade 6547 Brocade 6548 Brocade 6546 Brocade 6510 intégré Brocade 6520 Brocade 6558 Brocade 7800 Brocade 7810 commutateur d’extension Brocade 176.51 183.0 Brocade DCX Brocade-4S Backbone Brocade DCX8510-4 Brocade DCX8510-8 Brocade G610 Brocade G620 Brocade G630 Brocade	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 v7.0.0a v7.0.2f v7.4.v7.4 824494 01 3 855776 01

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		WWN	Mise en œuvre	SSH	
	Zone	Nom de la zone	Mise en œuvre	SSH	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
	Membre de la zone	Type	Ecart	SSH	
		WWN	Mise en œuvre	SSH	
	Fonctionnalités de segmentation	Configuration active	Mise en œuvre	SSH	
		Nom de la configuration	Mise en œuvre	SSH	
		Comportement de zonage par défaut	Mise en œuvre	SSH	
		WWN	Mise en œuvre	SSH	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		perte de synchronisation			perte de synchronisation
		Erreur de port : Échec d'annulation de la transmission	Mise en œuvre	SNMP	Dépassement du délai d'attente de la transmission
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Nombre total d'erreurs de port	Mise en œuvre	SNMP	Nombre total d'erreurs de port
		ID du serveur	Mise en œuvre	SNMP	
		Fréquence de trame de trafic	Mise en œuvre	SNMP	
		Fréquence de trame de trafic totale	Mise en œuvre	SNMP	
		Fréquence de trame de trafic	Mise en œuvre	SNMP	
		Taille moyenne des images	Mise en œuvre	SNMP	Taille moyenne des trames du trafic
		Images TX	Mise en œuvre	SNMP	taille moyenne des trames de trafic
		Taux de trafic reçu	Mise en œuvre	SNMP	
		Taux de trafic total	Mise en œuvre	SNMP	
		Vitesse de transmission du trafic	Mise en œuvre	SNMP	
		Utilisation reçue du trafic	Mise en œuvre	SNMP	
		Utilisation totale du trafic	Mise en œuvre	SNMP	Utilisation totale du trafic
		Utilisation de la transmission du trafic	Mise en œuvre	SNMP	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
Brocade SNMP	SNMP	SNMPv1, SNMPv2, SNMPv3	161		vrai	vrai	vrai	vrai
Brocade SSH	SSH	SSH	22		faux	faux	vrai	vrai
Assistant de configuration de la source de données	Saisie manuelle				vrai	vrai	vrai	vrai

Brocade Network Advisor 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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Connectivité inconnue	Mise en œuvre	HTTP/S	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Lame	Mise en œuvre	HTTP/S	
		Type GBIC	Mise en œuvre	HTTP/S	
	Commutateur	WWN	Mise en œuvre	HTTP/S	
		IP	Mise en œuvre	HTTP/S	
		Version du micrologiciel	Mise en œuvre	HTTP/S	
		Fabricant	Mise en œuvre	HTTP/S	
		Modèle	Mise en œuvre	HTTP/S	
		Nom	Mise en œuvre	HTTP/S	
		Changer de rôle	Mise en œuvre	HTTP/S	
		Type	Écart	HTTP/S	
		Numéro de série	Mise en œuvre	HTTP/S	
		Gérer URL	Mise en œuvre	HTTP/S	
		État du commutateur	Mise en œuvre	HTTP/S	
		Statut du commutateur	Mise en œuvre	HTTP/S	
		ID de domaine	Mise en œuvre	HTTP/S	
		VSAN activé	Mise en œuvre	HTTP/S	
	Inconnu	WWN	Mise en œuvre	HTTP/S	
		Fabricant	Mise en œuvre	HTTP/S	
		Micrologiciel	Mise en œuvre	HTTP/S	
		Conducteur	Mise en œuvre	HTTP/S	
		Modèle	Mise en œuvre	HTTP/S	
	Alias WWN	Alias de l’hôte	Mise en œuvre	HTTP/S	
		Type d’objet	Mise en œuvre	HTTP/S	
		Source	Mise en œuvre	HTTP/S	
		WWN	Mise en œuvre	HTTP/S	
	Zone	Nom de la zone	Mise en œuvre	HTTP/S	
	Membre de la zone	Type	Écart	HTTP/S	
		WWN	Mise en œuvre	HTTP/S	
	Fonctionnalités de segmentation	Configuration active	Mise en œuvre	HTTP/S	
		Nom de la configuration	Mise en œuvre	HTTP/S	
		WWN	Mise en œuvre	HTTP/S	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances	port	BB crédit zéro transmis	Mise en œuvre	HTTP/S	BB crédit zéro transmis
		Total du crédit BB zéro	Mise en œuvre	HTTP/S	Total du crédit BB zéro
		BB crédit zéro MS transmis	Mise en œuvre	HTTP/S	BB crédit zéro MS transmis

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST Brocade Network Advisor	HTTP/HTTPS	HTTP/HTTPS	80/443		vrai	vrai	vrai	vrai

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 861742 857687 v8.2.3a v8.2.3b v8.2.3c v8.2.3c1 v8.2.3d v8.2.3e v8.2 01.3e1 v9.0 01.0b v9.0.1b v9.0

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		WWN	Mise en œuvre	HTTPS	
	Zone	Nom de la zone	Mise en œuvre	HTTPS	
	Membre de la zone	Type	Écart	HTTPS	
		WWN	Mise en œuvre	HTTPS	
	Fonctionnalités de segmentation	Configuration active	Mise en œuvre	HTTPS	
		Nom de la configuration	Mise en œuvre	HTTPS	
		Comportement de zonage par défaut	Mise en œuvre	HTTPS	
		WWN	Mise en œuvre	HTTPS	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		perte de synchronisation			perte de synchronisation
		Nombre total d'erreurs de port	Mise en œuvre	HTTPS	Nombre total d'erreurs de port
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		ID du serveur	Mise en œuvre	HTTPS	
		Fréquence de trame de trafic	Mise en œuvre	HTTPS	
		Fréquence de trame de trafic totale	Mise en œuvre	HTTPS	
		Fréquence de trame de trafic	Mise en œuvre	HTTPS	
		Taille moyenne des images	Mise en œuvre	HTTPS	Taille moyenne des trames du trafic
		Images TX	Mise en œuvre	HTTPS	taille moyenne des trames de trafic
		Taux de trafic reçu	Mise en œuvre	HTTPS	
		Taux de trafic total	Mise en œuvre	HTTPS	
		Vitesse de transmission du trafic	Mise en œuvre	HTTPS	
		Utilisation reçue du trafic	Mise en œuvre	HTTPS	
		Utilisation totale du trafic	Mise en œuvre	HTTPS	Utilisation totale du trafic
		Utilisation de la transmission du trafic	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST BROCADE FOS	HTTPS		443		vrai	vrai	vrai	vrai

Commutateurs de structure Cisco MDS & Nexus

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 6332 6332 64108 6454	3 5.0 3 5.0 5.2 5.2 5.2 5.2 6.2 13 15 6.2 21 6.2 27 6.2 33 7 6.2(1c) 5.0 3 5.0 8 8 5.2 5.2 6.2 6.2 6.2 6.2 19 6.2 25 6.2 31 6.2 6.2 6.2(3a) 4.2 5.0 3 5.2 5.2 5.2 5.2 11 6.2 6.2 17 6.2 23 6.2 29 6.2 6.2 9 7.0(1a) 5.0(1a) 3(5.0)N2(3.11e) 5.0(3)N2(4.01d) 3(3)N2(4.13i) 5.0(5.0)N2(4.21e) 5.0(5.0)N2(4.21j) 3(3.3)N2(4.3)4.1 3 7.0 3 7.0 3 7.3 7.3 7.3 13 7.3 8 8.1 8.1 8.2 8.2 8.3 8.3 8.4 8.4 8.4 8.4 8.4 8.4 8.4 8.4 8.4 8.5 9.2 9.2 9.3 9.3 9.3 9.3 5 9.3 5 9.3 5 9.3 5 9.3 5 9.3 5 9.4 9.4 9.4 9.4 9.4 3

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		commutateur			
		Type	Écart	SNMP	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		VSAN active	Mise en œuvre	SNMP	
		WWN	Mise en œuvre	SNMP	
	Inconnu	Conducteur	Mise en œuvre	SNMP	
		Micrologiciel	Mise en œuvre	SNMP	
		Généré	Mise en œuvre	SNMP	
		Fabricant	Mise en œuvre	SNMP	
		Modèle	Mise en œuvre	SNMP	
		Nom	Mise en œuvre	SNMP	
		WWN	Mise en œuvre	SNMP	
	Alias WWN	Alias de l’hôte	Mise en œuvre	SNMP	
		Type d’objet	Mise en œuvre	SNMP	
		Source	Mise en œuvre	SNMP	
		WWN	Mise en œuvre	SNMP	
	Zone	Nom de la zone	Mise en œuvre	SNMP	
		Type de zone	Mise en œuvre	SNMP	
	Membre de la zone	Type	Écart	SNMP	
		WWN	Mise en œuvre	SNMP	
	Fonctionnalités de segmentation	Configuration active	Mise en œuvre	SNMP	
		Nom de la configuration	Mise en œuvre	SNMP	
		Comportement de zonage par défaut	Mise en œuvre	SNMP	
		Contrôle de fusion	Mise en œuvre	SNMP	
		WWN	Mise en œuvre	SNMP	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		d'annulation de la transmission			port
		Nombre total d'erreurs de port	Mise en œuvre	SNMP	Nombre total d'erreurs de port
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		ID du serveur	Mise en œuvre	SNMP	
		Fréquence de trame de trafic	Mise en œuvre	SNMP	
		Fréquence de trame de trafic totale	Mise en œuvre	SNMP	
		Fréquence de trame de trafic	Mise en œuvre	SNMP	
		Taille moyenne des images	Mise en œuvre	SNMP	Taille moyenne des trames du trafic
		Images TX	Mise en œuvre	SNMP	taille moyenne des trames de trafic
		Taux de trafic reçu	Mise en œuvre	SNMP	
		Taux de trafic total	Mise en œuvre	SNMP	
		Vitesse de transmission du trafic	Mise en œuvre	SNMP	
		Utilisation reçue du trafic	Mise en œuvre	SNMP	
		Utilisation totale du trafic	Mise en œuvre	SNMP	Utilisation totale du trafic
		Utilisation de la transmission du trafic	Mise en œuvre	SNMP	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
Le protocole SNMP de Cisco	SNMP	SNMPv1 (Inventaire uniquement), SNMPv2, SNMPv3	161		vrai	vrai	vrai	vrai

Cohesity

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 VIRTUELS	6.8.1_u1_release-20221022_6f58ed2a 6.8.2_u1_release-20240509_a5da4644 7.1.2_u2_release-20240925_66722648 7.1.2_u3_release-20241231_bb47fe77 7.2.1_release-20241114_794eae46 7.2.2_release-20250228_63eccf

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

					fin pour la couche de volume en haut de celui-ci
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Capacité totale allouée	Mise en œuvre		
		Capacité totale utilisée	Mise en œuvre		Capacité totale en Mo
		Type	Écart		
		Virtualisation	Mise en œuvre		S’agit-il d’un dispositif de virtualisation du stockage ?
		Chiffrées	Mise en œuvre		
performances	Stockage	Échec de la capacité brute	Mise en œuvre		
		Capacité brute	Mise en œuvre		
		Capacité brute disponible	Mise en œuvre		Capacité brute des disques de spare (somme de tous les disques de spare)
		Capacité des stockagePools	Mise en œuvre		
		Lecture IOPS	Mise en œuvre		Nombre d’IOPS de lecture sur le disque
		Total d’IOPS	Mise en œuvre		
		Écriture d’IOPS	Mise en œuvre		
		Clé	Mise en œuvre		
		Latence lecture	Mise en œuvre		
		Latence Total	Mise en œuvre		
		Écriture de latence	Mise en œuvre		
		ID du serveur	Mise en œuvre		
		Débit de lecture	Mise en œuvre		
		Débit total	Mise en œuvre		Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d’écriture	Mise en œuvre		
		Total d’utilisation	Mise en œuvre		

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST de Cohesity	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

					charge le provisionnement fin pour la
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires** de celui-ci
		Capacité totale allouée	Mise en œuvre	SSH	
		Capacité totale utilisée	Mise en œuvre	SSH	Capacité totale en Mo
		Type	Écart	SSH	
		Virtualisation	Mise en œuvre	SSH	S'agit-il d'un dispositif de virtualisation du stockage ?

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
Celerra CLI	SSH	SSH			vrai	faux	vrai	vrai

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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Cible de réplica	Mise en œuvre	CLI	
		ID du pool de stockage	Mise en œuvre	CLI	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Provisionnement fin	Mise en œuvre	CLI	
		Type	Écart	CLI	
		UUID	Mise en œuvre	CLI	
		Capacité utilisée	Mise en œuvre	CLI	
	Carte de volume	LUN	Mise en œuvre	CLI	Nom de la lun backend
		Contrôleur de protocole	Mise en œuvre	CLI	
		Port de stockage	Mise en œuvre	CLI	
		Type	Écart	CLI	
	Masque de volume	Initiateur	Mise en œuvre	CLI	
		Contrôleur de protocole	Mise en œuvre	CLI	
		Port de stockage	Mise en œuvre	CLI	
		Type	Écart	CLI	
	Membre du volume	Capacité	Mise en œuvre	CLI	Capacité utilisée de la copie Snapshot en Mo
		Nom	Mise en œuvre	CLI	
		Rang	Mise en œuvre	CLI	
		Capacité brute totale	Mise en œuvre	CLI	Capacité brute totale (somme de tous les disques de la baie)
		Redondance	Mise en œuvre	CLI	Niveau de redondance
		ID du pool de stockage	Mise en œuvre	CLI	
		Capacité utilisée	Mise en œuvre	CLI	
	Alias WWN	Alias de l’hôte	Mise en œuvre	CLI	
		IP	Mise en œuvre	CLI	
		Type d’objet	Mise en œuvre	CLI	
		Source	Mise en œuvre	CLI	
		WWN	Mise en œuvre	CLI	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Utilisation de la lecture	Mise en œuvre	CLI	
		Total d'utilisation	Mise en œuvre	CLI	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Utilisation, écriture	Mise en œuvre	CLI	
	Volumétrie	Taux de réussite du cache lecture	Mise en œuvre	CLI	
		Taux de réussite total du cache	Mise en œuvre	CLI	
		Écriture du taux de réussite du cache	Mise en œuvre	CLI	
		Capacité brute	Mise en œuvre	CLI	
		Capacité totale	Mise en œuvre	CLI	
		Capacité utilisée	Mise en œuvre	CLI	
		Rapport de capacité utilisé	Mise en œuvre	CLI	
		Lecture IOPS	Mise en œuvre	CLI	Nombre d'IOPS de lecture sur le disque
		Total d'IOPS	Mise en œuvre	CLI	
		Écriture d'IOPS	Mise en œuvre	CLI	
		Latence lecture	Mise en œuvre	CLI	
		Latence Total	Mise en œuvre	CLI	
		Écriture de latence	Mise en œuvre	CLI	
		Rapport de blocage partiel	Mise en œuvre	CLI	
		Débit de lecture	Mise en œuvre	CLI	
		Débit total	Mise en œuvre	CLI	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre	CLI	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
CLI Navi	CLI		6389,2162,2163,443 (HTTPS)/80 (HTTP)		vrai	vrai	vrai	faux

EMC Data Domain (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 DD6200 DD6300 DD9400 DD69400 DD9410 DD6800 DD690 DD69900 DD69910	…2.20-606786 6.2.1.30-663869 6.2.1.40-671977 6.2.1.60-686365 7.10.0.2.30-606339 6.1.0-1042928 7.10.1.0.90-692270 7.7.4.0-1017976 7.7.0.70-686759 7.2.0.20-658029 7.2.0.60-682124 7.2.20-1082704 7.2.50-1146826 7.11.0.0-1035502 7.13.0.40-1126469 7.10.1.20-1090468 7.10.1.30-1105324 7.10.1.15-1078832 7.10.1.1-1049892 7.10.1.10-1068159 7.10.1.5.1-1040473 7.7.5.11-1046187 7.7.20-1023227 7.10.1.5.30-1091295 8.0.0.10-1097914 8.1.0.10-1127744.2.051-633576 6.1.6.0.5.25-1078970 7.7

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		brut/utilisable			conversion de la capacité utilisable en capacité brute
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		ID du pool de stockage	Mise en œuvre	SSH	
		Provisionnement fin pris en charge	Mise en œuvre	SSH	Si ce volume interne prend en charge le provisionnement fin pour la couche de volume en haut de celui-ci
		Capacité totale allouée	Mise en œuvre	SSH	
		Capacité totale utilisée	Mise en œuvre	SSH	Capacité totale en Mo
		Type	Écart	SSH	
		Virtualisation	Mise en œuvre	SSH	S'agit-il d'un dispositif de virtualisation du stockage ?

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
Interface de ligne de commande Data Domain	SSH	SSH	22		vrai	vrai	vrai	vrai

EMC 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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		nœuds utilisable en Mo			
		Utilisation de la capacité des nœuds utilisée en Mo	Mise en œuvre	HTTPS	
Solution NetApp	**Catégorie**	**Capacité attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
	Pool de stockage	Inclure dans la capacité DWH	Mise en œuvre	HTTPS	Une façon de contrôler les pools de stockage intéressants dans DWH Capacity
		Nom	Mise en œuvre	HTTPS	
		Capacité sur disque physique (Mo)	Mise en œuvre	HTTPS	utilisé comme capacité brute pour le pool de stockage
		Groupe RAID	Mise en œuvre	HTTPS	Indique si StoragePool est un groupe raid
		Rapport brut/utilisable	Mise en œuvre	HTTPS	ratio pour la conversion de la capacité utilisable en capacité brute
		ID du pool de stockage	Mise en œuvre	HTTPS	
		Provisionnement fin pris en charge	Mise en œuvre	HTTPS	Si ce volume interne prend en charge le provisionnement fin pour la couche de volume en haut de celui-ci
		Capacité totale allouée	Mise en œuvre	HTTPS	
		Capacité totale utilisée	Mise en œuvre	HTTPS	Capacité totale en Mo
		Type	Écart	HTTPS	
		Virtualisation	Mise en œuvre	HTTPS	S’agit-il d’un dispositif de virtualisation du stockage ?

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
					des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre	HTTPS	
	StoragePool	Capacité provisionnée	Mise en œuvre	HTTPS	
		Capacité brute	Mise en œuvre	HTTPS	
		Capacité totale	Mise en œuvre	HTTPS	
		Capacité utilisée	Mise en œuvre	HTTPS	
		Rapport de capacité de surengagement	Mise en œuvre	HTTPS	Signalé comme une série chronologique
		Rapport de capacité utilisé	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST EMC ECS	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

					utilisable en capacité brute
Solution NetApp	**Catégorie**	**Capacité allouée des snapshots**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Capacité utilisée du snapshot	Mise en œuvre	HTTPS	
		ID du pool de stockage	Mise en œuvre	HTTPS	
		Provisionnement fin pris en charge	Mise en œuvre	HTTPS	Si ce volume interne prend en charge le provisionnement fin pour la couche de volume en haut de celui-ci
		Capacité totale allouée	Mise en œuvre	HTTPS	
		Capacité totale utilisée	Mise en œuvre	HTTPS	Capacité totale en Mo
		Type	Écart	HTTPS	
		Virtualisation	Mise en œuvre	HTTPS	S’agit-il d’un dispositif de virtualisation du stockage ?

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

					écriture sur tous les disques) en Mo/s.
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Débit d'écriture	Mise en œuvre	HTTPS	
		Total d'utilisation	Mise en œuvre	HTTPS	
	StoragePool	Capacité provisionnée	Mise en œuvre	HTTPS	
		Capacité brute	Mise en œuvre	HTTPS	
		Capacité totale	Mise en œuvre	HTTPS	
		Capacité utilisée	Mise en œuvre	HTTPS	
		Rapport de capacité de surengagement	Mise en œuvre	HTTPS	Signalé comme une série chronologique
		Rapport de capacité utilisé	Mise en œuvre	HTTPS	
		Capacité totale des données	Mise en œuvre	HTTPS	
		Capacité utile des données	Mise en œuvre	HTTPS	
		Lecture IOPS	Mise en œuvre	HTTPS	Nombre d'IOPS de lecture sur le disque
		Total d'IOPS	Mise en œuvre	HTTPS	
		Écriture d'IOPS	Mise en œuvre	HTTPS	
		Autre capacité totale	Mise en œuvre	HTTPS	
		Autre capacité utilisée	Mise en œuvre	HTTPS	
		Capacité réservée des snapshots	Mise en œuvre	HTTPS	
		Capacité utilisée du snapshot	Mise en œuvre	HTTPS	
		Rapport de capacité utilisé des snapshots	Mise en œuvre	HTTPS	Signalé comme une série chronologique
		Débit de lecture	Mise en œuvre	HTTPS	
		Débit total	Mise en œuvre	HTTPS	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST EMC Isilon & PowerScale	HTTPS		443		vrai	vrai	vrai	vrai

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) : 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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

					de celui-ci
		Capacité totale allouée	Mise en œuvre	SSH	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Capacité totale utilisée	Mise en œuvre	SSH	Capacité totale en Mo
		Type	Écart	SSH	
		Virtualisation	Mise en œuvre	SSH	S’agit-il d’un dispositif de virtualisation du stockage ?

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

					écriture sur tous les disques) en Mo/s.
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Débit d'écriture	Mise en œuvre	SSH	
		Total d'utilisation	Mise en œuvre	SSH	
	StoragePool	Capacité totale	Mise en œuvre	SSH	
		Rapport de capacité utilisé	Mise en œuvre	SSH	
		Capacité totale des données	Mise en œuvre	SSH	
		Capacité provisionnée	Mise en œuvre	SSH	
		Capacité utile des données	Mise en œuvre	SSH	
		Capacité utilisée	Mise en œuvre	SSH	
		Capacité brute	Mise en œuvre	SSH	
		Rapport de capacité de surengagement	Mise en œuvre	SSH	Signalé comme une série chronologique
		Capacité utilisée du snapshot	Mise en œuvre	SSH	
		Capacité réservée des snapshots	Mise en œuvre	SSH	
		Rapport de capacité utilisé des snapshots	Mise en œuvre	SSH	Signalé comme une série chronologique

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
Isilon (SSH	SSH	SSH	22		vrai	faux	vrai	vrai

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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Type	Écart		
		Virtualisation	Mise en œuvre		S’agit-il d’un

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
					stockage ?
	Volumétrie	Capacité	Mise en œuvre		Capacité utilisée de la copie Snapshot en Mo
		Chemin de jonction	Mise en œuvre		
		Nom	Mise en œuvre		
		Capacité brute totale	Mise en œuvre		Capacité brute totale (somme de tous les disques de la baie)
		ID du pool de stockage	Mise en œuvre		
		Provisionnement fin	Mise en œuvre		
		Type	Écart		
		UUID	Mise en œuvre		
		Capacité utilisée	Mise en œuvre		
		QoS - règle	Mise en œuvre		
	Carte de volume	LUN	Mise en œuvre		Nom de la lun backend
		Masquage requis	Mise en œuvre		
		Contrôleur de protocole	Mise en œuvre		
		Port de stockage	Mise en œuvre		
		Type	Écart		
	Masque de volume	Initiateur	Mise en œuvre		
		Contrôleur de protocole	Mise en œuvre		
		Type	Écart		
	Alias WWN	Alias de l’hôte	Mise en œuvre		
		Type d’objet	Mise en œuvre		
		Source	Mise en œuvre		
		WWN	Mise en œuvre		

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
					(lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre		
	Volumétrie	Capacité brute	Mise en œuvre		
		Capacité totale	Mise en œuvre		
		Capacité utilisée	Mise en œuvre		
		Rapport de capacité utilisé	Mise en œuvre		
		Lecture IOPS	Mise en œuvre		Nombre d'IOPS de lecture sur le disque
		Total d'IOPS	Mise en œuvre		
		Écriture d'IOPS	Mise en œuvre		
		Clé	Mise en œuvre		
		Latence lecture	Mise en œuvre		
		Latence Total	Mise en œuvre		
		Écriture de latence	Mise en œuvre		
		ID du serveur	Mise en œuvre		
		Débit de lecture	Mise en œuvre		
		Débit total	Mise en œuvre		Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre		

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST D'EMC POWERSTORE	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

EMC RecoverPoint (HTTP)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
RecoverPoint	5.1.SP4.P1(h. 89) 5.1.SP4.P2(h.138) 5.1.SP4.P3(h.77) 5.1.SP4.P4(h.97) 5.1.SP4.P5(h.138)

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

					disques de spare)
		Virtualisation	Mise en œuvre	HTTPS	S’agit-il d’un
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
	Nœud de stockage	Taille de la mémoire	Écart	HTTPS	Mémoire du périphérique en Mo
		Modèle	Mise en œuvre	HTTPS	
		Nom	Mise en œuvre	HTTPS	
		Nombre de processeurs	Mise en œuvre	HTTPS	Processeur du périphérique
		Numéro de série	Mise en œuvre	HTTPS	
		État	Mise en œuvre	HTTPS	texte libre décrivant l’état du périphérique
		UUID	Mise en œuvre	HTTPS	
		Version	Mise en œuvre	HTTPS	version logicielle
	Synchronisation du stockage	Mode	Mise en œuvre	HTTPS	
		Enum. Mode	Mise en œuvre	HTTPS	
		Stockage source	Mise en œuvre	HTTPS	
		Volume source	Mise en œuvre	HTTPS	
		État	Mise en œuvre	HTTPS	texte libre décrivant l’état du périphérique
		Enum. État	Mise en œuvre	HTTPS	
		Stockage cible	Mise en œuvre	HTTPS	
		Volume cible	Mise en œuvre	HTTPS	
		De déduplication	Mise en œuvre	HTTPS	technologie qui entraîne l’évolution de l’efficacité du stockage

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST RecoverPoint	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Type	Écart	HTTPS	
		Virtualisation	Mise en œuvre	HTTPS	S’agit-il d’un
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
	Volumétrie	Capacité	Mise en œuvre	HTTPS	stockage ? Capacité utilisée de la copie Snapshot en Mo
		Chemin de jonction	Mise en œuvre	HTTPS	
		Nom	Mise en œuvre	HTTPS	
		Capacité brute totale	Mise en œuvre	HTTPS	Capacité brute totale (somme de tous les disques de la baie)
		ID du pool de stockage	Mise en œuvre	HTTPS	
		Provisionnement fin	Mise en œuvre	HTTPS	
		UUID	Mise en œuvre	HTTPS	
		Adresses IP de l’hôte	Mise en œuvre	HTTPS	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances	Stockage	Échec de la capacité brute	Mise en œuvre		
		Capacité brute	Mise en œuvre		
		Capacité brute disponible	Mise en œuvre		Capacité brute des disques de spare (somme de tous les disques de spare)
		Capacité des stockagePools	Mise en œuvre		
		Lecture IOPS	Mise en œuvre		Nombre d'IOPS de lecture sur le disque
		Total d'IOPS	Mise en œuvre		
		Écriture d'IOPS	Mise en œuvre		
		Clé	Mise en œuvre		
		ID du serveur	Mise en œuvre		
		Débit de lecture	Mise en œuvre		
		Débit total	Mise en œuvre		Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre		

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
EMC ScaleIO et PowerFlex REST API	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

CLI EMC Symmetrix

Modèles et versions pris en charge par ce collecteur de données :

Versions API	Modèles	Versions du micrologiciel
V10.0.0.0 4.1 4.6 V10.0.1.1 4.2 4.7 V10.1.0.0 4.3 4.8 V10.1.1.0 V10.1.2.0 V10.1.3.0 V10.2.0.0 V8.3.0.6 V8.4.0.7 V8.4.0.9 V9.1.0.5 V9.1.0.6 V9.2.0.1 V9.2.0.3 V9.2.0.5 V9.2.3.1 V9.2.3.4 V9.2.3.6	PMAX8000 POWERMAX_2000 POWERMAX_8000 VMAX-1 VMAX100K VMAX10K VMAX200K VMAX250F VMAX400K VMAX40K VMAX450F VMAX850F VMAX950F	5876.286.194 484 5978.711.711 5978.714.714 117 5978.714.714 34 5978.714.714 79(16F40000) Build 115 5876.309.196 438 5978.711.711 542 5978.711.711 101 5978.714.714 137 5978.714.714 49 5978.714.714(16F40000) Build 153 5876.309.196 448 5978.711.711 581 5978.714.714 108 5978.714.714 145 5978.714.714 53 5978.714.714(16F40000) Build 335 5978.711.711(16F40000) Build 94 5977.1151.1151(17590000) Build 17590000(17590000) Build 60 5977.1151.1151(45 5977.1151.1151) Build 9 5978.711.711(175A0000) Build 320 5978.711.711(175A0000) Build 162 5876.309.196(175A0000) Build 365 5978.711.711(416 5978.711.711)(436 5978.711.711

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

	masque de volume	Initiateur	Mise en œuvre		
	volume	Contrôleur de protocole	Mise en œuvre		
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Port de stockage	Mise en œuvre		
		Type	Écart		
	Membre du volume	Hiérarchisation automatique	Mise en œuvre		indique si ce pool de stockage participe à la hiérarchisation automatique avec d'autres pools
		Capacité	Mise en œuvre		Capacité utilisée de la copie Snapshot en Mo
		Cylindres	Mise en œuvre		
		Nom	Mise en œuvre		
		Rang	Mise en œuvre		
		Capacité brute totale	Mise en œuvre		Capacité brute totale (somme de tous les disques de la baie)
		Redondance	Mise en œuvre		Niveau de redondance
		ID du pool de stockage	Mise en œuvre		
		UUID	Mise en œuvre		
	Réf. Volume	Nom	Mise en œuvre		
		IP de stockage	Mise en œuvre		
	Alias WWN	Alias de l'hôte	Mise en œuvre		
		Type d'objet	Mise en œuvre		
		Source	Mise en œuvre		
		WWN	Mise en œuvre		

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

					Mo/s.
		Débit d'écriture	Mise en œuvre		
Solution NetApp	**Catégorie**	**Énumération/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
	Volumétrie	Taux de réussite du cache lecture	Mise en œuvre		
		Taux de réussite total du cache	Mise en œuvre		
		Écriture du taux de réussite du cache	Mise en œuvre		
		Capacité brute	Mise en œuvre		
		Capacité totale	Mise en œuvre		
		Capacité utilisée	Mise en œuvre		
		Capacité écrite	Mise en œuvre		
		Rapport de capacité utilisé	Mise en œuvre		
		Ratio capacité écrit	Mise en œuvre		
		Lecture IOPS	Mise en œuvre		Nombre d'IOPS de lecture sur le disque
		Total d'IOPS	Mise en œuvre		
		Écriture d'IOPS	Mise en œuvre		
		Clé	Mise en œuvre		
		Latence lecture	Mise en œuvre		
		Latence Total	Mise en œuvre		
		Écriture de latence	Mise en œuvre		
		ID du serveur	Mise en œuvre		
		Débit de lecture	Mise en œuvre		
		Débit total	Mise en œuvre		Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre		
		Écriture en attente	Mise en œuvre		nombre total d'écritures en attente

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
symcli	CLI		2707		vrai	vrai	vrai	vrai
Symmetrix SMI-S	SMI-S	HTTP/HTTPS	5988/5989		vrai	faux	faux	vrai

REST Dell Unisphere

Modèles et versions pris en charge par ce collecteur de données :

Versions API	Modèles	Versions du micrologiciel
V10.0.V10.0.V10.1.V10.1.0.5 V10.1.V10.1.0.8 V10.2.4.12 V10.2.V9.2.3.15 V9.2.3.20 V9.2.4.9 V9.2.3.4 V9.2.4.1 V9.2.4.3 V9.2.4.11 V9.2.0.1 V9.2.4.10 V9.2.4.6 V9.2.4.7 V9.2.3.22 V9.2.0.2 V9.2.0.1 V9.2.0.6 V9.2.1.5 V9.2.0.5	PowerMax_2000 PowerMax_2500 PowerMax_8000 PowerMax_8500 VMAX200K VMAX250F VMAX400K VMAX450F VMAX950F	5977.1131.1131 149 5978.714.714 49 79 161 6079.175.0 127 216 6079.225.0 291 331 6079.225.0 221 build 615 5977.1151.1151 34 5978.714.714 49 5978.714.714 79 6079.175.0 259 127 6079.225.0 218 291 6079.225.0 86 221 build 60 49 5978.714.714 79 5978.714.714 161 259 6079.225.0 216 218 6079.225.0 331 86 6079.275.0 build 131 5978.714.714 build 137 5978.714.714 build 137 build 117 build 117 5978.714.714 build 131 build 101 5978.714.714 build 108 5978.714.714 build 117 5978.714.714 build 49 5978.714.714 build 5978.714.714 build 101 build 75 5978.711.711 build 8 build 8 5978.714.711 build 542 build 542 5978.711.711 build 581 5978.711.711 build 484 build 484 5978.711.711 build 542 5978.711.711 build 448 5978.711.711 build 1 build 1 471 5978.711.711 build 484 5978.711.711 build 436 build 436 5978.711.711 build 438 5978.711.711 build 335 5978.711.711 build 365 5978.711.711 build 416 5978.711.711 build 60 5978.711.711 build 205 5978.711.711 build 335 build 137 5978.714.714 build 145 5978.714.714 build 149 build

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

					virtualisation du stockage ?
		Capacité écrite	Mise en œuvre	HTTPS	Capacité totale
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Pourcentage de capacité utile effective utilisée	Mise en œuvre	HTTPS	
		Compression activée	Mise en œuvre	HTTPS	
		Groupes de stockage	Mise en œuvre	HTTPS	
	Carte de volume	LUN	Mise en œuvre	HTTPS	Nom de la lun backend
		Contrôleur de protocole	Mise en œuvre	HTTPS	
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mise en œuvre	HTTPS	
		Contrôleur de protocole	Mise en œuvre	HTTPS	
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Alias WWN	Alias de l’hôte	Mise en œuvre	HTTPS	
		Type d’objet	Mise en œuvre	HTTPS	
		Source	Mise en œuvre	HTTPS	
		WWN	Mise en œuvre	HTTPS	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
					des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d’écriture	Mise en œuvre	HTTPS	
	Volumétrie	Clé	Mise en œuvre	HTTPS	
		ID du serveur	Mise en œuvre	HTTPS	
		Débit de lecture	Mise en œuvre	HTTPS	
		Débit d’écriture	Mise en œuvre	HTTPS	
		Débit total	Mise en œuvre	HTTPS	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Latence lecture	Mise en œuvre	HTTPS	
		Écriture de latence	Mise en œuvre	HTTPS	
		Latence Total	Mise en œuvre	HTTPS	
		Lecture IOPS	Mise en œuvre	HTTPS	Nombre d’IOPS de lecture sur le disque
		Écriture d’IOPS	Mise en œuvre	HTTPS	
		Total d’IOPS	Mise en œuvre	HTTPS	
		Capacité totale	Mise en œuvre	HTTPS	
		Capacité brute	Mise en œuvre	HTTPS	
		Capacité utilisée	Mise en œuvre	HTTPS	
		Rapport de capacité utilisé	Mise en œuvre	HTTPS	
		Total des économies en termes de compression	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API Dell Unisphere	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
		Port de stockage	Mise en œuvre	SSH	
		Contrôleur de protocole	Mise en œuvre	SSH	
		Type	Écart	SSH	
	Masque de volume	Port de stockage	Mise en œuvre	SSH	
		Initiateur	Mise en œuvre	SSH	
		Contrôleur de protocole	Mise en œuvre	SSH	
		Type	Écart	SSH	
	Membre du volume	Nom	Mise en œuvre	SSH	
		ID du pool de stockage	Mise en œuvre	SSH	
		Rang	Mise en œuvre	SSH	
		Capacité	Mise en œuvre	SSH	Capacité utilisée de la copie Snapshot en Mo
		Capacité brute totale	Mise en œuvre	SSH	Capacité brute totale (somme de tous les disques de la baie)
		Capacité utilisée	Mise en œuvre	SSH	
		Redondance	Mise en œuvre	SSH	Niveau de redondance
	Alias WWN	Source	Mise en œuvre	SSH	
		Alias de l’hôte	Mise en œuvre	SSH	
		WWN	Mise en œuvre	SSH	
		Type d’objet	Mise en œuvre	SSH	
		IP	Mise en œuvre	SSH	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Capacité provisionnée	Mise en œuvre	SSH	
Solution NetApp	**Catégorie**	**Rapport d'attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Rapport de capacité de surengagement	Mise en œuvre	SSH	Information supplémentaire chronologique
	Volumétrie	Latence Total	Mise en œuvre	SSH	
		Rapport de blocage partiel	Mise en œuvre	SSH	
		Latence lecture	Mise en œuvre	SSH	
		Écriture d'IOPS	Mise en œuvre	SSH	
		Débit de lecture	Mise en œuvre	SSH	
		Total d'IOPS	Mise en œuvre	SSH	
		Écriture de latence	Mise en œuvre	SSH	
		Lecture IOPS	Mise en œuvre	SSH	Nombre d'IOPS de lecture sur le disque
		Taux de réussite du cache lecture	Mise en œuvre	SSH	
		Taux de réussite total du cache	Mise en œuvre	SSH	
		Écriture du taux de réussite du cache	Mise en œuvre	SSH	
		Débit d'écriture	Mise en œuvre	SSH	
		Débit total	Mise en œuvre	SSH	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
VNX SSH ET CLI	SSH	SSH	22		vrai	faux	vrai	vrai

EMC VNXe & Unity Unisphere (interface de ligne de commande)

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 VNX3200	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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Volume cible	Mise en œuvre	HTTPS	
		De déduplication	Mise en œuvre	HTTPS	technologie qui entraîne
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
	Volumétrie	Capacité	Mise en œuvre	HTTPS	Capacité utilisée de la copie Snapshot en Mo
		Chemin de jonction	Mise en œuvre	HTTPS	
		Nom	Mise en œuvre	HTTPS	
		Capacité brute totale	Mise en œuvre	HTTPS	Capacité brute totale (somme de tous les disques de la baie)
		ID du pool de stockage	Mise en œuvre	HTTPS	
		Provisionnement fin	Mise en œuvre	HTTPS	
		UUID	Mise en œuvre	HTTPS	
		Capacité utilisée	Mise en œuvre	HTTPS	
	Carte de volume	LUN	Mise en œuvre	HTTPS	Nom de la lun backend
		Contrôleur de protocole	Mise en œuvre	HTTPS	
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mise en œuvre	HTTPS	
		Contrôleur de protocole	Mise en œuvre	HTTPS	
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
					des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre	HTTPS	
	Volumétrie	Capacité brute	Mise en œuvre	HTTPS	
		Capacité totale	Mise en œuvre	HTTPS	
		Capacité utilisée	Mise en œuvre	HTTPS	
		Rapport de capacité utilisé	Mise en œuvre	HTTPS	
		Lecture IOPS	Mise en œuvre	HTTPS	Nombre d'IOPS de lecture sur le disque
		Total d'IOPS	Mise en œuvre	HTTPS	
		Écriture d'IOPS	Mise en œuvre	HTTPS	
		Latence Total	Mise en œuvre	HTTPS	
		Débit de lecture	Mise en œuvre	HTTPS	
		Débit total	Mise en œuvre	HTTPS	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
Interface de ligne de commande VNXe et Unisphere	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Type	Écart	HTTP/S	
		Virtualisation	Mise en œuvre	HTTP/S	S’agit-il d’un
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
	Volumétrie	Capacité	Mise en œuvre	HTTP/S	Capacité utilisée de la copie Snapshot en Mo
		Nom	Mise en œuvre	HTTP/S	
		Capacité brute totale	Mise en œuvre	HTTP/S	Capacité brute totale (somme de tous les disques de la baie)
		Redondance	Mise en œuvre	HTTP/S	Niveau de redondance
		ID du pool de stockage	Mise en œuvre	HTTP/S	
		Provisionnement fin	Mise en œuvre	HTTP/S	
		UUID	Mise en œuvre	HTTP/S	
		Virtualisation	Mise en œuvre	HTTP/S	S’agit-il d’un dispositif de virtualisation du stockage ?
	Carte de volume	LUN	Mise en œuvre	HTTP/S	Nom de la lun backend
		Contrôleur de protocole	Mise en œuvre	HTTP/S	
		Port de stockage	Mise en œuvre	HTTP/S	
		Type	Écart	HTTP/S	
	Masque de volume	Initiateur	Mise en œuvre	HTTP/S	
		Contrôleur de protocole	Mise en œuvre	HTTP/S	
		Port de stockage	Mise en œuvre	HTTP/S	
		Type	Écart	HTTP/S	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
					des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d’écriture	Mise en œuvre	SSH	
	Volumétrie	Capacité brute	Mise en œuvre	SSH	
		Capacité totale	Mise en œuvre	SSH	
		Total d’IOPS	Mise en œuvre	SSH	
		Clé	Mise en œuvre	SSH	
		Latence lecture	Mise en œuvre	SSH	
		Latence Total	Mise en œuvre	SSH	
		Écriture de latence	Mise en œuvre	SSH	
		ID du serveur	Mise en œuvre	SSH	
		Débit de lecture	Mise en œuvre	SSH	
		Débit total	Mise en œuvre	SSH	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d’écriture	Mise en œuvre	SSH	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
CLI EMC VPLEX	SSH	SSH	22		vrai	vrai	vrai	vrai
API EMC VPLEX	HTTP/HTTPS	HTTP/HTTPS	80/443		vrai	vrai	vrai	vrai

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 briques et 125 To 1 briques et 24 To 1 briques et 31 To 1 briques et 8 To 1X10 To 1X20 To 1X40 To 2 briques et 83 To 3 briques et 146 To 3 briques et 251 To 3 briques et 283 To 4 Bricks 20 To et 628 To 4 Bricks & 754 To 4X40 To 6X40 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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Volume cible	Mise en œuvre	HTTPS	
		De déduplication	Mise en œuvre	HTTPS	technologie qui entraîne
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
	Volumétrie	Capacité	Mise en œuvre	HTTPS	Capacité utilisée de la copie Snapshot en Mo
		Taille de disque	Mise en œuvre	HTTPS	Liste séparée par des virgules des tailles de disque (Go)
		Vitesse du disque	Mise en œuvre	HTTPS	liste séparée par des virgules des vitesses de disque (tr/min)
		Type de disque	Non disponible	HTTPS	
		Nom	Mise en œuvre	HTTPS	
		Capacité brute totale	Mise en œuvre	HTTPS	Capacité brute totale (somme de tous les disques de la baie)
		Redondance	Mise en œuvre	HTTPS	Niveau de redondance
		ID du pool de stockage	Mise en œuvre	HTTPS	
		Provisionnement fin	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	
		UUID	Mise en œuvre	HTTPS	
		Capacité utilisée	Mise en œuvre	HTTPS	
		Virtualisation	Mise en œuvre	HTTPS	S’agit-il d’un dispositif de virtualisation du stockage ?
	Carte de volume	LUN	Mise en œuvre	HTTPS	Nom de la lun backend
		Contrôleur de protocole	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mise en œuvre	HTTPS	
		Contrôleur de protocole	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
					(lecture et écriture sur tous les disques) en Mo/s.
		Débit d’écriture	Mise en œuvre	HTTPS	
	Volumétrie	Capacité brute	Mise en œuvre	HTTPS	
		Capacité totale	Mise en œuvre	HTTPS	
		Capacité utilisée	Mise en œuvre	HTTPS	
		Rapport de capacité utilisé	Mise en œuvre	HTTPS	
		Lecture IOPS	Mise en œuvre	HTTPS	Nombre d’IOPS de lecture sur le disque
		Total d’IOPS	Mise en œuvre	HTTPS	
		Écriture d’IOPS	Mise en œuvre	HTTPS	
		Clé	Mise en œuvre	HTTPS	
		Latence lecture	Mise en œuvre	HTTPS	
		Latence Total	Mise en œuvre	HTTPS	
		Écriture de latence	Mise en œuvre	HTTPS	
		Rapport de blocage partiel	Mise en œuvre	HTTPS	
		ID du serveur	Mise en œuvre	HTTPS	
		Débit de lecture	Mise en œuvre	HTTPS	
		Débit total	Mise en œuvre	HTTPS	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d’écriture	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST D'EMC XTREMIO	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

NetApp E-Series

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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					
990					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Type	Écart	RMI	
		Virtualisation	Mise en œuvre	RMI	S’agit-il d’un dispositif de virtualisation du stockage ?
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
	Volumétrie	Capacité	Mise en œuvre	RMI	Capacité utilisée de la copie Snapshot en Mo
		Type de disque	Non disponible	RMI	
		Nom	Mise en œuvre	RMI	
		Capacité brute totale	Mise en œuvre	RMI	Capacité brute totale (somme de tous les disques de la baie)
		Redondance	Mise en œuvre	RMI	Niveau de redondance
		ID du pool de stockage	Mise en œuvre	RMI	
		Provisionnement fin	Mise en œuvre	RMI	
		Type	Écart	RMI	
		UUID	Mise en œuvre	RMI	
		Capacité utilisée	Mise en œuvre	RMI	
		Virtualisation	Mise en œuvre	RMI	S’agit-il d’un dispositif de virtualisation du stockage ?
		Capacité écrite	Mise en œuvre	RMI	Capacité totale écrite sur ce volume par un hôte en Mo
	Carte de volume	LUN	Mise en œuvre	RMI	Nom de la lun backend
		Port de stockage	Mise en œuvre	RMI	
		Type	Écart	RMI	
	Masque de volume	Initiateur	Mise en œuvre	RMI	
		Port de stockage	Mise en œuvre	RMI	
		Type	Écart	RMI	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Utilisation de la lecture	Mise en œuvre	RMI	
		Total d'utilisation	Mise en œuvre	RMI	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Utilisation, écriture	Mise en œuvre	RMI	
	Volumétrie	Taux de réussite du cache lecture	Mise en œuvre	RMI	
		Taux de réussite total du cache	Mise en œuvre	RMI	
		Écriture du taux de réussite du cache	Mise en œuvre	RMI	
		Capacité brute	Mise en œuvre	RMI	
		Capacité totale	Mise en œuvre	RMI	
		Capacité utilisée	Mise en œuvre	RMI	
		Capacité écrite	Mise en œuvre	RMI	
		Rapport de capacité utilisé	Mise en œuvre	RMI	
		Ratio capacité écrit	Mise en œuvre	RMI	
		Lecture IOPS	Mise en œuvre	RMI	Nombre d'IOPS de lecture sur le disque
		Total d'IOPS	Mise en œuvre	RMI	
		Écriture d'IOPS	Mise en œuvre	RMI	
		Latence lecture	Mise en œuvre	RMI	
		Latence Total	Mise en œuvre	RMI	
		Écriture de latence	Mise en œuvre	RMI	
		Débit de lecture	Mise en œuvre	RMI	
		Débit total	Mise en œuvre	RMI	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre	RMI	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API SANtricity	RMI	TCP			vrai	vrai	faux	faux

Pure Storage 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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

					capacité brute
		Capacité utilisée du snapshot	Mise en œuvre	HTTPS	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		ID du pool de stockage	Mise en œuvre	HTTPS	
		Provisionnement fin pris en charge	Mise en œuvre	HTTPS	Si ce volume interne prend en charge le provisionnement fin pour la couche de volume en haut de celui-ci
		Capacité totale allouée	Mise en œuvre	HTTPS	
		Capacité totale utilisée	Mise en œuvre	HTTPS	Capacité totale en Mo
		Type	Écart	HTTPS	
		Virtualisation	Mise en œuvre	HTTPS	S’agit-il d’un dispositif de virtualisation du stockage ?

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

		grâce à la compression			
		Total des économies en termes de compression	Mise en œuvre	HTTPS	
Solution NetApp	**Catégorie**	**Fonctionnalité**	**État**	**Protocole utilisé**	**Informations supplémentaires**
	Stockage	Échec de la capacité brute	Mise en œuvre	HTTPS	
		Capacité brute	Mise en œuvre	HTTPS	
		Capacité brute disponible	Mise en œuvre	HTTPS	Capacité brute des disques de spare (somme de tous les disques de spare)
		Capacité des stockagePools	Mise en œuvre	HTTPS	
		Autres IOPS	Mise en œuvre	HTTPS	
		Lecture IOPS	Mise en œuvre	HTTPS	Nombre d'IOPS de lecture sur le disque
		Total d'IOPS	Mise en œuvre	HTTPS	
		Écriture d'IOPS	Mise en œuvre	HTTPS	
		Clé	Mise en œuvre	HTTPS	
		Latence lecture	Mise en œuvre	HTTPS	
		Latence Total	Mise en œuvre	HTTPS	
		Écriture de latence	Mise en œuvre	HTTPS	
		ID du serveur	Mise en œuvre	HTTPS	
		Débit de lecture	Mise en œuvre	HTTPS	
		Débit total	Mise en œuvre	HTTPS	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API Pure Storage FlashBlade	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

Google Cloud Compute

Modèles et versions pris en charge par ce collecteur de données : versions API :

- v1

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					
1014					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		IPS	Mise en œuvre	HTTPS	
		Fabricant	Mise en œuvre	HTTPS	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Nom	Mise en œuvre	HTTPS	
		OID	Mise en œuvre	HTTPS	
	Info	Description de l'API	Mise en œuvre	HTTPS	
		Nom de l'API	Mise en œuvre	HTTPS	
		Version de l'API	Mise en œuvre	HTTPS	
		Nom de la source de données	Mise en œuvre	HTTPS	Info
		Date	Mise en œuvre	HTTPS	
		ID émetteur	Mise en œuvre	HTTPS	
		Clé d'émetteur	Mise en œuvre	HTTPS	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances	vm	Capacité totale	Mise en œuvre	HTTPS	
		Rapport de capacité utilisé	Mise en œuvre	HTTPS	
		Utilisation totale du processeur	Mise en œuvre	HTTPS	
		Lecture IOPS	Mise en œuvre	HTTPS	Nombre d'IOPS de lecture sur le disque
		DiskIops.total	Mise en œuvre	HTTPS	
		Écriture d'IOPS du disque	Mise en œuvre	HTTPS	
		Latence Total	Mise en œuvre	HTTPS	
		Débit de lecture du disque	Mise en œuvre	HTTPS	
		Débit de lecture	Mise en œuvre	HTTPS	débit total en lecture du disque
		Écriture du débit du disque	Mise en œuvre	HTTPS	
		Lecture du débit IP	Mise en œuvre	HTTPS	
		Débit total	Mise en œuvre	HTTPS	Débit IP total
		Écriture ipThroughput	Mise en œuvre	HTTPS	
		Utilisation totale de la mémoire	Mise en œuvre	HTTPS	
		swapRate.inRate	Mise en œuvre	HTTPS	
		Taux de swap	Mise en œuvre	HTTPS	
		Taux de permutation total	Mise en œuvre	HTTPS	
		Planifier le temps d'attente	Mise en œuvre	HTTPS	Temps d'attente prévu en pourcentage
	VM	Capacité totale	Mise en œuvre	HTTPS	
		Rapport de capacité utilisé	Mise en œuvre	HTTPS	
		Clé	Mise en œuvre	HTTPS	
		ID du serveur	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST de Google Compute Platform	HTTPS		443		vrai	vrai	vrai	vrai

HDS HCP (HTTPS)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
Plate-forme 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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Capacité totale allouée	Mise en œuvre	HTTPS	
		Capacité totale utilisée	Mise en œuvre	HTTPS	Capacité totale en Mo
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Type	Écart	HTTPS	
		Virtualisation	Mise en œuvre	HTTPS	S’agit-il d’un dispositif de virtualisation du stockage ?
performances	Stockage	Échec de la capacité brute	Mise en œuvre		
		Capacité brute	Mise en œuvre		
		Capacité brute disponible	Mise en œuvre		Capacité brute des disques de spare (somme de tous les disques de spare)
		Capacité des stockagePools	Mise en œuvre		
		Clé	Mise en œuvre		
		ID du serveur	Mise en œuvre		
	Données du nœud de stockage	Clé	Mise en œuvre		
		ID du serveur	Mise en œuvre		
		Débit de lecture	Mise en œuvre		
		Débit total	Mise en œuvre		Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d’écriture	Mise en œuvre		
		Total d’utilisation	Mise en œuvre		

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST HCP HDS	HTTPS	HTTPS	9090		vrai	vrai	vrai	vrai

HiCommand Device Manager

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 80 00/00 96 05 83 60/00 53 08 88 60/00 12 08 88 60/01 81 09 90 00/00 24 09 90 08 08 06 06 06 06/A-H 80 06 80 00/00 46 05 83 60/00 08 08 88 60/00 13 08 90 00/00 21 09 90 00/00 24 09-25 21/00 54/00 30/00 76/02 86/00 91/00/B-H 80 00/02 91 06 83 60/00 50 05 88 60/00 10 08 88 60/00 13 08 90 00/00 23 09 90 00/01 60 60 70 80 80 80 83/B-S 70/A-H 0988/H-S DKC:60-08-22 DKC:60-08-65 DKC:0986-06-43 DKC SVP SVP DKC:0985-06-0984 05 50 60/00 83 05 54 60/00 83 05 57 60/00 88 08 10 60/00 88 08 12 60/00 88 08 14 60/00 88 08 15 60/00 90 08 81/00 90 09 21/00 90 09 23/00 90 09 24/00 90 09 25/00

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					
1024					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Cible de réplica	Mise en œuvre	API XML HDS	
		ID du pool de stockage	Mise en œuvre	API XML HDS	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Provisionnement fin	Mise en œuvre	API XML HDS	
		Type	Écart	API XML HDS	
		Capacité utilisée	Mise en œuvre	API XML HDS	
	Carte de volume	LUN	Mise en œuvre	API XML HDS	Nom de la lun backend
		Masquage requis	Mise en œuvre	API XML HDS	
		Contrôleur de protocole	Mise en œuvre	API XML HDS	
		Port de stockage	Mise en œuvre	API XML HDS	
	Masque de volume	Initiateur	Mise en œuvre	API XML HDS	
		Contrôleur de protocole	Mise en œuvre	API XML HDS	
		Port de stockage	Mise en œuvre	API XML HDS	
	Membre du volume	Capacité	Mise en œuvre	API XML HDS	Capacité utilisée de la copie Snapshot en Mo
		Cylindres	Mise en œuvre	API XML HDS	
		Nom	Mise en œuvre	API XML HDS	
		Rang	Mise en œuvre	API XML HDS	
		Capacité brute totale	Mise en œuvre	API XML HDS	Capacité brute totale (somme de tous les disques de la baie)
		ID du pool de stockage	Mise en œuvre	API XML HDS	
		Capacité utilisée	Mise en œuvre	API XML HDS	
	Alias WWN	Alias de l’hôte	Mise en œuvre	API XML HDS	
		Type d’objet	Mise en œuvre	API XML HDS	
		Source	Mise en œuvre	API XML HDS	
		WWN	Mise en œuvre	API XML HDS	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

					écriture sur tous les disques) en Mo/s.
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Débit d'écriture	Mise en œuvre	Exportation/CLI	
		Total d'utilisation	Mise en œuvre	Exportation/CLI	
	Volumétrie	Latence Total	Mise en œuvre	Exportation/CLI	
		Lecture IOPS	Mise en œuvre	Exportation/CLI	Nombre d'IOPS de lecture sur le disque
		Latence lecture	Mise en œuvre	Exportation/CLI	
		Taux de réussite du cache lecture	Mise en œuvre	Exportation/CLI	
		Écriture d'IOPS	Mise en œuvre	Exportation/CLI	
		Taux de réussite total du cache	Mise en œuvre	Exportation/CLI	
		Écriture du taux de réussite du cache	Mise en œuvre	Exportation/CLI	
		Débit de lecture	Mise en œuvre	Exportation/CLI	
		Débit d'écriture	Mise en œuvre	Exportation/CLI	
		Débit total	Mise en œuvre	Exportation/CLI	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Total d'IOPS	Mise en œuvre	Exportation/CLI	
		Écriture de latence	Mise en œuvre	Exportation/CLI	
		Capacité totale	Mise en œuvre	Exportation/CLI	
		Capacité brute	Mise en œuvre	Exportation/CLI	
		Capacité utilisée	Mise en œuvre	Exportation/CLI	
		Rapport de capacité utilisé	Mise en œuvre	Exportation/CLI	
	Volumétrie	Clé	Mise en œuvre	Exportation/CLI	
		ID du serveur	Mise en œuvre	Exportation/CLI	
		Capacité totale	Mise en œuvre	Exportation/CLI	
		Capacité brute	Mise en œuvre	Exportation/CLI	
		Capacité utilisée	Mise en œuvre	Exportation/CLI	
		Rapport de capacité utilisé	Mise en œuvre	Exportation/CLI	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
Utilitaire d'exportation (USPV) / CLI SNM (AMS)	Exportation/CLI				faux	faux	faux	faux
API XML HiCommand Device Manager	API XML HDS	HTTP/HTTPS	2001		vrai	vrai	vrai	vrai

Hitachi Ops Center

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 E790H VSP F1500 VSP F400 VSP F900 VSP G1000 VSP G1500 VSP G600 VSP G800 VSP G900 XP8	80 49 01 05 01 03/05 83 60 69 51 01 05 00 03/02 83 40 76 08 01 08 00 03/04 88 60 65 11 01 08 00 03/05 88 60 65 13 01 08 01 03/02 88-00 03/03 83 40 69 49 01 05 01 03/02 83 40 70 51 01 05 00 03/03 88 60 65 08 01 08 00 03/05 88 60 70 13 01 08 01 03/05 88 60 70 13 01-01 05 01 03/02 83 60 65 49 01 05 00 03/04 83 40 71 51 01 08 00 03/05 88 60 70 11 01 08 00 03/04 88 60 65 13 01 08 01 03/04 88 60 71-00/00:01-03/02 80-01-71-00-96/00:06-70-03/04 80-01-00-00/94:03/02 80-06-71-06-96-00/06-91-76 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

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Volume cible	Mise en œuvre		
		De déduplication	Mise en œuvre		technologie qui entraîne
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
	Volumétrie	Capacité	Mise en œuvre		Capacité utilisée de la copie Snapshot en Mo
		Chemin de jonction	Mise en œuvre		
		Nom	Mise en œuvre		
		Type de protection	Mise en œuvre		
		Capacité brute totale	Mise en œuvre		Capacité brute totale (somme de tous les disques de la baie)
		ID du pool de stockage	Mise en œuvre		
		Provisionnement fin	Mise en œuvre		
		Type	Écart		
		Capacité utilisée	Mise en œuvre		
		Compression activée	Mise en œuvre		
	Carte de volume	LUN	Mise en œuvre		Nom de la lun backend
		Masquage requis	Mise en œuvre		
		Contrôleur de protocole	Mise en œuvre		
		Port de stockage	Mise en œuvre		
		Type	Écart		
	Masque de volume	Initiateur	Mise en œuvre		
		Contrôleur de protocole	Mise en œuvre		
		Port de stockage	Mise en œuvre		
		Type	Écart		

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Débit total	Mise en œuvre		Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
	Volumétrie	Taux de réussite du cache lecture	Mise en œuvre		
		Taux de réussite total du cache	Mise en œuvre		
		Lecture IOPS	Mise en œuvre		Nombre d'IOPS de lecture sur le disque
		Total d'IOPS	Mise en œuvre		
		Écriture d'IOPS	Mise en œuvre		
		Clé	Mise en œuvre		
		Latence lecture	Mise en œuvre		
		Latence Total	Mise en œuvre		
		Écriture de latence	Mise en œuvre		
		ID du serveur	Mise en œuvre		
		Débit de lecture	Mise en œuvre		
		Débit total	Mise en œuvre		Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre		

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST Hitachi Ops Center	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

HDS HNAS (INTERFACE DE LIGNE DE COMMANDE)

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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					
1054					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		État	Mise en œuvre	SSH	texte libre décrivant l'état du périphérique
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		UUID	Mise en œuvre	SSH	
		Version	Mise en œuvre	SSH	version logicielle
	Pool de stockage	Capacité utile des données	Mise en œuvre	SSH	
		Déduplication activée	Mise en œuvre	SSH	Déduplication activée sur le pool de stockage
		Inclure dans la capacité DWH	Mise en œuvre	SSH	Une façon de contrôler les pools de stockage intéressants dans DWH Capacity
		Nom	Mise en œuvre	SSH	
		Groupe RAID	Mise en œuvre	SSH	Indique si StoragePool est un groupe raid
		Rapport brut/utilisable	Mise en œuvre	SSH	ratio pour la conversion de la capacité utilisable en capacité brute
		Capacité utilisée du snapshot	Mise en œuvre	SSH	
		ID du pool de stockage	Mise en œuvre	SSH	
		Provisionnement fin pris en charge	Mise en œuvre	SSH	Si ce volume interne prend en charge le provisionnement fin pour la couche de volume en haut de celui-ci
		Capacité totale allouée	Mise en œuvre	SSH	
		Capacité totale utilisée	Mise en œuvre	SSH	Capacité totale en Mo
		Type	Écart	SSH	
		Virtualisation	Mise en œuvre	SSH	S'agit-il d'un dispositif de virtualisation du stockage ?

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
CLI HDS HNAS	SSH	SSH	22		vrai	vrai	vrai	vrai

HPE Nimble / Alletra 6000 Storage

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 6.1 6.1.8.0 2.502 2.600-677726 1053701 1057650 1064273-opt 6.1.2.400-1042680-opt 6.1.2.300-1028597-opt 6.1.1.300-1020304-opt 6.1.1.200-1005932-opt 6.0.0.500-991061-opt 6.0.0.400-930936-opt 5.2.1.800-882343-opt 5.2.1.700-796142-opt 5.2.1.400-1027043-opt 5.2.1.1100-1048557-opt 6.1.2.500

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

	volume	Contrôleur de protocole	Mise en œuvre	HTTPS	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Alias WWN	Alias de l’hôte	Mise en œuvre	HTTPS	
		Type d’objet	Mise en œuvre	HTTPS	
		Source	Mise en œuvre	HTTPS	
		WWN	Mise en œuvre	HTTPS	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
					(lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre	HTTPS	
	Volumétrie	Capacité brute	Mise en œuvre	HTTPS	
		Capacité totale	Mise en œuvre	HTTPS	
		Capacité utilisée	Mise en œuvre	HTTPS	
		Rapport de capacité utilisé	Mise en œuvre	HTTPS	
		Total des économies en termes de compression	Mise en œuvre	HTTPS	
		Gain d'espace grâce à la compression	Mise en œuvre	HTTPS	
		Lecture IOPS	Mise en œuvre	HTTPS	Nombre d'IOPS de lecture sur le disque
		Total d'IOPS	Mise en œuvre	HTTPS	
		Écriture d'IOPS	Mise en œuvre	HTTPS	
		Latence lecture	Mise en œuvre	HTTPS	
		Latence Total	Mise en œuvre	HTTPS	
		Écriture de latence	Mise en œuvre	HTTPS	
		Débit de lecture	Mise en œuvre	HTTPS	
		Débit total	Mise en œuvre	HTTPS	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST HP NIMBLE	HTTPS	HTTPS	5392		vrai	faux	vrai	vrai

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 V500R007C71 V600R003C00 V6005C00 V600 V600 VC005C11

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					
1076					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Type	Écart	HTTPS	
		Virtualisation	Mise en œuvre	HTTPS	S’agit-il d’un

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
					stockage ?
	Volumétrie	Capacité	Mise en œuvre	HTTPS	Capacité utilisée de la copie Snapshot en Mo
		Chemin de jonction	Mise en œuvre	HTTPS	
		Nom	Mise en œuvre	HTTPS	
		Capacité brute totale	Mise en œuvre	HTTPS	Capacité brute totale (somme de tous les disques de la baie)
		Redondance	Mise en œuvre	HTTPS	Niveau de redondance
		ID du pool de stockage	Mise en œuvre	HTTPS	
		Provisionnement fin	Mise en œuvre	HTTPS	
		UUID	Mise en œuvre	HTTPS	
		Capacité utilisée	Mise en œuvre	HTTPS	
		Virtualisation	Mise en œuvre	HTTPS	S’agit-il d’un dispositif de virtualisation du stockage ?
	Carte de volume	LUN	Mise en œuvre	HTTPS	Nom de la lun backend
		Contrôleur de protocole	Mise en œuvre	HTTPS	
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mise en œuvre	HTTPS	
		Contrôleur de protocole	Mise en œuvre	HTTPS	
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					
1086					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
					des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre	HTTPS	
	Volumétrie	Taux de réussite du cache lecture	Mise en œuvre	HTTPS	
		Taux de réussite total du cache	Mise en œuvre	HTTPS	
		Écriture du taux de réussite du cache	Mise en œuvre	HTTPS	
		Capacité brute	Mise en œuvre	HTTPS	
		Capacité totale	Mise en œuvre	HTTPS	
		Capacité utilisée	Mise en œuvre	HTTPS	
		Rapport de capacité utilisé	Mise en œuvre	HTTPS	
		Lecture IOPS	Mise en œuvre	HTTPS	Nombre d'IOPS de lecture sur le disque
		Total d'IOPS	Mise en œuvre	HTTPS	
		Écriture d'IOPS	Mise en œuvre	HTTPS	
		Clé	Mise en œuvre	HTTPS	
		Latence lecture	Mise en œuvre	HTTPS	
		Latence Total	Mise en œuvre	HTTPS	
		Écriture de latence	Mise en œuvre	HTTPS	
		ID du serveur	Mise en œuvre	HTTPS	
		Débit de lecture	Mise en œuvre	HTTPS	
		Débit total	Mise en œuvre	HTTPS	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST Huawei OceanStor	HTTPS	HTTPS	8088		vrai	vrai	vrai	vrai
API REST OceanStor Performance Huawei	HTTPS	HTTPS	8088		vrai	faux	vrai	vrai

IBM Cleversafe

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		UUID	Mise en œuvre	HTTPS	
		Version	Mise en œuvre	HTTPS	version logicielle
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Adresses de gestion	Mise en œuvre	HTTPS	
	Pool de stockage	Inclure dans la capacité DWH	Mise en œuvre	HTTPS	Une façon de contrôler les pools de stockage intéressants dans DWH Capacity
		Nom	Mise en œuvre	HTTPS	
		Capacité sur disque physique (Mo)	Mise en œuvre	HTTPS	utilisé comme capacité brute pour le pool de stockage
		Groupe RAID	Mise en œuvre	HTTPS	Indique si StoragePool est un groupe raid
		Rapport brut/utilisable	Mise en œuvre	HTTPS	ratio pour la conversion de la capacité utilisable en capacité brute
		ID du pool de stockage	Mise en œuvre	HTTPS	
		Provisionnement fin pris en charge	Mise en œuvre	HTTPS	Si ce volume interne prend en charge le provisionnement fin pour la couche de volume en haut de celui-ci
		Capacité totale allouée	Mise en œuvre	HTTPS	
		Capacité totale utilisée	Mise en œuvre	HTTPS	Capacité totale en Mo
		Type	Écart	HTTPS	
		Virtualisation	Mise en œuvre	HTTPS	S'agit-il d'un dispositif de virtualisation du stockage ?

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST IBM CLEVERSAFE	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					
1100					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
	Masque de volume	Initiateur	Mise en œuvre	DSNI	
		Contrôleur de protocole	Mise en œuvre	DSNI	
		Port de stockage	Mise en œuvre	DSNI	
	Alias WWN	Alias de l’hôte	Mise en œuvre	DSNI	
		Système d’exploitation hôte	Mise en œuvre	DSNI	
		Type d’objet	Mise en œuvre	DSNI	
		Source	Mise en œuvre	DSNI	
		WWN	Mise en œuvre	DSNI	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Capacité brute	Mise en œuvre	DSNI	
		Capacité utilisée	Mise en œuvre	DSNI	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Rapport de capacité utilisé	Mise en œuvre	DSNI	
	Volumétrie	Taux de réussite du cache lecture	Mise en œuvre	DSNI	
		Taux de réussite total du cache	Mise en œuvre	DSNI	
		Écriture du taux de réussite du cache	Mise en œuvre	DSNI	
		Capacité brute	Mise en œuvre	DSNI	
		Capacité totale	Mise en œuvre	DSNI	
		Capacité utilisée	Mise en œuvre	DSNI	
		Rapport de capacité utilisé	Mise en œuvre	DSNI	
		Lecture IOPS	Mise en œuvre	DSNI	Nombre d'IOPS de lecture sur le disque
		Total d'IOPS	Mise en œuvre	DSNI	
		Écriture d'IOPS	Mise en œuvre	DSNI	
		Clé	Mise en œuvre	DSNI	
		Latence lecture	Mise en œuvre	DSNI	
		Latence Total	Mise en œuvre	DSNI	
		Écriture de latence	Mise en œuvre	DSNI	
		ID du serveur	Mise en œuvre	DSNI	
		Débit de lecture	Mise en œuvre	DSNI	
		Débit total	Mise en œuvre	DSNI	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre	DSNI	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
Assistant de configuration de la source de données	Saisie manuelle				vrai	vrai	vrai	vrai
INTERFACE DE LIGNE DE COMMANDE IBM DS	DSNI	DSNI			vrai	vrai	vrai	vrai

IBM PowerVM (SSH)

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Nom	Mise en œuvre	SSH	
		OID	Mise en œuvre	SSH	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Type de plate-forme	Mise en œuvre	SSH	
	Info	Nom de la source de données	Mise en œuvre	SSH	Info
		Date	Mise en œuvre	SSH	
		ID émetteur	Mise en œuvre	SSH	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
Accès SSH à IBM Hardware Management Console	SSH	SSH	22		vrai	faux	vrai	vrai

IBM SVC (CLI)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
-12F-12G-AFF 24C-24F-24G-2N4-3H4-3N2-3N4-92F-92G-12F-24F-24G-AFH4-AFP4—AGH4----------9848-9848—9848-9843-9848-9843-4680-9846-4680-4680-4983-4666-4680-4662-4662-4666-4657-2078-2078-324 2078-424 2078-4657-924 4662-2078-2078-224 2078-2078-2078-2077-424 2077-2078-2077-2076-2078-2077-2076-524 2076-624 2076-724 2076-824 2076-F-2076-124 2076-2076-224 2076-2076-2072-2072-2072-2072-2072-324 2072-2072-2072-2072-2072-2072-2072-224 2072-2072-F	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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Capacité utilisée	Mise en œuvre	SSH	
		Virtualisation	Mise en œuvre	SSH	S’agit-il d’un
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires** stockage ?
		Capacité écrite	Mise en œuvre	SSH	Capacité totale écrite sur ce volume par un hôte en Mo
		Compression activée	Mise en œuvre	SSH	
		Chiffrées	Mise en œuvre	SSH	
	Carte de volume	LUN	Mise en œuvre	SSH	Nom de la lun backend
		Contrôleur de protocole	Mise en œuvre	SSH	
		Port de stockage	Mise en œuvre	SSH	
	Masque de volume	Initiateur	Mise en œuvre	SSH	
		Contrôleur de protocole	Mise en œuvre	SSH	
		Port de stockage	Mise en œuvre	SSH	
		Type	Écart	SSH	
	Alias WWN	Alias de l’hôte	Mise en œuvre	SSH	
		Type d’objet	Mise en œuvre	SSH	
		Source	Mise en œuvre	SSH	
		WWN	Mise en œuvre	SSH	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Utilisation de la lecture	Mise en œuvre	SSH	
		Total d'utilisation	Mise en œuvre	SSH	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Utilisation, écriture	Mise en œuvre	SSH	
	Volumétrie	Taux de réussite du cache lecture	Mise en œuvre	SSH	
		Taux de réussite total du cache	Mise en œuvre	SSH	
		Écriture du taux de réussite du cache	Mise en œuvre	SSH	
		Capacité brute	Mise en œuvre	SSH	
		Capacité totale	Mise en œuvre	SSH	
		Capacité utilisée	Mise en œuvre	SSH	
		Capacité écrite	Mise en œuvre	SSH	
		Rapport de capacité utilisé	Mise en œuvre	SSH	
		Ratio capacité écrit	Mise en œuvre	SSH	
		Lecture IOPS	Mise en œuvre	SSH	Nombre d'IOPS de lecture sur le disque
		Total d'IOPS	Mise en œuvre	SSH	
		Écriture d'IOPS	Mise en œuvre	SSH	
		Latence lecture	Mise en œuvre	SSH	
		Latence Total	Mise en œuvre	SSH	
		Écriture de latence	Mise en œuvre	SSH	
		Débit de lecture	Mise en œuvre	SSH	
		Débit total	Mise en œuvre	SSH	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre	SSH	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
CLI IBM SVC	SSH	SSH	22		vrai	faux	vrai	vrai

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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

				XIV	
		Redondance	Mise en œuvre	INTERFACE DE LIGNE DE COMMANDE XIV	Niveau de redondance
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Compression activée	Mise en œuvre	INTERFACE DE LIGNE DE COMMANDE XIV	
	Carte de volume	LUN	Mise en œuvre	INTERFACE DE LIGNE DE COMMANDE XIV	Nom de la lun backend
		Contrôleur de protocole	Mise en œuvre	INTERFACE DE LIGNE DE COMMANDE XIV	
	Masque de volume	Initiateur	Mise en œuvre	INTERFACE DE LIGNE DE COMMANDE XIV	
		Contrôleur de protocole	Mise en œuvre	INTERFACE DE LIGNE DE COMMANDE XIV	
	Alias WWN	Source	Mise en œuvre	INTERFACE DE LIGNE DE COMMANDE XIV	
		Alias de l’hôte	Mise en œuvre	INTERFACE DE LIGNE DE COMMANDE XIV	
		WWN	Mise en œuvre	INTERFACE DE LIGNE DE COMMANDE XIV	
		Type d’objet	Mise en œuvre	INTERFACE DE LIGNE DE COMMANDE XIV	
		Système d’exploitation hôte	Mise en œuvre	INTERFACE DE LIGNE DE COMMANDE XIV	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
INTERFACE DE LIGNE DE COMMANDE IBM DS	DSNI	DSNI			vrai	vrai	vrai	vrai
INTERFACE DE LIGNE DE COMMANDE IBM XIV	INTERFACE DE LIGNE DE COMMANDE XIV	TCP	7778		vrai	faux	vrai	faux

Infinidat Box (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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

	masque de volume	Contrôleur de protocole	Mise en œuvre	HTTPS	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Alias WWN	Alias de l'hôte	Mise en œuvre	HTTPS	
		Type d'objet	Mise en œuvre	HTTPS	
		Source	Mise en œuvre	HTTPS	
		WWN	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST Infinidat	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

Ressources de calcul Microsoft Azure

Modèles et versions pris en charge par ce collecteur de données : versions API :

- 1 juin 2018

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

	Disque de Virtualmachine	OID	Mise en œuvre	HTTPS	
		ID objet virtualDisk	Mise en œuvre	HTTPS	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		OID de Virtualmachine	Mise en œuvre	HTTPS	
	Hôte	Système d’exploitation hôte	Mise en œuvre	HTTPS	
		IPS	Mise en œuvre	HTTPS	
		Fabricant	Mise en œuvre	HTTPS	
		Nom	Mise en œuvre	HTTPS	
		OID	Mise en œuvre	HTTPS	
	Info	Description de l’API	Mise en œuvre	HTTPS	
		Nom de l’API	Mise en œuvre	HTTPS	
		Version de l’API	Mise en œuvre	HTTPS	
		Nom de la source de données	Mise en œuvre	HTTPS	Info
		Date	Mise en œuvre	HTTPS	
		ID émetteur	Mise en œuvre	HTTPS	
		Clé d’émetteur	Mise en œuvre	HTTPS	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					
1150					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
					des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre	HTTPS	
	vm	Capacité totale	Mise en œuvre	HTTPS	
		Utilisation totale du processeur	Mise en œuvre	HTTPS	
		Lecture IOPS	Mise en œuvre	HTTPS	Nombre d'IOPS de lecture sur le disque
		DiskIops.total	Mise en œuvre	HTTPS	
		Écriture d'IOPS du disque	Mise en œuvre	HTTPS	
		Débit de lecture du disque	Mise en œuvre	HTTPS	
		Débit de lecture	Mise en œuvre	HTTPS	débit total en lecture du disque
		Écriture du débit du disque	Mise en œuvre	HTTPS	
		Lecture du débit IP	Mise en œuvre	HTTPS	
		Débit total	Mise en œuvre	HTTPS	Débit IP total
		Écriture ipThroughput	Mise en œuvre	HTTPS	
	VM	Capacité totale	Mise en œuvre	HTTPS	
		Clé	Mise en œuvre	HTTPS	
		ID du serveur	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST de calcul Microsoft Azure	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

Microsoft Hyper-V

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

	Disque de Virtualmachine	OID	Mise en œuvre	WMI	
		ID objet virtualDisk	Mise en œuvre	WMI	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		OID de Virtualmachine	Mise en œuvre	WMI	
	Hôte	Nombre de processeurs hôtes	Mise en œuvre	WMI	
		Vitesse du processeur de l'hôte	Mise en œuvre	WMI	
		Domaine hôte	Mise en œuvre	WMI	
		Mémoire installée sur l'hôte	Mise en œuvre	WMI	
		Modèle hôte	Mise en œuvre	WMI	
		Nombre de NIC	Mise en œuvre	WMI	
		Vitesse de la carte réseau	Mise en œuvre	WMI	
		IPS	Mise en œuvre	WMI	
		Fabricant	Mise en œuvre	WMI	
		Nom	Mise en œuvre	WMI	
		OID	Mise en œuvre	WMI	
		Type de plate-forme	Mise en œuvre	WMI	
	Nœud ISCSI	Alias de l'hôte	Mise en œuvre	WMI	
		Nom du nœud	Mise en œuvre	WMI	
		OID	Mise en œuvre	WMI	
		Type	Écart	WMI	
	Info	Nom de la source de données	Mise en œuvre	WMI	Info
		Date	Mise en œuvre	WMI	
		ID émetteur	Mise en œuvre	WMI	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

					(lecture et écriture sur tous les disques) en Mo/s.
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Débit d’écriture	Mise en œuvre	WS-Management	
	vm	Capacité totale	Mise en œuvre	WS-Management	
		Capacité utilisée	Mise en œuvre	WS-Management	
		Rapport de capacité utilisé	Mise en œuvre	WS-Management	
		Utilisation totale du processeur	Mise en œuvre	WS-Management	
		Lecture IOPS	Mise en œuvre	WS-Management	Nombre d’IOPS de lecture sur le disque
		DiskIops.total	Mise en œuvre	WS-Management	
		Écriture d’IOPS du disque	Mise en œuvre	WS-Management	
		Latence Total	Mise en œuvre	WS-Management	
		Débit de lecture du disque	Mise en œuvre	WS-Management	
		Débit de lecture	Mise en œuvre	WS-Management	débit total en lecture du disque
		Écriture du débit du disque	Mise en œuvre	WS-Management	
		Lecture du débit IP	Mise en œuvre	WS-Management	
		Débit total	Mise en œuvre	WS-Management	Débit IP total
		Écriture ipThroughput	Mise en œuvre	WS-Management	
	VM	Capacité totale	Mise en œuvre	WS-Management	
		Capacité utilisée	Mise en œuvre	WS-Management	
		Rapport de capacité utilisé	Mise en œuvre	WS-Management	
		Clé	Mise en œuvre	WS-Management	
		ID du serveur	Mise en œuvre	WS-Management	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
PowerShell	WS-Management	HTTP	5985		vrai	faux	faux	vrai
WMI	WMI	WMI	135		vrai	faux	vrai	vrai

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 7 Data ONTAP 8.2-mode 8.1 7 7.3.3 Data ONTAP 7.4P9D18 7 7 8.2.5 7-mode 7-mode 8.2.3 7-mode 8.2.3P2 7-mode 7.3P3 7-mode 8.2.4 7-mode 8.2.4P4 7-mode 8.2.4P5 8.2-mode 8.2.4P6 7-mode 8.2.5 7-mode 8.2.5P3 8.2.2 7-mode 8.2.5P4 7-mode 8.2 Data ONTAP

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

	Carte de volume	LUN	Mise en œuvre		Nom de la lun backend
		Contrôleur de protocole	Mise en œuvre		
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Type	Écart		
	Masque de volume	Initiateur	Mise en œuvre		
		Contrôleur de protocole	Mise en œuvre		
		Port de stockage	Mise en œuvre		
		Type	Écart		

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
		Débit d’écriture	Mise en œuvre		
		Utilisation de la lecture	Mise en œuvre		
		Total d’utilisation	Mise en œuvre		
		Utilisation, écriture	Mise en œuvre		
	Volumétrie	Capacité brute	Mise en œuvre		
		Capacité totale	Mise en œuvre		
		Capacité utilisée	Mise en œuvre		
		Rapport de capacité utilisé	Mise en œuvre		
		Lecture de densité d’E/S.	Mise en œuvre		
		Densité d’E/S totale	Mise en œuvre		
		Densité des E/S d’écriture	Mise en œuvre		
		Lecture IOPS	Mise en œuvre		Nombre d’IOPS de lecture sur le disque
		Total d’IOPS	Mise en œuvre		
		Écriture d’IOPS	Mise en œuvre		
		Latence lecture	Mise en œuvre		
		Latence Total	Mise en œuvre		
		Écriture de latence	Mise en œuvre		
		Rapport de blocage partiel	Mise en œuvre		
		Débit de lecture	Mise en œuvre		
		Débit total	Mise en œuvre		Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d’écriture	Mise en œuvre		
		Écriture en attente	Mise en œuvre		nombre total d’écritures en attente

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
NetApp 7 mode ZAPI	ZAPI	ZAPI			vrai	vrai	vrai	vrai

NetApp E-Series REST

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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Virtualisation	Mise en œuvre	HTTPS	S’agit-il d’un dispositif de virtualisation du stockage ?
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Chiffrées	Mise en œuvre	HTTPS	
	Volumétrie	Capacité	Mise en œuvre	HTTPS	Capacité utilisée de la copie Snapshot en Mo
		Type de disque	Non disponible	HTTPS	
		Nom	Mise en œuvre	HTTPS	
		Capacité brute totale	Mise en œuvre	HTTPS	Capacité brute totale (somme de tous les disques de la baie)
		Redondance	Mise en œuvre	HTTPS	Niveau de redondance
		ID du pool de stockage	Mise en œuvre	HTTPS	
		Provisionnement fin	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	
		UUID	Mise en œuvre	HTTPS	
		Capacité utilisée	Mise en œuvre	HTTPS	
		Virtualisation	Mise en œuvre	HTTPS	S’agit-il d’un dispositif de virtualisation du stockage ?
		Chiffrées	Mise en œuvre	HTTPS	
	Carte de volume	LUN	Mise en œuvre	HTTPS	Nom de la lun backend
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mise en œuvre	HTTPS	
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances	Stockage	Taux de réussite du cache lecture	Mise en œuvre	HTTPS	
		Taux de réussite total du cache	Mise en œuvre	HTTPS	
		Écriture du taux de réussite du cache	Mise en œuvre	HTTPS	
		Échec de la capacité brute	Mise en œuvre	HTTPS	
		Capacité brute	Mise en œuvre	HTTPS	
		Capacité brute disponible	Mise en œuvre	HTTPS	Capacité brute des disques de spare (somme de tous les disques de spare)
		Capacité des stockagePools	Mise en œuvre	HTTPS	
		Autres IOPS	Mise en œuvre	HTTPS	
		Lecture IOPS	Mise en œuvre	HTTPS	Nombre d'IOPS de lecture sur le disque
		Total d'IOPS	Mise en œuvre	HTTPS	
		Écriture d'IOPS	Mise en œuvre	HTTPS	
		Clé	Mise en œuvre	HTTPS	
		Latence lecture	Mise en œuvre	HTTPS	
		Latence Total	Mise en œuvre	HTTPS	
		Écriture de latence	Mise en œuvre	HTTPS	
		ID du serveur	Mise en œuvre	HTTPS	
		Débit de lecture	Mise en œuvre	HTTPS	
		Débit total	Mise en œuvre	HTTPS	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST NetApp E-Series	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

Amazon FSX pour NetApp ONTAP

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
FSX pour ONTAP	ONTAP de données

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					
1196					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

	Virtualmachine				
	Virtualmachine StoragePool lRef	ID du pool de stockage	Mise en œuvre	HTTPS	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
	Réf. Volume Virtualmachine	Nom du volume	Mise en œuvre	HTTPS	
	Volumétrie	Capacité	Mise en œuvre	HTTPS	Capacité utilisée de la copie Snapshot en Mo
		Groupe de disques	Mise en œuvre	HTTPS	Type de groupe de disques
		Chemin de jonction	Mise en œuvre	HTTPS	
		Heure du dernier accès connu	Mise en œuvre	HTTPS	Dernier accès au volume connu
		Nom	Mise en œuvre	HTTPS	
		ID de qtree	Mise en œuvre	HTTPS	id unique du qtree
		Capacité brute totale	Mise en œuvre	HTTPS	Capacité brute totale (somme de tous les disques de la baie)
		ID du pool de stockage	Mise en œuvre	HTTPS	
		Provisionnement fin	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	
		UUID	Mise en œuvre	HTTPS	
		Capacité utilisée	Mise en œuvre	HTTPS	
		Chiffrées	Mise en œuvre	HTTPS	
	Carte de volume	LUN	Mise en œuvre	HTTPS	Nom de la lun backend
		Contrôleur de protocole	Mise en œuvre	HTTPS	
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mise en œuvre	HTTPS	
		Contrôleur de protocole	Mise en œuvre	HTTPS	
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Capacité utilisée du snapshot	Mise en œuvre	HTTPS	
Solution NetApp	**Catégorie**	**Capacité/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Capacité réservée des snapshots	Mise en œuvre	HTTPS	
	Virtualmachine	Capacité totale	Mise en œuvre	HTTPS	
		Capacité utilisée	Mise en œuvre	HTTPS	
		Clé	Mise en œuvre	HTTPS	
		ID du serveur	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API NetApp ONTAP	HTTP/HTTPS	HTTP/HTTPS	80/443		vrai	vrai	vrai	vrai

NetApp clustered Data ONTAP versions 8.1 et supérieures

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
AFF ASA ASA ASA FAS8200 FAS8300 FAS8700-A150 AFF ASA ASA FAS2620 FAS2650 FAS2720 FAS2750 FAS2820 FAS9000 FAS9500-A1K AFF ASA ASA FAS500f-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	• 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
- 9.11.1X12
- 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

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases			• 9.12.1P6 • 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		
1222					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
			• 9.14.1X14 • 9.14.1X20 • 9.14.1X24 • 9.15.0P1 • 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 • 9.15.1X19 • 9.15.1X27 • 9.16.1 • 9.16.1P1 • 9.16.1X16 • 9.16.1X26 • 9.16.1X29 • 9.17.1 • 9.17.1X7 • 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		

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
			• 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 • 9.5.0P6 • 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		

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
			• 9.7.0P9 • 9.7.0X17 • 9.8.0 • 9.8.0P1 • 9.8.0P10 • 9.8.0P11 • 9.8.0P12 • 9.8.0P13 • 9.8.0P14 • 9.8.0P14X5 • 9.8.0P15 • 9.8.0P16 • 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 • 9.9.0 • 9.9.1 • 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		

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
			• 9.9.1P3 • 9.9.1P5X2 • 9.9.1P6 • 9.9.1P7 • 9.9.1P9		

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

					virtualisation du stockage ?
		Chiffrées	Mise en œuvre	HTTPS	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		IOPS limite de QoS	Mise en œuvre	HTTPS	
		Limite QUALITÉ de service MBIT/S	Mise en œuvre	HTTPS	
		Limite QoS brute	Mise en œuvre	HTTPS	
		QoS - règle	Mise en œuvre	HTTPS	
	Carte de volume	LUN	Mise en œuvre	HTTPS	Nom de la lun backend
		Contrôleur de protocole	Mise en œuvre	HTTPS	
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mise en œuvre	HTTPS	
		Contrôleur de protocole	Mise en œuvre	HTTPS	
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
	Virtualmachine	Capacité totale	Mise en œuvre	HTTPS	
		Capacité utilisée	Mise en œuvre	HTTPS	
		Clé	Mise en œuvre	HTTPS	
		ID du serveur	Mise en œuvre	HTTPS	
	Volumétrie	Capacité brute	Mise en œuvre	HTTPS	
		Capacité totale	Mise en œuvre	HTTPS	
		Capacité utilisée	Mise en œuvre	HTTPS	
		Rapport de capacité utilisé	Mise en œuvre	HTTPS	
		Lecture de densité d'E/S.	Mise en œuvre	HTTPS	
		Densité d'E/S totale	Mise en œuvre	HTTPS	
		Densité des E/S d'écriture	Mise en œuvre	HTTPS	
		Lecture IOPS	Mise en œuvre	HTTPS	Nombre d'IOPS de lecture sur le disque
		Total d'IOPS	Mise en œuvre	HTTPS	
		Écriture d'IOPS	Mise en œuvre	HTTPS	
		Latence lecture	Mise en œuvre	HTTPS	
		Latence Total	Mise en œuvre	HTTPS	
		Écriture de latence	Mise en œuvre	HTTPS	
		Rapport de blocage partiel	Mise en œuvre	HTTPS	
		Débit de lecture	Mise en œuvre	HTTPS	
		Débit total	Mise en œuvre	HTTPS	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API NetApp ONTAP	HTTP/HTTPS	HTTP/HTTPS	80/443		vrai	vrai	vrai	vrai

ASA

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
ASA-A1K ASA-A20 ASA-A90	NetApp version 9.16.1: Sam 18 19:31:15 UTC 2025 NetApp version 9.16.1RC1: Lundi 04 10 novembre 39:46 UTC 2024

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Contrôleur de protocole	Mise en œuvre	HTTPS	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mise en œuvre	HTTPS	
		Contrôleur de protocole	Mise en œuvre	HTTPS	
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	
performances	Disque	Lecture IOPS	Mise en œuvre	HTTPS	Nombre d'IOPS de lecture sur le disque
		Total d'IOPS	Mise en œuvre	HTTPS	
		Écriture d'IOPS	Mise en œuvre	HTTPS	
		Clé	Mise en œuvre	HTTPS	
		ID du serveur	Mise en œuvre	HTTPS	
		Débit de lecture	Mise en œuvre	HTTPS	
		Débit total	Mise en œuvre	HTTPS	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre	HTTPS	
		Utilisation de la lecture	Mise en œuvre	HTTPS	
		Total d'utilisation	Mise en œuvre	HTTPS	
		Utilisation, écriture	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
NetApp ASA API	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

NetApp ONTAP REST

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
AFF-A150 AFF-A220 AFF-A250 ASA-A300 ASA-A400 ASA-A70 AFF-A700 AFF-A700s AFF-A800 AFF-A90 AFF-A900 AFF-C190 AFF-C250 AFF-C400 AFF-C800 AFF-A250 AFF-A400 AFF-A800 ASA-C250 ASA-C800 CDvM200 FAS2720 FAS2750 FAS2820 FAS8200 FAS8300 FAS8700 FAS9000 FAS9500 FASDvM300 SIMBOX	• NetappRelease 9.14.1P10: Jeu nov 28 12:32:16 UTC 2024 • NetappRelease 9.14.1P11: Mercredi 22 11:55:28 UTC 2025 • NetappRelease 9.14.1P1 : jeu fév 15 00:45:21 UTC 2024 • NetappRelease 9.14.1P4: Jeu Avr 18 15:59:10 UTC 2024 • NetappRelease 9.14.1P5: Sam 18 19:42:16 UTC 2024 • NetappRelease 9.14.1P6: Mar juin 18 16:11:44 UTC 2024 • NetappRelease 9.14.1P7: Jeu août 01 03:07:44 UTC 2024 • NetappRelease 9.14.1P8: Ven Sep 13 07:12:27 UTC 2024 • NetappRelease 9.14.1P9: LUN Oct 21 18:04:05 UTC 2024 • NetappRelease 9.15.1: Jeu Jul 04 12:21:07 UTC 2024 • NetappRelease 9.15.1P1: Mar Jul 30 05:15:49 UTC 2024 • NetappRelease 9.15.1P2: Mar août 27 16:35:16 UTC 2024 • NetappRelease 9.15.1P3: Mer Sep 25 22:33:44 UTC 2024 • NetappRelease 9.15.1P4: Sun Oct 27 20:15:53 UTC 2024 • NetappRelease 9.15.1P5: Sun Nov 24 16:31:37 UTC 2024 • NetappRelease 9.15.1P6: Mer Déc 04 01:42:39 UTC 2024 • NetappRelease 9.15.1P7: Sam 18 21:34:02 UTC 2025 • NetappRelease 9.15.1RC2: Lundi 24 04 juin 49:55 UTC 2024 • NetappRelease 9.16.1: Sam 18 19:31:15 UTC 2025 • NetappRelease 9.16.1P1 : vendredi 14 03 février 53:50 UTC 2025

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					
1274					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Virtualisation	Mise en œuvre	HTTPS	S'agit-il d'un dispositif de virtualisation du stockage ?
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Chiffrées	Mise en œuvre	HTTPS	
	Carte de volume	LUN	Mise en œuvre	HTTPS	Nom de la lun backend
		Contrôleur de protocole	Mise en œuvre	HTTPS	
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mise en œuvre	HTTPS	
		Contrôleur de protocole	Mise en œuvre	HTTPS	
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					
1290					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Clé	Mise en œuvre	HTTPS	
		ID du serveur	Mise en œuvre	HTTPS	
Solution NetApp	**Catégorie**	**Capacité/attribut réservée des snapshots**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Capacité utilisée du snapshot	Mise en œuvre	HTTPS	
		Rapport de capacité utilisé des snapshots	Mise en œuvre	HTTPS	Signalé comme une série chronologique

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST NetApp ONTAP	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

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 SF9605 SF9608 H410S-0 H410S-1 H410S-2 H500S H610S-1 H610S-2 H610S-4 SF19210 SF38410 SF4805 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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		IOPS en rafale	Mise en œuvre	HTTPS	
		IOPS limite de QoS	Mise en œuvre	HTTPS	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		QoS minimale pour les IOPS	Mise en œuvre	HTTPS	
		QoS - règle	Mise en œuvre	HTTPS	
	Carte de volume	LUN	Mise en œuvre	HTTPS	Nom de la lun backend
		Masquage requis	Mise en œuvre	HTTPS	
		Contrôleur de protocole	Mise en œuvre	HTTPS	
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mise en œuvre	HTTPS	
		Contrôleur de protocole	Mise en œuvre	HTTPS	
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

					écriture sur tous les disques) en Mo/s.
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Débit d'écriture	Mise en œuvre	HTTPS	
		Total d'utilisation	Mise en œuvre	HTTPS	
	Volumétrie	Capacité brute	Mise en œuvre	HTTPS	
		Capacité totale	Mise en œuvre	HTTPS	
		Capacité utilisée	Mise en œuvre	HTTPS	
		Rapport de capacité utilisé	Mise en œuvre	HTTPS	
		Total des économies en termes de compression	Mise en œuvre	HTTPS	
		Lecture IOPS	Mise en œuvre	HTTPS	Nombre d'IOPS de lecture sur le disque
		Total d'IOPS	Mise en œuvre	HTTPS	
		Écriture d'IOPS	Mise en œuvre	HTTPS	
		Clé	Mise en œuvre	HTTPS	
		Latence lecture	Mise en œuvre	HTTPS	
		Latence Total	Mise en œuvre	HTTPS	
		Écriture de latence	Mise en œuvre	HTTPS	
		Rapport de blocage partiel	Mise en œuvre	HTTPS	
		ID du serveur	Mise en œuvre	HTTPS	
		Débit de lecture	Mise en œuvre	HTTPS	
		Débit total	Mise en œuvre	HTTPS	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre	HTTPS	
		Total d'utilisation	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST SolidFire	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					
1310					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Utilisation de la capacité des nœuds métadonnées utilisées en Mo	Mise en œuvre	HTTPS	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Nom du site	Mise en œuvre	HTTPS	
	Pool de stockage	Inclure dans la capacité DWH	Mise en œuvre	HTTPS	Une façon de contrôler les pools de stockage intéressants dans DWH Capacity
		Nom	Mise en œuvre	HTTPS	
		Capacité sur disque physique (Mo)	Mise en œuvre	HTTPS	utilisé comme capacité brute pour le pool de stockage
		Groupe RAID	Mise en œuvre	HTTPS	Indique si StoragePool est un groupe raid
		Rapport brut/utilisable	Mise en œuvre	HTTPS	ratio pour la conversion de la capacité utilisable en capacité brute
		ID du pool de stockage	Mise en œuvre	HTTPS	
		Provisionnement fin pris en charge	Mise en œuvre	HTTPS	Si ce volume interne prend en charge le provisionnement fin pour la couche de volume en haut de celui-ci
		Capacité totale allouée	Mise en œuvre	HTTPS	
		Capacité totale utilisée	Mise en œuvre	HTTPS	Capacité totale en Mo
		Type	Écart	HTTPS	
		Virtualisation	Mise en œuvre	HTTPS	S’agit-il d’un dispositif de virtualisation du stockage ?

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
					des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d’écriture	Mise en œuvre		
	Données du nœud de stockage	Clé	Mise en œuvre		
		Métadonnées autorisées d’utilisation de la capacité des nœuds	Mise en œuvre		
		Utilisation totale de la capacité des nœuds	Mise en œuvre		
		Utilisation de la capacité des nœuds utilisable	Mise en œuvre		
		Utilisation de la capacité des nœuds	Mise en œuvre		
		Métadonnées utilisées dans l’utilisation de la capacité des nœuds	Mise en œuvre		
		ID du serveur	Mise en œuvre		
		Débit de lecture	Mise en œuvre		
		Débit total	Mise en œuvre		Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d’écriture	Mise en œuvre		
	StoragePool	Capacité provisionnée	Mise en œuvre		
		Capacité brute	Mise en œuvre		
		Capacité totale	Mise en œuvre		
		Capacité utilisée	Mise en œuvre		
		Rapport de capacité de surengagement	Mise en œuvre		Signalé comme une série chronologique
		Rapport de capacité utilisé	Mise en œuvre		

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
L'API REST de StorageGRID	HTTPS	HTTPS	443		vrai	faux	vrai	vrai

Nutanix Storage (REST)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
NX—G7 NX—G7 HPE DX380 12LFF G11 HPE DX380-G10 HPE DX385-12 GEN10 PLUS NX—G6 NX—G7 NX-3170-G8 NX-3155G-G7 NX-3155G-G8 NX-8150-G6 NX—G8 NX-8150-G7 NX-8155-3170-G8 NX-8035-3060-G8 NX-X8070-3060-NX-3060-G8-NX-24-G8-X8070-NX-G80-G8 NX-8155	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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					
1320					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Contrôleur de protocole	Mise en œuvre	HTTPS	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mise en œuvre	HTTPS	
		Contrôleur de protocole	Mise en œuvre	HTTPS	
		Port de stockage	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					
1330					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
					(lecture et écriture sur tous les disques) en Mo/s.
		Débit d’écriture	Mise en œuvre	HTTPS	
	StoragePool	Lecture IOPS	Mise en œuvre	HTTPS	Nombre d’IOPS de lecture sur le disque
		Total d’IOPS	Mise en œuvre	HTTPS	
		Écriture d’IOPS	Mise en œuvre	HTTPS	
		Débit de lecture	Mise en œuvre	HTTPS	
		Débit total	Mise en œuvre	HTTPS	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d’écriture	Mise en œuvre	HTTPS	
	Volumétrie	Latence Total	Mise en œuvre	HTTPS	
		Lecture IOPS	Mise en œuvre	HTTPS	Nombre d’IOPS de lecture sur le disque
		Latence lecture	Mise en œuvre	HTTPS	
		Écriture d’IOPS	Mise en œuvre	HTTPS	
		Débit de lecture	Mise en œuvre	HTTPS	
		Débit d’écriture	Mise en œuvre	HTTPS	
		Débit total	Mise en œuvre	HTTPS	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Total d’IOPS	Mise en œuvre	HTTPS	
		Écriture de latence	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST de Nutanix	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

Oracle ZFS (HTTPS)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
Sun ZFS Storage 7120 Sun ZFS Storage 7320 Sun ZFS Storage 7330 Sun ZFS Storage 7335 Sun ZFS Storage 7350 Sun ZFS Storage 7370 Sun ZFS Storage 7390 Sun ZFS Storage 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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					
1334					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Capacité utilisée	Mise en œuvre	HTTP/S	
		Virtualisation	Mise en œuvre	HTTP/S	S’agit-il d’un
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires** stockage ?
	Carte de volume	LUN	Mise en œuvre	HTTP/S	Nom de la lun backend
		Masquage requis	Mise en œuvre	HTTP/S	
		Contrôleur de protocole	Mise en œuvre	HTTP/S	
		Port de stockage	Mise en œuvre	HTTP/S	
		Type	Écart	HTTP/S	
	Masque de volume	Initiateur	Mise en œuvre	HTTP/S	
		Contrôleur de protocole	Mise en œuvre	HTTP/S	
		Port de stockage	Mise en œuvre	HTTP/S	
		Type	Écart	HTTP/S	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Capacité des stockagePools	Mise en œuvre		
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Clé	Mise en œuvre		
		ID du serveur	Mise en œuvre		
	Nœud de stockage	Lecture IOPS	Mise en œuvre		Nombre d'IOPS de lecture sur le disque
		Écriture d'IOPS	Mise en œuvre		
		Total d'IOPS	Mise en œuvre		
		Taux de réussite total du cache	Mise en œuvre		
		Débit total	Mise en œuvre		Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Total d'utilisation	Mise en œuvre		
		Débit d'écriture	Mise en œuvre		
		Débit de lecture	Mise en œuvre		
	Données du nœud de stockage	Taux de réussite total du cache	Mise en œuvre		
		Lecture IOPS	Mise en œuvre		Nombre d'IOPS de lecture sur le disque
		Total d'IOPS	Mise en œuvre		
		Écriture d'IOPS	Mise en œuvre		
		Clé	Mise en œuvre		
		ID du serveur	Mise en œuvre		
		Débit de lecture	Mise en œuvre		
		Débit total	Mise en œuvre		Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre		
		Total d'utilisation	Mise en œuvre		
	StoragePool	Total d'IOPS	Mise en œuvre		

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST ORACLE ZFS	HTTP/HTTPS	HTTP/HTTPS	215		vrai	vrai	vrai	vrai

Pure Storage FlashArray (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-X70FA-XFA-X70FA-X70 FA-XFA-X70 FA-XFA-X70FA-X70 FA-X70 FA-X70 FA-X70 FA-X70 FA-X70 FA-X70 FA-X50R3	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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Capacité écrite	Mise en œuvre	HTTP/S	Capacité totale écrite sur ce volume par un hôte en Mo
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Compression activée	Mise en œuvre	HTTP/S	
	Carte de volume	LUN	Mise en œuvre	HTTP/S	Nom de la lun backend
		Contrôleur de protocole	Mise en œuvre	HTTP/S	
		Port de stockage	Mise en œuvre	HTTP/S	
		Type	Écart	HTTP/S	
	Masque de volume	Initiateur	Mise en œuvre	HTTP/S	
		Contrôleur de protocole	Mise en œuvre	HTTP/S	
		Port de stockage	Mise en œuvre	HTTP/S	
		Type	Écart	HTTP/S	
	Alias WWN	Alias de l’hôte	Mise en œuvre	HTTP/S	
		Type d’objet	Mise en œuvre	HTTP/S	
		Source	Mise en œuvre	HTTP/S	
		WWN	Mise en œuvre	HTTP/S	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Capacité utilisée du snapshot	Mise en œuvre		
Solution NetApp	**Catégorie**	**Rapport/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Capacité utilisé des snapshots	Mise en œuvre		Espace chronologique
	Volumétrie	Capacité brute	Mise en œuvre		
		Capacité totale	Mise en œuvre		
		Capacité utilisée	Mise en œuvre		
		Rapport de capacité utilisé	Mise en œuvre		
		Lecture IOPS	Mise en œuvre		Nombre d'IOPS de lecture sur le disque
		Total d'IOPS	Mise en œuvre		
		Écriture d'IOPS	Mise en œuvre		
		Latence lecture	Mise en œuvre		
		Latence Total	Mise en œuvre		
		Écriture de latence	Mise en œuvre		
		Débit de lecture	Mise en œuvre		
		Débit total	Mise en œuvre		Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre		

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST de Pure Storage	HTTP/HTTPS	HTTP/HTTPS	80/443		vrai	vrai	vrai	vrai

Red Hat RHV (REST)

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

	Disque de Virtualmachine	OID	Mise en œuvre	HTTP/S	
		ID objet virtualDisk	Mise en œuvre	HTTP/S	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		OID de Virtualmachine	Mise en œuvre	HTTP/S	
	Hôte	Nombre de processeurs hôtes	Mise en œuvre	HTTP/S	
		Vitesse du processeur de l'hôte	Mise en œuvre	HTTP/S	
		Mémoire installée sur l'hôte	Mise en œuvre	HTTP/S	
		Modèle hôte	Mise en œuvre	HTTP/S	
		Nombre de NIC	Mise en œuvre	HTTP/S	
		Vitesse de la carte réseau	Mise en œuvre	HTTP/S	
		IPS	Mise en œuvre	HTTP/S	
		Fabricant	Mise en œuvre	HTTP/S	
		Nom	Mise en œuvre	HTTP/S	
		OID	Mise en œuvre	HTTP/S	
		Type de plate-forme	Mise en œuvre	HTTP/S	
	Nœud ISCSI	Nom du nœud	Mise en œuvre	HTTP/S	
		OID	Mise en œuvre	HTTP/S	
		Type	Écart	HTTP/S	
	Info	Nom de la source de données	Mise en œuvre	HTTP/S	Info
		Date	Mise en œuvre	HTTP/S	
		ID émetteur	Mise en œuvre	HTTP/S	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST Red Hat RHEV	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					
1366					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Capacité totale allouée	Mise en œuvre	HTTPS	
		Capacité totale utilisée	Mise en œuvre	HTTPS	Capacité totale en Mo
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Type	Écart	HTTPS	
		Virtualisation	Mise en œuvre	HTTPS	S’agit-il d’un dispositif de virtualisation du stockage ?
		Pourcentage de capacité utile effective utilisée	Mise en œuvre	HTTPS	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

					écriture sur tous les disques) en Mo/s.
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Débit d'écriture	Mise en œuvre	HTTPS	
		Total d'utilisation	Mise en œuvre	HTTPS	
	StoragePool	Lecture IOPS	Mise en œuvre	HTTPS	Nombre d'IOPS de lecture sur le disque
		Écriture d'IOPS	Mise en œuvre	HTTPS	
		Débit de lecture	Mise en œuvre	HTTPS	
		Débit d'écriture	Mise en œuvre	HTTPS	
		Débit total	Mise en œuvre	HTTPS	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Total d'IOPS	Mise en œuvre	HTTPS	
		Capacité totale	Mise en œuvre	HTTPS	
		Capacité utilisée	Mise en œuvre	HTTPS	
		Autre capacité utilisée	Mise en œuvre	HTTPS	
		Capacité brute	Mise en œuvre	HTTPS	
		Rapport de capacité utilisé	Mise en œuvre	HTTPS	
		Capacité utile des données	Mise en œuvre	HTTPS	
		Capacité utilisée du snapshot	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST de stockage Rubrik	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

VASTE stock de données

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
VA2437096 VAST Data	Version de build :Release-5.0 1700467 5.0.0.94.0-sp24-1389206 1682647 5.0.0.94 5.1.0.210 version de build : Release-5.0 5.1 5.0.0.133 5.1.0.231.0-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-5.1.1630237-5.1 version de système

Produits pris en charge par ce collecteur de données :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					
1376					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

					en Mo
		Capacité utilisée du snapshot	Mise en œuvre	HTTPS	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		ID du pool de stockage	Mise en œuvre	HTTPS	
		Provisionnement fin pris en charge	Mise en œuvre	HTTPS	Si ce volume interne prend en charge le provisionnement fin pour la couche de volume en haut de celui-ci
		Capacité totale allouée	Mise en œuvre	HTTPS	
		Capacité totale utilisée	Mise en œuvre	HTTPS	Capacité totale en Mo
		Type	Écart	HTTPS	
		Virtualisation	Mise en œuvre	HTTPS	S'agit-il d'un dispositif de virtualisation du stockage ?
		Chiffrées	Mise en œuvre	HTTPS	
	Storage Virtualmachine	Capacité allouée (Mo)	Mise en œuvre	HTTPS	Capacité allouée des snapshots
		Commentaire	Mise en œuvre	HTTPS	
		Clé GUID	Mise en œuvre	HTTPS	Clé globale unique du serveur virtuel de stockage
		Nom	Mise en œuvre	HTTPS	
		Type	Écart	HTTPS	
		UUID	Mise en œuvre	HTTPS	
		Capacité utilisée	Mise en œuvre	HTTPS	
	Réf. Volume interne de Virtualmachine	ID du volume interne	Mise en œuvre	HTTPS	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances	Stockage	Échec de la capacité brute	Mise en œuvre	HTTPS	
		Capacité brute	Mise en œuvre	HTTPS	
		Capacité brute disponible	Mise en œuvre	HTTPS	Capacité brute des disques de spare (somme de tous les disques de spare)
		Capacité des stockagePools	Mise en œuvre	HTTPS	
		Lecture de densité d'E/S.	Mise en œuvre	HTTPS	
		Densité d'E/S totale	Mise en œuvre	HTTPS	
		Densité des E/S d'écriture	Mise en œuvre	HTTPS	
		Autres IOPS	Mise en œuvre	HTTPS	
		Lecture IOPS	Mise en œuvre	HTTPS	Nombre d'IOPS de lecture sur le disque
		Total d'IOPS	Mise en œuvre	HTTPS	
		Écriture d'IOPS	Mise en œuvre	HTTPS	
		Clé	Mise en œuvre	HTTPS	
		Latence lecture	Mise en œuvre	HTTPS	
		Latence Total	Mise en œuvre	HTTPS	
		Écriture de latence	Mise en œuvre	HTTPS	
		ID du serveur	Mise en œuvre	HTTPS	
		Débit de lecture	Mise en œuvre	HTTPS	
		Débit total	Mise en œuvre	HTTPS	Taux total moyen des disques (lecture et écriture sur tous les disques) en Mo/s.
		Débit d'écriture	Mise en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API de VASTES datastores	HTTPS	HTTPS	443		vrai	vrai	vrai	vrai

Centre virtuel NetApp HCI

Modèles et versions pris en charge par ce collecteur de données : versions 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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

	Nœud ISCSI	Alias de l’hôte	Mise en œuvre	Services Web	
		Nom du nœud	Mise en œuvre	Services Web	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		OID	Mise en œuvre	Services Web	
		Type	Écart	Services Web	
	Info	Description de l’API	Mise en œuvre	Services Web	
		Nom de l’API	Mise en œuvre	Services Web	
		Version de l’API	Mise en œuvre	Services Web	
		Nom de l’API du client	Mise en œuvre	Services Web	
		Version de l’API client	Mise en œuvre	Services Web	
		Nom de la source de données	Mise en œuvre	Services Web	Info
		Date	Mise en œuvre	Services Web	
		ID émetteur	Mise en œuvre	Services Web	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Utilisation totale du processeur	Mise en œuvre	Services Web	
Solution NetApp	**Catégorie**	**Fonction de temps d'attente**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		DiskIops.total	Mise en œuvre	Services Web	
		Taux de permutation total	Mise en œuvre	Services Web	
		Débit de lecture	Mise en œuvre	Services Web	débit total en lecture du disque

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST de VMware	Services Web	HTTP/HTTPS	80/443		vrai	vrai	vrai	vrai

VMware Cloud sur AWS

Modèles et versions pris en charge par ce collecteur de données : versions 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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					
1398					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Nom	Mise en œuvre	Services Web	
		OID	Mise en œuvre	Services Web	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Type de plate-forme	Mise en œuvre	Services Web	
	Info	Description de l’API	Mise en œuvre	Services Web	
		Nom de l’API	Mise en œuvre	Services Web	
		Version de l’API	Mise en œuvre	Services Web	
		Nom de l’API du client	Mise en œuvre	Services Web	
		Version de l’API client	Mise en œuvre	Services Web	
		Nom de la source de données	Mise en œuvre	Services Web	Info
		Date	Mise en œuvre	Services Web	
		ID émetteur	Mise en œuvre	Services Web	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances	Hôte	Utilisation totale du processeur	Mise en œuvre	Services Web	
		Lecture IOPS	Mise en œuvre	Services Web	Nombre d'IOPS de lecture sur le disque
		DiskIops.total	Mise en œuvre	Services Web	
		Écriture d'IOPS du disque	Mise en œuvre	Services Web	
		Latence lecture	Mise en œuvre	Services Web	
		Latence Total	Mise en œuvre	Services Web	
		Écriture de latence	Mise en œuvre	Services Web	
		Débit de lecture du disque	Mise en œuvre	Services Web	
		Débit de lecture	Mise en œuvre	Services Web	débit total en lecture du disque
		Écriture du débit du disque	Mise en œuvre	Services Web	
		Lecture du débit IP	Mise en œuvre	Services Web	
		Débit total	Mise en œuvre	Services Web	Débit IP total
		Écriture ipThroughput	Mise en œuvre	Services Web	
		Clé	Mise en œuvre	Services Web	
		Utilisation totale de la mémoire	Mise en œuvre	Services Web	
		ID du serveur	Mise en œuvre	Services Web	
		swapRate.inRate	Mise en œuvre	Services Web	
		Taux de swap	Mise en œuvre	Services Web	
		Taux de permutation total	Mise en œuvre	Services Web	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de la 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 pare-feu (ports statiques)
API REST de VMware	Services Web	HTTP/HTTPS	80/443		vrai	vrai	vrai	vrai

VMware vSphere (services Web)

Modèles et versions pris en charge par ce collecteur de données : versions 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 :

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
bases					
1408					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

	Nœud ISCSI	Alias de l’hôte	Mise en œuvre	Services Web	
		Nom du nœud	Mise en œuvre	Services Web	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		OID	Mise en œuvre	Services Web	
		Type	Écart	Services Web	
	Info	Description de l’API	Mise en œuvre	Services Web	
		Nom de l’API	Mise en œuvre	Services Web	
		Version de l’API	Mise en œuvre	Services Web	
		Nom de l’API du client	Mise en œuvre	Services Web	
		Version de l’API client	Mise en œuvre	Services Web	
		Nom de la source de données	Mise en œuvre	Services Web	Info
		Date	Mise en œuvre	Services Web	
		ID émetteur	Mise en œuvre	Services Web	

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires
performances					

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

Solution NetApp	Catégorie	Fonction/attribut	État	Protocole utilisé	Informations supplémentaires

		Écriture du débit du disque	Mise en œuvre	Services Web	
		Lecture du débit	Mise en œuvre	Services Web	
Solution NetApp	**Catégorie**	**Fonction/attribut**	**État**	**Protocole utilisé**	**Informations supplémentaires**
		Débit total	Mise en œuvre	Services Web	Débit IP total
		Écriture ipThroughput	Mise en œuvre	Services Web	
		Utilisation totale de la mémoire	Mise en œuvre	Services Web	
		swapRate.inRate	Mise en œuvre	Services Web	
		Taux de swap	Mise en œuvre	Services Web	
		Taux de permutation total	Mise en œuvre	Services Web	
		Planifier le temps d'attente	Mise en œuvre	Services Web	Temps d'attente prévu en pourcentage

API de gestion utilisées par ce collecteur de données :

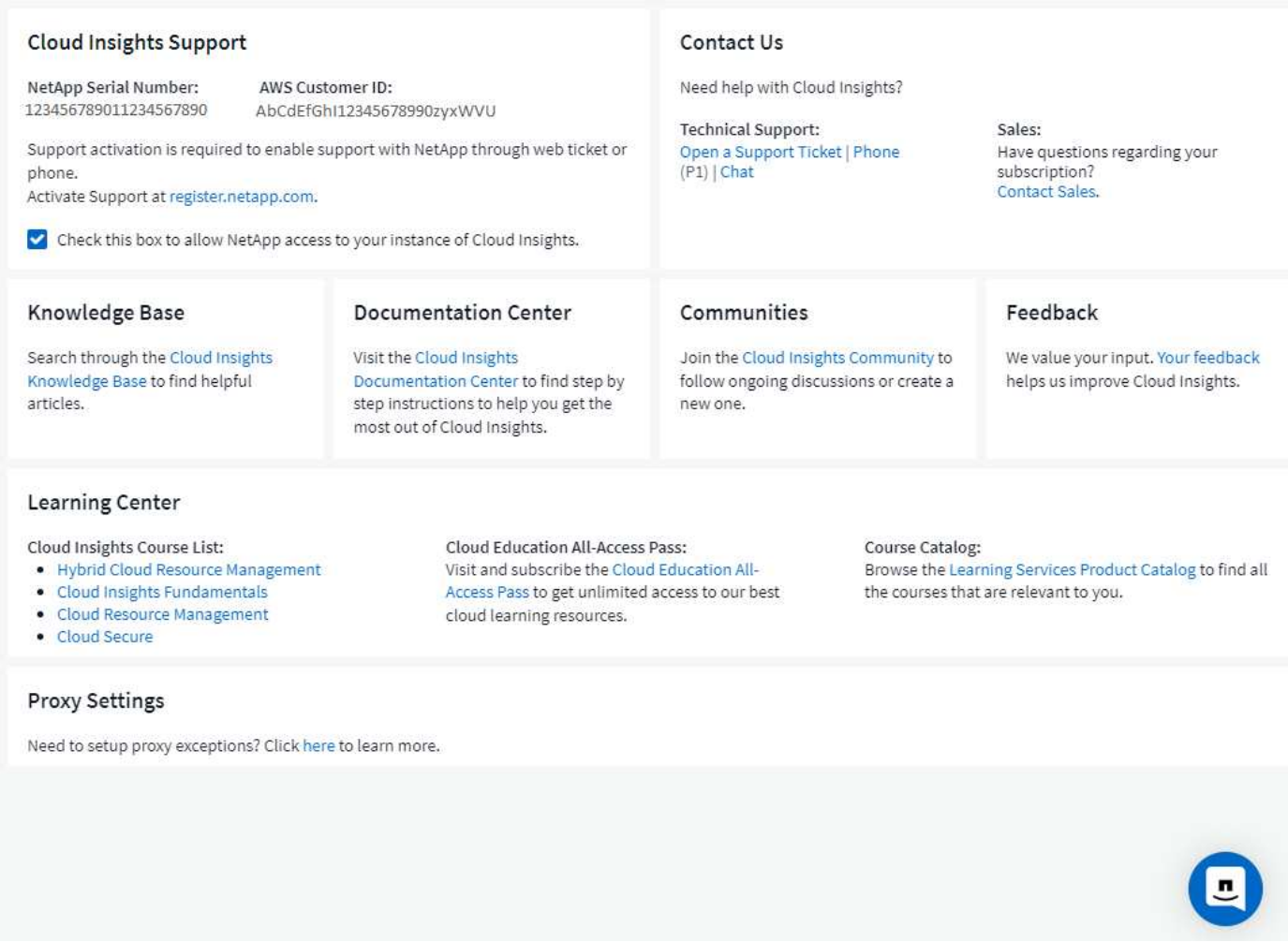
API	Protocole utilisé	Protocole de la couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en lecture seule	Prend en charge le cryptage	Compatible pare-feu (ports statiques)
API REST de VMware	Services Web	HTTP/HTTPS	80/443		vrai	vrai	vrai	vrai

Référence et support

Demande d’aide

sommaire :[]

Vous pouvez accéder aux options de support dans Data Infrastructure Insights en cliquant sur **aide > support**. Les options de support disponibles dépendent de votre édition Data Infrastructure Insights.



Activation des droits de support

Data Infrastructure Insights offre un support en libre-service et par e-mail lorsqu’il est exécuté en mode d’essai. Une fois que vous êtes abonné au service, il est fortement recommandé d’activer les droits de support. L’activation du support technique vous permet d’accéder au support technique via le chat en ligne, le système de gestion de tickets Web et le téléphone. Le mode d’assistance par défaut est en libre-service jusqu’à ce que l’enregistrement soit terminé. Voir détails ci-dessous.

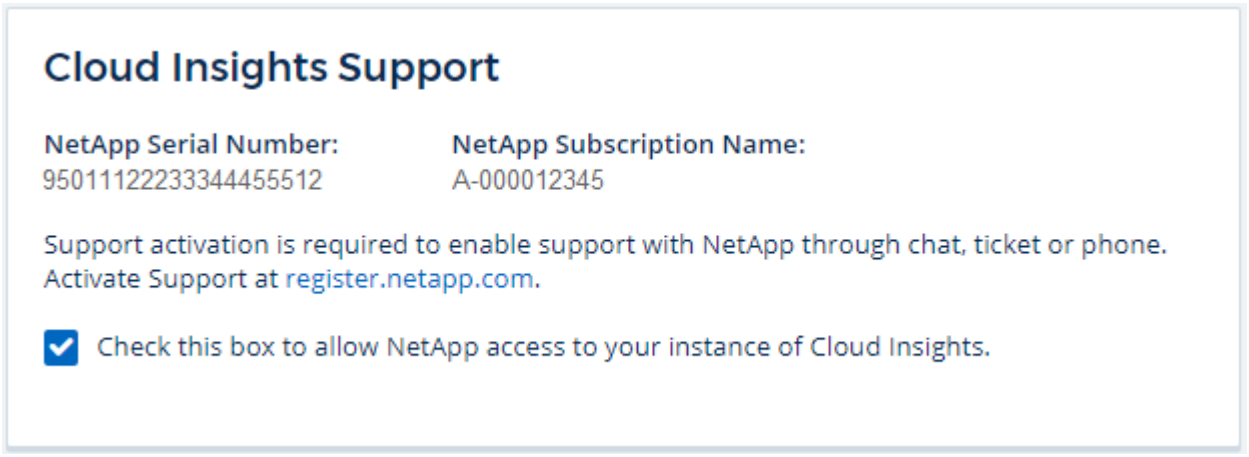
Au cours du processus d’abonnement initial, votre instance Data Infrastructure Insights génère un numéro de série NetApp à 20 chiffres commençant par « 950 ». Ce numéro de série NetApp représente l’abonnement à l’analyse de l’infrastructure de données associé à votre compte. Vous devez enregistrer le numéro de série NetApp pour activer les droits au support. Nous proposons deux options d’inscription aux services de support :

1. Utilisateur avec un compte SSO existant sur le site de support NetApp (NSS) (par exemple, client NetApp actuel)
2. Nouveau client NetApp sans compte SSO existant sur le site de support NetApp (NSS)

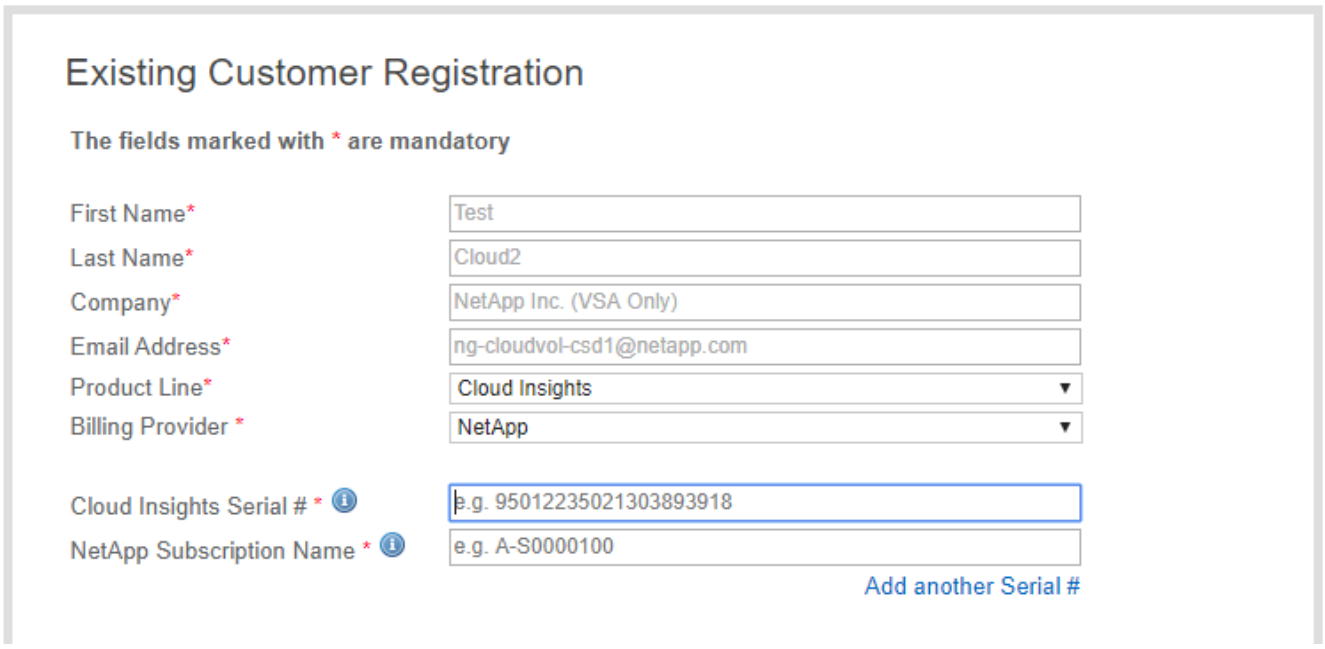
Option 1 : étapes pour un utilisateur avec un compte SSO existant sur le site de support NetApp (NSS)

Étapes

1. Accédez au site Web d'enregistrement NetApp https://register.netapp.com
2. Sélectionnez « Je suis déjà enregistré comme client NetApp » et choisissez « informations sur l'infrastructure de données » comme gamme de produits. Sélectionnez votre fournisseur de facturation (NetApp ou AWS) et indiquez votre numéro de série ainsi que votre nom d'abonnement NetApp ou votre identifiant client AWS en vous reportant au menu « aide > support » de l'interface utilisateur Data Infrastructure Insights :



3. Remplissez le formulaire d'inscription client existant et cliquez sur **Envoyer**.



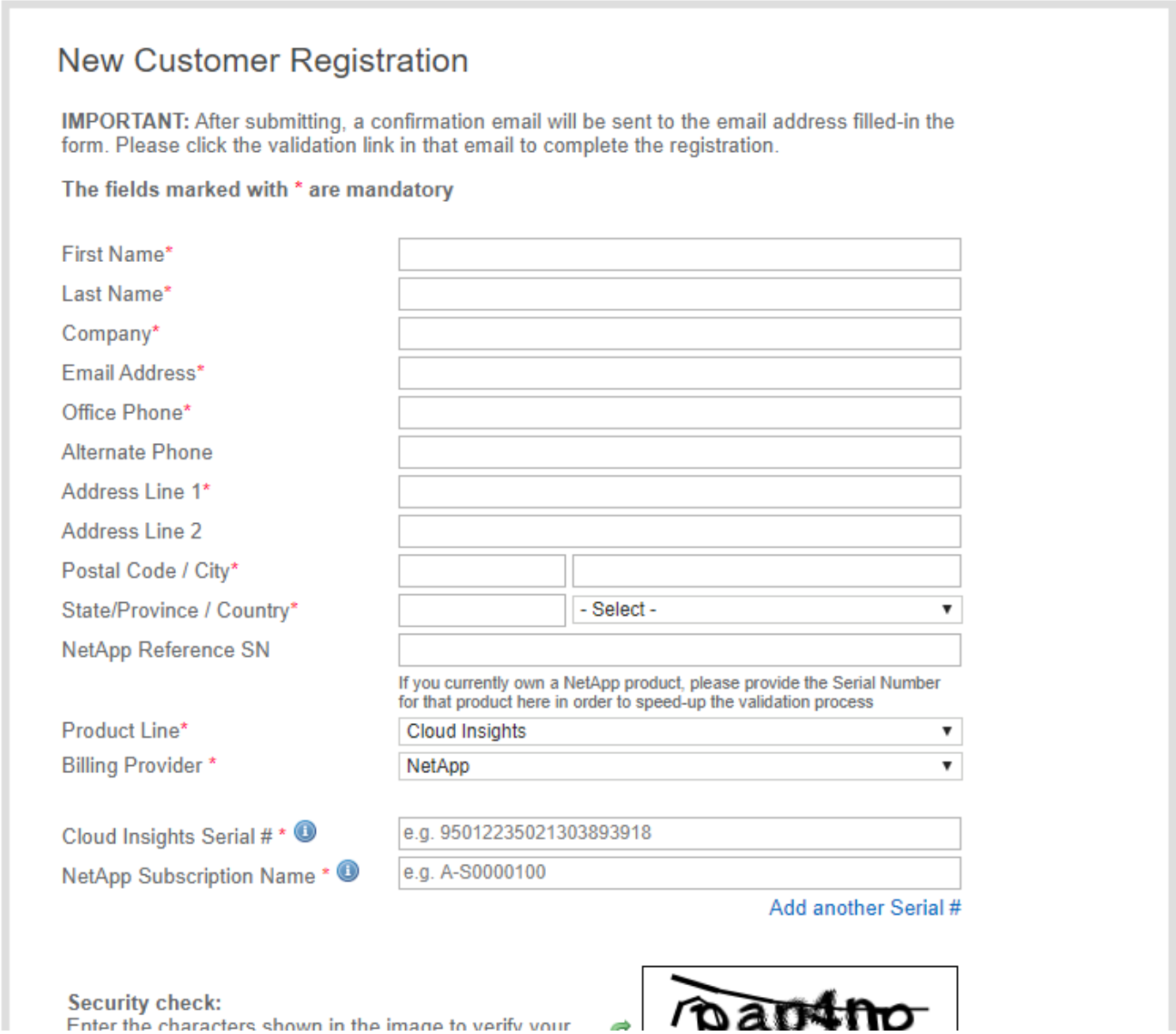
4. Si aucune erreur ne se produit, l'utilisateur est dirigé vers une page "enregistrement soumis avec succès". L'adresse e-mail associée au nom d'utilisateur SSO NSS utilisé pour l'enregistrement recevra un e-mail dans quelques minutes indiquant « votre produit est maintenant éligible pour l'assistance ».

5. Il s'agit d'un enregistrement unique pour le numéro de série de Data Infrastructure Insights NetApp.

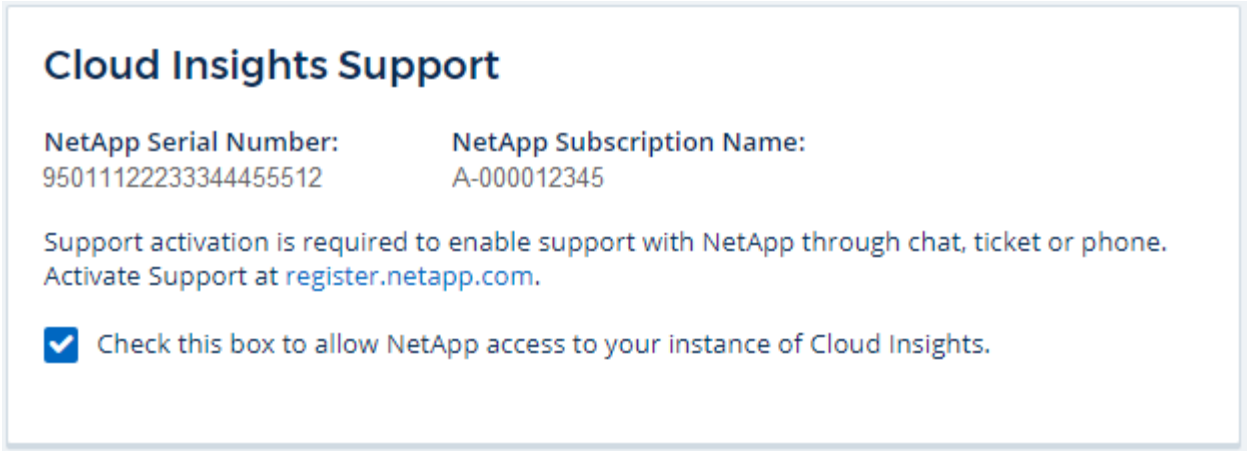
Option 2 : étapes pour un nouveau client NetApp sans compte SSO existant sur le site de support NetApp (NSS)

Étapes

1. Accédez au site Web d'enregistrement NetApp https://register.netapp.com
2. Sélectionnez « Je ne suis pas un client NetApp enregistré » et remplissez le formulaire d'exemple 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 ainsi que votre nom d'abonnement NetApp ou votre identifiant client AWS en vous reportant au menu « aide > support » de l'interface utilisateur Data Infrastructure Insights :



2. Si aucune erreur ne se produit, l'utilisateur est dirigé vers une page "enregistrement soumis avec succès". L'adresse e-mail associée au nom d'utilisateur SSO NSS utilisé pour l'enregistrement recevra un e-mail dans quelques heures indiquant « votre produit est maintenant éligible pour l'assistance ».
3. En tant que nouveau client NetApp, vous devrez également créer un compte utilisateur sur le site de support NetApp (NSS) pour les inscriptions futures et accéder au portail de support pour accéder au chat qui fournit des informations sur le support technique et à la création de tickets en ligne. Ce lien est situé à https://mysupport.netapp.com/eservice/public/now.do. Pour accélérer le processus, vous pouvez fournir le numéro de série Data Infrastructure Insights que vous venez d'enregistrer.
4. Il s'agit d'un enregistrement unique pour le numéro de série Data Infrastructure Insights NetApp.

Obtention d'informations de support

NetApp prend en charge les informations d'infrastructure de données de différentes manières. De nombreuses options de support en libre-service sont disponibles 24 h/24, 7 j/7, comme 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 via la billetterie Web. Un compte SSO du site de support NetApp (NSS) est nécessaire pour la gestion des dossiers en ligne.

*Le support est disponible avec Basic Edition tant que tous vos systèmes de stockage NetApp sont couverts au moins par le niveau Premium support.

De nombreuses offres NetApp incluent Data Infrastructure Insights Basic Edition dans le package. Si vous souhaitez effectuer une mise à niveau vers Premium Edition, contactez votre représentant commercial.

Support en libre-service :

Ces options d'assistance sont disponibles en mode d'essai et sont disponibles gratuitement 24h/24, 7j/7 :

- **KnowledgeBase**

  Cliquez sur les liens de cette section pour accéder à la base de connaissances NetApp. Vous pouvez rechercher des articles pertinents et des méthodes d'utilisation, et plus encore.

- * * *"Documentation"

  Pour accéder à ce centre de documentation, cliquez sur le lien Documentation.

- * * *"Communauté"

  En cliquant sur le lien de la communauté, vous accédez à la communauté NetApp Data Infrastructure

Insights, qui vous permet d'entrer en contact avec des pairs et des experts.

Un lien vers des xref:./"* Retour*"informations utiles sur l'infrastructure de données est également disponible.

Assistance par abonnement

En plus des options de libre-service ci-dessus, si vous disposez d'un abonnement aux informations sur l'infrastructure de données ou d'un support payant pour des produits ou des services NetApp surveillés, vous pouvez travailler avec un ingénieur du support NetApp pour résoudre votre problème.

Vous devez vous inscrire activer le supportpour bénéficier des produits cloud NetApp. Pour vous inscrire, rendez-vous sur NetApp's "Inscription au support Services de données cloud".

Lors de votre session de support, il est fortement recommandé de cocher la case afin qu'un ingénieur du support NetApp puisse accéder à votre locataire Data Infrastructure Insights. Ainsi, le technicien pourra résoudre le problème rapidement. Lorsque votre problème est résolu ou que votre session d'assistance a pris fin, vous pouvez décocher la case.

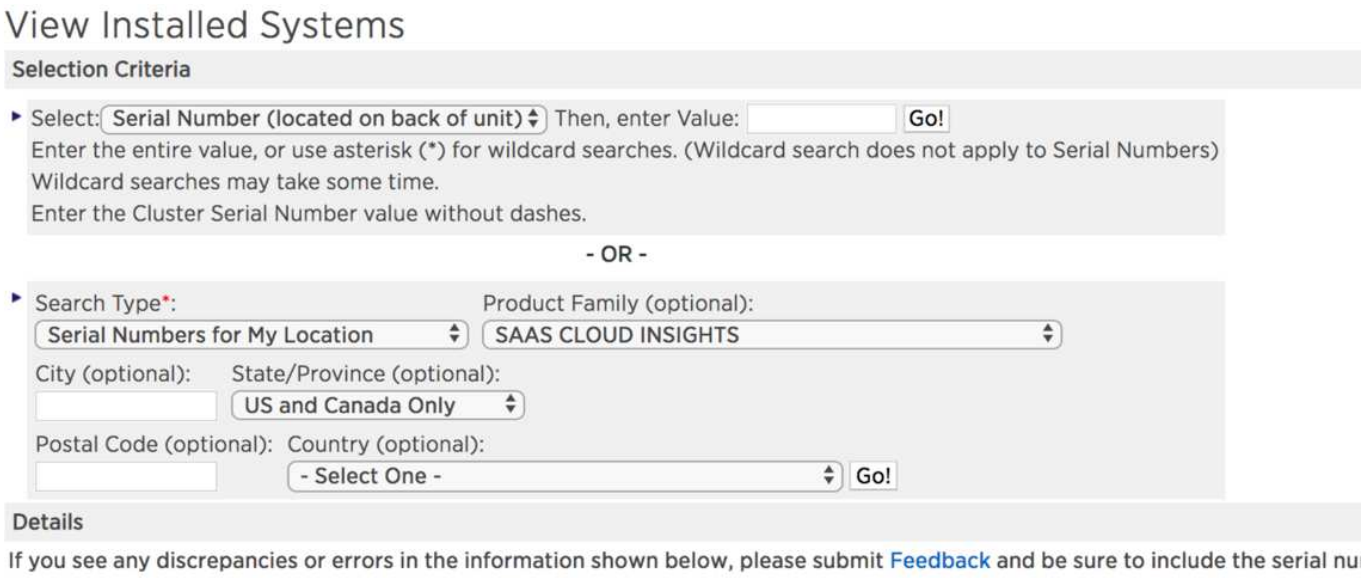
Vous pouvez demander de l'aide par l'une des méthodes suivantes. Vous devez disposer d'un abonnement actif à Data Infrastructure Insights pour utiliser les options de support suivantes :

- **"Téléphone"**
- **"Support Ticket"**
- **Chat** - vous serez mis en relation avec le personnel d'assistance NetApp pour obtenir de l'aide (en semaine seulement). Le chat est disponible dans l'option de menu **aide > Live Chat** en haut à droite de tout écran Data Infrastructure Insights.

Vous pouvez également demander un support commercial en cliquant sur le **"Contactez-nous"** lien.

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 précédemment enregistré un numéro de série avec NetApp, vous pouvez également consulter la liste des numéros de série Data Infrastructure Insights sur le site de support NetApp, en procédant comme suit :

- Connectez-vous à mysupport.netapp.com
- Dans l'onglet produits > Mes produits, utilisez la famille de produits « informations sur l'infrastructure de données SaaS » pour localiser tous les numéros de série enregistrés :



Matrice de prise en charge du Data Collector Data Infrastructure Insights

Vous pouvez afficher ou télécharger des informations et des détails sur les collecteurs de données pris en charge dans le **Data Infrastructure Insights Data Collector support Matrix**, role=« externe ».

Centre de formation

Quel que soit votre abonnement, **aide > support** propose des liens vers plusieurs offres de cours de l'Université NetApp pour vous aider à tirer le meilleur parti des informations sur l'infrastructure de données. Découvrez-les !

Data Collector Reference - 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 aurez peut-être besoin d'informations ou de commandes supplémentaires pour configurer correctement le collecteur de données.

Cliquez sur un **fournisseur** dans le menu à gauche pour afficher les informations relatives à 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 performance à partir des instances EC2.

De formation

Pour collecter des données à partir de terminaux Amazon EC2, vous devez disposer des informations suivantes :

- Vous devez disposer de l'une des options suivantes :
  - 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 **IAM Access Key** et la clé d'accès secrète pour votre compte Cloud Amazon EC2, si vous utilisez l'authentification IAM Access Key.
- Vous devez disposer du privilège « organisation de liste »
- Port 443 HTTPS
- Les instances EC2 peuvent être signalées comme un ordinateur virtuel ou (moins naturellement) comme un hôte. Les volumes EBS peuvent être signalés comme des virtualDisk utilisés par la machine virtuelle, ainsi qu'un datastore fournissant la capacité pour la virtuelleDisk.

Les clés d'accès comprennent un ID de clé d'accès (par exemple, AKIAIOSFONDN7EXAMPLE) et une clé d'accès secrète (par exemple, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). Utilisez des clés d'accès pour signer les demandes de programmation que vous créez à EC2 si vous utilisez les opérations des kits de développement logiciel Amazon EC2, REST ou API de requête. Ces clés sont fournies avec votre contrat Amazon.

Configuration

Entrez 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 lorsqu'il est acquis sur un au dans AWS. Voir ci-dessous pour plus d'informations sur Rôle IAM.
ID de clé d'accès IAM AWS	Entrez l'ID de clé d'accès IAM AWS. Obligatoire si vous n'utilisez pas le rôle IAM.
Clé d'accès secrète AWS IAM	Entrez la clé d'accès secrète IAM AWS. Obligatoire si vous n'utilisez pas le rôle IAM.
J'ai compris les factures AWS pour les demandes d'API	Vérifiez que vous savez qu'AWS vous facture pour les requêtes d'API formulées par l'interrogation Data Infrastructure Insights.

Configuration avancée

Champ	Description
Inclure régions supplémentaires	Spécifiez les régions supplémentaires à inclure dans l'interrogation.
Rôle inter-comptes	Rôle d'accès aux ressources de différents comptes AWS.
Intervalle d'interrogation des stocks (min)	La valeur par défaut est 60
Choisissez exclure ou inclure pour appliquer le filtrage des VM par balises	Indiquez s'il faut inclure ou exclure des VM par des étiquettes lors de la collecte de données. Si l'option "inclure" est sélectionnée, le champ clé d'étiquette ne peut pas être vide.

Champ	Description
Clés de balise et valeurs sur lesquelles filtrer les machines virtuelles	Cliquez sur **+ Filter Tag** pour choisir les VM (et les disques associés) à inclure/exclure en filtrant les clés et les valeurs qui correspondent aux clés et aux valeurs des balises de la VM. La clé d'étiquette est requise, la valeur d'étiquette 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 (s)	La valeur par défaut est 1800
Espace de noms des metrics de CloudWatch Agent	Espace de noms dans EC2/EBS à partir duquel collecter des données. Notez que si les noms des metrics par défaut dans cet espace de noms sont modifiés, Data Infrastructure Insights risque de ne pas pouvoir collecter les données renommées. Il est recommandé de conserver les noms de mesures par défaut.

Clé d'accès IAM

Les clés d'accès sont des identifiants à long terme pour un utilisateur IAM ou l'utilisateur root du compte AWS. Les clés d'accès sont utilisées pour signer des demandes de programmation vers l'interface de ligne de commande AWS ou l'API AWS (directement ou à l'aide du kit de développement logiciel AWS).

Les clés d'accès sont constituées de deux parties : un ID 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 requêtes. Pour plus d'informations, consultez la documentation Amazon sur "Touches d'accès".

Rôle IAM

Lorsque vous utilisez l'authentification *IAM role* (par opposition à l'authentification IAM Access Key), 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 règle pour accorder l'autorisation d'accès à la liste en lecture seule EC2 à toutes les ressources EC2 pour ce rôle IAM. En outre, vous devez accorder l'accès STS (Security Token Service) pour que ce rôle soit autorisé à assumer des comptes croisés de rôles.

Une fois que vous avez créé un rôle IAM, vous pouvez le rattacher à une nouvelle instance EC2 ou à toute instance EC2 existante.

Après avoir associé le rôle IAM *InstanceEc2ReadOnly* à une instance EC2, vous pourrez récupérer les informations d'identification temporaires via les métadonnées de l'instance par le nom de rôle IAM et les utiliser pour accéder aux ressources AWS par toute application exécutée sur cette instance EC2.

Pour plus d'informations, reportez-vous au document Amazon sur "Rôles IAM".

Remarque : le rôle IAM ne peut être utilisé que lorsque l'unité d'acquisition est exécutée dans une instance AWS.

Mappage des balises Amazon avec les annotations Data Infrastructure Insights

Le collecteur de données Amazon EC2 inclut une option qui vous permet de remplir les annotations Data Infrastructure Insights avec des balises configurées sur EC2. Les annotations doivent être nommées exactement comme balises EC2. Data Infrastructure Insights remplit toujours les annotations de type texte portant le même nom et fera une « meilleure tentative » pour remplir les annotations d'autres types (nombre, booléen, etc.). Si votre annotation est de type différent et que le collecteur de données ne parvient pas à la remplir, il peut être nécessaire de supprimer l'annotation et de la recréer en tant que type de texte.

AWS est sensible à la casse, tandis que Data Infrastructure Insights n'est pas sensible à la casse. Par conséquent, si vous créez une annotation nommée « PROPRIÉTAIRE » dans Data Infrastructure Insights et des balises nommées « PROPRIÉTAIRE », « propriétaire » et « propriétaire » dans EC2, toutes les variations EC2 de « propriétaire » seront mappées sur l'annotation « PROPRIÉTAIRE » de Cloud Insight.

Inclure régions supplémentaires

Dans la section AWS Data Collector **Advanced Configuration**, vous pouvez définir le champ **inclure les 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 sur toutes les régions AWS des États-Unis. Pour collecter sur *toutes* régions, définissez ce champ sur **.**. Si le champ **inclure les régions supplémentaires** est vide, le collecteur de données collecte les ressources spécifiées dans le champ **région AWS** comme spécifié dans la section **Configuration**.

Collecte depuis les comptes enfants AWS

Data Infrastructure Insights prend en charge la collecte de comptes enfants pour AWS dans un collecteur de données AWS unique. 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 informations EC2 à partir du compte enfants.
- Chaque compte enfant doit avoir le nom du rôle configuré comme la même chaîne.
- Entrez cette chaîne de nom de rôle dans la section Data Infrastructure Insights AWS Data Collector **Advanced Configuration**, dans le champ **Cross account role**.
- Le compte sur lequel le collecteur est installé doit disposer de *déléguer l'accès administrateur* Privileges. Pour "Documentation AWS"plus d'informations, reportez-vous à la section.

Meilleure pratique : il est fortement recommandé d'attribuer la politique AWS prédéfinie *Amazon EC2ReadOnlyAccess* au compte principal EC2. En outre, l'utilisateur configuré dans la source de données doit avoir au moins la stratégie prédéfinie *AWOrganiztionsReadOnlyAccess*, afin d'interroger AWS.

Pour plus d'informations sur la configuration de votre environnement afin que des informations sur l'infrastructure de données puissent être collectées à partir de comptes enfants AWS, consultez les documents suivants :

"Tutoriel : déléguer l'accès aux comptes AWS à l'aide des rôles IAM"

"Configuration AWS : accès à un utilisateur IAM dans un autre compte AWS dont vous disposez"

"Création d'un rôle pour déléguer des autorisations à un utilisateur IAM"

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Amazon FSX pour le collecteur de données NetApp ONTAP

Ce collecteur de données fait l'acquisition des données d'inventaire et de performance par Amazon FSX pour NetApp ONTAP. Ce collecteur de données sera mis à disposition de manière incrémentielle dans les régions de service Data Infrastructure Insights. Contactez votre représentant commercial si vous ne voyez pas l'icône de ce collecteur dans votre environnement Data Infrastructure Insights.

Ce collecteur d'informations d'infrastructure de données requiert un utilisateur ONTAP avec un rôle *Filesystem-scoped*. Veuillez consulter la "Rôles et règles"documentation AWS pour connaître les options disponibles. À l'heure actuelle, AWS ne prend en charge qu'un seul type de rôle utilisateur avec le champ d'application 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 les trois applications qui lui sont affectées : http, ontapi, ssh.

Terminologie

Les informations d'infrastructure de données font l'acquisition de données d'inventaire et de performances à partir du collecteur de données FSX-NetApp. Pour chaque type d'actif acquis, la terminologie la plus utilisée pour l'actif est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Cluster	Stockage
LUN	Volumétrie
Volumétrie	Volume interne

Terminologie FSX-NetApp

Les termes suivants s'appliquent aux objets ou aux références que vous trouverez sur les pages d'accueil des ressources de stockage FSX-NetApp. Un grand nombre de ces termes s'appliquent également à d'autres collecteurs de données.

Stockage

- Modèle – liste délimitée par des virgules des noms de modèles uniques et discrets de ce cluster.
- Fournisseur : AWS
- Numéro de série – le numéro de série de la baie.
- IP : il s'agit généralement des adresses IP ou des noms d'hôte configurés dans la source de données.
- Capacité brute : somme de base 2 de tous les disques SSD affectés au système de fichiers FSX.
- Latence : représentation des charges de travail côté hôte, à la fois en lecture et en écriture. Idéalement, les informations sur l'infrastructure de données génèrent directement cette valeur, mais ce n'est souvent pas le cas. À la place de la baie qui propose cela, Data Infrastructure Insights effectue généralement un calcul pondéré par IOPS à partir des statistiques des volumes internes individuels.
- Débit : agrégé à partir de volumes internes. Gestion – il peut contenir un lien hypertexte pour l'interface de gestion du périphérique. Créé par programmation par la source de données Data Infrastructure Insights dans le cadre du reporting d'inventaire.

Pool de stockage

- Stockage : sur quelle baie de stockage ce pool vit. Obligatoire.
- Type – valeur descriptive d'une liste de possibilités énumérées. Le plus souvent sera "agrégat" ou "RAID Group".
- Capacité : les valeurs indiquées ici sont les valeurs logiques utilisées, la capacité utilisable et la capacité totale logique, ainsi que le pourcentage utilisé sur ces valeurs.
- IOPS : somme des IOPS de tous les volumes affectés sur ce pool de stockage.
- Débit : somme du débit de tous les volumes affectés sur ce pool de stockage.

De formation

Les conditions 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 affectées : ssh, ontapi, http
- Les détails du compte incluent le nom d'utilisateur et le mot de passe.
- Exigences relatives aux ports : 443

Configuration

Champ	Description
IP de gestion NetApp	Adresse IP ou nom de domaine complet du cluster NetApp
Nom d'utilisateur	Nom d'utilisateur du 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 système FSX pour le stockage NetApp ONTAP :

- fpolicy
- nfsv3
- nfsv3:nœud
- nfsv4
- nfsv4_1
- nfsv4_1:nœud
- nfsv4:nœud
- groupe_de_règles
- qtree
- volumétrie
- volume_charge_de_travail

Notez que les commandes de l'interface de ligne de commande FSX et de l'API récupère des 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 qu'elles se trouvent sur FSX elle-même.

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
Réception 401 réponse HTTP ou 13003 code d'erreur ZAPI et ZAPI renvoie "privilèges insuffisants" ou "non autorisés pour cette commande"	Vérifiez le nom d'utilisateur et le mot de passe, ainsi que les privilèges/autorisations utilisateur.
ZAPI renvoie « le rôle de cluster n'est pas Cluster_mgmt LIF ».	L'au doit communiquer avec l'IP de gestion de cluster. Vérifiez l'adresse IP et remplacez-la par une autre adresse IP si nécessaire
La commande ZAPI échoue après une nouvelle tentative	Problème de communication au 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 l'ordinateur au.
Echec de la connexion à ZAPI via HTTP	Vérifiez si le port ZAPI accepte le texte en clair. Si l'au tente d'envoyer du texte en texte clair vers une socket SSL, la communication échoue.
La communication échoue avec SSLException	Au tente d'envoyer SSL vers un port en texte clair sur un filer. Vérifiez si le port ZAPI accepte SSL ou utilise un autre port.
Autres erreurs de connexion : la réponse ZAPI a 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 n'a pas terminé à temps" la réponse ZAPI contient "initialize_session() retourné environnement NULL" le code d'erreur ZAPI est 14007 et la réponse contient "noeud 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 l'ordinateur au.

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

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 performance à partir des instances de calcul Azure.

De formation

Vous avez besoin des informations suivantes pour configurer ce collecteur de données.

- Port requis : 443 HTTPS

- URI de redirection Azure OAuth 2.0 (login.microsoftonline.com)
- IP REST Azure Management (management.azure.com)
- IP Azure Resource Manager (management.core.windows.net)
- Identifiant d'application principale (client) du service Azure (rôle du lecteur requis)
- Clé d'authentification principale du service Azure (mot de passe utilisateur)
- Vous devez configurer un compte Azure pour la découverte Data Infrastructure Insights.

  Une fois le compte correctement configuré et que vous enregistrez l'application dans Azure, vous disposez des identifiants requis pour découvrir l'instance Azure avec Data Infrastructure Insights. Le lien suivant explique comment configurer le compte pour la découverte. https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

Configuration

Entrez les données dans les champs du collecteur de données conformément au tableau ci-dessous :

Champ	Description
Identifiant d'application principale (client) du service Azure (rôle du lecteur requis)	ID de connexion à Azure. Nécessite un accès au rôle Reader.
ID locataire Azure	ID locataire Microsoft
Clé d'authentification principale du service Azure	Clé d'authentification de connexion
J'ai bien compris que Microsoft me facture pour les demandes d'API	Vérifiez que vous avez bien compris que Microsoft vous facture des demandes d'API formulées par l'interrogation Insight.

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	La valeur par défaut est 60
Choisissez exclure ou inclure pour appliquer le filtrage des VM par balises	Indiquez s'il faut inclure ou exclure des VM par des étiquettes lors de la collecte de données. Si l'option "inclure" est sélectionnée, le champ clé d'étiquette ne peut pas être vide.
Clés de balise et valeurs sur lesquelles filtrer les machines virtuelles	Cliquez sur **+ Filter Tag** pour choisir les VM (et les disques associés) à inclure/exclure en filtrant les clés et les valeurs qui correspondent aux clés et aux valeurs des balises de la VM. La clé d'étiquette est requise, la valeur d'étiquette 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 (s)	La valeur par défaut est 300

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Broadcom

Collecteur de données Brocade Network Advisor

Les informations d'infrastructure de données utilisent le collecteur de données Brocade Network Advisor pour acquérir des données d'inventaire et de performance à partir de commutateurs Brocade.

Terminologie

Les informations d'infrastructure de données font l'acquisition des informations d'inventaire suivantes à partir du collecteur de données Brocade Network Advisor. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Commutateur	Commutateur
Port	Port
Structure virtuelle, structure physique	Structure
Commutateur logique	Commutateur logique

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

Les éléments suivants sont nécessaires pour configurer ce collecteur de données :

- L'unité d'acquisition Data Infrastructure Insights initera les 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 d'administrateur
- Port requis : HTTP/HTTPS 443

Configuration

Champ	Description
IP du serveur Brocade Network Advisor	Adresse IP du serveur Network Advisor
Nom d'utilisateur	Nom d'utilisateur du 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 ce champ est 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 du commutateur
Intervalle d'interrogation des stocks (min)	La valeur par défaut est 40
Passerelle d'accès aux rapports	Cochez cette case pour inclure les périphériques en mode passerelle d'accès
Intervalle d'interrogation des performances (s)	La valeur par défaut est 1800

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
Recevez un message indiquant que plus d'un nœud est connecté 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'obtenez pas directement le périphérique NPV. L'acquisition du commutateur principal de la structure collecte plutôt les données du dispositif NPV.

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données du commutateur FC Brocade

Les informations d'infrastructure de données utilisent la source de données Brocade FC Switch (SSH) pour détecter l'inventaire des commutateurs Brocade ou des commutateurs rebrandés exécutant le micrologiciel FOS (système d'exploitation factorisé) version 4.2 et ultérieure. Les périphériques en mode commutateur FC et passerelle d'accès sont pris en charge.

Terminologie

Les informations d'inventaire suivantes sont acquises à partir du collecteur de données du commutateur FC Brocade. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Commutateur	Commutateur

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Port	Port
Structure virtuelle, structure physique	Structure
Zone	Zone
Commutateur logique	Commutateur logique
Volume virtuel	Volumétrie
Zone LSAN	Zone IVR

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

- L'unité d'acquisition Data Infrastructure Insights (au) initie les connexions au port TCP 22 sur les commutateurs Brocade pour collecter les données d'inventaire. L'UA initiera également les connexions au port UDP 161 pour la collecte des données de performances.
- Il doit y avoir une connectivité IP à tous les commutateurs de la structure. Si vous cochez la case détecter tous les switchs dans la structure, Data Infrastructure Insights identifie tous les switchs de la structure. Cependant, la connectivité IP à ces switchs supplémentaires est nécessaire pour les découvrir.
- Le même compte est nécessaire au niveau global pour tous les commutateurs du maillage. 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 en lecture seule SNMP

Configuration

Champ	Description
IP du commutateur	Adresse IP ou nom de domaine complet du serveur EFC
Nom d'utilisateur	Nom d'utilisateur du commutateur
Mot de passe	Mot de passe du commutateur
SNMP	Version SNMP
Chaîne de communauté SNMP	Chaîne de communauté en lecture seule SNMP 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 de la structure	Nom de la structure à indiquer par le collecteur de données. Laissez vide pour signaler le nom de la structure comme WWN.
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 15.
Périphériques exclus	Liste des ID de périphériques séparés par des virgules à exclure de l'interrogation
Domaines d'administration actifs	Sélectionnez si vous utilisez des domaines Admin
Récupérer les données MPR	Sélectionnez cette option pour acquérir des données de routage à partir de votre routeur multiprotocole.
Activer le recouvrement	Sélectionnez cette option pour activer l'acquisition lors de la réception d'une interruption SNMP à partir du périphérique. Si vous sélectionnez Activer le recouvrement, vous devez également activer SNMP.
Temps minimum entre les recouvrements (s)	Temps minimum entre les tentatives d'acquisition déclenchées par les interruptions. La valeur par défaut est 10.
Découvrir tous les commutateurs du tissu	Sélectionnez pour découvrir tous les commutateurs de la structure
Choisissez de favoriser HBA par rapport aux alias de zone	Choisissez de favoriser les alias de HBA ou de zone
Intervalle d'interrogation des performances (s)	Intervalle entre les sondages de performances. La valeur par défaut est 300.
Protocole d'autorisation 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 SNMP

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
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 survenir lorsque le commutateur Brocade prend trop de temps pour revenir avec une invite, dépassant le délai par défaut de 5 secondes. Dans les paramètres de configuration avancée du collecteur de données dans Data Infrastructure Insights, essayez d'augmenter la valeur *SSH Banner Wait Timeout (sec)* à une valeur supérieure.
Erreur : « les informations de l'infrastructure de données ont reçu un rôle de châssis non valide »	Vérifiez que l'utilisateur configuré dans cette source de données a reçu l'autorisation de rôle de châssis.
Erreur : « adresse IP du châssis non concordante »	En règle générale, DII ne prend pas en charge la traduction d'adresses réseau ni la traduction d'adresses de port entre l'unité d'acquisition et les appareils. DII peut détecter que le nom d'hôte ou l'adresse IP dans la configuration du collecteur ne correspond à aucune des adresses que l'appareil pense détenir.
Recevez un message indiquant que plus d'un nœud est connecté au port Access Gateway	Vérifiez que le périphérique NPV fonctionne correctement et que tous les WWN connectés sont attendus. N'obtenez pas directement le périphérique NPV. L'acquisition du commutateur principal de la structure collecte plutôt les données du dispositif NPV.
Erreur : ….Nombre maximal de sessions à distance pour la connexion…	FOS impose différentes limites quant au nombre de sessions SSH simultanées prises en charge par rôle utilisateur. La session SSH de DII sur cet appareil est rejetée à la connexion pour non-respect de ces limites. Cela peut indiquer que des collecteurs en double découvrent la même ressource, ce qui est à éviter.

Performances

Problème :	Essayer :
Échec de la collecte des performances avec « délai dépassé lors de l'envoi de la requête SNMP ».	Selon les variables de requête et la configuration du commutateur, certaines requêtes peuvent dépasser le délai 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 des réponses SNMP incorrectes. Vous utilisez probablement FOS 8.2.3e. Effectuez la mise à niveau vers la version 8.2.3e2 ou supérieure.

Problème :	Essayer :
Les collectes de performances échouent avec… Nom d'utilisateur inconnu…	Vous avez configuré votre collecteur DII avec un « Nom d'utilisateur SNMP » qui n'est pas attribué à l'un des emplacements utilisateur SNMPv3. La simple création d'un utilisateur sur Brocade FOS ne l'active pas nécessairement comme utilisateur SNMPv3 ; vous devez le placer dans l'un des emplacements utilisateur v3.
Les collections 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 appareil avec plusieurs Virtual Fabrics activés, mais l'utilisateur SNMPv3 ne dispose pas des droits pour le NN VF. DII ne prend pas en charge la découverte partielle d'une ressource physique ; vous devez toujours lui accorder l'accès aux 128 VF possibles de manière proactive, car il tentera toujours de récupérer les données de performances de toute VF existante sur un appareil physique donné.

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données REST Brocade FOS

Data Infrastructure Insights utilise le collecteur REST Brocade FOS pour détecter l'inventaire et les performances des commutateurs Brocade exécutant le firmware FabricOS (FOS) version 8.2 et ultérieure. 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 possible de FOS prise en charge par votre plateforme.

Remarque : le niveau « utilisateur » par défaut de FOS n'est pas suffisamment puissant pour que Data Infrastructure Insights affiche tous les aspects logiques d'un périphérique. Nous avons besoin d'un compte utilisateur avec le rôle « châssis » activé, ainsi que des autorisations sur toutes les structures virtuelles configurées sur un commutateur.

Voici un exemple de procédure permettant de créer un compte utilisateur « avec le moins de privilèges » pour l'utilisation de Data Infrastructure Insights dans une session SSH vers un périphérique FOS :

UserConfig --add NetAppCIUser -r user -l 1-128 -c user -p Qwerty !

Cela créera un utilisateur « NetAppCIUser » avec le mot de passe « Qwerty! ». Cet utilisateur a le rôle « user » (-r) sur les 128 structures virtuelles possibles (-l). Cet utilisateur possède en outre le rôle “Chassis” (-c) requis, avec un accès de niveau utilisateur attribué.

Par défaut, ce collecteur tentera de découvrir tous les périphériques FOS faisant partie de toutes les structures dont le commutateur fait partie.

Remarque : l’utilisateur en lecture seule par défaut de FOS, « utilisateur », NE dispose PAS d’autorisations d’affichage sur toutes les structures virtuelles et ne dispose PAS d’autorisations de « rôle châssis ». Cela signifie que vous aurez peu de chances de réussir à utiliser l’option « 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 à partir du collecteur de données REST Brocade FOS. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l’affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l’esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l’infrastructure de données
Commutateur	Commutateur
Port	Port
Structure virtuelle, structure physique	Structure
Zone	Zone
Commutateur logique	Commutateur logique
Zone LSAN	Zone IVR

Remarque : il s’agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

- Il doit y avoir une connectivité TCP à 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 cochez la case *détecter tous les commutateurs dans la structure*, Data Infrastructure Insights identifie tous les commutateurs de la structure. Cependant, il faut que la connectivité TCP à ces commutateurs supplémentaires soit nécessaire pour les découvrir.
- Le même compte est nécessaire au niveau global pour tous les commutateurs du maillage. Vous pouvez utiliser l’interface Web du périphérique pour confirmer l’accès.

Configuration

Champ	Description
IP du commutateur	Adresse IP ou nom de domaine complet du commutateur FOS
Nom d’utilisateur	Nom d’utilisateur du commutateur
Mot de passe	Mot de passe du commutateur

Configuration avancée

Champ	Description
Périphériques exclus	Liste séparée par des virgules des adresses IPv4 de périphérique à exclure de l'interrogation.
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 60.
Découvrir tous les commutateurs du tissu	Sélectionnez pour découvrir tous les switchs de la structure.
Choisissez de favoriser HBA par rapport aux alias de zone	Choisissez de favoriser les alias de HBA ou de zone.
Type de connexion	HTTP ou HTTPS.
Notez que ce paramètre ne modifie que l'EC de protocole qui tente d'utiliser d'abord par périphérique. L'EC essaiera automatiquement le protocole opposé si la valeur par défaut échoue	Remplacer le port TCP
Spécifiez un port si la valeur par défaut n'est pas utilisée.	Intervalle d'interrogation des performances (s)

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
La fonction de test m'avertit qu'un protocole est inaccessible	Un périphérique Brocade FOS 8.2+ donné ne veut parler que sur HTTP ou HTTPS. Si un commutateur est équipé d'un certificat numérique, le commutateur affichera des erreurs HTTP si l'on tente de communiquer avec lui avec HTTP ou HTTPS non chiffré. La fonction de test tente de communiquer avec HTTP et HTTPS. Si le test vous indique qu'un protocole réussit, vous pouvez enregistrer le collecteur en toute sécurité et ne vous inquiétez pas que l'autre protocole a échoué. Le collecteur tentera les deux protocoles pendant la collecte et n'échouera que si aucun des deux protocoles ne fonctionne.
Erreur : l'inventaire échoue avec l'erreur 401 Non autorisé… Clé de session non valide…	Il s'agit d'un bug spécifique présent dans certaines versions 8.2 FOS très anciennes, comme la 8.2.1c, qui ne prennent pas correctement en charge l'authentification HTTP de base. Effectuez une mise à niveau vers une version 8.2 ou 9.* ultérieure.
Erreur : « les informations de l'infrastructure de données ont reçu un rôle de châssis non valide »	Vérifiez que l'utilisateur configuré dans cette source de données a reçu l'autorisation de rôle de châssis.
Erreur : « adresse IP du châssis non concordante »	Modifiez la configuration de la source de données pour utiliser l'adresse IP du châssis.

Problème :	Essayer :
Échec de l'inventaire avec un 403 interdit	Il peut s'agir simplement de mauvaises informations d'identification ou indiquer que vous essayez d'utiliser un rôle suffisamment puissant. Rappelez-vous que les utilisateurs de niveau « utilisateur » NE disposent PAS du droit requis de « rôle de châssis », ou consultez l'accès aux structures virtuelles non par défaut.

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données des commutateurs Cisco MDS Fabric

Les informations d'infrastructure de données utilisent le collecteur de données de commutateurs de structure MDS Cisco pour découvrir l'inventaire des commutateurs de structure MDS Cisco ainsi que de plusieurs commutateurs FCoE Cisco Nexus sur lesquels le service FC est activé.

De plus, vous pouvez découvrir de nombreux modèles de périphériques Cisco fonctionnant en mode NPV avec ce collecteur de données.

Terminologie

Les informations d'inventaire suivantes sont acquises à partir du collecteur de données du commutateur FC Cisco. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Commutateur	Commutateur
Port	Port
VSAN	Structure
Zone	Zone
Commutateur logique	Commutateur logique
Entrée de serveur de noms	Entrée de serveur de noms
Zone IVR (Inter-VSAN Routing)	Zone IVR

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

- Adresse IP d'un commutateur dans la structure ou sur des commutateurs individuels
- Découverte de châssis, pour activer la découverte de structure
- Si vous utilisez SNMP V2, chaîne de communauté en lecture seule

- Le port 161 est utilisé pour accéder au périphérique

Configuration

Champ	Description
IP du commutateur Cisco	Adresse IP ou nom de domaine complet du commutateur
Version SNMP	Sélectionnez V1, V2 ou V3. V2 ou ultérieur est requis pour l'acquisition de performances.
Chaîne de communauté SNMP	Chaîne de communauté en lecture seule SNMP utilisée pour accéder au commutateur (non applicable pour SNMP v3)
Nom d'utilisateur	Nom d'utilisateur du commutateur (SNMP v3 uniquement)
Mot de passe	Mot de passe utilisé pour le commutateur (SNMPv3 uniquement)

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire (40 minutes par défaut)
Protocole d'autorisation SNMP	Protocole d'authentification SNMP (SNMPv3 uniquement)
Protocole de confidentialité SNMP	Protocole SNMP Privacy (SNMPv3 uniquement)
Mot de passe de confidentialité SNMP	Mot de passe de confidentialité SNMP
Nouvelles tentatives SNMP	Nombre de tentatives SNMP
Délai d'expiration SNMP (ms)	SNMP timeout (5000 ms par défaut)
Activer le recouvrement	Sélectionnez pour activer le recouvrement. Si vous activez le recouvrement, vous devez également activer les notifications SNMP.
Temps minimum entre les recouvrements (s)	Temps minimum entre les tentatives d'acquisition déclenchées par des interruptions (par défaut 10 secondes)
Découvrez tous les commutateurs Fabric	Sélectionnez pour découvrir tous les commutateurs de la structure
Périphériques exclus	Liste des adresses IP des périphériques à exclure de l'interrogation, séparées par des virgules
Appareils inclus	Liste des adresses IP des périphériques à inclure dans l'interrogation, séparées par des virgules
Vérifiez le type de périphérique	Sélectionnez pour accepter uniquement les périphériques qui se annoncent explicitement comme périphériques Cisco

Champ	Description
Premier type d'alias	Fournissez 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, si nécessaire. Tous les commutateurs de la gamme Cisco MDS 9000 prennent en charge les services d'alias de périphérique distribués (alias de périphérique). **Aucun** ne signale aucun alias. **Port Description** Description pour aider à identifier le port dans une liste de ports. **Alias de zone (tous)** Nom convivial pour un port qui ne peut être utilisé que pour la configuration active. Il s'agit de la valeur par défaut.
Deuxième type d'alias	Fournissez une deuxième préférence pour la résolution de l'alias
Troisième type d'alias	Fournissez une troisième préférence pour la résolution de l'alias
Activez la prise en charge du mode proxy SNAP	Sélectionnez si votre commutateur Cisco utilise SANTap en mode proxy. Si vous utilisez EMC RecoverPoint, vous utilisez probablement SANTap.
Intervalle d'interrogation des performances (s)	Intervalle entre les sondages de performance (par défaut 300 secondes)

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
Erreur : échec de détection du châssis - aucun commutateur n'a été détecté	• Ping sur le périphérique avec l'adresse IP configurée • connexion au périphérique à l'aide de l'interface graphique de Cisco Device Manager • connexion au périphérique à l'aide de l'interface CLI • essayez d'exécuter SNMP Walk
Erreur : le périphérique n'est pas un commutateur Cisco MDS	• Assurez-vous que l'adresse IP de la source de données configurée pour le périphérique est correcte • connexion au périphérique à l'aide de l'interface utilisateur graphique de Cisco Device Manager • connexion au périphérique à l'aide de l'interface CLI
Erreur : Data Infrastructure Insights ne peut pas obtenir le WWN du commutateur.	Il ne peut pas s'agir d'un commutateur FC ou FCoE, et ne sera donc pas pris en charge. Assurez-vous que l'IP/FQDN configuré dans la source de données est véritablement un commutateur FC/FCoE.
Erreur : plusieurs nœuds connectés au port de commutation NPV ont été détectés	Désactiver l'acquisition directe du commutateur NPV

Problème :	Essayer :
Erreur : impossible de se connecter au commutateur	• Assurez-vous que le périphérique EST ACTIVÉ • Vérifiez l'adresse IP et le port d'écoute • Ping sur le périphérique • connexion au périphérique à l'aide de l'interface utilisateur graphique de Cisco Device Manager • connexion au périphérique à l'aide de l'interface CLI • Exécuter la fonction SNMP Walk

Performances

Problème :	Essayer :
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 supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Le collecteur de données SmartFiles de Cohesity

Ce collecteur basé sur l'API REST va acquérir un cluster Cohesity, découvrant les « vues » (comme les volumes internes Data Infrastructure Insights), les différents nœuds, ainsi que la collecte des metrics de performance.

Configuration

Champ	Description
Groupe d'instruments IP de Cohesity	Adresse IP du cluster Cohesity
Nom d'utilisateur	Nom d'utilisateur du 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 des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 60 minutes.
Intervalle d'interrogation des performances (min)	Intervalle entre les sondages de performances. La valeur par défaut est 900 secondes.

Dépannage

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Dell

Collecteur de données de la série Dell EMC XC

Data Infrastructure Insights utilise ce collecteur de données pour découvrir les informations d'inventaire et de performances des baies de stockage Dell EMC XC Series.

Configuration

Champ	Description
Adresse IP externe prismes	Adresse IP du serveur XC
Nom d'utilisateur	Nom d'utilisateur du 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 des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 60 minutes.
Intervalle d'interrogation des performances (min)	Intervalle entre les sondages de performances. La valeur par défaut est 300 secondes.

Dépannage

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Dell EMC

Collecteur de données DELL EMC Data Domain

Ce collecteur de données rassemble les informations d'inventaire et de performances des systèmes de stockage Dell EMC Data Domain Deduplication. Pour configurer ce collecteur de données, vous devez suivre des instructions de configuration spécifiques et des recommandations d'utilisation.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir du collecteur de données Data Domain. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Disque	Disque
Baie	Stockage
Port FC	Port
Système de fichiers	Volume interne
Quota	Quota
Partage NFS et CIFS	Fileshare

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce coletor de données.

De formation

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	Adresse IP ou nom de domaine complet de la baie de stockage Data Domain
Nom d'utilisateur	Nom d'utilisateur de la baie de stockage Data Domain
Mot de passe	Mot de passe de la matrice de stockage Data Domain

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 20.
Port SSH	Port de service SSH

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Configuration du collecteur de données EMC ECS

Ce collecteur de données acquiert les données d'inventaire et de performance 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 de To brut différent vers l'unité gérée. Tous les 40 To de capacité ECS non formatée sont facturés comme 1 "Unité gérée (UM)".

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir du collecteur de données ECS. Pour chaque type d'actif acquis, la terminologie la plus utilisée pour ce bien est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Cluster	Stockage
Locataire	Pool de stockage
Godet	Volume interne
Disque	Disque

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

- 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
ID utilisateur ECS	ID utilisateur pour ECS
Mot de passe	Mot de passe utilisé pour ECS

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	La valeur par défaut est 360 minutes.

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
Erreur : l'authentification de l'utilisateur a échoué.	Assurez-vous que vos informations d'identification pour ce périphérique sont correctes.

Performances

Problème :	Essayer :
Erreur : données collectées insuffisantes.	* 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 important.	Vérifiez l'horodatage de collecte dans le fichier journal ${logfile} et modifiez l'intervalle d'interrogation en conséquence

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données Dell EMC PowerScale

Data Infrastructure Insights utilise le collecteur de données SSH Dell EMC PowerScale (précédemment Isilon) pour acquérir des données d'inventaire et de performances à partir du stockage NAS scale-out de PowerScale.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir de ce collecteur de données. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Lecteur	Disque
Cluster	Stockage
Nœud	Nœud de stockage
Système de fichiers	Volume interne

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

Vous avez besoin des informations suivantes pour configurer ce collecteur de données :

- Autorisations d'administrateur pour 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 du cluster PowerScale
Mot de passe	Mot de passe utilisé pour le cluster PowerScale

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 20.
Intervalle d'interrogation des performances (s)	Intervalle entre les sondages de performances. La valeur par défaut est 300.
Port SSH	Port de service SSH. La valeur par défaut est 22.

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
"Informations d'identification non valides" avec des messages 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 : > version isi osrelease > statut isi -q > statut isi -n > périphériques isi -d %s > licence isi * Vérifiez que les informations d'identification utilisées dans l'assistant correspondent aux informations d'identification de l'appareil
"Erreur interne" avec les messages d'erreur "commande <votre commande> l'exécution a échoué avec l'autorisation: <votre autorisation actuelle>. Problème d'autorisation d'exécution de la commande sudo »	Vérifiez que l'utilisateur dispose des autorisations de sudo pour exécuter la commande suivante sur le périphérique

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données DE REPOS 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 baies

exécutant OneFS 8.0.0+.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir de ce collecteur de données. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Lecteur	Disque
Cluster	Stockage
Nœud	Nœud de stockage
Système de fichiers OneFS	Volume interne
Système de fichiers OneFS	Pool de stockage
Qtree	Qtree

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

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 admin/root, mais vous DEVEZ accorder un nombre important 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 de privilège	Description	r(lecture) ou rw (lecture+écriture)
ISI_PRIV_LOGIN_PAPI	API de plateforme	r
ISI_PRIV_SYS_TIME	Heure	r
ISI_PRIV_AUTH	Auth	r
ISI_PRIV_ROLE	Privilège	r
ISI_PRIV_DEVICES	Périphériques	r
ISI_PRIV_EVENT	Événement	r
ISI_PRIV_HDFS	HDFS	r
ISI_PRIV_NDMP	NDMP	r
ISI_PRIV_NETWORK	Le réseau	r
ISI_PRIV_NFS	NFS	r

Nom de privilège	Description	r(lecture) ou rw (lecture+écriture)
ISI_PRIV_PAPI_CONFIG	Configurer l'API de la plate-forme	r
ISI_PRIV_QUOTA	Quota	r
ISI_PRIV_SMARTPOOLS	SmartPools	r
ISI_PRIV_SMB	PME	r
ISI_PRIV_STATISTICS	Statistiques	r
ISI_PRIV_SWIFT	SWIFT	r
ISI_PRIV_JOB_ENGINE	Moteur de tâches	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 de l'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 des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 20.
Intervalle d'interrogation des performances (s)	Intervalle entre les sondages de performances. La valeur par défaut est 300.

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
"Informations d'identification non valides" avec des messages 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 : > version isi osrelease > statut isi -q > statut isi -n > périphériques isi -d %s > licence isi * Vérifiez que les informations d'identification utilisées dans l'assistant correspondent aux informations d'identification de l'appareil

Problème :	Essayer :
"Erreur interne" avec les messages d'erreur "commande <votre commande> l'exécution a échoué avec l'autorisation: <votre autorisation actuelle>. Problème d'autorisation d'exécution de la commande sudo »	Vérifiez que l'utilisateur dispose des autorisations de sudo pour exécuter la commande suivante sur le périphérique

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données Dell EMC PowerStore

Le collecteur de données EMC PowerStore rassemble 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 volume-volume que PowerStore coordonne entre les autres matrices de stockage. Data Infrastructure Insights affiche une matrice de stockage pour chaque cluster PowerStore et collecte les données d'inventaire pour les nœuds et les ports de stockage de ce cluster. Aucune donnée de volume ou de pool de stockage n'est collectée.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir de ce collecteur de données. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
hôte	hôte
host_volume_mapping	host_volume_mapping
Matériel (il a des disques sous objet "extra_details"): Lecteurs	Disque
Appliance	Poolde stockage
Cluster	Baie de stockage
Nœud	StorageNode
port fc	Port
volumétrie	Volumétrie
Volume interne	système_fichiers

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

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 des stocks (minutes)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 60 minutes.

La collecte des performances PowerStore de Cloud Insight utilise les données sources de granularité de 5 minutes de PowerStore. C'est pourquoi Data Infrastructure Insights interroge ces données toutes les cinq minutes, mais elles ne sont pas configurables.

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données Dell EMC RecoverPoint

L'utilisation principale du collecteur de données EMC RecoverPoint consiste à découvrir les relations de réplication volume-volume que l'appliance de stockage RecoverPoint facilite. Ce collecteur découvre également l'appliance RecoverPoint elle-même. Veuillez noter que Dell/EMC vend une solution de sauvegarde VMware pour VM--« RecoverPoint for VM »--non 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 volume-volume que RecoverPoint coordonne sur les autres matrices de stockage. Data Infrastructure Insights affiche une baie de stockage pour chaque cluster RecoverPoint et collecte les données d'inventaire pour les nœuds et les ports de stockage sur ce cluster. Aucune donnée de volume ou de pool de stockage n'est collectée.

De formation

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 du 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 des stocks (minutes)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 20 minutes.
Clusters exclus	Liste séparée par des virgules d'ID ou de noms de cluster à exclure lors de l'interrogation.

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

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 à partir du collecteur de données ScaleIO/PowerFlex. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Cluster MDM (Meta Data Manager)	Stockage

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
SDS (ScaleIO/serveur de données PowerFlex)	Nœud de stockage
Pool de stockage	Pool de stockage
Volumétrie	Volumétrie
Périphérique	Disque

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

- Accès en lecture seule au compte utilisateur Admin
- Port requis : 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 Admin utilisé pour se connecter au périphérique ScaleIO/PowerFlex
Mot de passe	Mot de passe utilisé pour se connecter au périphérique ScaleIO/PowerFlex

Configuration avancée

Cochez la case Inventaire pour activer la collecte de stock.

Champ	Description
Port HTTPS	443
Intervalle d'interrogation des stocks (min)	La valeur par défaut est 60.
Délai de connexion (s)	La valeur par défaut est 60.

Dépannage

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Configuration du collecteur de données EMC Unity

Le collecteur de données Dell EMC Unity (anciennement VNXe) fournit une prise en charge de l'inventaire des baies de stockage unifiées VNXe. Data Infrastructure Insights prend actuellement en charge les protocoles iSCSI et NAS.

De formation

- Le collecteur de données Unity est basé sur la CLI ; vous devez installer Unisphere for 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 doit donc pouvoir lancer des connexions HTTPS vers Unity.
- Adresse IP ou nom de domaine complet du périphérique Unity
- Vous devez disposer d'au moins un utilisateur en lecture seule à utiliser par le collecteur de données.
- HTTPS pour le port 443 est requis
- Le collecteur de données EMC Unity prend en charge les protocoles NAS et iSCSI pour l'inventaire ; les volumes Fibre Channel seront découverts, mais Data Infrastructure Insights ne fournit pas de rapport sur le mappage FC, le masquage ou les ports de stockage.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir du collecteur de données Unity. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Disque	Disque
Baie de stockage	Stockage
Processeur	Nœud de stockage
Pool de stockage	Pool de stockage
Informations générales sur les blocs iSCSI, VMware VMFS	Partagez
Réplication du système distant	Synchronisation
Nœud iSCSI	Nœud cible iSCSI
Initiateur iSCSI	Initiateur cible iSCSI

Remarque : il s'agit uniquement de mappages terminologiques courants et peuvent ne pas représenter tous les cas pour cette source de données.

Configuration

Champ	Description
Stockage unitaire	Adresse IP ou nom de domaine complet du périphérique Unity
Nom d'utilisateur	Nom d'utilisateur du périphérique Unity
Mot de passe	Mot de passe du périphérique Unity
Chemin complet vers l'UEMCLI exécutable	Chemin d'accès complet au dossier contenant l'exécutable *uemcli.exe*

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 40 minutes
Port CLI Unity	Port utilisé pour l'interface de ligne de commande Unity
Intervalle d'interrogation des performances (s)	La valeur par défaut est 300.

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
« Impossible d'exécuter l'utilitaire externe » avec les messages d'erreur « Impossible de trouver le fichier exécutable Unisphere uemcli ».	* Vérifiez que l'adresse IP, le nom d'utilisateur et le mot de passe sont corrects * Vérifiez que la CLI Unisphere est installée sur l'unité d'acquisition Data Infrastructure Insights * Vérifiez que le répertoire d'installation de la CLI Unisphere est correct dans la configuration de la source de données * Vérifiez que l'adresse IP du VNXe est correcte dans la configuration de la source de données. Dans l'unité d'acquisition Data Infrastructure Insights, ouvrez un CMD et passez 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 supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Dell EMC VMAX et PowerMax Family of Devices Data Collector

Data Infrastructure Insights découvre les baies de stockage EMC VMAX et PowerMax à l'aide des commandes symcli Solutions Enabler associées à un serveur Solutions Enabler existant dans votre environnement. Le serveur Solutions Enabler existant est connecté à la baie de stockage VMAX/PowerMax par l'accès aux volumes du contrôleur d'accès.

De formation

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 détecte toutes les baies Symmetrix qui sont « locales » sur ce serveur, comme indiqué dans la sortie « liste symcfg » de ce serveur.

- L'outil EMC Solutions Enabler (CLI) avec l'application SMI-S Provider doit être installé sur le serveur de l'unité d'acquisition et la version doit correspondre ou être antérieure à la version exécutée sur Solutions

Enabler Server.

- 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 en lecture/écriture au niveau du nœud de stockage, le SMI-S Provider doit communiquer avec une instance en cours d'exécution de l'application UNISPHERE pour VMAX.
- Adresse IP du serveur Managing 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 for VMAX doit exécuter et collecter des statistiques pour les baies EMC VMAX et PowerMax sStorage gérées par l'installation SMI-S Provider
- Validation de l'accès pour les performances : dans un navigateur Web de votre unité d'acquisition, accédez à *https://<SMI-S Hostname ou IP>:5989/ecomconfig* où « SMI-S Hostname or IP » est l'adresse IP ou le nom d'hôte de votre serveur SMI-S. Cette URL est destinée à un portail d'administration pour le service EMC SMI-S (ou « 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 utilisée pour ce bien est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Disque	Disque
Groupe de disques	Groupe de disques

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Stockage	Stockage de baies
Directeur	Nœud de stockage
Pool de périphériques, pool de ressources de stockage (SRP)	Pool de stockage
Dispositif TDEV	Volumétrie

Remarque : il s'agit uniquement de mappages terminologiques communs et 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 de service comme spécifié dans le fichier *netcnfg*
Chemin complet vers l'interface de ligne de commande	Chemin d'accès complet au dossier contenant l'interface de ligne de commande Symmetrix
Adresse IP de l'hôte SMI-S	Adresse IP de l'hôte SMI-S.

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 40 minutes.
Choisissez 'exclure' ou 'inclure' pour spécifier une liste	Indiquez si vous souhaitez inclure ou exclure la liste des matrices ci-dessous lors de la collecte des données.
Liste des périphériques de filtre d'inventaire	Liste des ID de périphériques à inclure ou exclure, séparés par des virgules

Champ	Description
Mise en cache de la connexion	Choisissez une méthode de mise en cache de connexion : * LOCAL signifie que le service d'acquisition Cloud Insights s'exécute sur le serveur Solutions Enabler, qui bénéficie d'une connectivité Fibre Channel aux baies Symmetrix que vous recherchez à détecter et a accès aux volumes gatekeeper. Ceci peut être observé dans certaines configurations RAU (Remote acquisition Unit). * REMOTE_CACHED est la valeur par défaut et devrait être utilisé dans la plupart des cas. Les paramètres de fichier NETCNFG sont utilisés pour se connecter à l'aide d'IP au serveur Solutions Enabler, qui doit disposer d'une connectivité Fibre Channel aux baies Symmetrix que vous recherchez et qui a accès aux volumes Gatekeeper. * Si les options REMOTE_CACHED font échouer les commandes CLI, utilisez l'option REMOTE. N'oubliez pas qu'il ralentira le processus d'acquisition (voire quelques heures, voire plusieurs jours, dans des cas extrêmes). Les paramètres de fichier NETCNFG sont toujours utilisés pour une connexion IP au serveur Solutions Enabler qui dispose d'une connectivité Fibre Channel aux baies Symmetrix découvertes. **Remarque :** ce paramètre ne modifie pas le comportement de Data Infrastructure Insights par rapport aux tableaux répertoriés comme DISTANTS par la sortie "symcfg list". Data Infrastructure Insights collecte les données uniquement sur les terminaux affichés comme LOCAUX par cette commande.
Protocole SMI-S	Protocole utilisé pour la connexion au fournisseur SMI-S. Affiche également le port par défaut utilisé.
Remplacer le port SMIS	Si ce champ est 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 SMI-S Provider
Mot de passe SMI-S.	Nom d'utilisateur pour l'hôte SMI-S Provider
Intervalle d'interrogation des performances (en secondes)	Intervalle entre les sondages de performance (par défaut 1000 secondes)
Hoose 'exclure' ou 'inclure' pour spécifier une liste	Indiquez si vous souhaitez inclure ou exclure la liste des matrices ci-dessous lors de la collecte des données de performances
Liste des périphériques de filtre de performances	Liste des ID de périphériques à inclure ou exclure, séparés par des virgules

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Problème :	Essayer :
Erreur : la fonction demandée n’est pas actuellement sous licence	Installez la licence du serveur SYMAPI.
Erreur : aucun périphérique n’a été trouvé	Assurez-vous que les périphériques Symmetrix sont configurés pour être gérés par le serveur Solutions Enabler : - exécutez la liste symcfg -v pour afficher la liste des périphériques Symmetrix configurés.
Erreur : un service réseau demandé est introuvable 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 : l’établissement de liaisons client/serveur distant a échoué	Consultez les fichiers storsrvd.log* les plus récents sur l’hôte Solutions Enabler que nous essayons de découvrir.
Erreur : nom commun dans le certificat client non valide	Modifiez le fichier *hosts* sur le serveur Solutions Enabler afin que le nom d’hôte de l’unité d’acquisition soit résolu 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 disponible dans le système pour exécuter Solutions Enabler
Erreur : Solutions Enabler n’a pas pu traiter toutes les données requises.	Étudier 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 recueillie avec Solutions Enabler 7.x à partir d’un serveur Solutions Enabler 8.x. • La commande "symcfg list -srp" CLI peut renvoyer des données incorrectes lorsqu’elle est recueillie avec Solutions Enabler 8.1.0 ou une version antérieure à partir d’un serveur Solutions Enabler 8.3 ou une version ultérieure.	Vérifiez que vous utilisez la même version principale de Solutions Enabler

Problème :	Essayer :
J'ai constaté des erreurs de collecte de données avec le message "code inconnu"	Ce message peut s'afficher si les autorisations ne sont pas déclarées dans le fichier de configuration du démon du serveur Solutions Enabler (voir De formationci-dessus). 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 de 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, éditez le fichier /var/symapi/config/daemon_users et assurez-vous que l'utilisateur cisys possède l'autorisation <all> spécifiée pour le démon storapid. Exemple : 14:11:25 # queue /var/symapi/config/daemon_users … cisys storapid <all>

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

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 de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Disque	Disque
Stockage	Stockage
Le processeur de stockage	Nœud de stockage
Ce pool, groupe RAID	Pool de stockage
LUN	Volumétrie

Remarque : il s'agit uniquement de mappages terminologiques courants et peuvent ne pas représenter tous les cas pour cette source de données.

De formation

Pour collecter des données, les exigences suivantes doivent être respectées :

- Une adresse IP de chaque processeur de stockage bloc VNX
- Nom d'utilisateur et mot de passe Navisphere en lecture seule des baies de stockage bloc VNX
- Naviseccli doit être installé sur Data Infrastructure Insights au
- Validation de l'accès : exécutez NaviSecCLI à partir de Data Infrastructure Insights au sur chaque baie en utilisant le nom d'utilisateur et le mot de passe.
- Configuration requise pour les ports : 80, 443
- La version naviseccli doit correspondre au code FLARE le plus récent de votre matrice
- Pour les performances, la journalisation des statistiques doit être activée.

Syntaxe de l'interface de ligne de commande Navisphere

naviseccli.exe -h <adresse IP> -utilisateur <utilisateur> -password <password> -scope <scope,utiliser 0 pour global scope> -port <use 443 par défaut> commande

Configuration

Champ	Description
Adresse IP du stockage VNX Block Storage	Adresse IP ou nom de domaine complet du stockage bloc VNX
Nom d'utilisateur	Nom utilisé pour se connecter au périphérique de stockage bloc VNX.
Mot de passe	Mot de passe utilisé pour se connecter au périphérique de stockage bloc VNX.
Chemin de la CLI vers naviseccli.exe	Chemin complet vers le dossier contenant l'exécutable *naviseccli.exe*

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 40 minutes.
Portée	Périmètre client sécurisé. La valeur par défaut est Global.
Intervalle d'interrogation des performances (s)	Intervalle entre les sondages de performances. La valeur par défaut est 300 secondes.

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
Erreur : • L'agent ne fonctionne pas • Impossible de trouver naviseccli • Impossible d'exécuter une commande	• Vérifiez que Navisphere CLI est installé sur l'unité d'acquisition Cloud Insight • Vous n'avez pas sélectionné l'option « utiliser le client sécurisé » dans l'assistant de configuration du collecteur de données et vous n'avez pas installé de version non sécurisée de Navisphere CLI. • Vérifiez que le répertoire d'installation de Navisphere CLI est correct dans la configuration du collecteur de données • Vérifiez que l'adresse IP du stockage en mode bloc VNX est correcte dans la configuration du collecteur de données : • Dans l'unité d'acquisition Data Infrastructure Insights : ◦ Ouvrez un CMD. ◦ Remplacez le répertoire par le répertoire d'installation configuré ◦ Essayez d'établir une connexion avec le périphérique de stockage en mode bloc VNX en tapant « navicli -h {ip} getagent » (remplacez le {ip} par l'adresse ip réelle)
Erreur : 4.29 emc235848 emc241018 getall n'a pas pu analyser les informations d'alias de l'hôte	Cela est probablement dû à un problème DE corruption FLARE 29 de la base de données d'initiateurs hôtes sur la baie elle-même. Consultez 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 d'accès CLI vers navicli.exe OU naviseccli.exe • Remarque : la version navicli.jar est obsolète à partir de la version 6.26 d'EMC Navisphere • Le navicli.jar peut être disponible sur http://powerlink.emc.com
Erreur : les pools de stockage ne signalant pas les disques sur le Service Processor à l'adresse IP configurée	Configurez le collecteur de données avec les deux adresses IP du processeur de service, séparées par une virgule

Problème :	Essayer :
Erreur : erreur de non-concordance de révision	• Ceci est généralement dû à la mise à jour du micrologiciel sur le périphérique de stockage en mode bloc VNX, mais pas à la mise à jour de l'installation de NaviCLI.exe. Cela peut également être dû à l'installation de différents périphériques avec des firmwares différents, mais à une seule interface de ligne de commande (avec une version de micrologiciel différente). • Vérifiez que le périphérique et l'hôte exécutent des versions identiques du logiciel : ◦ Dans l'unité d'acquisition Data Infrastructure Insights, ouvrez une fenêtre de ligne de commande ◦ Remplacez le répertoire par le répertoire d'installation configuré ◦ Établir une connexion avec le périphérique CLARiiON en tapant « navicli -h <ip> getagent » ◦ Recherchez le numéro de version sur les deux premières lignes. Exemple : « Agent Rév. : 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 - pas de ports Fibre Channel	Le périphérique n'est configuré avec aucun port Fibre Channel. Actuellement, seules les configurations FC sont prises en charge. Vérifiez que cette version/micrologiciel est prise en charge.

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données DELL EMC VNX File (anciennement Celerra Unified Storage System)

Ce collecteur de données acquiert les 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 VNX File. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Celerra Network Server/Celerra Storage Pool	Pool de stockage
Système de fichiers	Volume interne
Data Mover	Contrôleur
Système de fichiers monté sur un mécanisme de déplacement des données	Partage de fichiers
Exports CIFS et NFS	Partagez
Volume de disque	LUN interne

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

Vous devez disposer 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 VNX File
Nom d'utilisateur	Nom utilisé pour se connecter au périphérique VNX File
Mot de passe	Mot de passe utilisé pour se connecter au périphérique VNX File

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (minutes)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 20 minutes.

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
Erreur : impossible de continuer pendant la mise à jour DART en cours	Solution possible : interrompre le collecteur de données et attendre la fin de la mise à niveau du DART avant de tenter une autre demande d'acquisition.

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

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 pilote 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 de ce collecteur de données. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Disque	Disque
Dossier de disques	Groupe de disques
Système de fichiers	Volume interne
Stockage	Stockage
Le processeur de stockage	Nœud de stockage
Pool de stockage, groupe RAID	Pool de stockage
LUN	Volumétrie
Data Mover	Contrôleur
Système de fichiers monté sur un mécanisme de déplacement des données	Partage de fichiers
Exports CIFS et NFS	Partagez
Volume de disque	LUN interne

De formation

Vous devez disposer des éléments suivants pour configurer le collecteur de données VNX (SSH) :

- Adresse IP et informations d'identification du VNX vers la station pilote Celerra.
- Nom d'utilisateur et mot de passe en lecture seule.
- Le collecteur de données peut exécuter des commandes NaviCLI/NaviSecCLI contre la baie backend en utilisant les têtes NAS du système d'exploitation DART

Configuration

Champ	Description
Adresse IP du VNX	Adresse IP ou nom de domaine complet de la station de contrôle VNX
Nom d'utilisateur	Nom d'utilisateur de la station de contrôle VNX
Mot de passe	Mot de passe de la station pilote VNX

Transpiration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 40 minutes.
Intervalle d'interrogation des performances (s).	Intervalle entre les sondages de performances. La valeur par défaut est 300 secondes.

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Configuration du collecteur de données EMC VPLEX

Ce collecteur de données acquiert les données d'inventaire et de performance 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 de clusters VPLEX nécessite que le service d'archivage des performances soit opérationnel, afin de remplir 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 niveau/station de gestion du firmware VPLEX ne seront pas opérationnelles. Les clients qui planifient de telles mises à niveau peuvent demander à Dell/EMC de manière proactive si leur mise à niveau prévue laissera cette fonctionnalité inutilisable, et, dans l'affirmative, comment peuvent-ils la réactiver afin de réduire les lacunes dans la visibilité des performances ? Le code de performances VPLEX de Cloud Insight évalue 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 consigne les défaillances de collecte des performances.

Terminologie

Data Infrastructure Insight acquiert les informations d'inventaire suivantes à partir du collecteur de données VPLEX. Pour chaque type d'actif acquis, la terminologie la plus utilisée pour ce bien est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Cluster	Stockage
Moteur	Nœud de stockage
Périphérique, extension du système	Pool de stockage interne
Volume virtuel	Volumétrie
Port frontal, port arrière	Port
Périphérique distribué	Synchronisation du stockage
Vue du stockage	Carte de volume, masque de volume
Volume de stockage	LUN interne
ITL	Chemin interne

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

- Une adresse IP de VPLEX Management Console
- Compte de domaine de niveau administratif pour le serveur VPLEX
- Port 443 (HTTPS). Nécessite une connectivité sortante vers le port TCP 443 de la station de gestion VPLEX.
- Pour des performances optimales, le nom d'utilisateur et le 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 VPLEX Management Console	Adresse IP ou nom de domaine complet de VPLEX Management Console
Nom d'utilisateur	Nom d'utilisateur pour la CLI VPLEX
Mot de passe	Mot de passe utilisé pour la CLI VPLEX
Adresse IP distante de performance	Adresse IP distante des performances de la console VPLEX Management Console
Nom d'utilisateur à distance de performance	Performance Nom d'utilisateur distant de VPLEX Management Console
Mot de passe de performance à distance	Mot de passe de performance à distance de VPLEX Management Console

Configuration avancée

Champ	Description
Port de communication	Port utilisé pour la CLI VPLEX. La valeur par défaut est 443.
Intervalle d'interrogation des stocks (min)	La valeur par défaut est 20 minutes.
Nombre de tentatives de connexion	La valeur par défaut est 3.
Intervalle d'interrogation des performances (s)	Intervalle entre les sondages de performances. La valeur par défaut est 600 secondes.
Nombre de tentatives	La valeur par défaut est 2.

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
Erreur : l'authentification de l'utilisateur a échoué.	Assurez-vous que vos informations d'identification pour ce périphérique sont correctes.

Performances

Problème :	Essayer :
Erreur : les performances VPLEX pour la version inférieure à 5.3 ne sont pas prises en charge.	Mettez à niveau VPLEX vers 5.3 ou une version supérieure
Erreur : données collectées insuffisantes.	• Vérifiez l'horodatage de collecte dans le fichier journal et modifiez l'intervalle de vote en conséquence • attendez plus longtemps
Erreur : les fichiers journaux permanents ne sont pas mis à jour.	Veuillez contacter le support EMC pour activer la mise à jour des fichiers journaux permanents
Erreur : l'intervalle d'interrogation des performances est trop important.	Vérifiez l'horodatage de collecte dans le fichier journal ${logfile} et modifiez l'intervalle d'interrogation en conséquence
Erreur : l'adresse IP distante de performances de VPLEX Management Console n'est pas configurée.	Modifiez la source de données pour définir l'adresse IP de performance à distance de VPLEX Management Console.
Erreur : aucune donnée de performance signalée par le directeur	• Vérifiez que les moniteurs de performances du système fonctionnent correctement • Veuillez contacter le support EMC pour permettre la mise à jour des fichiers journaux du moniteur de performances du système

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données Dell EMC XtremeIO

Le collecteur de données EMC XtremIO fait l'acquisition des données d'inventaire et de performance du système de stockage EMC XtremIO.

De formation

Pour configurer le collecteur de données EMC XtremIO (HTTP), vous devez avoir :

- Adresse 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 à partir du collecteur de données EMC XtremIO. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de cette source de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Disque (SSD)	Disque
Cluster	Stockage
Contrôleur	Nœud de stockage
Volumétrie	Volumétrie
Mappage de LUN	Carte de volume
Initiateur FC cible	Masque de volume

Remarque : il s'agit uniquement de mappages terminologiques courants et peuvent ne pas représenter tous les cas pour cette source de données.

De formation

- Adresse IP de l'hôte XtremIO Management Server (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 du serveur de gestion XtremIO
Mot de passe	Mot de passe du serveur de gestion XtremIO

Configuration avancée

Champ	Description
Port TCP	Port TCP utilisé pour la connexion au serveur de gestion XTreXtremIO. La valeur par défaut est 443.
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 60 minutes.
Intervalle d'interrogation des performances (s)	Intervalle entre les sondages de performances. La valeur par défaut est 300 secondes.

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données ETERNUS de Fujitsu

Le collecteur de données ETERNUS de Fujitsu acquiert les données d'inventaire en utilisant un accès d'administration au système de stockage.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir du système de stockage ETERNUS de Fujitsu. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Disque	Disque
Stockage	Stockage
Thin Pool, pool de niveaux flexible, groupe RAID	Pool de stockage
Volume standard, volume de données Snap (SDV), volume de pool de données Snap (SDPV), volume de provisionnement fin (TPV), volume de niveau flexible (FTV), volume de répartition large (WSV)	Volumétrie
Adaptateur de canal	Contrôleur

Remarque : il s'agit uniquement de mappages de terminologie communs et ne représentent peut-être pas tous les cas pour ce collectior de données.

De formation

Les éléments suivants sont nécessaires pour configurer ce collecteur de données :

- Adresse IP du stockage ETERNUS, qui ne peut pas être délimitée par des virgules
- Nom d'utilisateur et mot de passe SSH Administration

- Orifice 22
- Assurez-vous que le défilement de page est désactivé (Click-show-more-SCROLL DESACTIVE)

Configuration

Champ	Description
Adresse IP du stockage ETERNUS	Adresse IP du stockage ETERNUS
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 des stocks (min)	La valeur par défaut est 20 minutes.

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
"Erreur lors de la récupération des données" avec les messages d'erreur "interface de ligne de commande de l'invite de recherche d'erreur" ou "invite de recherche d'erreur à la fin des résultats de l'interpréteur de commandes"	Cause probable : le défilement des pages est activé pour le système de stockage. 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 : * identifiants incorrects. * Adresse IP incorrecte. * Problème de réseau. * Le stockage est peut-être arrêté ou ne répond pas. Solutions possibles : * Vérifiez les informations d'identification et l'adresse IP saisies. * Essayez de communiquer avec le stockage à l'aide de SSH client.

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données NetApp Google Compute

Ce collecteur de données prend en charge l'inventaire et la collecte de performances à partir des configurations de plateforme cloud Google Compute. Ce collecteur s'efforcera de découvrir toutes les ressources de calcul de tous les projets au sein d'une seule organisation Google. Si vous souhaitez découvrir plusieurs entreprises Google à l'aide de Data Infrastructure Insights, vous pouvez déployer un collecteur Data Infrastructure Insights par entreprise.

Exigences de compte de service

- Vous devez créer un compte de service en suivant les instructions de la section "Création/gestion de comptes de service". Ce compte de service est identifié par un ID unique, appelé *ClientID*, qui sera utilisé comme nom d'utilisateur.
- En outre, créez une clé de compte de service en suivant les instructions de la section "Création/gestion des clés de compte de service". Cette clé peut être téléchargée en tant que fichier json dont le contenu sera utilisé comme mot de passe.
- Le compte de service doit être étendu pour *Compute.readonly*, *monitoring.read* et *cloud-Platform*.

Configuration

Champ	Description
ID d'organisation	ID d'organisation que vous souhaitez découvrir avec ce collecteur. Ce champ est obligatoire si votre compte de service peut afficher plusieurs organisations
Choisissez exclure ou inclure pour filtrer les projets GCP par ID	Vous souhaitez limiter les ressources des projets qui sont intégrées aux informations Data Infrastructure.
ID de projet	La liste des ID de projet que vous souhaitez filtrer ou retirer de la découverte, en fonction de la valeur de la valeur choisir « exclure »…. La liste par défaut est vide
ID client	ID client pour la configuration 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 des stocks (min)	La valeur par défaut est 60 minutes
Choisissez 'exclure' ou 'inclure' pour appliquer au filtre des VM par étiquettes	Indiquez s'il faut inclure ou exclure les VM par étiquettes lors de la collecte de données. Si 'inclure' est sélectionné, le champ clé d'étiquette ne peut pas être vide.
Étiqueter les clés et les valeurs sur lesquelles filtrer les VM	Cliquez sur **+ Filter Label** pour choisir les VM (et les disques associés) à inclure/exclure en filtrant les clés et les valeurs correspondant aux clés et aux valeurs des étiquettes de la VM. La clé d'étiquette est requise, la valeur d'étiquette est facultative. Lorsque la valeur d'étiquette est vide, la machine virtuelle est filtrée tant qu'elle correspond à la clé d'étiquette.
Intervalle d'interrogation des performances (s)	La valeur par défaut est 1800 secondes

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le

"Matrice de prise en charge du Data Collector".

Collecteur de données Google Cloud NetApp Volumes

Ce collecteur de données prend en charge l'inventaire et la collecte des performances à partir des configurations Google Cloud NetApp Volumes . Il détecte les volumes NetApp et les ressources de stockage de tous les projets d'une organisation Google. Si vous souhaitez surveiller plusieurs organisations Google avec Data Infrastructure Insights, déployez un collecteur par organisation.

Exigences de compte de service

- Vous devez créer un compte de service en suivant les instructions de la section "Création/gestion de comptes de service". Ce compte de service est identifié par un identifiant unique, appelé *clientId*, qui sera utilisé comme nom d'utilisateur.
- En outre, créez une clé de compte de service en suivant les instructions de la section "Création/gestion des clés de compte de service". Cette clé peut être téléchargée en tant que fichier json dont le contenu sera utilisé comme mot de passe.
- Le compte de service doit être étendu pour *Compute.readonly*, *monitoring.read* et *cloud-Platform*.

Configuration

Champ	Description
ID d'organisation	ID d'organisation que vous souhaitez découvrir avec ce collecteur. Ce champ est obligatoire si votre compte de service peut afficher plusieurs organisations
Choisissez « exclure » ou « inclure » pour filtrer les ressources GCNV par emplacement	Cette 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 option est vide par défaut et est utilisée conjointement avec l'option « Choisir entre Exclure et Inclure ». Si vous souhaitez découvrir des ressources 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 retirer de la découverte, en fonction de la valeur de la valeur choisir « exclure »…. La liste par défaut est vide
ID client	ID client pour la configuration 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 des stocks (min)	La valeur par défaut est 60 minutes
Utilisez le proxy au pour les appels API REST	Sélectionnez cette option pour que le collecteur utilise le même proxy que l'unité d'acquisition sur laquelle il réside. Par défaut, cette option est désactivée, ce qui signifie que le collecteur tente d'envoyer des appels API HTTPS directement à Google.
Étiqueter les clés et les valeurs sur lesquelles filtrer les VM	Cliquez sur **+ Filter Label** pour choisir les VM (et les disques associés) à inclure/exclure en filtrant les clés et les valeurs correspondant aux clés et aux valeurs des étiquettes de la VM. La clé d'étiquette est requise, la valeur d'étiquette est facultative. Lorsque la valeur d'étiquette est vide, la machine virtuelle est filtrée tant qu'elle correspond à la clé d'étiquette.
Intervalle d'interrogation des performances (s)	La valeur par défaut est 300 secondes

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

HP Enterprise

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 à partir de ce collecteur de données. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Champ	Description
Disque physique	Disque
System de stockage	Stockage
Nœud contrôleur	Nœud de stockage
Groupe de provisionnement commun	Pool de stockage
Volume virtuel	Volumétrie

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

Les éléments suivants sont nécessaires 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, consultez le nom d'utilisateur en lecture-écriture et le mot de passe du serveur StoreServ
- Exigences relatives au port : 22 (collecte des inventaires), 5988 ou 5989 (collecte des 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 SMI-S Provider
Mot de passe SMI-S.	Mot de passe utilisé pour l'hôte SMI-S Provider

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 40 minutes.
Connectivité SMI-S.	Protocole utilisé pour la connexion au fournisseur SMI-S.
Remplacer le port par défaut SMI-S.	Si ce champ est vide, utilisez le port par défaut de SMI-S Connectivity, sinon entrez le port de connexion à utiliser
Intervalle d'interrogation des performances (s)	Intervalle entre les sondages de performances. La valeur par défaut est 300 secondes.

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
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 :	Essayer :
Échec de la connexion ou de la connexion. Échec de l'initialisation du fournisseur.	Un nom de tableau numérique peut causer des problèmes avec le serveur SMI-S. Essayez de changer le nom de la matrice.
L'utilisateur SMI-S configuré ne possède aucun domaine	Accordez des privilèges de domaine appropriés à l'utilisateur SMI-S configuré
Data Infrastructure Insights indique qu'il ne peut pas se connecter au service SMI-S.	Vérifiez qu'il n'y a pas de pare-feu entre ci au et la matrice qui bloquera l'EC au de créer des connexions TCP à 5988 ou 5989. Une fois cela terminé, et si vous avez confirmé qu'il n'y a pas de pare-feu, vous devez utiliser SSH pour la baie et utiliser la commande « showcim » pour confirmer. Vérifiez que : * le service est activé * HTTPS est activé * le port HTTPS devrait être 5989 si tous ces éléments sont ainsi, vous pouvez essayer de "stopcim" puis un "startcim" pour redémarrer le CIM (c.-à-d. Service SMI-S).

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

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 à partir du collecteur de données HP Enterprise Command View. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
PDEV	Disque
Pool de journaux	Groupe de disques
Baie de stockage	Stockage
Contrôleur de port	Nœud de stockage
Groupe de baies, DP Pool	Pool de stockage
Unité logique, LDEV	Volumétrie

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences d’inventaire

Vous devez disposer des éléments suivants pour collecter les données de stock :

- Adresse IP du serveur CVAE
- Nom d’utilisateur et mot de passe en lecture seule pour le logiciel CVAE et les privilèges peer
- Port requis : 2001

Exigences en matière de performances

Les exigences suivantes doivent être respectées pour collecter les données de performance :

- Performances HDS USP, USP V, et VSP
  - Le moniteur de performances doit être sous licence.
  - L’interrupteur de surveillance doit être activé.
  - L’outil d’exportation (Export.exe) doit être copié dans Data Infrastructure Insights au et extrait dans un emplacement. Sur ci Linux AUS, assurez-vous que "cisys" dispose d’autorisations de lecture et d’exécution.
  - La version de l’outil d’exportation doit correspondre à la version du microcode de la matrice cible.
- Performances AMS :
  - Le moniteur de performances doit être sous licence.
  - L’utilitaire CLI de Storage Navigator Modular 2 (SNM2) doit être installé sur Data Infrastructure Insights au.
- Exigences liées au réseau
  - Les outils d’exportation sont basés sur Java et utilisent RMI pour parler à la baie. Ces outils peuvent ne pas être adaptés au pare-feu car ils peuvent négocier de manière dynamique les ports TCP source et de destination sur chaque invocation. De plus, les outils d’exportation de différentes baies de modèles peuvent fonctionner différemment sur l’ensemble du réseau. Consultez HPE pour connaître les exigences de votre modèle

Configuration

Champ	Description
Serveur d’affichage des commandes	Adresse IP ou nom de domaine complet du serveur Command View
Nom d’utilisateur	Nom d’utilisateur du serveur Command View.
Mot de passe	Mot de passe utilisé pour le serveur Command View.
PÉRIPHÉRIQUES : STOCKAGES VSP G1000 (R800), VSP (R700), HUS VM (HM700) ET USP	Liste des appareils pour les stockages VSP G1000 (R800), VSP (R700), HUS VM (HM700) et USP. Chaque stockage nécessite : * adresse IP de la matrice : 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 - WMS/SMS/AMS Storages	Liste des périphériques pour les stockages WMS/SMS/AMS. Chaque stockage nécessite : * adresse IP de la baie : adresse IP de la baie de stockage * chemin de la CLI du Storage Navigator : chemin de la CLI SNM2 * authentification du 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
L'hôte de Tuning Manager	Adresse IP ou nom de domaine complet du gestionnaire de réglages
Port du gestionnaire de réglage	Port utilisé pour Tuning Manager
Nom d'utilisateur du gestionnaire de réglage	Nom d'utilisateur pour Tuning Manager
Mot de passe du gestionnaire de réglage	Mot de passe pour Tuning Manager

Remarque : dans les HDS USP, USP V et VSP, tout disque peut appartenir à plusieurs groupes de baies.

Configuration avancée

Champ	Description
Commande Afficher le port du serveur	Port utilisé pour le serveur Command View
HTTPS activé	Sélectionnez pour activer HTTPS
Intervalle d'interrogation des stocks (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 des matrices ci-dessous lors de la collecte des données.
Exclure ou inclure des périphériques	Liste séparée par des virgules des noms d'ID de périphérique ou de tableau à inclure ou exclure
Gestionnaire d'hôte de requêtes	Sélectionnez cette option pour interroger le gestionnaire d'hôte
Intervalle d'interrogation des performances (en secondes)	Intervalle entre les sondages de performances. La valeur par défaut est 300.

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
Erreur : l'utilisateur ne dispose pas d'une autorisation suffisante	Utilisez un compte utilisateur différent qui a plus de privilèges ou augmente le privilège du compte utilisateur configuré dans le collecteur de données
Erreur : la liste des stockages est vide. Soit les périphériques 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 qui a plus de privilèges ou augmentez le privilège du compte utilisateur
Erreur : la baie de stockage HDS n'a pas été actualisée depuis quelques jours	Étudiez les raisons pour lesquelles cette baie n'est pas actualisée dans HP CommandView AE.

Performances

Problème :	Essayer :
Erreur : * erreur lors de l'exécution de l'utilitaire d'exportation * erreur lors de l'exécution de la commande externe	* Vérifiez que l'utilitaire d'exportation est installé sur l'unité d'acquisition Data Infrastructure Insights * Vérifiez que l'emplacement de l'utilitaire d'exportation est correct dans la configuration du collecteur de données * Vérifiez que l'adresse IP de la matrice 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 * Vérifiez que la version de l'utilitaire d'exportation est compatible avec la matrice de stockage version du microcode de la matrice de stockage runWin.bat
Erreur : la connexion de l'outil d'exportation a échoué pour l'adresse IP cible	* Confirmez que le nom d'utilisateur/mot de passe est correct * Créez un ID utilisateur principalement pour ce collecteur de données HDS * Confirmez qu'aucun autre collecteur de données n'est configuré pour acquérir ce tableau
Erreur : les outils d'exportation sont consignés « Impossible d'obtenir la plage de temps pour la surveillance ».	* Vérifiez que la surveillance des performances est activée sur la matrice. * 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 : matrice de stockage non prise en charge par l'utilitaire d'exportation * erreur de configuration : matrice de stockage non prise en charge par l'interface CLI modulaire de Storage Navigator	* Configurez uniquement les matrices de stockage prises en charge. * Utilisez "Filtrer la liste de périphériques" pour exclure les matrices de stockage non prises en charge.
Erreur : * erreur d'exécution de la commande externe * erreur de configuration : la matrice de stockage n'a pas été signalée par Inventory * erreur de configuration : le dossier d'exportation ne contient pas de fichiers JAR	* Vérifier l'emplacement de l'utilitaire d'exportation. * Vérifiez si la matrice de stockage en question est configurée dans Command View Server * définissez l'intervalle d'interrogation des performances sur plusieurs 60 secondes.

Problème :	Essayer :
Erreur : * erreur de l'interface CLI du navigateur de stockage * erreur lors de l'exécution de la commande auPerform * erreur lors de l'exécution de la commande externe	* Vérifiez que l'interface de ligne de commande modulaire Storage Navigator est installée sur l'unité d'acquisition Data Infrastructure Insights * Vérifiez que l'emplacement de l'interface de ligne de commande modulaire Storage Navigator est correct dans la configuration du collecteur de données * Vérifiez que l'adresse IP de la matrice WMS/SMS/SMS/SMS est correcte dans la configuration du collecteur de données * Vérifiez que la version de l'interface de ligne de commande Storage Navigator Modular CLI est compatible avec la version de stockage configurée dans le répertoire d'acquisition de données *.
Erreur : erreur de configuration : matrice de stockage non signalée par Inventory	Vérifiez si la matrice de stockage en question est configurée dans le serveur Command View
Erreur : * aucune matrice n'est enregistrée avec la matrice CLI * Storage Navigator modulaire 2 n'est pas enregistrée avec la CLI * Storage Navigator modulaire 2 erreur de configuration : la matrice de stockage n'est pas enregistrée avec la CLI modulaire StorageNavigator	* Ouvrir l'invite de commande et changer le répertoire pour le chemin configuré * Exécuter la commande "set=STONARVM_HOME=." * Exécutez la commande "auunitref" * Confirmez que la sortie de la commande contient les détails de la matrice avec IP * si la sortie ne contient pas les détails de la matrice, enregistrez la matrice avec Storage Navigator CLI: - Ouvrir l'invite de commande et changer le répertoire avec le chemin configuré - exécutez la commande "SET=STONVM_HOME=". - Exécutez la commande "auunitaddauto -ip ${ip}". Remplacez ${ip} par une adresse IP réelle

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collection de données HPE Alletra 6000

Le collecteur de données HP Enterprise Alletra 6000 (anciennement Nimble) prend en charge les données d'inventaire et de performance des baies de stockage Alletra 6000.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir de ce collecteur. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Baie	Stockage
Disque	Disque
Volumétrie	Volumétrie
Piscine	Pool de stockage

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Initiateur	Alias de l'hôte de stockage
Contrôleur	Nœud de stockage
Interface Fibre Channel	Contrôleur

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

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.
- La baie 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 ayant au moins le rôle « opérateur ». Le rôle « invité » ne dispose pas d'un accès suffisant pour comprendre les configurations des initiateurs.
- Le port 5392 doit être ouvert sur la matrice.

Pour collecter les données de performances de la baie de stockage, vous devez disposer des éléments suivants :

- La baie doit exécuter NimbleOS 4.0.0 ou une version ultérieure
- Les volumes de la matrice doivent être configurés. La seule API de performances dont NimbleOS dispose concerne les volumes et les rapports statistiques Data Infrastructure Insights sont dérivés des statistiques sur les volumes

Configuration

Champ	Description
Adresse IP de gestion de baie	Nom de domaine complet (FQDN) ou adresse IP de gestion de baie.
Nom d'utilisateur	Nom d'utilisateur de la matrice
Mot de passe	Mot de passe de la matrice

Configuration avancée

Champ	Description
Port	Port utilisé par l'API REST Nimble. La valeur par défaut est 5392.
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 60 minutes.

Remarque : l'intervalle d'interrogation 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.

Hitachi Data Systems

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 de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
PDEV	Disque
Pool de journaux	Groupe de disques
Baie de stockage	Stockage
Contrôleur de port	Nœud de stockage
Groupe de baies, HDS Pool	Pool de stockage
Unité logique, LDEV	Volumétrie

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

Stockage

Les termes suivants s'appliquent aux objets ou références que vous pouvez trouver sur les pages d'accueil des ressources de stockage HDS. Un grand nombre de ces termes s'appliquent également à d'autres collecteurs de données.

- Nom – provient directement de l'attribut « nom » de HDS HiCommand Device Manager via l'appel de l'API XML GetStorageArray
- Modèle - provient directement de l'attribut « arrayType » de HDS HiCommand Device Manager via l'appel de l'API XML GetStorageArray
- Fournisseur : HDS
- Famille - provient directement de l'attribut « arrayFamily » de HDS HiCommand Device Manager via l'appel de l'API XML GetStorageArray
- IP : il s'agit de l'adresse IP de gestion de la baie, mais pas d'une liste exhaustive de toutes les adresses IP de la baie
- Capacité brute : valeur de base 2 représentant la somme de la capacité totale de tous les disques du système, quel que soit le rôle du disque.

Pool de stockage

Les termes suivants s'appliquent aux objets ou références que vous pouvez trouver sur les pages d'accueil des ressources du pool de stockage HDS. Un grand 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 d'autres fins que les volumes de données, par exemple, la journalisation, les snapshots
  - Provisionnement fin, s'il s'agit d'un pool HDP
  - RAID Group, mais les raisons ne seront pas les suivantes :

    Les données de l'infrastructure de données permettent d'éviter de doubler les capacités à tous les coûts. Sur les solutions HDS, il faut généralement construire des groupes RAID à partir des disques, créer des volumes de pool sur ces groupes RAID et construire des pools (souvent HDP, mais un usage spécial) à partir de ces volumes de pool. Si les informations sur l'infrastructure de données indiquent à la fois les groupes RAID sous-jacents tels qu'ils sont, ainsi que les pools, la somme de leur capacité brute dépasserait largement la somme des disques.

  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 du pool. Cela peut entraîner l'absence totale de rapports sur le groupe RAID par les informations sur l'infrastructure de données. De plus, tous les groupes RAID résultants sont marqués d'une manière telle qu'ils ne sont pas visibles dans l'interface utilisateur Web Data Infrastructure Insights, mais ils circulent dans le data warehouse DWH (Data Infrastructure Insights Data Warehouse). L'objectif de ces décisions est d'éviter l'encombrement de l'interface utilisateur pour les éléments qui ne sont pas importants pour la plupart des utilisateurs. Si votre baie HDS dispose de groupes RAID de 50 Mo libres, vous ne pouvez probablement pas utiliser cet espace libre pour des résultats significatifs.

- Node : N/A, car les pools HDS ne sont liés à aucun nœud spécifique
- Redondance : niveau RAID du pool. Il est possible que plusieurs valeurs pour un pool HDP comprennent plusieurs types RAID
- Capacity % : pourcentage utilisé par le pool pour l'utilisation des données, avec les Go utilisés et la taille totale des Go logiques du pool
- Capacité sur-engagée - valeur dérivée indiquant « la capacité logique de ce pool est sursouscrite par ce pourcentage en raison de la somme des volumes logiques dépassant la capacité logique du pool par ce pourcentage »
- Snapshot : affiche la capacité réservée à l'utilisation des snapshots sur ce pool

Nœud de stockage

Les termes suivants s'appliquent aux objets ou aux références que vous trouverez sur les pages d'accueil des ressources des nœuds de stockage HDS. Un grand nombre de ces termes s'appliquent également à d'autres collecteurs de données.

- Nom – Nom du responsable frontal (FED) ou de l'adaptateur de canal sur des baies monolithiques, ou nom du contrôleur sur une baie modulaire. Une baie HDS donnée possède au moins 2 nœuds de stockage
- Volumes – la table Volume affiche tout volume mappé sur un port appartenant à ce nœud de stockage

Exigences d'inventaire

Vous devez disposer des éléments suivants pour collecter les données de stock :

- Adresse IP du serveur HiCommand Device Manager
- Nom d'utilisateur et mot de passe en lecture seule pour le logiciel HiCommand Device Manager et les privilèges homologues
- Exigences relatives aux ports : 2001 (http) ou 2443 (https)
- Connectez-vous au logiciel HiCommand Device Manager à l'aide du nom d'utilisateur et du mot de passe
- Vérifiez l'accès au gestionnaire de périphériques HiCommand http://<HiCommand_Device_Manager_IP>:2001/service/StorageManager

Exigences en matière de performances

Les exigences suivantes doivent être respectées pour collecter les données de performance :

- Performances HDS USP, USP V, et VSP
  - Le moniteur de performances doit être sous licence.
  - L'interrupteur de surveillance doit être activé.
  - L'outil d'exportation (Export.exe) doit être copié dans Data Infrastructure Insights au.
  - La version de l'outil d'exportation doit correspondre à la version du microcode de la matrice cible.
- Performances AMS :
  - NetApp recommande fortement de créer un compte de service dédié sur les baies AMS pour les informations d'infrastructure de données à utiliser pour récupérer les données de performances. Storage Navigator n'autorise qu'un compte utilisateur à ouvrir une session simultanée sur la matrice. Si Data Infrastructure Insights utilise le même compte utilisateur que les scripts de gestion ou HiCommand, Data Infrastructure Insights, les scripts de gestion ou HiCommand peuvent ne pas communiquer avec la baie en raison de la limite de connexion à un compte utilisateur simultané
  - Le moniteur de performances doit être sous licence.
  - L'utilitaire CLI de Storage Navigator Modular 2 (SNM2) doit être installé sur Data Infrastructure Insights au.

Configuration

Champ	Description
Serveur HiCommand	Adresse IP ou nom de domaine complet du serveur HiCommand Device Manager
Nom d'utilisateur	Nom d'utilisateur du serveur HiCommand Device Manager.
Mot de passe	Mot de passe utilisé pour le serveur HiCommand Device Manager.

Champ	Description
PÉRIPHÉRIQUES : STOCKAGES VSP G1000 (R800), VSP (R700), HUS VM (HM700) ET USP	Liste des appareils pour les stockages VSP G1000 (R800), VSP (R700), HUS VM (HM700) et USP. Chaque stockage nécessite : * adresse IP de la matrice : 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 - WMS/SMS/AMS Storages	Liste des périphériques pour les stockages WMS/SMS/AMS. Chaque stockage nécessite : * adresse IP de la baie : adresse IP de la baie de stockage * chemin de la CLI du Storage Navigator : chemin de la CLI SNM2 * authentification du 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
L'hôte de Tuning Manager	Adresse IP ou nom de domaine complet du gestionnaire de réglages
Remplacer le port Tuning Manager	Si ce champ est vide, utilisez le port par défaut dans le champ choisir Tuning Manager for Performance, sinon entrez le port à utiliser
Nom d'utilisateur du gestionnaire de réglage	Nom d'utilisateur pour Tuning Manager
Mot de passe du gestionnaire de réglage	Mot de passe pour Tuning Manager

Remarque : dans les HDS USP, USP V et VSP, tout 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 HiCommand Device Manager
Intervalle d'interrogation des stocks (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 des matrices ci-dessous lors de la collecte des données.
Filtrer la liste des périphériques	Liste séparée par des virgules des numéros de série de périphérique à inclure ou exclure
Intervalle d'interrogation des performances (s)	Intervalle entre les sondages de performances. La valeur par défaut est 300.
Délai d'exportation en secondes	Expiration du délai de l'utilitaire d'exportation. La valeur par défaut est 300.

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
Erreur : l'utilisateur ne dispose pas d'une autorisation suffisante	Utilisez un compte utilisateur différent qui a plus de privilèges ou augmente le privilège du compte utilisateur configuré dans le collecteur de données
Erreur : la liste des stockages est vide. Soit les périphériques 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 qui a plus de privilèges ou augmentez le privilège du compte utilisateur
Erreur : la baie de stockage HDS n'a pas été actualisée depuis quelques jours	Étudier pourquoi cette matrice n'est pas actualisée dans HDS HiCommand.

Performances

Problème :	Essayer :
Erreur : * erreur lors de l'exécution de l'utilitaire d'exportation * erreur lors de l'exécution de la commande externe	* Vérifiez que l'utilitaire d'exportation est installé sur l'unité d'acquisition Data Infrastructure Insights * Vérifiez que l'emplacement de l'utilitaire d'exportation est correct dans la configuration du collecteur de données * Vérifiez que l'adresse IP de la matrice 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 * Vérifiez que la version de l'utilitaire d'exportation est compatible avec la matrice de stockage version du microcode de la matrice de stockage runWin.bat
Erreur : la connexion de l'outil d'exportation a échoué pour l'adresse IP cible	* Confirmez que le nom d'utilisateur/mot de passe est correct * Créez un ID utilisateur principalement pour ce collecteur de données HDS * Confirmez qu'aucun autre collecteur de données n'est configuré pour acquérir ce tableau
Erreur : les outils d'exportation sont consignés « Impossible d'obtenir la plage de temps pour la surveillance ».	* Vérifiez que la surveillance des performances est activée sur la matrice. * 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 : matrice de stockage non prise en charge par l'utilitaire d'exportation * erreur de configuration : matrice de stockage non prise en charge par l'interface CLI modulaire de Storage Navigator	* Configurez uniquement les matrices de stockage prises en charge. * Utilisez "Filtrer la liste de périphériques" pour exclure les matrices de stockage non prises en charge.

Problème :	Essayer :
Erreur : * erreur d'exécution de la commande externe * erreur de configuration : la matrice de stockage n'a pas été signalée par Inventory * erreur de configuration : le dossier d'exportation ne contient pas de fichiers JAR	* Vérifier l'emplacement de l'utilitaire d'exportation. * Vérifiez si la matrice de stockage en question est configurée dans le serveur HiCommand * définissez l'intervalle d'interrogation des performances sur plusieurs 60 secondes.
Erreur : * erreur de l'interface CLI du navigateur de stockage * erreur lors de l'exécution de la commande auPerform * erreur lors de l'exécution de la commande externe	* Vérifiez que l'interface de ligne de commande modulaire Storage Navigator est installée sur l'unité d'acquisition Data Infrastructure Insights * Vérifiez que l'emplacement de l'interface de ligne de commande modulaire Storage Navigator est correct dans la configuration du collecteur de données * Vérifiez que l'adresse IP de la matrice WMS/SMS/SMS/SMS est correcte dans la configuration du collecteur de données * Vérifiez que la version de l'interface de ligne de commande Storage Navigator Modular CLI est compatible avec la version de stockage configurée dans le répertoire d'acquisition de données *.
Erreur : erreur de configuration : matrice de stockage non signalée par Inventory	Vérifiez si la matrice de stockage en question est configurée dans le serveur HiCommand
Erreur : * aucune matrice n'est enregistrée avec la matrice CLI * Storage Navigator modulaire 2 n'est pas enregistrée avec la CLI * Storage Navigator modulaire 2 erreur de configuration : la matrice de stockage n'est pas enregistrée avec la CLI modulaire StorageNavigator	* Ouvrir l'invite de commande et changer le répertoire pour le chemin configuré * Exécuter la commande "set=STONARVM_HOME=." * Exécutez la commande "auunitref" * Confirmez que la sortie de la commande contient les détails de la matrice avec IP * si la sortie ne contient pas les détails de la matrice, enregistrez la matrice avec Storage Navigator CLI: - Ouvrir l'invite de commande et changer le répertoire avec le chemin configuré - exécutez la commande "SET=STONVM_HOME=". - Exécutez la commande "auunitaddauto -ip <ip>". Remplacez <ip> par le tableau de bord correct.

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Configuration du collecteur de données NAS Hitachi Vantara

Le collecteur de données NAS Hitachi Vantara est un collecteur de données d'inventaire et de configuration qui prend en charge la découverte des clusters HDS NAS. 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 à partir du collecteur de données HNAS. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Niveau	Groupe de disques
Cluster	Stockage
Nœud	Nœud de stockage
De la plage	Pool de stockage
Entraînement du système	LUN interne
Système de fichiers	Volume interne

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

- Adresse IP du périphérique
- 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'UA qui l'héberge doit donc être capable d'initier des sessions SSH vers TCP 22 sur le HNAS lui-même, ou 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 la CLI HNAS
Mot de passe	Mot de passe utilisé pour la CLI HNAS

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 30 minutes.

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
"Erreur lors de la connexion" avec les messages d'erreur "erreur lors de la configuration du canal du shell :" ou "erreur lors de l'ouverture du canal du shell"	La cause est probablement des problèmes de connectivité réseau ou de configuration incorrecte du système SSH. Vérifiez la connexion avec un autre client SSH
"Timeout" ou "erreur lors de la récupération des données" avec les messages d'erreur "la commande: XXX a expiré".	* Essayez la commande avec un autre client SSH * augmentez le délai d'attente
« Erreur lors de la connexion » ou « informations d'identification non valides » avec des messages d'erreur « Impossible de communiquer avec le périphérique : »	* Vérifiez l'adresse IP * Vérifiez le nom d'utilisateur et le mot de passe * Confirmez la connexion avec un autre client SSH

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données Hitachi Ops Center

Ce collecteur de données utilise la suite intégrée d'applications d'Hitachi Ops Center pour accéder aux données d'inventaire et de performances de plusieurs périphériques de stockage. Pour la découverte des stocks et de la capacité, l'installation du centre d'exploitation doit inclure les composants « Services communs » et « Administrateur ». Pour la collecte des performances, vous devez également avoir déployé « Analyzer ».

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir de ce collecteur de données. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Systèmes de stockage	Stockage
Volumétrie	Volumétrie
Groupes de parité	Pool de stockage (RAID), groupes de disques
Disque	Disque
Pool de stockage	Pool de stockage (fin, SNAP)
Groupes de parité externes	Storage Pool(interne), groupes de disques
Port	Nœud de stockage → nœud de contrôleur → port
Groupes d'hôtes	Mappage de volume et masquage
Paires de volume	Synchronisation du stockage

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences d'inventaire

Vous devez disposer des éléments suivants pour collecter les données de stock :

- Adresse IP ou nom d'hôte du serveur Ops Center hébergeant le composant « Common Services »
- Compte utilisateur root/sysadmin et mot de passe existant sur tous les serveurs hébergeant les composants Ops Center. HDS n'a pas implémenté de prise en charge des API REST pour l'utilisation par les utilisateurs LDAP/SSO jusqu'à Ops Center 10.8+

Exigences en matière de performances

Les exigences suivantes doivent être respectées pour collecter les données de performance :

Le module « Analyzer » du HDS Ops Center doit être installé. Les matrices de stockage doivent alimenter le module « analyseur » 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 "Common Services"
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 l'option par défaut
Remplacer le port TCP	Spécifiez le port à utiliser si ce n'est pas le port par défaut
Intervalle d'interrogation des stocks (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 des matrices ci-dessous lors de la collecte des données.
Filtrer la liste des périphériques	Liste séparée par des virgules des numéros de série de périphérique à inclure ou exclure
Intervalle d'interrogation des performances (s)	Intervalle entre les sondages de performances. La valeur par défaut est 300.

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données Infinidat Box d'Infinidat

Le collecteur de données Infinidat Box (HTTP) est utilisé pour recueillir des informations d'inventaire à partir du système de stockage Infinidat Box d'Infinidat.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès du collecteur de données Infinidat InfiniBox. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Pool de stockage	Pool de stockage
Nœud	Contrôleur
Système de fichiers	Volume interne
Système de fichiers	Partage de fichiers
Exportations des systèmes de fichiers	Partagez

De formation

Les conditions suivantes sont requises lors de la configuration de ce collecteur de données.

- Adresse IP ou FQDN du noeud de gestion InfiniBox
- ID utilisateur et mot de passe administrateur
- Le 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 du nœud de gestion InfiniBox
Mot de passe	Mot de passe du noeud de gestion de l'InfiniBox

Configuration avancée

Champ	Description
Port TCP	Port TCP utilisé pour se connecter au serveur InfiniBox. La valeur par défaut est 443.
Intervalle de sondage des stocks	Intervalle entre les sondages d'inventaire. La valeur par défaut est 60 minutes.

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données Huawei OceanStor

Data Infrastructure Insights utilise le collecteur de données Huawei OceanStor (REST/HTTPS) pour détecter l'inventaire et les performances des systèmes de stockage Huawei OceanStor et OceanStor Dorado.

Terminologie

Data Infrastructure Insights acquiert les informations suivantes sur l'inventaire et les performances à partir de Huawei OceanStor. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Pool de stockage	Pool de stockage
Système de fichiers	Volume interne
Contrôleur	Nœud de stockage
Port FC (mappé)	Carte de volume
Initiateur FC hôte (mappé)	Masque de volume
Partage NFS/CIFS	Partagez
Cible de liaison iSCSI	Nœud cible iSCSI
Initiateur de liaison iSCSI	Nœud initiateur iSCSI
Disque	Disque
LUN	Volumétrie

De formation

Les conditions suivantes sont requises pour configurer ce collecteur de données :

- Adresse IP du périphérique
- Informations d'identification permettant d'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 OceanStor Device Manager
Nom d'utilisateur	Nom utilisé pour se connecter à OceanStor Device Manager
Mot de passe	Mot de passe utilisé pour se connecter à OceanStor Device Manager

Configuration avancée

Champ	Description
Port TCP	Port TCP utilisé pour la connexion à OceanStor Device Manager. La valeur par défaut est 8088.
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 60 minutes.
Intervalle d'interrogation des performances (s).	La valeur par défaut est 300 secondes.

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

IBM

Collecteur de données IBM Cleversafe

Data Infrastructure Insights utilise ce collecteur de données pour détecter les données d'inventaire et de performance des systèmes de stockage IBM Cleversafe.

IBM Cleversafe est mesuré à un taux de TB brut différent de celui de l'unité gérée. Chaque 40 To de capacité non formatée IBM Cleversafe est chargée comme 1 "Unité gérée (UM)".

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir du collecteur de données IBM Cleversafe. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Pool de stockage	Pool de stockage
Conteneur	Volume interne
Conteneur	Partage de fichiers
Partage NFS	Partagez

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

- L'adresse IP des services de données externes pour le cluster
- Nom d'utilisateur et mot de passe administrateur
- Orifice 9440

Configuration

Champ	Description
IP Manager ou nom d'hôte	Adresse IP ou nom d'hôte du nœud de gestion
Nom d'utilisateur	Nom d'utilisateur du compte utilisateur avec le rôle super utilisateur ou administrateur système
Mot de passe	Mot de passe du compte utilisateur avec le rôle super utilisateur ou administrateur système

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire.
Délai d'expiration de la connexion HTTP (sec)	Délai d'attente HTTP en secondes.

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données IBM CS

Data Infrastructure Insights utilise ce collecteur de données pour détecter les données d'inventaire et de performance des systèmes de stockage IBM CS.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir du collecteur de données IBM CS. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Pool de stockage	Pool de stockage
Conteneur	Volume interne
Conteneur	Partage de fichiers
Partage NFS	Partagez

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

- L'adresse IP des services de données externes pour le cluster
- Nom d'utilisateur et mot de passe administrateur
- Orifice 9440

Configuration

Champ	Description
Adresse IP externe prismes	L'adresse IP des services de données externes pour le cluster
Nom d'utilisateur	Nom d'utilisateur du compte Admin
Mot de passe	Mot de passe du compte admin

Configuration avancée

Champ	Description
Port TCP	Port TCP utilisé pour la connexion à la baie IBM CS. La valeur par défaut est 9440.
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 60 minutes.
Intervalle(s) d'interrogation de performance	Intervalle entre les sondages de performances. La valeur par défaut est 300 secondes.

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données de la gamme IBM System Storage DS8000

Le collecteur de données IBM DS (CLI) prend en charge l'acquisition de données d'inventaire et de performance pour les périphériques DS6xxx et DS8xxx.

Les périphériques DS3xxx, DS4xxx et DS5xxx sont pris en charge par le "Collecteur de données NetApp E-Series". Consultez le tableau de prise en charge de Data Infrastructure Insights pour connaître les modèles et les versions de micrologiciel pris en charge.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir du collecteur de données IBM DS. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Module de lecteur de disque	Disque
Image stockage	Stockage
Pool d'extension	Nœud de stockage
Volume du bloc fixe	Volumétrie
Initiateur FC hôte (mappé)	Masque de volume

Remarque : il s'agit uniquement de mappages de terminologie communs et ne représentent peut-être pas tous les cas pour ce collectant de données.

De formation

Vous devez disposer des éléments suivants pour configurer ce collecteur de données :

- Adresse IP de chaque matrice DS
- Nom d'utilisateur et mot de passe en lecture seule sur chaque baie DS
- Logiciel tiers installé sur Data Infrastructure Insights au : IBM *dscli*
- Validation des accès : exécutez les commandes *dscli* à l'aide du nom d'utilisateur et du mot de passe
- Configuration minimale requise pour les ports : 80, 443 et 1750

Configuration

Champ	Description
Stockage DS	Adresse IP ou nom de domaine complet du périphérique DS
Nom d'utilisateur	Nom d'utilisateur pour l'interface de ligne de commande DS
Mot de passe	Mot de passe pour l'interface de ligne de commande DS
dscli chemin exécutable	Chemin complet vers l'exécutable *dscli*

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (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
Périphériques d'exclusion d'inventaire	Liste des numéros de série des périphériques séparés par des virgules à exclure de la collecte des stocks
Intervalle d'interrogation des performances (s)	La valeur par défaut est 300.
Type de filtre de performances	Inclure : données collectées uniquement à partir des périphériques de la liste. Exclure : aucune donnée de ces périphériques n'est collectée
Liste des périphériques de filtre de performances	Liste séparée par des virgules d'ID de périphérique à inclure ou exclure de la collecte de performances

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
Erreur contenant : CMUC00192E, CMUC00191E ou CMUC00190E	* Vérifier les informations d'identification et l'adresse IP saisies. * 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 PROGRAM * erreur d'exécution de la commande	* À partir de l'unité d'acquisition Data Infrastructure Insights Ouvrez un fichier CMD * Ouvrez un fichier CLI.CFG dans le répertoire principal/lib de CLI et vérifiez la propriété JAVA_INSTALL, modifiez la valeur pour qu'elle corresponde à votre environnement * Afficher la version java installée sur cet ordinateur, en tapant: "java -version" * Ping l'adresse IP du périphérique de stockage IBM spécifiée dans la commande CLI émise. * Si toutes les réponses ci-dessus fonctionnent correctement, exécutez manuellement une commande CLI

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Configuration du collecteur de données IBM PowerVM

Le collecteur de données IBM PowerVM (SSH) est utilisé pour collecter des informations sur les partitions virtuelles exécutées sur des instances matérielles IBM POWER gérées par une console de gestion du matériel (HMC).

Terminologie

Data Infrastructure Insights acquiert des informations d'inventaire à partir des partitions virtuelles s'exécutant sur des instances matérielles IBM POWER. Pour chaque type d'actif acquis, la terminologie la plus utilisée pour l'actif est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
hdisque	Disque virtuel
Système géré	Hôte
LPAR, serveur VIO	Ordinateur virtuel
Groupe de volumes	Datastore
Volume physique	LUN

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

Les conditions suivantes doivent être remplies pour configurer et utiliser ce collecteur de données :

- Adresse IP de la console de gestion du matériel (HMC)
- Nom d'utilisateur et mot de passe permettant d'accéder à la console HMC (Hardware Management Console) via SSH
- Port requis SSH-22
- Afficher les autorisations sur tous les systèmes de gestion et les domaines de sécurité des partitions logiques

  L'utilisateur doit également disposer de l'autorisation Afficher sur les configurations HMC et de la possibilité de collecter des informations VPD pour le regroupement de sécurité de la console HMC. L'utilisateur doit également être autorisé à accéder aux commandes Virtual IO Server sous le regroupement de sécurité de partition logique. Il est recommandé de commencer par un rôle d'opérateur, puis de supprimer tous les rôles. Les utilisateurs en lecture seule de la console HMC ne disposent pas des privilèges nécessaires pour exécuter des commandes proxy sur les hôtes AIX.

- La meilleure pratique d'IBM consiste à faire contrôler les appareils par deux ou plusieurs NCSM. Sachez que OnCommand Insight peut signaler les périphériques dupliqués. Il est donc fortement recommandé d'ajouter des périphériques redondants à la liste « exclure les périphériques » de la configuration avancée pour ce collecteur de données.

Configuration

Champ	Description
Adresse IP de la console de gestion du matériel (HMC)	Adresse IP ou nom de domaine complet de la console PowerVM Hardware Management Console
Utilisateur HMC	Nom d'utilisateur de la console de gestion du matériel
Mot de passe	Mot de passe utilisé pour la console de gestion du matériel

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 20 minutes.
Port SSH	Port utilisé pour SSH vers PowerVM
Mot de passe	Mot de passe utilisé pour la console de gestion du matériel
Nombre de tentatives	Nombre de tentatives d'inventaire
Exclure les périphériques	Liste séparée par des virgules d'ID de périphérique ou de noms d'affichage à exclure

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Configuration du collecteur de données du contrôleur de volume SAN IBM

Le collecteur de données du contrôleur de volume SAN (SVC) IBM 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 périphériques pris en charge comprend des modèles tels que le SVC, le v7000, le v5000 et le v3700. Consultez le tableau de prise en charge de Data Infrastructure Insights pour connaître les modèles et les versions de firmware pris en charge.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir du collecteur de données IBM SVC. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Lecteur	Disque
Cluster	Stockage
Nœud	Nœud de stockage
Groupe Mdisk	Pool de stockage
Disque virtuel	Volumétrie
Disque Mdisk	LUN et chemins back-end

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences d'inventaire

- Adresse IP de chaque cluster SVC
- Port 22 disponible
- Nom d'utilisateur et mot de passe en lecture seule

Exigences en matière de performances

- Console SVC, obligatoire pour tout cluster SVC et requise pour le package de base de découverte SVC.
- Les identifiants exigent 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 par 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 du service.

Configuration

Champ	Description
Adresses IP de cluster	Adresses IP ou noms de domaine complets du stockage SVC
Nom de l'utilisateur de stock	Nom d'utilisateur pour l'interface de ligne de commande du CSPR
Mot de passe d'inventaire	Mot de passe pour l'interface CLI du CSPR

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 40 minutes.
Intervalle d'interrogation des performances (s)	Intervalle entre les sondages de performances. La valeur par défaut est 300 secondes.
Pour nettoyer les fichiers de statistiques sous-évaluées	Cochez cette case pour nettoyer les fichiers de statistiques sous-évaluées

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Problème :	Essayer :
Erreur : « la commande ne peut pas être initialisée, car elle n'a pas été exécutée sur le nœud de configuration. »	La commande doit être exécutée sur le nœud de configuration.

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Problème :	Essayer :
Erreur : « la commande ne peut pas être initialisée, car elle n'a pas été exécutée sur le nœud de configuration. »	La commande doit être exécutée sur le nœud de configuration.

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

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 effectuée en effectuant des appels SMI-S vers la baie XIV/A9000, qui exécute un fournisseur SMI-S sur le port 7778.

Terminologie

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Disque	Disque
System de stockage	Stockage
Pool de stockage	Pool de stockage
Volumétrie	Volumétrie

De formation

Les conditions suivantes doivent être remplies pour configurer et utiliser ce collecteur de données :

- Port requis : port TCP 7778
- Nom d'utilisateur et mot de passe en lecture seule
- La CLI XIV doit être installée sur l'au

Exigences en matière de performances

Les conditions suivantes sont requises pour la collecte des performances :

- Agent SMI-S 1.4 ou supérieur
- CIMService compatible SMI-S s'exécutant sur une baie. La plupart des baies XIV disposent d'un cimserveur installé par défaut.
- Le nom d'utilisateur doit être fourni pour le cimserver. La connexion doit disposer d'un accès complet en lecture à la configuration et aux propriétés de la matrice.
- Espace de noms SMI-S. La valeur par défaut est root/ibm. Ceci est configurable dans le cimserver.
- Configuration requise : 5988 pour HTTP, 5989 pour HTTPS.
- Reportez-vous au 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
Adresse IP de XIV	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 complet vers l'annuaire de l'interface de ligne de commande XIV	Chemin d'accès complet au dossier contenant l'interface de ligne de commande XIV
Adresse IP de l'hôte SMI-S	Adresse IP de l'hôte SMI-S.

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 40 minutes.
Protocole SMI-S	Protocole utilisé pour la connexion au fournisseur SMI-S. Affiche également le port par défaut.
Remplacer le port SMI-S	Si ce champ est 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 SMI-S Provider
Mot de passe	Mot de passe de l'hôte SMI-S Provider
Intervalle d'interrogation des performances (s)	Intervalle entre les sondages de performances. La valeur par défaut est 300 secondes.

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données Lenovo

Data Infrastructure Insights utilise le collecteur de données Lenovo pour détecter les données d'inventaire et de performances des systèmes de stockage Lenovo HX.

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

- Adresse IP externe prismes
- Nom d'utilisateur et mot de passe administrateur
- Port TCP requis : 9440

Configuration

Champ	Description
Adresse IP externe prismes	L'adresse IP des services de données externes pour le cluster
Nom d'utilisateur	Nom d'utilisateur du compte Admin
Mot de passe	Mot de passe du compte admin

Configuration avancée

Champ	Description
Port TCP	Port TCP utilisé pour la connexion à la matrice. La valeur par défaut est 9440.
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 60 minutes.
Intervalle d'interrogation des performances (s)	Intervalle entre les sondages de performances. La valeur par défaut est 300 secondes.

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Microsoft

Configuration du collecteur de données Azure NetApp Files

Les informations d'infrastructure de données utilisent le collecteur de données Azure NetApp Files pour acquérir des données d'inventaire et de performance.

De formation

Vous avez besoin des informations suivantes pour configurer ce collecteur de données.

- Port requis : 443 HTTPS
- IP REST Azure Management (management.azure.com)
- ID client principal du service Azure (compte utilisateur)
- Clé d'authentification principale du service Azure (mot de passe utilisateur)
- Vous devez configurer un compte Azure pour la découverte Data Infrastructure Insights.

  Une fois le compte correctement configuré et que vous enregistrez l'application dans Azure, vous disposez des identifiants requis pour découvrir l'instance Azure avec Data Infrastructure Insights. Le lien suivant explique comment configurer le compte pour la découverte :

https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

Configuration

Entrez les données dans les champs du collecteur de données conformément au tableau ci-dessous :

Champ	Description
ID client principal du service Azure	ID de connexion à Azure
ID de locataire Azure	ID de locataire Azure
Clé d'authentification principale du service Azure	Clé d'authentification de connexion

Champ	Description
J'ai bien compris que Microsoft me facture pour les demandes d'API	Vérifiez que vous avez bien compris que Microsoft vous facture des demandes d'API formulées par l'interrogation Insight.

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	La valeur par défaut est 60

Dépannage

- Les identifiants utilisés par votre collecteur de données ANF doivent avoir accès à tous les abonnements Azure qui contiennent des volumes ANF.
- Si l'accès au lecteur provoque l'échec de la collecte des performances, essayez d'accorder l'accès au collaborateur au niveau d'un groupe de ressources.

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

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 de serveur virtualisé. Ce collecteur de données peut découvrir un hôte Hyper-V autonome ou un cluster entier. Il peut en créer un 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 de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Disque dur virtuel	Disque virtuel
Hôte	Hôte
Ordinateur virtuel	Ordinateur virtuel
CSV (Cluster Shared volumes), Volume de partitions	Datastore
Périphérique SCSI Internet, LUN SCSI Multi Path	LUN
Port Fibre Channel	Port

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

Les éléments suivants sont nécessaires pour configurer ce collecteur de données :

- Hyper-V requiert l'ouverture du port 5985 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 flottante du cluster constitue probablement l'approche la plus fiable au lieu de pointer le collecteur vers un seul nœud spécifique d'un cluster.
- Compte utilisateur de niveau administrateur qui fonctionne sur tous les hyperviseurs du cluster.
- WinRM doit être activé et être à l'écoute de tous les hyperviseurs
- Configuration requise du port : le port 135 via les ports WMI et TCP dynamique a été attribué à 1024-65535 pour Windows 2003 et versions antérieures et à 49152-65535 pour Windows 2008.
- La résolution DNS doit réussir, même si le collecteur de données est pointé à une seule adresse IP
- Chaque hyperviseur Hyper-V doit avoir la fonction de mesure des ressources activée pour chaque machine virtuelle, sur chaque hôte. Ainsi, chaque hyperviseur peut disposer de plus de données pour que Data Infrastructure Insights soit disponible sur chaque invité. Si ce paramètre n'est pas défini, moins de mesures de performance sont acquises pour chaque client. Pour plus d'informations sur la mesure des ressources, consultez 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 un hyperviseur autonome non mis en cluster
Nom d'utilisateur	Nom d'utilisateur administrateur de l'hyperviseur
Mot de passe	Mot de passe de l'hyperviseur
Suffixe de domaine DNS	Le suffixe de nom d'hôte associé au nom d'hôte simple pour afficher le nom de domaine complet d'un hyperviseur

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	La valeur par défaut est 20 minutes.

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

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 Volusens ONTAP
Nom d'utilisateur	Nom d'utilisateur de 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 si ce n'est pas le cas par défaut.
Intervalle d'interrogation des stocks (min)	La valeur par défaut est 60 minutes.
Inventaire nombre de threads simultanés	Nombre de threads simultanés.
Forcer TLS pour HTTPS	Forcer TLS sur HTTPS
Recherche automatique des groupes réseau	Recherche automatique des groupes réseau
Extension de groupe réseau	Sélectionnez coque ou fichier
Délai de lecture HTTP en secondes	La valeur par défaut est 30 secondes
Forcer les réponses au format UTF-8	Forcer les réponses au format UTF-8
Intervalle d'interrogation des performances (min)	La valeur par défaut est 900 secondes.
Nombre de threads simultanés de performance	Nombre de threads simultanés.
Collecte avancée des données du compteur	Cochez cette case pour que Data Infrastructure Insights collecte les metrics avancés à partir de la liste ci-dessous.

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données NetApp Cloud volumes Services pour AWS

Ce collecteur de données prend en charge la collecte d'inventaire depuis les configurations NetApp Cloud volumes Services pour AWS.

Configuration

Champ	Description
Région Cloud volumes	Région de NetApp Cloud volumes Services pour AWS
Clé API	Clé Cloud volumes API
Clé secrète	Clé secrète Cloud volumes

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	La valeur par défaut est 60 minutes

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Problème :	Essayer :
J'ai reçu une erreur similaire à celle-ci : « échec de l'exécution de la demande : connexion à <point de terminaison de la région AWS>:8080 [<point de terminaison de la région AWS>/IP du point de terminaison de la région AWS] échec : connexion expirée : OBTENTION DU nom de domaine complet du point de terminaison de la région https://<AWS>:8080/v1/stockage/IPRanges HTTP/1.1 »	Le système "proxy" utilisé par Data Infrastructure Insights pour communiquer avec l'unité d'acquisition ne communique pas entre Data Infrastructure Insights et le Data Collector lui-même. Voici quelques éléments que vous pouvez essayer : assurez-vous que l'unité d'acquisition est capable de résoudre le fqdn et d'atteindre le port requis. Confirmez qu'un proxy n'est pas nécessaire pour atteindre le noeud final spécifié dans le message d'erreur. Curl peut être utilisé pour tester la communication entre l'unité d'acquisition et le noeud final. Assurez-vous que vous utilisez **pas** un proxy pour ce test. Exemple : root@acquisition Unit# curl -s -H Accept:application/json -H « Content-type: Application/json » -H api-key:<clé api utilisée dans les informations d'identification du collecteur de données -H secret-key:<clé secrète utilisée dans les informations d'identification du collecteur de données> -X GET https://<AWS Regional Endpoint>:8080/v1/Storage/IPRanges Voir ce "Article de la base de connaissances NetApp".

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur des données du logiciel de gestion des données NetApp ONTAP

Ce collecteur de données acquiert les données d'inventaire et de performance des systèmes de stockage exécutant ONTAP en utilisant des appels d'API en lecture seule à partir d'un compte ONTAP. Ce collecteur de données crée également un enregistrement dans le registre d'applications du cluster pour accélérer le support.

Terminologie

Les informations d'infrastructure de données font l'acquisition des données d'inventaire et de performance du collecteur de données ONTAP. Pour chaque type d'actif acquis, la terminologie la plus utilisée pour l'actif est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Disque	Disque
Groupe RAID	Groupe de disques
Cluster	Stockage
Nœud	Nœud de stockage
Agrégat	Pool de stockage
LUN	Volumétrie
Volumétrie	Volume interne

Terminologie de la gestion des données ONTAP

Les termes suivants s'appliquent aux objets ou aux références que vous trouverez sur les pages d'accueil des ressources de stockage de gestion des données ONTAP. Un grand nombre de ces termes s'appliquent également à d'autres collecteurs de données.

Stockage

- Modèle – liste délimitée par des virgules des noms de modèles de nœud 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 apparaît.
- Fournisseur : même nom de fournisseur que vous pouvez voir si vous configurez une nouvelle source de données.
- Numéro de série – le numéro de série de la baie. Sur les systèmes de stockage en cluster, tels que le logiciel de gestion des données ONTAP, ce numéro de série peut être moins utile que les différents numéros de série des « nœuds de stockage ».
- IP : il s'agit généralement des adresses IP ou des noms d'hôte configurés dans la source de données.
- Version du microcode : micrologiciel.
- Capacité brute : somme de base 2 de tous les disques physiques du système, quel que soit leur rôle.
- Latence : représentation des charges de travail côté hôte, à la fois en lecture et en écriture. Idéalement, les informations sur l'infrastructure de données génèrent directement cette valeur, mais ce n'est souvent pas le cas. À la place de la baie qui propose cela, Data Infrastructure Insights effectue généralement un calcul pondéré par IOPS à partir des statistiques des volumes internes individuels.
- Débit : agrégé à partir de volumes internes. Gestion – il peut contenir un lien hypertexte pour l'interface de gestion du périphérique. Créé par programmation par la source de données Data Infrastructure Insights dans le cadre du reporting d'inventaire.

Pool de stockage

- Stockage : sur quelle baie de stockage ce pool vit. Obligatoire.

- Type – valeur descriptive d'une liste de possibilités énumérées. Le plus souvent sera "agrégat" ou "RAID Group".
- Node – si l'architecture de cette matrice 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 d'accueil.
- Utilise Flash Pool – valeur Oui/non – ce pool basé sur SATA/SAS utilise-t-il des disques SSD pour accélérer la mise en cache ?
- Redondance : niveau RAID ou schéma de protection. RAID_DP est la double parité, RAID_TP est la triple parité.
- Capacité : les valeurs indiquées ici sont les valeurs logiques utilisées, la capacité utilisable et la capacité totale logique, ainsi que le pourcentage utilisé sur ces valeurs.
- Capacité sursollicitée : si grâce aux 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, le pourcentage de valeur ici est supérieur à 0 %.
- Snapshot : les capacités des copies Snapshot utilisées et totales, si l'architecture des pools de stockage consacre une partie de sa capacité à la segmentation uniquement des snapshots. Ce document présente notamment la solution ONTAP dans les configurations MetroCluster, tandis que les autres configurations ONTAP sont moins nombreuses.
- Utilisation : pourcentage indiquant le pourcentage le plus élevé d'occupation du disque de tout disque contribuant à la capacité de ce pool de stockage. L'utilisation du disque n'est pas forcément synonyme de performances de la baie. L'utilisation peut être élevée en raison des reconstructions des disques et des activités de déduplication, etc. En l'absence de charges de travail pilotées par l'hôte. De plus, les implémentations de réplication de nombreuses baies peuvent conduire à l'utilisation du disque sans apparaître comme volume interne ou charge de travail du volume.
- IOPS : somme des IOPS de tous les disques qui fournissent la capacité à ce pool de stockage. Débit : somme du débit de tous les disques qui fournissent la capacité à ce pool de stockage.

Nœud de stockage

- Stockage : de quelle baie de stockage ce nœud fait partie. Obligatoire.
- Partenaire HAUTE DISPONIBILITÉ : sur les plateformes où un nœud bascule vers un seul et même nœud, cela se voit généralement ici.
- State : santé du nœud. Uniquement disponible lorsque la matrice est suffisamment saine pour être inventoriée par une source de données.
- Model : nom de modèle du nœud.
- Version : nom de version du périphérique.
- Numéro de série – numéro de série du nœud.
- Mémoire – mémoire de base 2 si disponible.
- Utilisation – sur ONTAP, il s'agit d'un indice de contrainte de contrôleur provenant d'un algorithme propriétaire. À chaque sondage sur les performances, un nombre compris entre 0 et 100 % est indiqué, soit plus le conflit entre le disque WAFL, soit l'utilisation moyenne du CPU. Si vous constatez des valeurs durables supérieures à 50 %, c'est-à-dire un sous-dimensionnement. Un contrôleur/nœud peut être trop volumineux ou pas assez de disques rotatifs pour absorber la charge de travail d'écriture.
- IOPS : provient directement des appels ZAPI ONTAP sur l'objet de nœud.
- Latence : dérivée des appels ZAPI ONTAP sur l'objet de nœud.
- Débit : dérivé directement des appels ZAPI ONTAP sur l'objet de nœud.

- Processeurs – nombre de processeurs.

De formation

Les conditions 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.
- Configuration requise pour les ports : 80 ou 443
- Autorisations de compte :
  - Nom de rôle en lecture seule pour l'application ontapi au Vserver par défaut
  - Vous pouvez demander des autorisations d'écriture supplémentaires. Reportez-vous à la remarque sur les autorisations ci-dessous.
- Exigences relatives aux licences ONTAP :
  - Une licence FCP et des volumes mappés/masqués sont requis pour la détection Fibre Channel

Exigences d'autorisation pour la collecte des mesures de commutateur ONTAP

Les informations d'infrastructure de données peuvent collecter en option les données des commutateurs de cluster ONTAP dans Configuration avancéeles paramètres du collecteur. En plus de l'activer sur le collecteur de données d'informations d'infrastructure de données, vous devez également **configurer le système ONTAP** lui-même pour fournir "informations sur le commutateur", et vous assurer que les bonnes autorisations sont définies, afin de permettre l'envoi des données de commutateur aux informations d'infrastructure de données.

Configuration

Champ	Description
IP de gestion NetApp	Adresse IP ou nom de domaine complet du cluster NetApp
Nom d'utilisateur	Nom d'utilisateur du 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 autre port si vous ne souhaitez pas utiliser le port par défaut
Intervalle d'interrogation des stocks (min)	La valeur par défaut est 60 minutes.
Pour TLS pour HTTPS	Autoriser TLS uniquement en tant que protocole lors de l'utilisation de HTTPS
Recherche automatique des groupes réseau	Activez les recherches de groupe réseau automatiques pour les règles de stratégie d'exportation

Champ	Description
Extension de groupe réseau	Stratégie d'extension de groupe réseau. Choisissez *file* ou *shell*. La valeur par défaut est *shell*.
Délai de lecture HTTP en secondes	La valeur par défaut est 30
Forcer les réponses au format 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 (s)	La valeur par défaut est 900 secondes.
Collecte avancée des données du compteur	Activez l'intégration ONTAP. Sélectionnez cette option pour inclure les données de compteur avancé ONTAP dans les sondages. Choisissez les compteurs souhaités dans la liste.
Metrics des commutateurs de cluster	Permettez à Data Infrastructure Insights de collecter les données des commutateurs de cluster. Notez qu'en plus de l'activer du côté informations sur l'infrastructure de données, vous devez également configurer le système ONTAP pour fournir "informations sur le commutateur"et vous assurer que les bonnes autorisations sont définies, afin de permettre l'envoi des données de commutation aux informations sur l'infrastructure de données. Reportez-vous à la section « Note sur les autorisations » ci-dessous.

Mesures de puissance ONTAP

Plusieurs modèles ONTAP fournissent des metrics de puissance pour les informations exploitables de l'infrastructure de données, qui peuvent être utilisés à des fins de surveillance ou d'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, la prise en charge devrait être identique, mais ce n'est pas garanti. Si vous n'êtes pas sûr que votre modèle prenne en charge les mesures de puissance, contactez le support ONTAP.

Modèles pris en charge :

A200 A250 A300 A320 A400 A700 A220 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

Comme plusieurs tableaux de bord ONTAP de Data Infrastructure Insights reposent sur des compteurs ONTAP avancés, vous devez activer **Advanced Counter Data Collection** dans la section Data Collector Advanced Configuration.

Vous devez également vous assurer que l'autorisation d'écriture à l'API ONTAP est activée. Ces opérations nécessitent généralement un compte au niveau du cluster avec les autorisations nécessaires.

Pour créer un compte local pour les données d'infrastructure de données au niveau du cluster, connectez-vous à ONTAP avec le nom d'utilisateur/mot de passe de l'administrateur de gestion du cluster et exécutez les commandes suivantes sur le serveur ONTAP :

1. Avant de commencer, vous devez être connecté à ONTAP avec un compte *Administrator* et *diagnostics-level commands* doit être activé.
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 create exécutée, vous êtes 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 le 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 les données des commutateurs du 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 de l'utilisateur ainsi obtenus seront similaires à ceux qui suivent. 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 défini correctement, les appels REST de Data Infrastructure Insights peuvent échouer et entraîner des lacunes dans les données du périphérique. Par exemple, si vous l'avez activé sur le collecteur d'informations sur l'infrastructure de données mais que vous n'avez pas configuré les autorisations sur ONTAP, l'acquisition échouera. En outre, 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

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
Réception 401 réponse HTTP ou 13003 code d'erreur ZAPI et ZAPI renvoie "privilèges insuffisants" ou "non autorisés pour cette commande"	Vérifiez le nom d'utilisateur et le mot de passe, ainsi que les privilèges/autorisations utilisateur.
La version du cluster est < 8.1	La version minimale prise en charge par le cluster est 8.1. Passez à la version minimale prise en charge.
ZAPI renvoie « le rôle de cluster n'est pas Cluster_mgmt LIF ».	L'au doit communiquer avec l'IP de gestion de cluster. Vérifiez l'adresse IP et remplacez-la par une autre adresse IP si nécessaire
Erreur : "les filers 7 mode ne sont pas pris en charge"	Cela peut se produire si vous utilisez ce collecteur de données pour découvrir le filer 7 mode. Remplacez l'IP par un cluster cdot.
La commande ZAPI échoue après une nouvelle tentative	Problème de communication au 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 l'ordinateur au.
Echec de la connexion à ZAPI via HTTP	Vérifiez si le port ZAPI accepte le texte en clair. Si l'au tente d'envoyer du texte en texte clair vers une socket SSL, la communication échoue.
La communication échoue avec SSLException	Au tente d'envoyer SSL vers un port en texte clair sur un filer. Vérifiez si le port ZAPI accepte SSL ou utilise un autre port.

Problème :	Essayer :
Autres erreurs de connexion : la réponse ZAPI a 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 n'a pas terminé à temps" la réponse ZAPI contient "initialize_session() retourné environnement NULL" le code d'erreur ZAPI est 14007 et la réponse contient "noeud 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 l'ordinateur au.

Performances

Problème :	Essayer :
Erreur "Echec de la collecte des performances à partir de ZAPI"	Ce chiffre est généralement dû à une baisse des performances. Essayez la commande suivante sur chaque nœud : > *system node systemshell -node * -command "spmctl -h cmd –stop; spmctl -h cmd –exec"*

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données REST NetApp ONTAP

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 REST ONTAP peut être utilisé en remplacement du collecteur basé sur ONTAPI précédent. Ainsi, il peut y avoir des différences dans les mesures qui sont collectées ou déclarées. Pour plus d'informations sur les différences entre ONTAPI et REST, consultez la "Mappage de ONTAP 9.14.1 ONTAPI-to-REST" documentation.

De formation

Les conditions 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 si vous créez un nouvel utilisateur/rôle REST.
  - Fonctionnellement, Data Infrastructure Insights effectue principalement des requêtes de lecture, mais certaines autorisations d'écriture sont requises pour que les informations d'infrastructure de données s'enregistrent sur la baie ONTAP. Voir la *remarque sur les autorisations* ci-dessous.
- ONTAP version 9.14.1 ou supérieure.
- Exigences relatives aux ports : 443

Remarque sur les autorisations

Comme plusieurs tableaux de bord ONTAP de Data Infrastructure Insights reposent sur des compteurs

ONTAP avancés, vous devez conserver **Activer la collecte avancée de données de compteur** activé dans la section Configuration avancée du collecteur de données.

Pour créer un compte local pour les données d'infrastructure de données au niveau du cluster, connectez-vous à ONTAP avec le nom d'utilisateur/mot de passe de l'administrateur de gestion du cluster et exécutez les commandes suivantes sur le serveur ONTAP :

1. Avant de commencer, vous devez être connecté à ONTAP avec un compte *Administrator* et *diagnostics-level commands* doit être activé.
2. Récupérer le nom du vServer 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 create exécutée, vous êtes invité à saisir un mot de passe pour cet utilisateur. Notez que dans la commande suivante, le jeu de rôles est *ci_readonly*. Si vous créez un rôle portant un nom différent à l'étape 3 ci-dessus, utilisez ce nom de rôle personnalisé.

```
 security login create -user-or-group-name {username} -application http
-authentication-method password -role {role name}
Si le 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 de l'utilisateur ainsi obtenus seront similaires
à ceux qui suivent. 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 précédent collecteur de données ONTAP (ontapi) vers le nouveau collecteur de données REST ONTAP, procédez comme suit :

1. Ajoutez le collecteur de REPOS. Il est recommandé de saisir des informations pour un utilisateur différent de celui configuré pour le collecteur précédent. Par exemple, utilisez l'utilisateur noté dans la section autorisations ci-dessus.
2. Mettez le collecteur précédent en pause pour qu'il ne continue pas à collecter des données.
3. Laissez le nouveau collecteur de REPOS acquérir les données pendant au moins 30 minutes. Ignorez les données qui n'apparaissent pas « normales » pendant cette période.
4. Après la période de repos, vous devriez voir vos données se stabiliser au fur et à mesure que le collecteur de REPOS continue à 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 Cluster Management.
Nom d'utilisateur REST ONTAP	Nom d'utilisateur du cluster NetApp
Mot de passe REST ONTAP	Mot de passe pour le cluster NetApp

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	La valeur par défaut est 60 minutes.
Intervalle d'interrogation des performances (s)	La valeur par défaut est 60 secondes.
Collecte avancée des données du compteur	Sélectionnez cette option pour inclure les données de compteur avancé ONTAP dans les sondages. Activé par défaut.
Activer la collecte d'événements EMS	Sélectionnez cette option pour inclure les données des événements du journal EMS ONTAP. Activé par défaut.
Intervalle d'interrogation EMS (s)	La valeur par défaut est 60 secondes.

Terminologie

Les informations d'infrastructure de données font l'acquisition d'inventaires, de journaux et de données de performances à partir du collecteur de données ONTAP. Pour chaque type d'actif acquis, la terminologie la plus utilisée pour l'actif est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Disque	Disque
Groupe RAID	Groupe de disques
Cluster	Stockage
Nœud	Nœud de stockage
Agrégat	Pool de stockage
LUN	Volumétrie
Volumétrie	Volume interne
Storage Virtual machine/Vserver	Storage Virtual machine (SVM)

Terminologie de la gestion des données ONTAP

Les termes suivants s'appliquent aux objets ou aux références que vous trouverez sur les pages d'accueil des ressources de stockage de gestion des données ONTAP. Un grand nombre de ces termes s'appliquent

également à d'autres collecteurs de données.

Stockage

- Modèle – liste délimitée par des virgules des noms de modèles de nœud 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 apparaît.
- Fournisseur : même nom de fournisseur que vous pouvez voir si vous configurez une nouvelle source de données.
- Numéro de série : UUID de la baie
- IP : il s'agit généralement des adresses IP ou des noms d'hôte configurés dans la source de données.
- Version du microcode : micrologiciel.
- Capacité brute : somme de base 2 de tous les disques physiques du système, quel que soit leur rôle.
- Latence : représentation des charges de travail côté hôte, à la fois en lecture et en écriture. Idéalement, les informations sur l'infrastructure de données génèrent directement cette valeur, mais ce n'est souvent pas le cas. À la place de la baie qui propose cela, Data Infrastructure Insights effectue généralement un calcul pondéré par IOPS à partir des statistiques des volumes internes individuels.
- Débit : agrégé à partir de volumes internes. Gestion – il peut contenir un lien hypertexte pour l'interface de gestion du périphérique. Créé par programmation par la source de données Data Infrastructure Insights dans le cadre du reporting d'inventaire.

Pool de stockage

- Stockage : sur quelle baie de stockage ce pool vit. Obligatoire.
- Type – valeur descriptive d'une liste de possibilités énumérées. Le plus souvent sera "agrégat" ou "RAID Group".
- Node – si l'architecture de cette matrice 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 d'accueil.
- Utilise Flash Pool – valeur Oui/non – ce pool basé sur SATA/SAS utilise-t-il des disques SSD pour accélérer la mise en cache ?
- Redondance : niveau RAID ou schéma de protection. RAID_DP est la double parité, RAID_TP est la triple parité.
- Capacité : les valeurs indiquées ici sont les valeurs logiques utilisées, la capacité utilisable et la capacité totale logique, ainsi que le pourcentage utilisé sur ces valeurs.
- Capacité sursollicitée : si grâce aux 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, le pourcentage de valeur ici est supérieur à 0 %.
- Snapshot : les capacités des copies Snapshot utilisées et totales, si l'architecture des pools de stockage consacre une partie de sa capacité à la segmentation uniquement des snapshots. Ce document présente notamment la solution ONTAP dans les configurations MetroCluster, tandis que les autres configurations ONTAP sont moins nombreuses.
- Utilisation : pourcentage indiquant le pourcentage le plus élevé d'occupation du disque de tout disque contribuant à la capacité de ce pool de stockage. L'utilisation du disque n'est pas forcément synonyme de performances de la baie. L'utilisation peut être élevée en raison des reconstructions des disques et des activités de déduplication, etc. En l'absence de charges de travail pilotées par l'hôte. De plus, les implémentations de réplication de nombreuses baies peuvent conduire à l'utilisation du disque sans apparaître comme volume interne ou charge de travail du volume.
- IOPS : somme des IOPS de tous les disques qui fournissent la capacité à ce pool de stockage. Débit :

somme du débit de tous les disques qui fournissent la capacité à ce pool de stockage.

Nœud de stockage

- Stockage : de quelle baie de stockage ce nœud fait partie. Obligatoire.
- Partenaire HAUTE DISPONIBILITÉ : sur les plateformes où un nœud bascule vers un seul et même nœud, cela se voit généralement ici.
- State : santé du nœud. Uniquement disponible lorsque la matrice est suffisamment saine pour être inventoriée par une source de données.
- Model : nom de modèle du nœud.
- Version : nom de version du périphérique.
- Numéro de série – numéro de série du nœud.
- Mémoire – mémoire de base 2 si disponible.
- Utilisation – sur ONTAP, il s'agit d'un indice de contrainte de contrôleur provenant d'un algorithme propriétaire. À chaque sondage sur les performances, un nombre compris entre 0 et 100 % est indiqué, soit plus le conflit entre le disque WAFL, soit l'utilisation moyenne du CPU. Si vous constatez des valeurs durables supérieures à 50 %, c'est-à-dire un sous-dimensionnement. Un contrôleur/nœud peut être trop volumineux ou pas assez de disques rotatifs pour absorber la charge de travail d'écriture.
- IOPS : provient directement des appels REST ONTAP sur l'objet de nœud.
- Latence : dérivée des appels REST ONTAP sur l'objet de nœud.
- Débit : dérivé directement des appels REST ONTAP sur l'objet de nœud.
- Processeurs – nombre de processeurs.

Mesures de puissance ONTAP

Plusieurs modèles ONTAP fournissent des metrics de puissance pour les informations exploitables de l'infrastructure de données, qui peuvent être utilisés à des fins de surveillance ou d'alerte. Les listes des modèles pris en charge et non pris en charge ci-dessous ne sont pas exhaustives, mais doivent fournir des conseils ; en général, si un modèle se trouve dans la même famille qu'un modèle de la liste, le support doit être le même.

Modèles pris en charge :

A200 A250 A300 A320 A400 A700 A220 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

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Problème :	Essayer :
Lors de la tentative de création d'un collecteur de données REST ONTAP, une erreur du type suivant s'affiche : configuration : 10.193.70.14 : l'API REST ONTAP à l'adresse 10.193.70.14 n'est pas disponible : 10.193.70.14 échec de l'OBTENTION DE /api/cluster : 400 demande incorrecte	Cela est probablement dû à une baie de ONTAP olDeer, par exemple, ONTAP 9.6) qui ne possède pas de fonctionnalités d'API REST. ONTAP 9.14.1 est la version minimale de ONTAP prise en charge par le collecteur REST ONTAP. Les réponses « 400 Bad Request » doivent être attendues sur les versions ONTAP pré-REST. Pour les versions ONTAP qui prennent en charge REST mais qui ne sont pas 9.14.1 ou plus tard, vous pouvez voir le message simillar suivant: Configuration: 10.193.98.84: ONTAP Rest API at 10.193.98.84 n'est pas disponible: 10.193.98.84: ONTAP Rest API at 10.193.98.84 est disponible: Cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7 mais n'est pas de la version minimale 9.14.1.
Je vois des métriques vides ou « 0 » où le collecteur ONTAP ontapi affiche des données.	ONTAP REST ne signale pas les mesures 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 REST ONTAP qui peuvent signaler zéro ou des données vides : Internalvolumes : REST n'indique plus vol0. Agrégats : REST ne signale plus aggr0. Stockage : la plupart des mesures sont un cumul des mesures du volume interne et seront affectées par ce qui précède. Machines virtuelles de stockage : REST ne signale plus des SVM de type autre que « données » (par exemple, « cluster », « gmt », « nœud »). Vous pouvez également remarquer un changement dans l'apparence des graphiques qui ont des données, en raison de la modification de la période d'interrogation de performance par défaut de 15 minutes à 5 minutes. Une interrogation plus fréquente signifie plus de points de données à tracer.

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données NetApp Data ONTAP 7-mode

Pour les systèmes de stockage qui utilisent le logiciel Data ONTAP 7-mode, vous utilisez le collecteur de données 7-mode qui utilise l'interface de ligne de commandes pour obtenir des données de capacité et de performances.

Terminologie

Les informations d'inventaire suivantes sont acquises depuis le collecteur de données NetApp 7-mode. Pour chaque type d'actif acquis, la terminologie la plus utilisée pour ce bien est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Ce collecteur de données est "obsolète".

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Disque	Disque
Groupe RAID	Groupe de disques
Fichier	Stockage
Fichier	Nœud de stockage
Agrégat	Pool de stockage
LUN	Volumétrie
Volumétrie	Volume interne

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

Vous devez disposer des éléments suivants pour configurer et utiliser ce collecteur de données :

- Les adresses IP du contrôleur de stockage FAS et du partenaire.
- Orifice 443
- Nom d'utilisateur et mot de passe personnalisés de niveau administrateur pour les contrôleurs et les contrôleurs partenaires, avec les fonctionnalités suivantes pour 7-mode :
  - « api-* » : utilisez-le pour permettre à OnCommand Insight d'exécuter toutes les commandes de l'API de stockage NetApp.
  - « Login-http-admin » : utilisez ce pour permettre à OnCommand Insight de se connecter au stockage NetApp via HTTP.
  - « Security-api-vfiler » : utilisez cette option pour permettre à OnCommand Insight d'exécuter les commandes de l'API de stockage NetApp et de récupérer les informations relatives à l'unité vFiler.
  - « cli-options » : permet de lire les options du système de stockage.
  - cli-lun : accédez à ces commandes pour gérer les LUN. Affiche le statut (chemin de LUN, taille, état en ligne/hors ligne et état partagé) de la LUN ou classe de LUN donnée.
  - « cli-df » : utilisez ce système pour afficher l'espace disque disponible.
  - « cli-ifconfig » : utilisez-le 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 du système de stockage NetApp
Mot de passe	Mot de passe du système de stockage NetApp

Champ	Description
Adresse du partenaire de haute disponibilité dans le Cluster	Adresse IP ou nom de domaine complet pour le partenaire de haute disponibilité
Nom d'utilisateur du partenaire de haute disponibilité dans le cluster	Nom d'utilisateur du partenaire HA
Mot de passe du serveur de fichiers du partenaire HA dans le cluster	Mot de passe du partenaire HA

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 20 minutes.
Type de connexion	HTTPS ou HTTP, affiche également le port par défaut
Remplacer le port de connexion	Si ce champ est 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 (s)	Intervalle entre les sondages de performances. La valeur par défaut est 300 secondes.

Connexion des systèmes de stockage

Comme alternative à l'utilisation de l'utilisateur d'administration par défaut pour ce collecteur de données, vous pouvez configurer un utilisateur avec des droits d'administration directement sur les systèmes de stockage NetApp. Ainsi, ce collecteur de données peut acquérir des données à partir des systèmes de stockage NetApp.

Pour se connecter aux systèmes de stockage NetApp, l'utilisateur, qui est spécifié lors de l'acquisition du filer principal (là où il existe le système de stockage), doit respecter les conditions suivantes :

- L'utilisateur doit se trouver sur vfiler0 (filer racine/pFiler).

  Les systèmes de stockage sont acquis lors de l'acquisition du filer principal.

- Les commandes suivantes définissent les fonctions de rôle utilisateur :
  - « api-* » : permet aux informations de l'infrastructure de données d'exécuter toutes les commandes de l'API de stockage NetApp.

    Cette commande est nécessaire pour utiliser le ZAPI.

  - « Login-http-admin » : permet aux informations de l'infrastructure de données de se connecter au stockage NetApp via HTTP. Cette commande est nécessaire pour utiliser le ZAPI.
  - « Security-api-vfiler » : permet aux informations de l'infrastructure de données d'exécuter des commandes de l'API de stockage NetApp pour récupérer les informations de l'unité vFiler.
  - « cli-options » : pour la commande « options » et utilisée pour les licences IP du partenaire et activées.
  - cli-lun : accédez à cette commande pour gérer les LUN. Affiche le statut (chemin de LUN, taille, état en ligne/hors ligne et état partagé) de la LUN ou classe de LUN donnée.

- « cli-df » : pour les commandes df –s », « df -r » et « df -A -r » et l'espace utilisé pour afficher l'espace disponible.
- « cli-ifconfig » : pour la commande « ifconfig -a » et utilisée pour obtenir l'adresse IP du filer.
- « cli-rdfile » : pour la commande « rdfile /etc/netgroup » et utilisée pour obtenir des netgroups.
- CLI-date : pour la commande « date » et utilisée pour obtenir des dates complètes pour la copie Snapshot.
- CLI-snap : pour la commande « snap list » et utilisée pour obtenir les copies Snapshot.

Si vous ne disposez pas d'autorisations CLI-date ou CLI-snap, l'acquisition peut être terminée, 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, définissez les rôles à l'aide de l'une des chaînes de commandes suivantes. 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-*,security-api-vfile,cli-

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
Réception 401 réponse HTTP ou 13003 code d'erreur ZAPI et ZAPI renvoie "privilèges insuffisants" ou "non autorisés pour cette commande"	Vérifiez le nom d'utilisateur et le mot de passe, ainsi que les privilèges/autorisations utilisateur.
Erreur "échec de l'exécution de la commande"	Vérifiez si l'utilisateur dispose des autorisations suivantes sur le périphérique : • 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 de ONTAP est prise en charge par les informations d'identification de l'infrastructure de données et vérifiez si les informations d'identification utilisées correspondent aux informations d'identification du périphérique
La version du cluster est < 8.1	La version minimale prise en charge par le cluster est 8.1. Passez à la version minimale prise en charge.
ZAPI renvoie « le rôle de cluster n'est pas Cluster_mgmt LIF ».	L'au doit communiquer avec l'IP de gestion de cluster. Vérifiez l'adresse IP et remplacez-la par une autre adresse IP si nécessaire
Erreur : "les filers 7 mode ne sont pas pris en charge"	Cela peut se produire si vous utilisez ce collecteur de données pour découvrir le filer 7 mode. Remplacez l'IP par un filer cdot.

Problème :	Essayer :
La commande ZAPI échoue après une nouvelle tentative	Problème de communication au 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 l'ordinateur au.
Echec de la connexion à ZAPI	Vérifiez la connectivité IP/port et activez la configuration ZAPI.
Echec de la connexion à ZAPI via HTTP	Vérifiez si le port ZAPI accepte le texte en clair. Si l'au tente d'envoyer du texte en texte clair vers une socket SSL, la communication échoue.
La communication échoue avec SSLException	Au tente d'envoyer SSL vers un port en texte clair sur un filer. Vérifiez si le port ZAPI accepte SSL ou utilise un autre port.
Autres erreurs de connexion : la réponse ZAPI a 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 n'a pas terminé à temps" la réponse ZAPI contient "initialize_session() retourné environnement NULL" le code d'erreur ZAPI est 14007 et la réponse contient "noeud 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 l'ordinateur au.
Erreur d'expiration de socket avec ZAPI	Vérifiez la connectivité du filer et/ou augmentez le délai d'expiration.
"Les clusters C mode ne sont pas pris en charge par la source de données 7 mode"	Vérifiez l'IP et remplacez l'IP par un cluster 7 mode.
Erreur « échec de la connexion à vFiler »	Vérifiez que les fonctionnalités utilisateur acquises incluent les éléments suivants au minimum : api-* Security-api-vfiler login-http-admin Confirmez que le filer exécute la version minimale de ONTAPI version 1.7.

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données de l'API SANtricity héritée NetApp E-Series

Le collecteur de données de l'API SANtricity héritée NetApp E-Series collecte les données d'inventaire et de performance. Le collecteur prend en charge le micrologiciel 7.x+ en utilisant les mêmes configurations et en signalant les mêmes données.

Terminologie

Cloud Insight acquiert les informations d'inventaire suivantes auprès du collecteur de données NetApp E-Series. Pour chaque type d'actif acquis, la terminologie la plus utilisée pour ce bien est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Disque	Disque
Groupe de volumes	Groupe de disques
Baie de stockage	Stockage
Contrôleur	Nœud de stockage
Groupe de volumes	Pool de stockage
Volumétrie	Volumétrie

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

Terminologie E-Series (page d'accueil)

Les termes suivants s'appliquent aux objets ou aux références que vous trouverez sur les pages d'accueil des ressources NetApp E-Series. Un grand nombre de ces termes s'appliquent également à d'autres collecteurs de données.

Stockage

- Modèle : nom de modèle du périphérique.
- Fournisseur : même nom de fournisseur que vous pouvez voir si vous configurez une nouvelle source de données
- Numéro de série – le numéro de série de la baie. Sur les systèmes de stockage en cluster comme NetApp clustered Data ONTAP, ce numéro de série peut être moins utile que les numéros de série individuels de nœuds de stockage
- IP : il s'agit généralement des adresses IP ou des noms d'hôte configurés dans la source de données
- Version du microcode : micrologiciel
- Capacité brute : somme de base 2 de tous les disques physiques du système, quel que soit leur rôle
- Latence : représentation des charges de travail côté hôte, à la fois en lecture et en écriture. Idéalement, les informations sur l'infrastructure de données génèrent directement cette valeur, mais ce n'est souvent pas le cas. À la place de la baie qui propose cela, Data Infrastructure Insights effectue généralement un calcul pondéré en IOPS à partir des statistiques des volumes individuels.
- Débit : débit de la baie hôte total. Idéalement situé directement à partir de la baie, Data Infrastructure Insights additionne le débit des volumes pour tirer parti de cette valeur en cas d'indisponibilité
- Gestion – il peut contenir un lien hypertexte pour l'interface de gestion du périphérique. Créé par programmation par la source de données Data Infrastructure Insights dans le cadre du reporting d'inventaire

Pool de stockage

- Stockage : sur quelle baie de stockage ce pool vit. Obligatoire
- Type – valeur descriptive d'une liste de possibilités énumérées. Le plus souvent, il s'agit de « provisionnement fin » ou de « groupe RAID ».
- Node – si l'architecture de cette matrice 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 d'accueil

- Utilise Flash Pool – valeur Oui/non
- Redondance : niveau RAID ou schéma de protection. E-Series signale « RAID 7 » pour les pools DDP
- Capacité : les valeurs indiquées ici sont les valeurs logiques utilisées, la capacité utilisable et la capacité totale logique, ainsi que le pourcentage utilisé sur ces valeurs. Cette valeur inclut la capacité de « conservation » des baies E-Series, ce qui se traduit par des chiffres et par un pourcentage supérieur à ce que peut afficher la propre interface utilisateur de la gamme E-Series
- Capacité surdédiée : si grâce aux 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, le pourcentage est supérieur à 0 % dans ce cas.
- Snapshot : les capacités des copies Snapshot utilisées et totales, si l'architecture des pools de stockage consacre une partie de sa capacité à la segmentation uniquement des snapshots
- Utilisation : pourcentage indiquant le pourcentage le plus élevé d'occupation du disque de tout disque contribuant à la capacité de ce pool de stockage. L'utilisation du disque n'est pas forcément synonyme de performances de la baie. L'utilisation peut être élevée en raison des reconstructions des disques et des activités de déduplication, etc. En l'absence de charges de travail pilotées par l'hôte. De plus, les implémentations de réplication de nombreuses baies peuvent conduire à l'utilisation du disque sans s'afficher en tant que charge de travail du volume.
- IOPS : somme des IOPS de tous les disques qui fournissent la capacité à ce pool de stockage. Si les IOPS du disque ne sont pas disponibles sur une plateforme donnée, cette valeur provient de la somme des IOPS du volume pour tous les volumes présents sur ce pool de stockage
- Débit : somme du débit de tous les disques qui fournissent la capacité à ce pool de stockage. Si le débit des disques n'est pas disponible sur une plateforme donnée, cette valeur provient de la somme des volumes au sein de tous les volumes situés sur ce pool de stockage

Nœud de stockage

- Stockage : de quelle baie de stockage ce nœud fait partie. Obligatoire
- Partenaire HAUTE DISPONIBILITÉ : sur les plateformes où un nœud bascule vers un seul et même nœud, cela se voit généralement ici
- State : santé du nœud. Uniquement disponible lorsque la matrice est suffisamment saine pour être inventoriée par une source de données
- Model : nom de modèle du nœud
- Version : nom de version du périphérique.
- Numéro de série – numéro de série du nœud
- Mémoire – mémoire de base 2 si disponible
- Utilisation : généralement un nombre d'utilisation du CPU ou, dans le cas de NetApp ONTAP, un indice de stress du contrôleur. L'utilisation n'est pas disponible pour le moment pour NetApp E-Series
- IOPS – chiffre représentant les IOPS pilotées par l'hôte sur ce contrôleur. Idéalement, les données proviennent directement de la baie, s'ils ne sont pas disponibles, elles sont calculées en additionnant tous les IOPS pour les volumes appartenant exclusivement à ce nœud.
- Latence : chiffre représentant le temps de réponse ou de latence de l'hôte type sur ce contrôleur. Idéalement, il sera calculé en effectuant un calcul pondéré par IOPS à partir des volumes qui appartiennent exclusivement à ce nœud.
- Débit : chiffre représentant le débit piloté par l'hôte sur ce contrôleur. Idéalement, les données proviennent directement de la baie, s'ils ne sont pas disponibles, elles sont calculées en additionnant tout le débit pour les volumes appartenant exclusivement à ce nœud.

- Processeurs – nombre de processeurs

De formation

- L'adresse IP de chaque contrôleur de la baie
- Port requis 2463

Configuration

Champ	Description
Liste des adresses IP de contrôleur de matrice SANtricity séparées par une virgule	Adresses IP et/ou noms de domaine complets pour les contrôleurs de matrice

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	La valeur par défaut est 30 minutes
Intervalle d'interrogation des performances jusqu'à 3600 secondes	La valeur par défaut est 300 secondes

Dépannage

Vous trouverez des informations supplémentaires sur ce collecteur de données sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données REST NetApp E-Series

Le collecteur de données REST NetApp E-Series collecte les données d'inventaire et de performance. Le collecteur prend en charge le micrologiciel 7.x+ en utilisant les mêmes configurations et en signalant les mêmes données. Le collecteur REST surveille l'état de cryptage des pools de stockage ainsi que l'état de cryptage des disques et volumes associés. Il fournit également l'utilisation du CPU du nœud de stockage comme compteurs de performances, une fonctionnalité non fournie dans le collecteur SANtricity E-Series existant.

Terminologie

Cloud Insight acquiert les informations d'inventaire suivantes à partir des baies NetApp E-Series, à l'aide du protocole REST. Pour chaque type d'actif acquis, la terminologie la plus utilisée pour ce bien est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Disque	Disque
Groupe de volumes	Groupe de disques
Baie de stockage	Stockage
Contrôleur	Nœud de stockage

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Groupe de volumes	Pool de stockage
Volumétrie	Volumétrie

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

- L'adresse IP de chaque contrôleur de la baie
- Ce collecteur ne prend en charge que les baies de modèle E-Series dotées de **fonctionnalités d'API REST natives**. L'entreprise E-Series expédie une distribution d'API REST hors baie et installable pour les baies E-Series plus anciennes : ce collecteur ne prend pas en charge ce scénario. Les utilisateurs disposant de baies plus anciennes doivent continuer à utiliser le "API E-Series SANtricity"collecteur Data Infrastructure Insights.
- Le champ « adresses IP des contrôleurs E-Series » prend en charge une chaîne de 2 noms IP/hôtes délimitée par des virgules ; le collecteur essaiera intelligemment la deuxième adresse IP/nom d'hôte si la première est inaccessible.
- Port HTTPS : la valeur par défaut est 8443.

Configuration

Champ	Description
Adresses IP du contrôleur E-Series	Adresses IP séparées par des virgules et/ou noms de domaine complets pour les contrôleurs de baie

Configuration avancée

Champ	Description
Intervalle d'interrogation des stocks (min)	La valeur par défaut est 30 minutes
Intervalle d'interrogation des performances jusqu'à 3600 secondes	La valeur par défaut est 300 secondes

Terminologie E-Series (page d'accueil)

Les termes suivants s'appliquent aux objets ou aux références que vous trouverez sur les pages d'accueil des ressources NetApp E-Series. Un grand nombre de ces termes s'appliquent également à d'autres collecteurs de données.

Stockage

- Modèle : nom de modèle du périphérique.
- Fournisseur : même nom de fournisseur que vous pouvez voir si vous configurez une nouvelle source de données
- Numéro de série – le numéro de série de la baie. Sur les systèmes de stockage en cluster comme NetApp clustered Data ONTAP, ce numéro de série peut être moins utile que les numéros de série individuels de nœuds de stockage

- IP : il s'agit généralement des adresses IP ou des noms d'hôte configurés dans la source de données
- Version du microcode : micrologiciel
- Capacité brute : somme de base 2 de tous les disques physiques du système, quel que soit leur rôle
- Latence : représentation des charges de travail côté hôte, à la fois en lecture et en écriture. Idéalement, les informations sur l'infrastructure de données génèrent directement cette valeur, mais ce n'est souvent pas le cas. À la place de la baie qui propose cela, Data Infrastructure Insights effectue généralement un calcul pondéré en IOPS à partir des statistiques des volumes individuels.
- Débit : débit de la baie hôte total. Idéalement situé directement à partir de la baie, Data Infrastructure Insights additionne le débit des volumes pour tirer parti de cette valeur en cas d'indisponibilité
- Gestion – il peut contenir un lien hypertexte pour l'interface de gestion du périphérique. Créé par programmation par la source de données Data Infrastructure Insights dans le cadre du reporting d'inventaire

Pool de stockage

- Stockage : sur quelle baie de stockage ce pool vit. Obligatoire
- Type – valeur descriptive d'une liste de possibilités énumérées. Le plus souvent, il s'agit de « provisionnement fin » ou de « groupe RAID ».
- Node – si l'architecture de cette matrice 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 d'accueil
- Utilise Flash Pool – valeur Oui/non
- Redondance : niveau RAID ou schéma de protection. E-Series signale « RAID 7 » pour les pools DDP
- Capacité : les valeurs indiquées ici sont les valeurs logiques utilisées, la capacité utilisable et la capacité totale logique, ainsi que le pourcentage utilisé sur ces valeurs. Cette valeur inclut la capacité de « conservation » des baies E-Series, ce qui se traduit par des chiffres et par un pourcentage supérieur à ce que peut afficher la propre interface utilisateur de la gamme E-Series
- Capacité surdédiée : si grâce aux 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, le pourcentage est supérieur à 0 % dans ce cas.
- Snapshot : les capacités des copies Snapshot utilisées et totales, si l'architecture des pools de stockage consacre une partie de sa capacité à la segmentation uniquement des snapshots
- Utilisation : pourcentage indiquant le pourcentage le plus élevé d'occupation du disque de tout disque contribuant à la capacité de ce pool de stockage. L'utilisation du disque n'est pas forcément synonyme de performances de la baie. L'utilisation peut être élevée en raison des reconstructions des disques et des activités de déduplication, etc. En l'absence de charges de travail pilotées par l'hôte. De plus, les implémentations de réplication de nombreuses baies peuvent conduire à l'utilisation du disque sans s'afficher en tant que charge de travail du volume.
- IOPS : somme des IOPS de tous les disques qui fournissent la capacité à ce pool de stockage. Si les IOPS du disque ne sont pas disponibles sur une plateforme donnée, cette valeur provient de la somme des IOPS du volume pour tous les volumes présents sur ce pool de stockage
- Débit : somme du débit de tous les disques qui fournissent la capacité à ce pool de stockage. Si le débit des disques n'est pas disponible sur une plateforme donnée, cette valeur provient de la somme des volumes au sein de tous les volumes situés sur ce pool de stockage

Nœud de stockage

- Stockage : de quelle baie de stockage ce nœud fait partie. Obligatoire

- Partenaire HAUTE DISPONIBILITÉ : sur les plateformes où un nœud bascule vers un seul et même nœud, cela se voit généralement ici
- State : santé du nœud. Uniquement disponible lorsque la matrice est suffisamment saine pour être inventoriée par une source de données
- Model : nom de modèle du nœud
- Version : nom de version du périphérique.
- Numéro de série – numéro de série du nœud
- Mémoire – mémoire de base 2 si disponible
- Utilisation : généralement un nombre d'utilisation du CPU ou, dans le cas de NetApp ONTAP, un indice de stress du contrôleur. L'utilisation n'est pas disponible pour le moment pour NetApp E-Series
- IOPS – chiffre représentant les IOPS pilotées par l'hôte sur ce contrôleur. Idéalement, les données proviennent directement de la baie, s'ils ne sont pas disponibles, elles sont calculées en additionnant tous les IOPS pour les volumes appartenant exclusivement à ce nœud.
- Latence : chiffre représentant le temps de réponse ou de latence de l'hôte type sur ce contrôleur. Idéalement, il sera calculé en effectuant un calcul pondéré par IOPS à partir des volumes qui appartiennent exclusivement à ce nœud.
- Débit : chiffre représentant le débit piloté par l'hôte sur ce contrôleur. Idéalement, les données proviennent directement de la baie, s'ils ne sont pas disponibles, elles sont calculées en additionnant tout le débit pour les volumes appartenant exclusivement à ce nœud.
- Processeurs – nombre de processeurs

Dépannage

Vous trouverez des informations supplémentaires sur ce collecteur de données sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

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 ne s'acquiert qu'auprès du serveur de gestion **NetApp HCI**. Pour collecter des données du système de stockage, vous devez également configurer le "NetApp SolidFire"collecteur de données.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir de ce collecteur de données. Pour chaque type d'actif acquis, la terminologie la plus utilisée pour l'actif est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Disque virtuel	Disque
Hôte	Hôte
Ordinateur virtuel	Ordinateur virtuel

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Magasin de données	Magasin de données
LUN	Volumétrie
Port Fibre Channel	Port

Il s'agit uniquement de mappages terminologiques communs et il est possible qu'ils ne représentent pas tous les cas pour ce collecteur de données.

De formation

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.
- Configuration requise pour le port : http-80 https-443
- Validation de l'accès :
  - Connectez-vous au serveur de gestion NetApp HCI à l'aide du nom d'utilisateur et du mot de passe ci-dessus
  - Vérifiez que le SDK est activé : telnet <vc_ip> 443

Configuration et connexion

Champ	Description
Nom	Nom unique du 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 (nœud M)	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 de vCenter
Mot de passe vCenter	Mot de passe pour vCenter

Configuration avancée

Dans l'écran de configuration avancée, cochez la case **VM Performance** pour collecter les données de performances. La collecte des stocks est activée par défaut. Les champs suivants peuvent être configurés :

Champ	Description
Intervalle d'interrogation des stocks (min)	Le deafult est 20
Filtrer les VM par	Sélectionnez CLUSTER, DATA CENTER ou HÔTE ESX
Choisissez 'exclure' ou 'inclure' pour spécifier une liste	Indiquez s'il faut inclure ou exclure des VM
Filtrer la liste des périphériques	Liste des machines virtuelles à filtrer (séparées par des virgules ou séparées par un point-virgule si la valeur est utilisée) pour le filtrage par ESX_HOST, CLUSTER et DATACENTER uniquement
Intervalle d'interrogation des performances (s)	La valeur par défaut est 300

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	**Essayer :**
Erreur : la liste à inclure pour filtrer les machines virtuelles ne peut pas être vide	Si l'option inclure la liste est sélectionnée, veuillez indiquer des noms de datacenter, de cluster ou d'hôte valides pour filtrer les VM
Erreur : échec de l'instanciation d'une connexion à VirtualCenter sur IP	Solutions possibles : * Vérifiez les informations d'identification et l'adresse IP saisies. * Essayez de communiquer avec Virtual Center à l'aide de Infrastructure client. * Essayez de communiquer avec Virtual Center à l'aide du navigateur d'objets gérés (par exemple, MOB).
Erreur : VirtualCenter at IP possède un certificat non conforme requis par JVM	Solutions possibles: * Recommandé: Re-générer le certificat pour Virtual Center en utilisant plus fort (p. ex. 1024 bits) clé RSA. * Non recommandé : modifiez la configuration de la JVM java.security pour utiliser la contrainte jdk.certpath.disabedAlgorithms pour permettre la clé RSA 512 bits. Voir les notes de version de la mise à jour 40 du JDK 7 à l’adresse "http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html"

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données des baies 100 % Flash NetApp SolidFire

Le collecteur de données de la baie 100 % Flash NetApp SolidFire 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 sur laquelle réside le collecteur de données doit pouvoir établir des connexions HTTPS vers le port TCP 443 sur l'adresse IP de gestion du cluster SolidFire. Le collecteur de données doit disposer d'identifiants capables d'effectuer des requêtes d'API REST sur le cluster SolidFire.

Terminologie

Les informations d'inventaire suivantes sont recueillies auprès du collecteur de données de la baie 100 % Flash NetApp SolidFire. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Lecteur	Disque
Cluster	Stockage
Nœud	Nœud de stockage
Volumétrie	Volumétrie
Port Fibre Channel	Port
Groupe d'accès de volume, affectation de LUN	Carte de volume
Session iSCSI	Masque de volume

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

Les conditions 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
- Orifice 443

Configuration

Champ	Description
Adresse IP virtuelle de gestion (MVIP)	Adresse IP virtuelle de gestion 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 des stocks (min)	La valeur par défaut est 20 minutes
Intervalle d'interrogation des performances (s)	La valeur par défaut est 300 secondes

Dépannage

Lorsque SolidFire signale une erreur, elle s'affiche dans les informations d'infrastructure de données comme suit :

Un message d'erreur a été reçu d'un périphérique SolidFire lors de la tentative de récupération des données. L'appel était <method> (<parameterString>). Le message d'erreur de l'appareil était (consultez le manuel de l'appareil) : <message>

Où ?

- La <méthode> est une méthode HTTP, COMME GET ou PUT.
- Le <parameterString> est une liste de paramètres séparés par des virgules qui ont été inclus dans l'appel REST.
- Le <message> correspond au périphérique renvoyé comme message d'erreur.

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données NetApp StorageGRID

Le collecteur de données NetApp StorageGRID prend en charge l'inventaire et la collecte des performances à partir des configurations StorageGRID.

StorageGRID est mesuré en To brut différent du taux unitaire géré. Toutes les 40 To de capacité StorageGRID non formatée sont facturés comme 1 "Unité gérée (UM)".

Terminologie

Les informations d'inventaire suivantes sont acquises depuis le collecteur NetApp StorageGRID. Pour chaque type d'actif acquis, la terminologie la plus utilisée pour ce bien est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
StorageGRID	Stockage
Nœud	Nœud
Locataire	Pool de stockage
Godet	Volume interne

De formation

La configuration de cette source de données est requise pour :

- Adresse IP de l'hôte StorageGRID
- Nom d'utilisateur et mot de passe pour un utilisateur auquel les rôles de requête métrique et d'accès au locataire ont été attribués
- Orifice 443

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 des stocks (min)	La valeur par défaut est 60 minutes
Intervalle d'interrogation des performances (s)	La valeur par défaut est 900 secondes

Authentification unique (SSO)

Les "StorageGRID"versions de micrologiciel ont les versions d'API correspondantes ; l'API 3.0 et les versions plus récentes prennent en charge la connexion SSO (Single Sign-on).

Version du micrologiciel	Version API	Prise en charge d'un SSO
11,1	2	Non
11,2	3,0	Oui
11,5	3,3	Oui

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données Nutanix NX

Data Infrastructure Insights utilise le collecteur de données Nutanix pour découvrir les données d'inventaire et de performance des systèmes de stockage Nutanix NX.

Terminologie

Les informations d'inventaire suivantes sont acquises par le collecteur de données Nutanix. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Pool de stockage	Pool de stockage
Conteneur Nutanix	Volume interne
Conteneur Nutanix	Partage de fichiers
Partage NFS	Partagez

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

- L'adresse IP des services de données externes pour le cluster
- Nom d'utilisateur et mot de passe en lecture seule, sauf si des groupes_volumes sont utilisés, auquel cas, le nom d'utilisateur et le mot de passe administrateur sont requis
- Port requis : HTTPS 443

Configuration

Champ	Description
Adresse IP externe prismes	L'adresse IP des services de données externes pour le cluster
Nom d'utilisateur	Nom d'utilisateur du compte Admin
Mot de passe	Mot de passe du compte admin

Configuration avancée

Champ	Description
Port TCP	Port TCP utilisé pour la connexion à la baie Nutanix. La valeur par défaut est 9440.
Intervalle d'interrogation des stocks (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 60 minutes.
Intervalle(s) d'interrogation de performance	Intervalle entre les sondages de performances. La valeur par défaut est 300 secondes.

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données Oracle ZFS Storage Appliance

Data Infrastructure Insights utilise le collecteur de données Oracle ZFS Storage Appliance pour collecter les données d'inventaire et de performances.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire avec le collecteur de données Oracle ZFS. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Disque (SSD)	Disque
Cluster	Stockage
Contrôleur	Nœud de stockage
LUN	Volumétrie
Mappage de LUN	Carte de volume
Initiateur,cible	Masque de volume
Partagez	Volume interne

Remarque : il s'agit uniquement de mappages terminologiques courants et peuvent ne pas représenter tous les cas pour cette source de données.

De formation

- Noms d'hôte pour le ZFS Controller-1 et le ZFS Controller-2
- Nom d'utilisateur et mot de passe administrateur
- Port requis : 215 HTTP/HTTPS

Mesures de performances requises

Les appliances Oracle ZFS offrent aux administrateurs de stockage une flexibilité considérable pour la capture des statistiques de performances. Data Infrastructure Insights attend de vous que *chaque* contrôleur d'une paire haute disponibilité soit configuré pour capturer les mesures suivantes :

- smb2.ops[part]
- nfs3.ops[part]
- nfs4.ops[part]
- nfs4-1.ops[part]

Si le contrôleur n'est pas en mesure de capturer l'un ou l'autre de ces éléments, les informations sur l'infrastructure de données n'auront probablement pas, ou ne sous-auront pas, la charge de travail sur les « volumes internes ».

Configuration

Champ	Description
Nom d’hôte ZFS Controller-1	Nom d’hôte du contrôleur de stockage 1
Nom d’hôte ZFS Controller-2	Nom d’hôte du contrôleur de stockage 2
Nom d’utilisateur	Nom d’utilisateur du compte d’administrateur du système de stockage
Mot de passe	Mot de passe du 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 ce champ est vide, utilisez le port par défaut dans le champ Type de connexion, sinon entrez le port de connexion à utiliser
Intervalle d’interrogation d’inventaire	La valeur par défaut est 60 secondes
Intervalle d’interrogation des performances (s)	La valeur par défaut est 300.

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
« Identifiants de connexion non valides »	Valider le compte utilisateur et le mot de passe ZFS
« Échec de la demande avec l’état 404 https://…..:215/api/access/v1"	Votre baie ZFS est peut-être trop ancienne pour prendre en charge l’API REST. AK 2013.1.3.0 a été la première version de ZFS compatible avec l’API REST, et toutes les appliances ZFS ne peuvent pas être mises à niveau vers celle-ci.
"Erreur de configuration" avec le message d’erreur "le service REST est désactivé"	Vérifiez que le service REST est activé sur ce périphérique.

Problème :	Essayer :
"Erreur de configuration" avec message d'erreur "utilisateur non autorisé pour la commande"	Cette erreur est probablement due à certains rôles (par exemple, 'Advanced_analytics') qui ne sont pas inclus pour l'utilisateur configuré. L'application de la portée analytique pour l'utilisateur avec un rôle en lecture seule peut supprimer l'erreur. Voici la procédure à suivre : 1. Sur le système ZFS, à partir de l'écran Configuration → utilisateurs, déplacez votre souris sur le rôle et double-cliquez pour autoriser la modification 2. Sélectionnez « analyse » dans le menu déroulant objectif. Une liste des propriétés possibles s'affiche. 3. Cliquez sur la case la plus en haut pour sélectionner les trois propriétés. 4. Cliquez sur le bouton Ajouter à droite. 5. Cliquez sur le bouton appliquer en haut à droite de la fenêtre contextuelle. La fenêtre contextuelle se ferme.

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données FlashArray de Pure Storage

Data Infrastructure Insights utilise le collecteur de données Pure Storage FlashArray pour collecter les données d'inventaire et de performance.

Terminologie

Pour chaque type de ressource acquise par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Disque (SSD)	Disque
Baie	Stockage
Contrôleur	Nœud de stockage
Volumétrie	Volumétrie
Mappage de LUN	Carte de volume
Initiateur,cible	Masque de volume

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

- Adresse IP du système de stockage
- Nom d'utilisateur et mot de passe du compte Administrateur du système Pure Storage.
- Port requis : 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 du compte admin privilégié	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 ce champ est vide, utilisez le port par défaut dans le champ Type de connexion, sinon entrez le port de connexion à utiliser
Intervalle d'interrogation des stocks (min)	La valeur par défaut est 60 minutes
Intervalle d'interrogation des performances (s)	La valeur par défaut est 300

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
"Informations d'identification non valides" avec les messages d'erreur "la stratégie n'autorise pas" ou "vous n'êtes pas autorisé"	Valider le compte utilisateur et le mot de passe Pure via l'interface http Pure

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données Red Hat Virtualization

Data Infrastructure Insights utilise le collecteur de données Red Hat Virtualization pour collecter les données d'inventaire des charges de travail Linux et Microsoft Windows virtualisées.

Terminologie

Pour chaque type de ressource acquise par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Disque	Disque virtuel
Hôte	Hôte
Ordinateur virtuel	Ordinateur virtuel
Domaine de stockage	Datastore
Unité logique	LUN

Remarque : il s'agit uniquement de mappages terminologiques communs et peuvent ne pas représenter tous les cas pour ce collecteur de données.

De formation

- 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 du compte admin privilégié	Mot de passe

Configuration avancée

Champ	Description
Port de communication HTTPS	Port utilisé pour la communication HTTPS vers RHEV
Intervalle d'interrogation des stocks (min)	La valeur par défaut est 20 minutes.

Dépannage

Vous trouverez des informations supplémentaires sur ce Data Collector sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Data Collector 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 à partir du collecteur de données Rubrik. Pour chaque type de ressource acquis par Data Infrastructure Insights, la terminologie la plus courante est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Cluster	Stockage, pool de stockage
Nœud	Nœud de stockage
Disque	Disque

Remarque : il s'agit uniquement de mappages terminologiques courants et peuvent ne pas représenter tous les cas pour cette source de données.

De formation

Les éléments suivants sont nécessaires pour configurer ce collecteur de données :

- L'unité d'acquisition Data Infrastructure Insights initie 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 pour le 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 devez disposer d'un compte de service, d'un secret et d'un ID d'organisation
- Port requis : HTTPS 443

Configuration

Champ	Description
IP	Adresse IP du cluster Rubrik
Nom d'utilisateur / Compte de service	Nom d'utilisateur du 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 des stocks (min)	La valeur par défaut est 60
Intervalle d'interrogation des performances (s)	La valeur par défaut est 300

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
J'ai reçu un message indiquant que plusieurs stockages sont 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 supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Configuration du collecteur de données VMware vSphere

Le collecteur de données pour VMware vSphere collecte des informations sur les performances et la configuration de l'hôte VMware ESXi et de l'hôte VM invité, et requiert une Privileges en lecture seule sur tous les objets de vSphere. Depuis août 2024, le collecteur vSphere intègre en outre des messages de journalisation provenant des environnements vSphere et des mesures spécifiques à VMware. Notez que Data Infrastructure Insights ne peut récupérer les informations des journaux VMware que dans les environnements vSphere 8.0.1 ou supérieur. De même, les mesures propres au fournisseur ne sont prises en charge que pour les environnements vSphere 7+. Par conséquent, vous pouvez désactiver la case journaux et/ou mesures propres au fournisseur sur un collecteur donné s'il est pointé vers une ancienne instance vSphere.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir du collecteur de données VMware vSphere. Pour chaque type d'actif acquis, la terminologie la plus utilisée pour l'actif est indiquée. Lors de l'affichage ou du dépannage de ce collecteur de données, gardez la terminologie suivante à l'esprit :

Terme du fournisseur/modèle	Terme informations exploitables sur l'infrastructure de données
Disque virtuel	Disque
Hôte	Hôte
Ordinateur virtuel	Ordinateur virtuel
Magasin de données	Magasin de données
LUN	Volumétrie
Port Fibre Channel	Port

Il s'agit uniquement de mappages terminologiques communs et il est possible qu'ils ne représentent pas tous les cas pour ce collecteur de données.

De formation

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 avons besoin de privilèges en lecture seule pour tous les objets du Virtual Center.
- Accès au SDK sur le serveur Virtual Center – normalement déjà configuré.
- Configuration requise pour le port : http-80 https-443
- Validation de l'accès :
  - Connectez-vous au client Virtual Center à l'aide du nom d'utilisateur et du mot de passe ci-dessus
  - Vérifiez que le SDK est activé : telnet <vc_ip> 443

Configuration et connexion

Champ	Description
Nom	Nom unique du collecteur de données
Unité d'acquisition	Nom de l'unité d'acquisition

Configuration

Champ	Description
Adresse IP du centre virtuel	Adresse IP du Virtual Center
Nom d'utilisateur	Nom d'utilisateur utilisé pour accéder au Virtual Center
Mot de passe	Mot de passe utilisé pour accéder au Virtual Center

Configuration avancée

Dans l'écran de configuration avancée, cochez la case **VM Performance** pour collecter les données de performances. La collecte des stocks est activée par défaut. Les champs suivants peuvent être configurés :

Champ	Description
Intervalle d'interrogation des stocks (min)	La valeur par défaut est 20
Filtrer les VM	Sélectionnez CLUSTER, DATA CENTER ou HÔTE ESX
Choisissez 'exclure' ou 'inclure' pour spécifier une liste	Créer une liste de filtres (CLUSTER, DATA CENTER 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 périphériques…	Cette liste doit contenir des correspondances de chaînes exactes. Si vous avez l'intention de filtrer par ESX_HOST, vous devez créer une liste séparée par des virgules des « noms » exacts de vos hôtes ESX, comme indiqué dans Data Infrastructure Insights et vSphere. Ces « noms » peuvent être des adresses IP, des noms d'hôte simples ou des noms de domaine complets (FQDN). Ils sont déterminés par la façon dont ces hôtes ont été nommés lorsqu'ils ont été ajoutés à vSphere à l'origine. 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 prédéfinit le nom du cluster vSphere avec le nom du data Center vSphere et une barre oblique. « DC1/clusterA » est le nom du cluster. Data Infrastructure Insights indique un hyperviseur dans le cluster a au sein du data Center DC1.
Intervalle d'interrogation des performances (s)	La valeur par défaut est 300

Mappage des balises VMware avec les annotations Data Infrastructure Insights

Le collecteur de données VMware vous permet de remplir 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 remplit toujours les annotations de type texte portant le même nom et fera une « meilleure tentative » pour remplir les annotations d'autres types (nombre, booléen, etc.). Si votre annotation est de type différent et que le collecteur de données ne parvient pas à la remplir, 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 sont pas sensibles à la casse. Par conséquent, si vous créez une annotation nommée « PROPRIÉTAIRE » dans Data Infrastructure Insights et des balises nommées « PROPRIÉTAIRE », « propriétaire » et « propriétaire » dans VMware, toutes ces variations de « propriétaire » sont associées à l'annotation « PROPRIÉTAIRE » DE Cloud Insight.

Gardez à l'esprit les éléments suivants :

- Informations sur l'infrastructure de données ne publie actuellement que automatiquement les informations de support pour les périphériques NetApp.
- Étant donné que ces informations de support 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 de l'annotation, la valeur est automatiquement redéfinie lorsque Data Infrastructure Insights met à jour les annotations, ce qui fait une fois par jour.

Dépannage

Certaines choses à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème :	Essayer :
Erreur : la liste à inclure pour filtrer les machines virtuelles ne peut pas être vide	Si l'option inclure la liste est sélectionnée, veuillez indiquer des noms de datacenter, de cluster ou d'hôte valides pour filtrer les VM
Erreur : échec de l'instanciation d'une connexion à VirtualCenter sur IP	Solutions possibles : * Vérifiez 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 at IP possède un certificat non conforme requis par JVM	Solutions possibles: * Recommandé: Re-générer le certificat pour Virtual Center en utilisant plus fort (p. ex. 1024 bits) clé RSA. * Non recommandé : modifiez la configuration de la JVM java.security pour utiliser la contrainte jdk.certpath.disabedAlgorithms pour permettre la clé RSA 512 bits. Voir "Notes de version de la mise à jour 40 du JDK 7".
Le message suivant s'affiche : « le package VMware Logs n'est pas pris en charge sur VMware sous la version 8.0.1 »	La collecte des journaux n'est pas prise en charge sur les versions VMware antérieures à la version 8.0.1. Mettez à niveau votre infrastructure VI Center vers la version 8.0.1 ou ultérieure si vous souhaitez utiliser la fonction Collections de journaux dans Data Infrastructure Insights. Pour plus d'informations, voir "Article de la base de connaissances".

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Data Collector Reference - Services

Collecte des données de nœud

Data Infrastructure Insights collecte les metrics à partir du nœud sur lequel vous installez un agent.

Installation

1. Dans **observabilité > Collectors**, choisissez un système d'exploitation/une plate-forme. Notez que l'installation d'un collecteur de données d'intégration (Kubernetes, Docker, Apache, etc.) configure également la collecte des données du nœud.
2. Suivez les instructions pour configurer l'agent. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés sous forme de metrics de nœud :

Objet :	Identifiants :	Attributs :	Points de données :
Système de fichiers de nœuds	Type de chemin d'accès de périphérique UUID de nœud	Nœud IP nœud Nom nœud mode OS	Inodes libres inodes libres nombre total d'inodes utilisé Total utilisé
Disque de nœud	Disque UUID de nœud	Nom de nœud IP de nœud OS	Temps d'E/S nombre total d'IOPS en cours lecture octets (par seconde) temps de lecture durée totale des lectures (par seconde) temps d'E/S pondéré durée totale des écritures (par seconde) temps d'écriture total des écritures (par seconde) durée actuelle de la file d'attente des disques temps d'écriture temps d'E/S de lecture
Processeur des nœuds	CPU UUID de nœud	Nom de nœud IP de nœud OS	Utilisation du CPU système utilisation du CPU utilisateur utilisation du CPU inactif utilisation du processeur interruption utilisation du CPU DPC utilisation du CPU

Objet :	Identifiants :	Attributs :	Points de données :
Nœud	UUID du nœud	Nom de nœud IP de nœud OS	Temps d'amorçage du noyau commutateurs de contexte du noyau (par seconde) interruption du noyau interruptions du noyau disponibles (par seconde) processus du noyau forgés (par seconde) Mémoire mémoire active mémoire active disponible mémoire totale mémoire disponible mémoire tampon mémoire cache limite mémoire cache mémoire vive comme mémoire non volatile mémoire libre mémoire haute mémoire libre mémoire haute capacité mémoire énorme taille de page mémoire énorme pages mémoire libre pages nombreuses pages mémoire libre mémoire totale mémoire faible mémoire disponible Table de pages mémoire mappée totale Mémoire partagée mémoire Bloc mémoire Bloc mémoire vive mémoire cache échange mémoire libre échange mémoire totale mémoire totale utilisée mémoire totale mémoire utilisée mémoire totale mémoire utilisée Vmalloc Bloc mémoire Vmalloc mémoire totale Vmalloc mémoire utilisée mémoire saturée mémoire filaire Retour mémoire totale mémoire mémoire Writeback mémoire mémoire tmp mémoire cache mémoire demande zéro pannes mémoire page mémoire pages mémoire Mémoire non paginée mémoire à l'origine mémoire à l'état principal mémoire à l'état de repos mémoire à la réserve mémoire à l'état normal processus à l'état

Objet :	Identifiants :	Attributs :	Points de données :
Réseau de nœuds	UUID de nœud d'interface réseau	OS de nœud Nom du nœud IP	Octets reçus octets envoyés paquets envoyés Outboud paquets rejetés erreurs Outboud paquets reçus paquets rejetés erreurs reçues paquets reçus erreurs paquets reçus paquets envoyés

Configuration

Des informations sur la configuration et le dépannage sont disponibles sur la "Configuration d'un agent" page.

Data Collector ActiveMQ

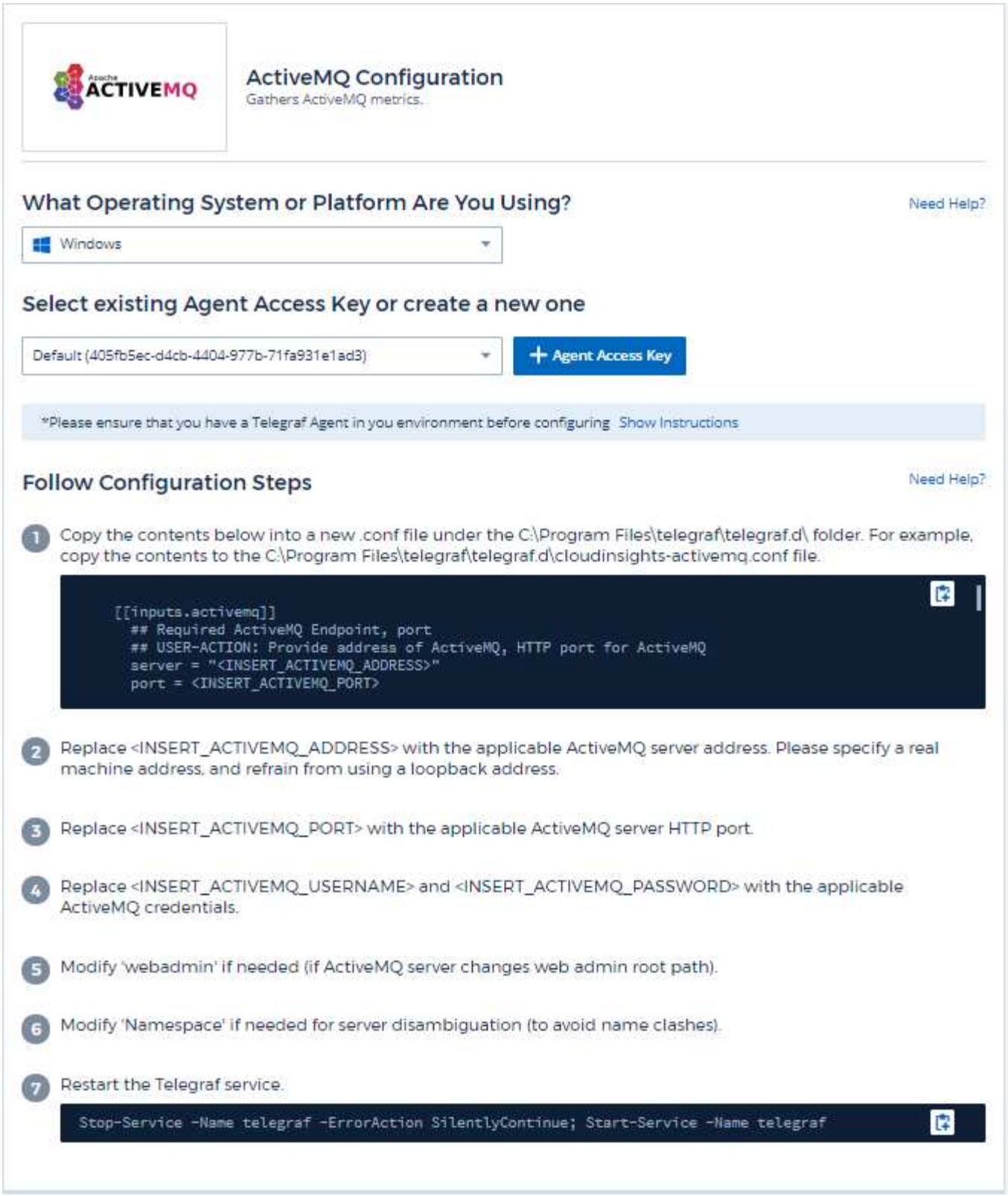
Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir d'ActiveMQ.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez ActiveMQ.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un 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 les "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 à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
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 utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans le "Documentation ActiveMQ"

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
ActiveMQ Queue	Serveur de port de file d'attente d'espace de noms	UUID de nœud Nom du nœud IP	Nombre de consommateurs - nombre de files d'attente - nombre de files 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 nœud IP nœud UUID Sélecteur de nœud d'exploitation	Nombre de files d'attente nombre de files d'attente expédiées taille de file d'attente nombre de files d'attente en attente taille de file d'attente
Thème ActiveMQ	Rubrique espace de noms du serveur de port	Nom de nœud nœud nœud IP nœud UUID de nœud OS	Nombre de consommateurs - nombre de files d'attente - taille du nombre de files d'attente

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données Apache

Ce collecteur de données permet la collecte de données à partir des serveurs Apache de votre locataire.

Conditions préalables

- Votre serveur HTTP Apache doit être configuré et en cours d'exécution
- Vous devez disposer d'autorisations sudo ou administrateur sur votre hôte agent/machine virtuelle
- En général, 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, reportez-vous à la documentation du module Apache : https://httpd.apache.org/docs/2.4/mod/mod_status.html#enable

Installation

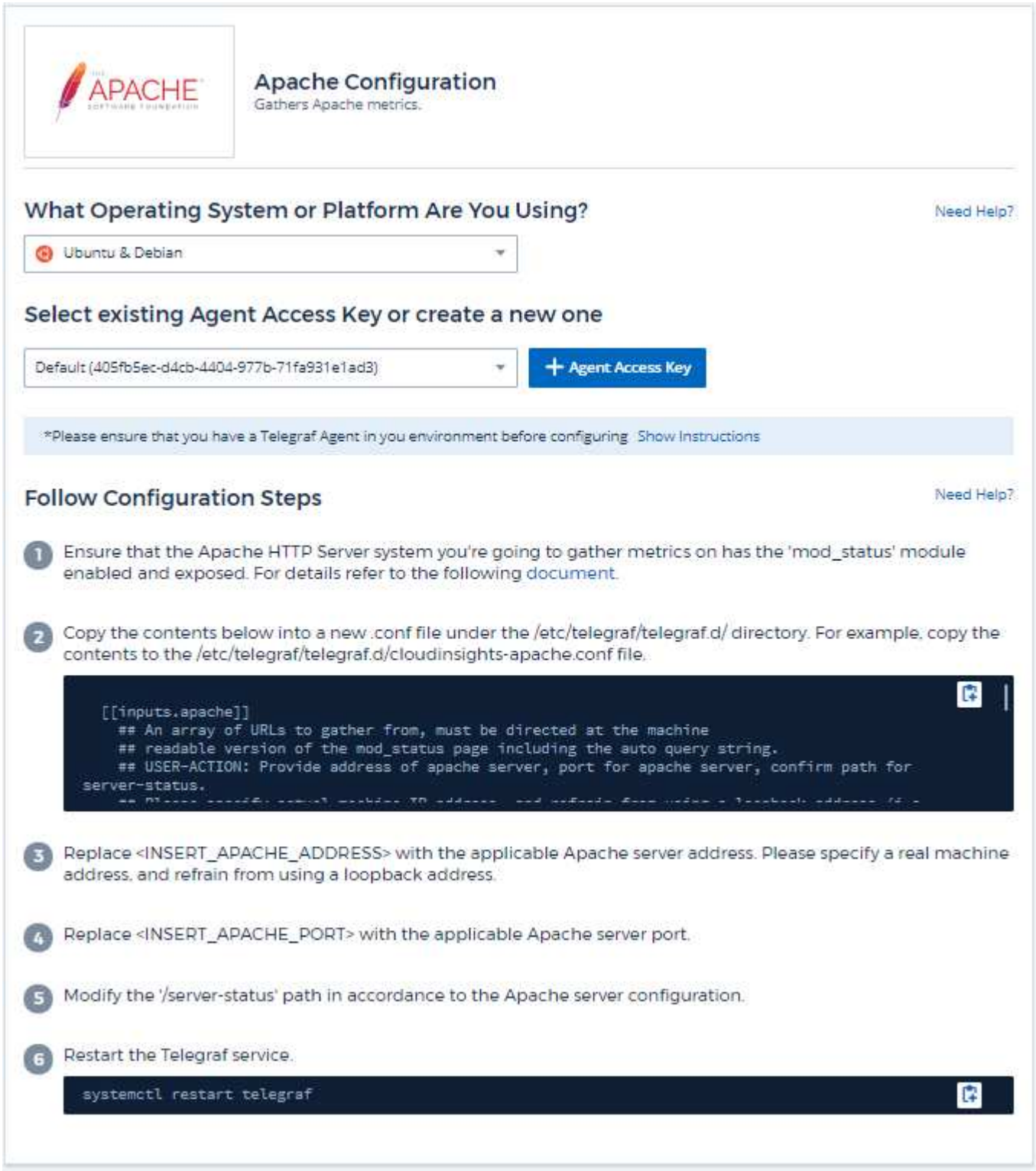
1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Apache.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un 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 les "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 à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de

données, par exemple, par OS/plate-forme.

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 utilisé pour collecter des données.



Configuration

Le plug-in Telegraf pour le serveur HTTP Apache dépend du module 'mod_status' pour être activé. Lorsque cette option est activée, le serveur HTTP d'Apache expose un noeud final HTML qui peut être affiché sur votre navigateur ou gratté pour l'extraction de l'état de toute la configuration du serveur HTTP d'Apache.

Compatibilité :

La configuration a été développée par le serveur HTTP Apache version 2.4.38.

Activation de mod_status :

L'activation et l'exposition des modules « od_status » implique deux étapes :

- Activation du module
- Exposition des stats à partir 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 annulez le commentaire des lignes suivantes :

```
LoadModule status_module modules/mod_status.so
Include conf/extra/httpd-info.conf
```

Exposition des statistiques à partir 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 que vous disposez des éléments suivants dans ce fichier de configuration (au moins, d'autres directives seront disponibles) :

```
# 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 obtenir des instructions détaillées sur le module 'mod_status', reportez-vous au "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 Nom de nœud IP Port de configuration du serveur parent génération du serveur parent la continuité du serveur de génération MPM est en cours d'arrêt	Nombre de travailleurs occupés octets par requête par seconde UC enfants système processeur enfants charge UC utilisateur CPU système CPU utilisateurs connexions asynchrones fermeture connexions asynchrones connexion asynchrones maintien actif connexions asynchrones écriture connexions durée totale par demande travailleurs inactifs moyenne de charge (1 m dernier) moyenne de charge (15 m dernier) moyenne de charge (5 m dernier) Traitement des demandes par seconde Total des accès durée totale des Ko Tableau de bord fermeture Tableau de bord des recherches DNS Tableau de bord finition Tableau de bord nettoyage automatique Tableau de bord Tableau de bord garder actif Tableau de bord Tableau de bord Ouvrir Tableau de bord lecture Tableau de bord envoi Tableau de bord démarrage Tableau de bord en attente

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données consul

Data Infrastructure Insights utilise ce collecteur de données pour recueillir des mesures auprès de Consul.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Consul.

   Si vous n'avez pas configuré un agent pour la collecte, vous êtes invité à "installez un agent"le faire sur

votre locataire.

Si un agent est déjà configuré, sélectionnez le système d'exploitation ou la plate-forme approprié et cliquez sur **Continuer**.

2. Suivez les instructions de l'écran Configuration consul pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.

Configuration

Vous trouverez des informations dans le "Documentation consul".

Objets et compteurs pour consul

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
Consul	Numéro de contrôle d'espace de noms nœud de service	Nœud IP nœud OS UUID Nom du nœud Nom du service Vérification Nom ID de service État	Avertissement de réussite critique

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données Couchbase

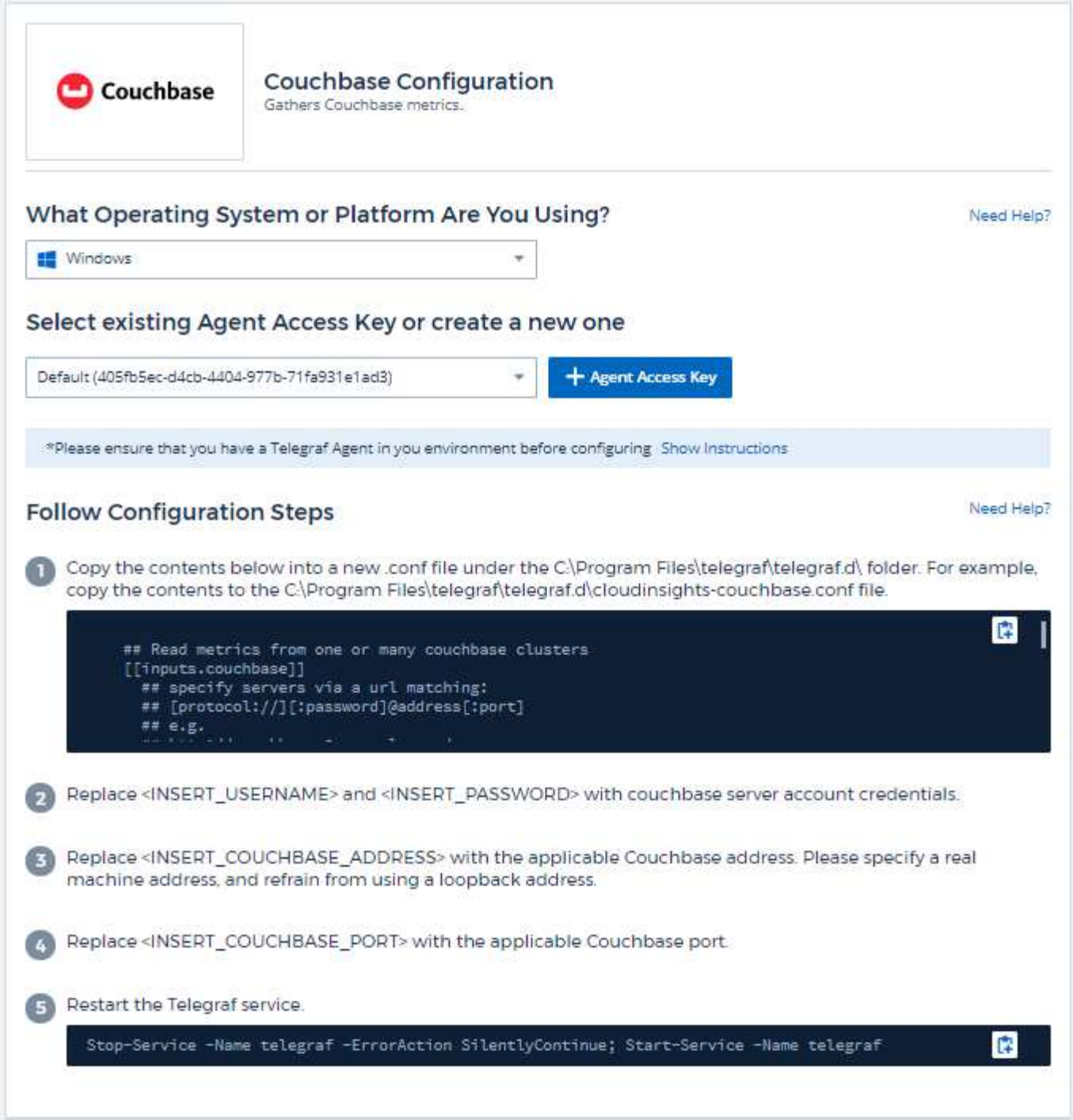
Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir de Couchbase.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Couchbase.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un 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 les "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 à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
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 utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans le "Documentation Couchbase".

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
Couchbase Node	Nom d'hôte du nœud Couchbase du cluster namespace	IP du nœud de nom de nœud	Mémoire mémoire mémoire disponible totale
Compartiment Couchbase	Cluster des compartiments d'espace de noms	IP du nœud de nom de nœud	Données utilisées Fetches Disk Used Item Count Memory Used opérations par seconde quota utilisé

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données CouchDB

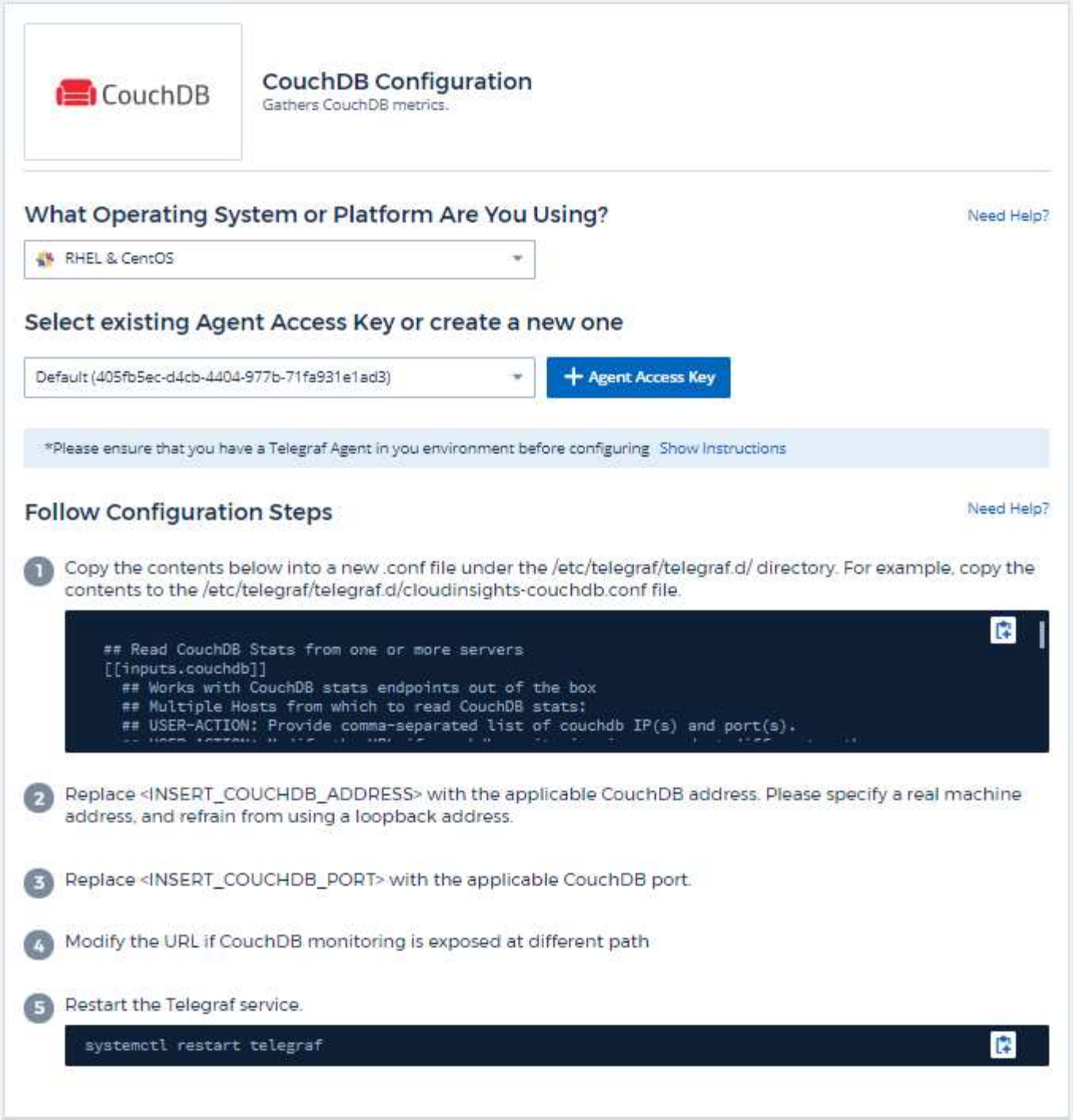
Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir de CouchDB.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez CouchDB.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un 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 les "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 à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
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 utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans le "Documentation CouchDB".

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
CouchDB	Serveur d'espace de noms	IP du nœud de nom de nœud	Cache d'authentification Hits cache d'authentification Miss base de données lit base de données écrit bases Open fichiers système d'exploitation Max temps de demande min temps de demande httpd méthodes de demande httpd Copier méthodes de demande httpd suivre méthodes de demande httpd méthodes de requête post méthodes de requête httpd mettre les 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

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données Docker

Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir de Docker.

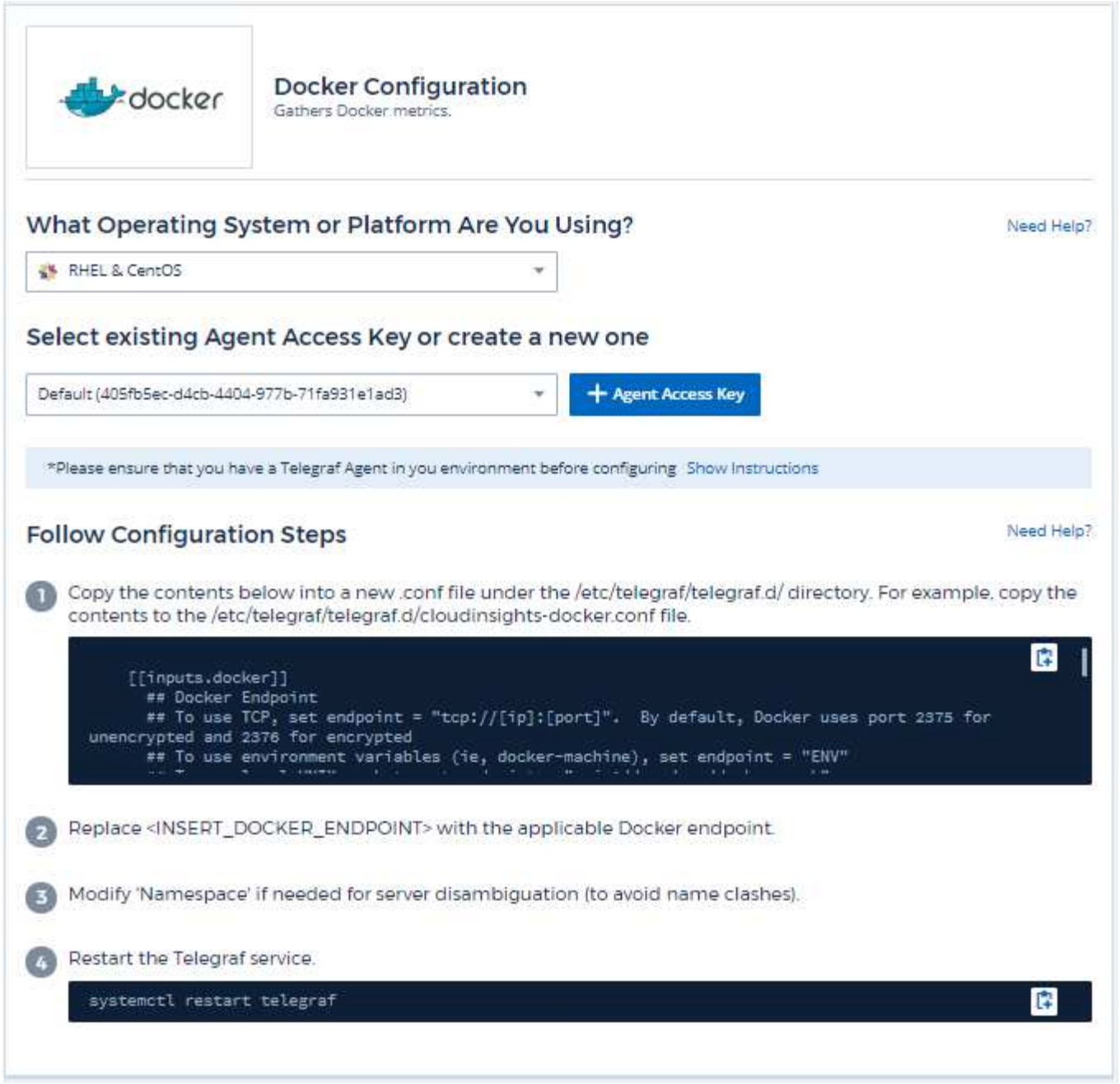
Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Docker.

   Si vous n'avez pas configuré un agent pour la collecte, vous êtes invité à "installez un agent"le faire sur votre locataire.

   Si un agent est déjà configuré, sélectionnez le système d'exploitation ou la plate-forme approprié et cliquez sur **Continuer**.

2. Suivez les instructions de l'écran de configuration de Docker pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.



Configuration

Le plug-in d'entrée Telegraf pour Docker collecte des mesures via une socket UNIX ou un noeud final TCP spécifié.

Compatibilité

La configuration a été développée à partir de la version 1.12.6 de Docker.

Configuration

Accès à Docker via un socket UNIX

Si l'agent Telegraf s'exécute sur une base sans système d'exploitation, ajoutez l'utilisateur telegraf Unix au groupe docker Unix 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 effectuant le mappage du socket dans le pod en tant que
volume, puis en le montant dans /var/run/docker.Sock. Par exemple, ajoutez
ce qui suit à PodSpec :
```

```
volumes:
...
- name: docker-sock
hostPath:
path: /var/run/docker.sock
type: File
```

Ajoutez ensuite les éléments suivants au conteneur :

```
volumeMounts:
...
- name: docker-sock
mountPath: /var/run/docker.sock
```

Notez que le programme d'installation Data Infrastructure Insights fourni pour la plateforme Kubernetes prend automatiquement en charge ce mappage.

Accès à Docker via un terminal TCP

Par défaut, Docker utilise le port 2375 pour un accès non chiffré et le port 2376 pour un accès crypté.

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
Moteur Docker	Namespace Docker Engine	Noeud Nom noeud IP noeud UUID noeud OS Kubernetes Cluster version unité Docker	Conteneurs de mémoire conteneurs conteneurs utilisés conteneurs exécution de conteneurs CPU arrêtés routines Images Listener événements descripteurs de fichiers utilisés données disponibles Total des données utilisées métadonnées disponibles métadonnées totales utilisées nombre de métadonnées utilisées nombre total de blocs de données utilisés

Objet :	Identifiants :	Attributs :	Points de données :
Conteneur Docker	Nom du conteneur de l’espace de noms moteur Docker	Hachage en conteneurs Kubernetes ports de conteneur Kubernetes nombre de redémarrage du conteneur Kubernetes résiliation du message chemin de terminaison du conteneur Kubernetes politique de message de résiliation du conteneur Kubernetes Pod délai de grâce image conteneur Statut du conteneur version Nom du nœud Kubernetes Container chemin du journal Kubernetes Docker Type Kubernetes Pod Nom du pod Kubernetes espace de noms Kubernetes UID pod UID Kubernetes Sandbox ID nœud IP UUID Docker version Kubernetes IO Config vu Kubernetes IO Source OpenShift IO SCC Kubernetes Description Kubernetes Nom d’affichage balises OpenShift Kompose modèle de pod de service modèle Hash Controller révision modèle de pod modèle de hachage création de schéma de licence schéma de création de la date de création de schéma de licence URL de schéma de schéma de licence de schéma de schéma de schéma de nom de schéma Schéma URL du schéma du fournisseur version du schéma du schéma du fournisseur version Maintainer client Pod Kubernetes StatefulSet Nom du pod tenant webconsole Architecture autorité URL source Date de création RH hôte RH distribution étendue installation Résumé de l’exécution	Mémoire active mémoire anonyme active mémoire cache de fichiers active mémoire cache limite hiérarchique mémoire inactive mémoire inactive mémoire morte mémoire mappée fichier mémoire usage maximal mémoire page défaut mémoire principale panne mémoire paginée dans la mémoire mise en mémoire mémoire affectation de mémoire mémoire taille de l’ensemble mémoire interne taille de l’ensemble de mémoire énorme mémoire active totale Mémoire anonyme mémoire totale des fichiers actifs mémoire totale mémoire cache totale inactive mémoire totale des fichiers inactifs mémoire totale des fichiers mappés mémoire totale des pages défaut mémoire totale des pages mémoire principale des pannes mémoire totale des erreurs Total des pages en mémoire Total de la mémoire paginée taille totale des ensembles résidents taille totale des ensembles résidents taille totale des ensembles de mémoire énorme Total des données des résidents Mémoire inévitable mémoire inévitable mémoire usage mémoire pourcentage Code de sortie OOM Code de sortie PID tué démarré à Streak défaillant

Objet :	Identifiants :	Attributs :	Points de données :
Les E/S de bloc de conteneur Docker	Espace de noms Container Name Device Docker Engine	Hachage en conteneurs Kubernetes ports de conteneur Kubernetes nombre de redémarrage du conteneur Kubernetes résiliation du message chemin de terminaison du conteneur Kubernetes politique de message de résiliation du conteneur Kubernetes Pod délai de grâce image conteneur Statut du conteneur version Nom du nœud Kubernetes Container chemin du journal Kubernetes Docker Type Kubernetes Pod Nom du pod Kubernetes espace de noms Kubernetes UID de pod ID de test Kubernetes nœud IP UUID de nœud UUID de conteneur Docker version Kubernetes Config vu Kubernetes Config Source OpenShift SCC Description Kubernetes Nom d'affichage balises OpenShift Schema version modèle de pod modèle de hachage de révision de contrôleur génération de modèle de hachage Kompose de schéma de service Date de création de schéma de licence Nom de schéma de licence client du fournisseur Pod Kubernetes StatefulSet Nom du pod tenant webconsole Date de création Licence Architecture du fournisseur URL source faisant autorité RH build hôte RH composant distribution Scope installation Maintainer version Résumé Désinstaller VCS Type version schéma URL Schéma URL VCS version conteneur ID	Octets de service d'E/S recursive Async octets de service d'E/S en lecture récursive Sync octets de service d'E/S récursives octets de service d'E/S en écriture récursive Write Serviced E/S récursives Recursive Read ursive Read IO Serviced Recursive Write Serviced

Objet :	Identifiants :	Attributs :	Points de données :
Réseau de conteneurs Docker	Nom du conteneur de l’espace de noms moteur Docker réseau	Image conteneur conteneur conteneur version conteneur Nom de nœud nœud IP nœud UUID nœud OS K8s Cluster version ID de conteneur	RX a déposé RX octets RX erreurs RX paquets RX paquets TX a abandonné TX octets TX erreurs TX paquets TX

Objet :	Identifiants :	Attributs :	Points de données :
Processeur du conteneur Docker	Namespace Container Name CPU Docker Engine	Hachage en conteneurs Kubernetes ports de conteneur Kubernetes nombre de redémarrage du conteneur Kubernetes nombre de messages de terminaison du conteneur Kubernetes politique de message de terminaison du conteneur Kubernetes délai de grâce période de suppression de la configuration Kubernetes Config. Vue de l'état du conteneur OpenShift SCC image conteneur conteneur version Nom du nœud Kubernetes Container Log Path Kubernetes Container name Kubernetes Docker Type Kubernetes Pod Name Kubernetes Pod espace de noms Kubernetes Pod UID Kubernetes Sandbox ID noeud IP nœud UUID nœud OS Kubernetes Cluster version Kubernetes Description Kubernetes Nom d'affichage OpenShift Tags Schema version Pod modèle Hash Controller Revision modèle Hash Pod génération Kompose Service Schema Date de création Nom de schéma de licence Schéma Vendor Customer Pod Kubernetes StatefulSet Pod Name tenant webconsole Date de création Licence Vendor Architecture autorité Source URL RH build Host RH composant distribution Scope installation Maintainer version Résumé Désinstaller VCS Ref Type version schéma URL schéma URL VCS version conteneur ID	Périodes de restriction périodes de restriction périodes de restriction durée de restriction utilisation en mode noyau utilisation en mode utilisateur pourcentage utilisation du système Total

Dépannage

Problème :	Essayer :
Après avoir suivi les instructions de la page de configuration, je ne vois pas mes metrics Docker dans Data Infrastructure Insights.	Vérifiez les journaux de l'agent Telegraf pour voir s'il signale l'erreur suivante : E! Erreur dans le plug-in [inputs.docker] : obtention de l'autorisation refusée lors de la tentative de connexion à la socket du démon Docker si c'est le cas, suivez les étapes nécessaires pour fournir l'accès de l'agent Telegraf au socket Docker Unix, comme indiqué ci-dessus.

Vous trouverez des informations supplémentaires sur la "Assistance" page.

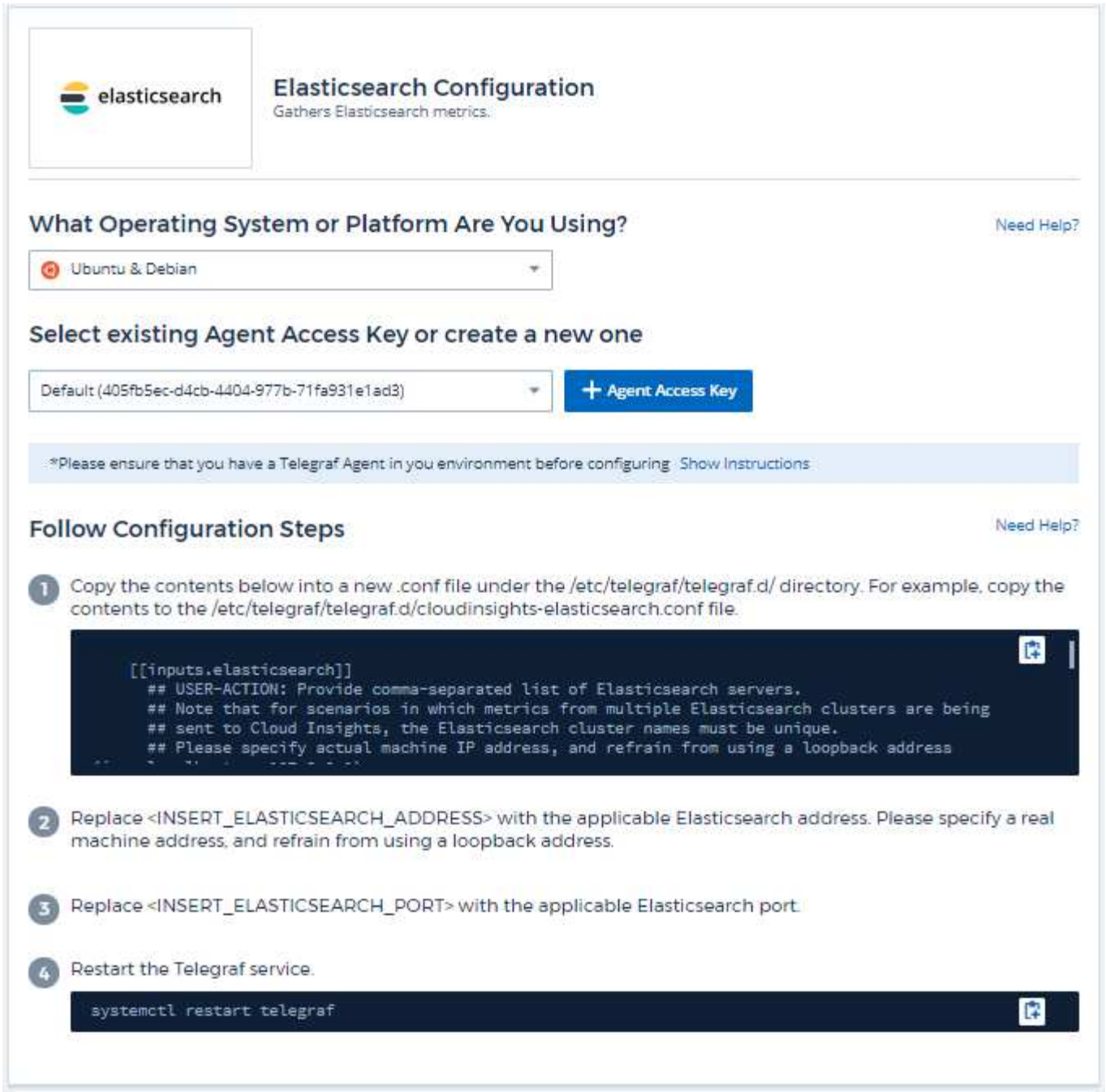
Collecteur de données Elasticsearch

Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir de Elasticsearch.

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Elasticsearch.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un 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 les "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 à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
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 utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans le "Documentation relative à Elasticsearch".

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :
Cluster Elasticsearch	Cluster de namespace	Nom de nœud IP du nœud État du cluster

Objet :	Identifiants :	Attributs :
Nœud Elasticsearch	Nom du nœud ES du cluster d'espace de noms noeud ES noeud IP noeud ES	ID de zone

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données Flink

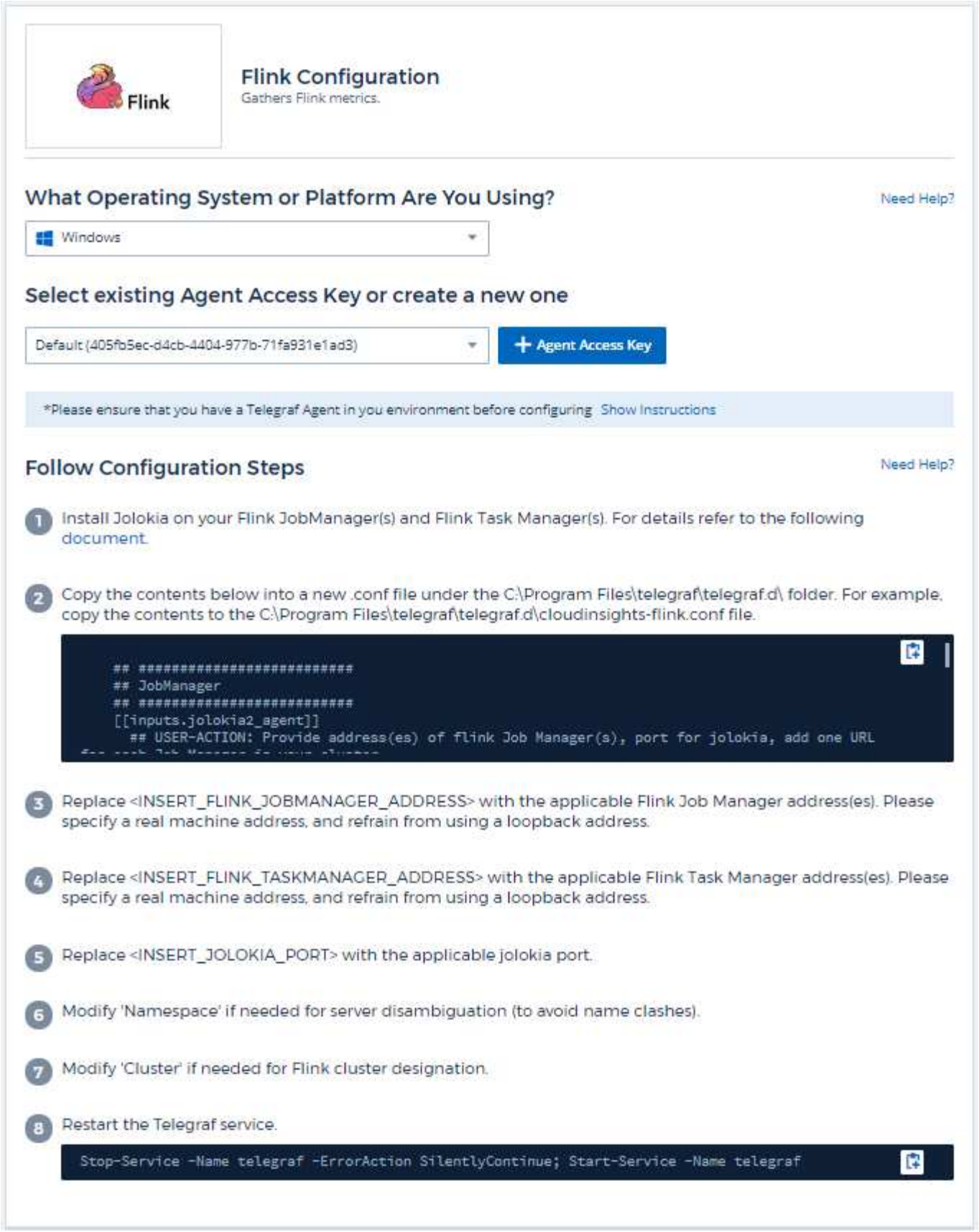
Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir de Flink.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Flink.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un 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 les "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 à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
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 utilisé pour collecter des données.



Configuration

Un déploiement de Flink complet implique les composants suivants :

JobManager : système principal de Flink. Coordonne une série de gestionnaires de tâches. Dans une configuration haute disponibilité, le système aura plusieurs JobManager. TaskManager : c'est là que les opérateurs Flink sont exécutés. Le plug-in Flink est basé sur le plug-in Jolokia de telegraf. Par exemple, pour collecter des informations de tous les composants de 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.

Configuration

Bol d'agent Jolokia

Pour tous les composants individuels, une version du fichier JAR de l'agent Jolokia doit être téléchargée. La version testée était "Agent de 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/'.

JobManager

Pour configurer JobManager de manière à 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 autre port pour Jolokia (8778). Si vous avez un IP
interne pour verrouiller Jolokia sur vous pouvez remplacer le 0.0.0.0
"tout capturer" par votre propre IP. Notez que cette adresse IP doit être
accessible à partir du plug-in telegraf.
```

Gestionnaire des tâches

Pour configurer TaskManager(s) pour exposer l'API Jolokia, vous pouvez configurer la variable d'environnement suivante sur vos nœuds, puis redémarrer TaskManager :

```
 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 autre port pour Jolokia (8778). Si vous avez un IP
interne pour verrouiller Jolokia sur vous pouvez remplacer le 0.0.0.0
"tout capturer" par votre propre IP. Notez que cette adresse IP doit être
accessible à partir du plug-in 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 disponibles réseau Total des segments de mémoire Garbage Collection PS MarkSweep nombre de déchets collecte PS MarkSweep temps Garbage Collection PS Svenge Combage Collection PS Scravenge temps démon de récupération mémoire vive mémoire vive mémoire vive mémoire vive mémoire vive mémoire vive mémoire vive maximale nombre de threads utilisés nombre de threads maximum nombre de threads Total démarré
Travail de cartouche	ID du travail du serveur d’espace de noms de cluster	Nom du nœud Nom du travail noeud IP dernier point de contrôle chemin externe heure de redémarrage	Temps d’arrêt redémarrage complet dernière alignement du point de contrôle durée du dernier point de contrôle Date du dernier point de contrôle taille nombre de points de contrôle terminés nombre de points de contrôle en cours nombre de points de contrôle en cours nombre de points de contrôle disponibilité

Objet :	Identifiants :	Attributs :	Points de données :
Gestionnaire des travaux de Flink	Serveur d’espace de noms de cluster	IP du nœud de nom de nœud	Garbage Collection PS MarkSweep nombre Garbage Collection PS MarkSweep temps Garbage Collection PS Scravenge nombre Garbage Collection PS Scravenge temps mémoire Heap mémoire vive mémoire vive mémoire vive mémoire vive saturée nombre maximum de mémoire utilisée nombre de tâches enregistrées gestionnaires nombre de tâches exécution tâches nombre de tâches nombre de threads disponibles emplacements de tâches du démon total Nombre maximum de threads nombre total de threads démarré

Objet :	Identifiants :	Attributs :	Points de données :
Tâche de Flink	ID de tâche d'espace de noms de cluster	Nom du nœud du serveur Nom du travail sous-index des tâches ID de la tâche tentative Numéro Nom de la tâche ID du gestionnaire des tâches noeud IP filigrane actuel	Tampons dans utilisation de pool tampons dans longueur de file tampons utilisation de pool tampons utilisation de pool tampons sortie longueur de file d'attente tampons dans nombre local Buffers dans local nombre par seconde nombre de tampons dans local par seconde nombre de taux nombre de tampons dans nombre distant tampons dans nombre distant par seconde nombre de tampons dans Remote par distant Second Rate Number tampons Out Number tampons Out Number Buffers Out par seconde Count Number Buffers Out par seconde Rate Number Bytes in local Number Bytes in local par seconde Count Number Bytes in local par seconde Rate Number Bytes in Remote Number Bytes in Remote Number Bytes in Remote per second Count Number Bytes in Remote Par seconde Numéro de taux octets hors nombre octets hors par seconde nombre nombre octets hors par seconde Numéro de taux enregistrements nombre enregistrements en nombre en nombre par seconde nombre enregistrements en nombre de taux en nombre de seconde nombre de taux enregistrements hors nombre par seconde nombre de nombres enregistrements hors nombre par seconde nombre de nombres enregistrements hors taux par seconde

Objet :	Identifiants :	Attributs :	Points de données :
Opérateur de tâche Flink	Nom du cluster ID de tâche ID d'opérateur ID de tâche	Nom du noeud du serveur Nom du travail Nom de l'opérateur sous-index des tâches ID de la tâche tentative Numéro Nom de la tâche ID du gestionnaire des tâches IP du noeud	Watermark Current Input Current Output Watermark Number enregistrements en nombre enregistrements en nombre enregistrements par seconde nombre nombre enregistrements en par seconde nombre de débits en dehors nombre enregistrements en dehors par seconde nombre d'enregistrements en dehors par seconde nombre de débits en retard enregistrements en chute partitions attribuées octets en retard latence de validation de taux en moyenne Le taux maximal de validation a échoué les validations de connexion a réussi le nombre de connexions de fermeture nombre de connexions nombre de taux de création de connexion durée de récupération moyenne de latence de récupération débit maximal taille de récupération taille de récupération moyenne de l'accélérateur temps de récupération moyenne de l'accélérateur vitesse de transfert max. Taux de pulsation nombre d'octets entrants taux d'E/S moy Rapport d'attente temps d'attente d'E/S moy (ns) temps d'assemblage temps d'attente moy. Dernier Heartbeat ago débit d'E/S débit d'octets sortant enregistrements taux de consommation décalage max enregistrements par demande débit moyen taille de demande moyenne vitesse de réponse max. Sélection temps de synchronisation de taux moyenne réponse

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données Hadoop

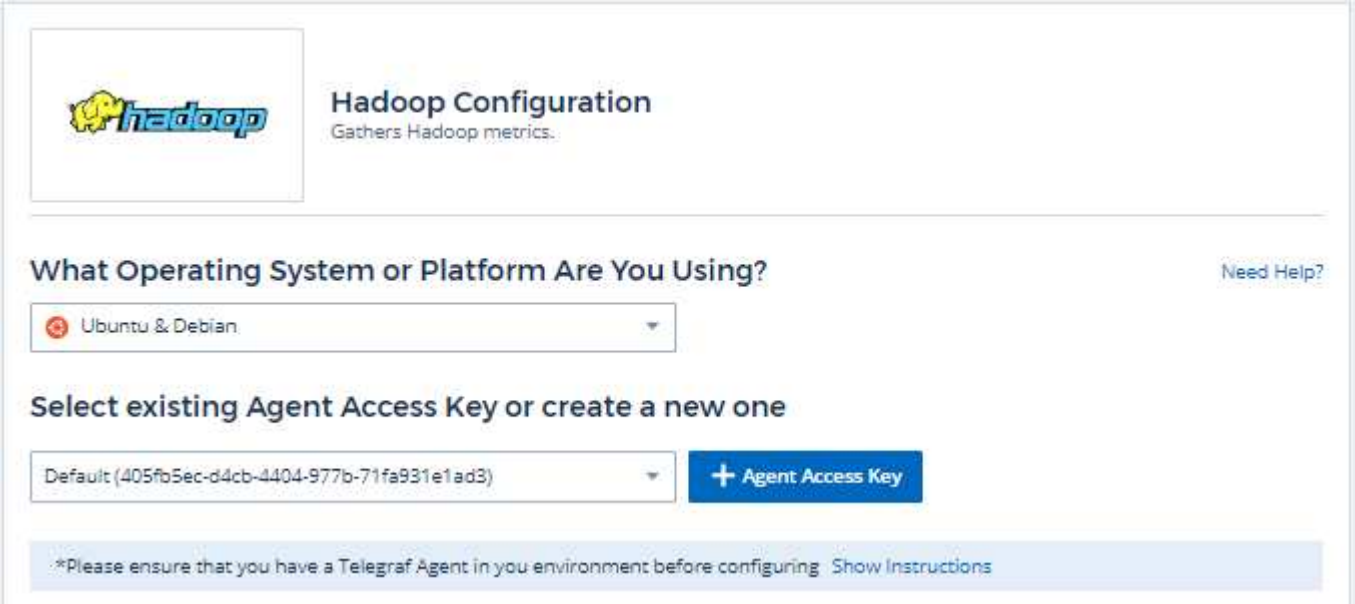
Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir de Hadoop.

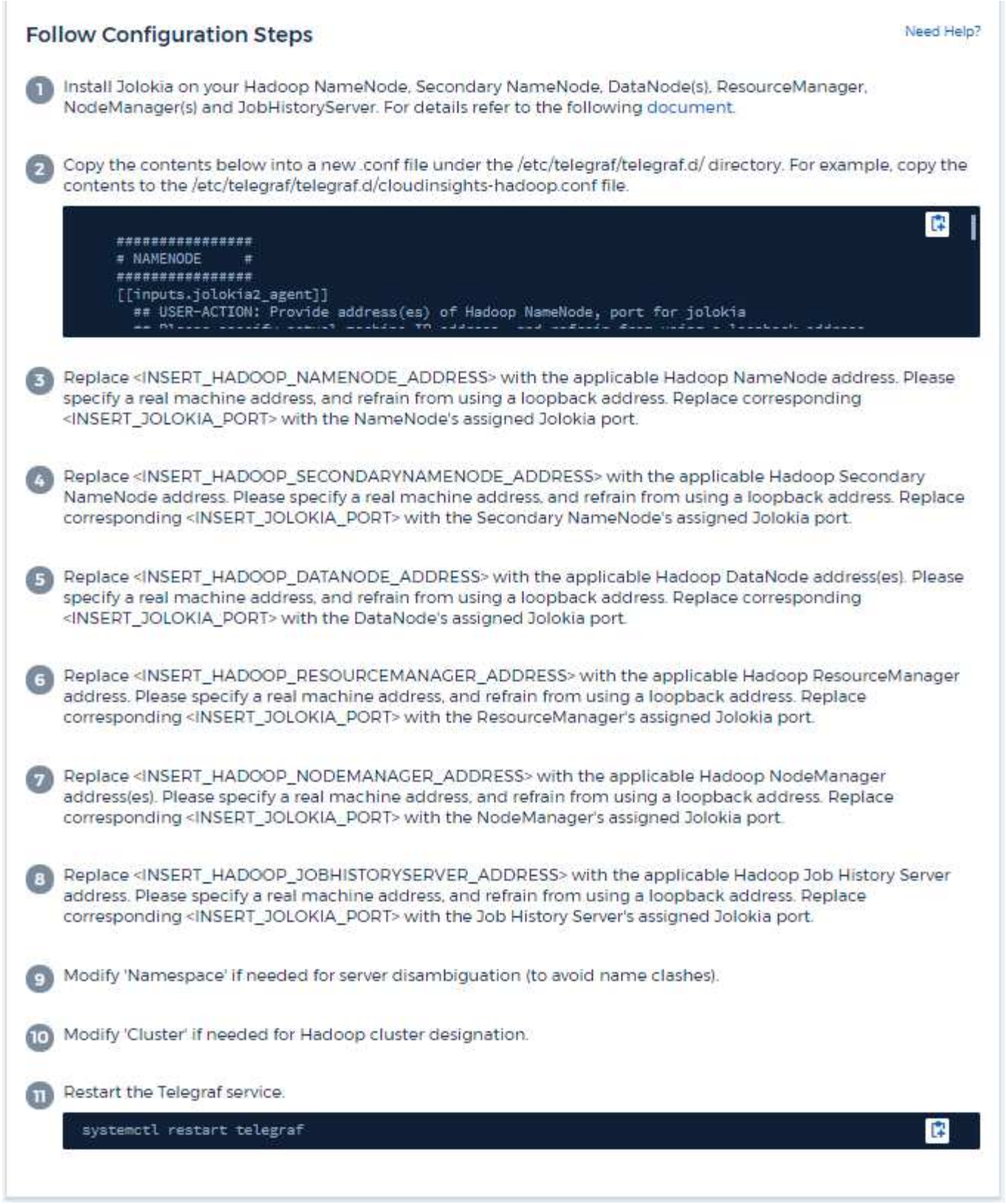
Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Avec Hadoop

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un 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 les "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 à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
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 utilisé pour collecter des données.





Configuration

Un déploiement Hadoop complet nécessite les composants suivants :

- NameNode : système principal Hadoop Distributed File System (HDFS). Coordonne une série de DataNodes.

- Second NameNode : basculement à chaud pour le NameNode principal. Dans Hadoop, la promotion vers NameNode n'a pas lieu automatiquement. Second NameNode collecte les informations du NameNode pour être prêt à être promu au besoin.
- DataNode : propriétaire réel des données.
- ResourceManager : le système principal de calcul (Yarn). Coordonne une série de gestionnaires de nœud.
- NodeManager : la ressource pour le calcul. Emplacement réel pour l'exécution des applications.
- JobHistoriyServer : responsable du traitement de toutes les requêtes liées à l'historique des travaux.

Le plug-in Hadoop est basé sur le plug-in Jolokia de telegraf. Par exemple, pour collecter des 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 à partir de la version Hadoop 2.9.2.

Configuration

Bol d'agent Jolokia

Pour tous les composants individuels, une version du fichier JAR de l'agent Jolokia doit être téléchargée. La version testée était "Agent de 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/'.

Nom de nœud

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 de nœud secondaire

Pour configurer le NameNode secondaire pour 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 pour 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.
```

ResourceManager

Pour configurer ResourceManager pour 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 nœud

Pour configurer les gestionnaires de nœud 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.
```

JobHistoriyServer

Pour configurer JobHistoriyServer 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 de nœud secondaire Hadoop	Serveur d'espace de noms de cluster	Noeud Nom noeud IP Compile Info version
Hadoop NodeManager	Serveur d'espace de noms de cluster	IP du nœud de nom de nœud
Gestionnaire de ressources Hadoop	Serveur d'espace de noms de cluster	IP du nœud de nom de nœud
Nœud de données Hadoop	Serveur d'espace de noms de cluster	Version de l'ID de cluster IP du nœud de nom de nœud
Nom de nœud Hadoop	Serveur d'espace de noms de cluster	Nom du nœud Nom de la transaction IP ID de transaction dernière heure écrite depuis la dernière édition de l'état HA fichier Etat du système Etat du système ID de bloc ID de groupe Infos de cluster version distincte nombre de versions
Hadoop JobHistoriyServer	Serveur d'espace de noms de cluster	IP du nœud de nom de nœud

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données HAProxy

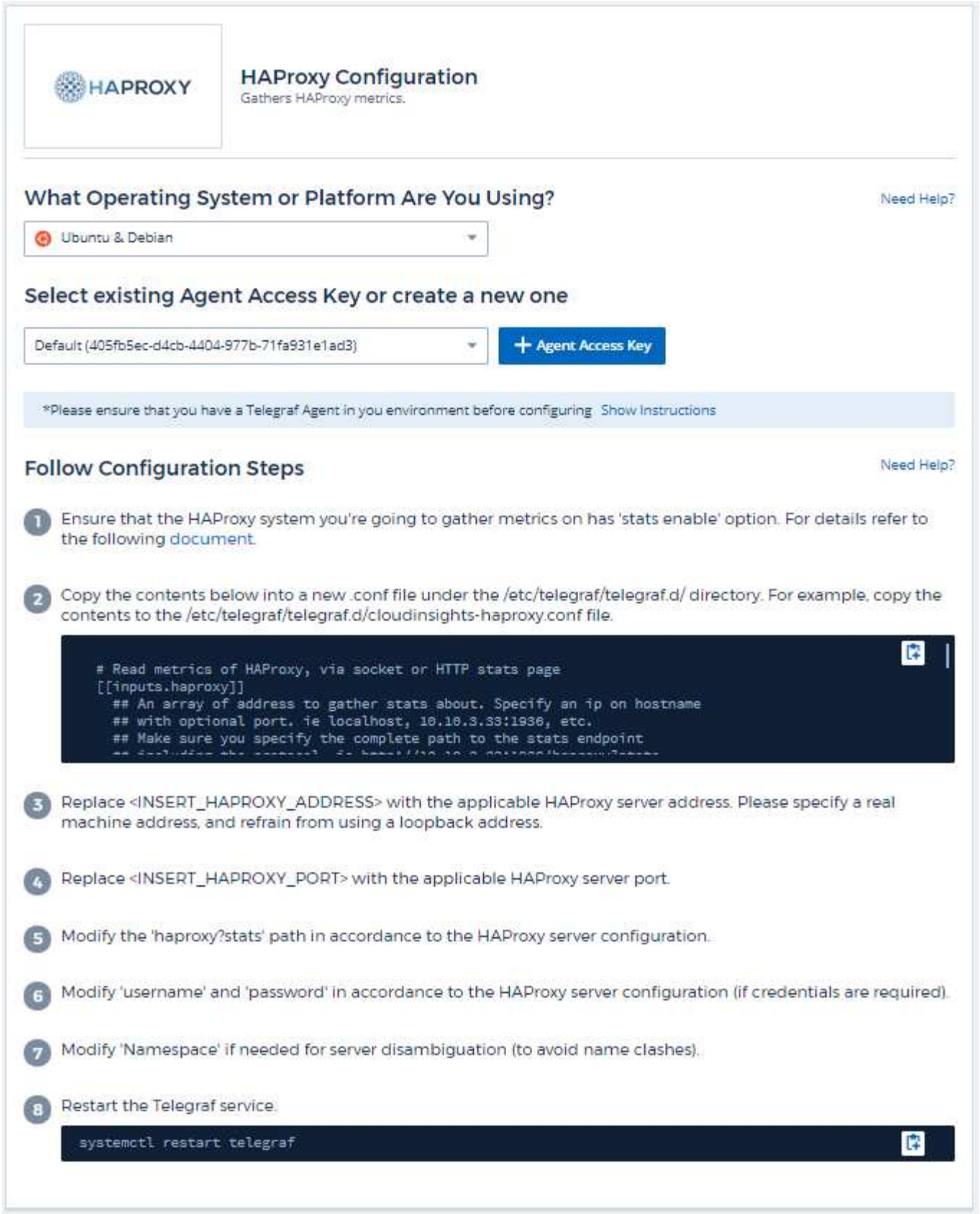
Data Infrastructure Insights utilise ce collecteur de données pour collecter des mesures à partir de HASProxy.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez HASProxy.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un 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 les "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 à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
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 utilisé pour collecter des données.



Configuration

Le plug-in de Telegraf pour HAProxy repose sur l'activation des statistiques HAProxy. Il s'agit d'une configuration intégrée dans HAProxy, mais elle n'est pas prête à l'emploi. Lorsqu'il est activé, HAProxy expose

un noeud final HTML qui peut être affiché sur votre navigateur ou gratté pour extraction de l'état de toutes les configurations HAProxy.

Compatibilité :

La configuration a été développée par HAProxy version 1.9.4.

Configuration :

Pour activer les statistiques, modifiez votre fichier de configuration hproxy et ajoutez les lignes suivantes après la section « attaques », en utilisant votre propre utilisateur/mot de passe et/ou URL de proxy :

```
stats enable
stats auth myuser:mypassword
stats uri  /haproxy?stats
```

Voici un exemple de fichier de configuration simplifié avec des 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 obtenir des instructions complètes et à jour, reportez-vous au "Documentation HABProxy".

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
HAVANCHAproxy frontal	Proxy d'adresse d'espace de noms	Noeud IP Nom de noeud ID proxy mode ID de processus sessions limite de taux sessions ID de serveur Etat limite de limite de nombre de sessions	Octets en octets hors cache Hits cache recherches cache octets de compression Bytes de compression Bytes de compression réponses de compression taux de connexion nombre maximal de demandes refusées par règle de connexion demandes refusées par des problèmes de sécurité réponses refusées par des demandes de sécurité refusées par la règle de session demandes d'erreurs réponses 1xx Réponses 2xx réponses 3xx réponses 4xx réponses 5xx autres demandes interceptées sessions Rate sessions demandes Rate Max demandes Rate demandes Rate nombre max sessions nombre max sessions nombre total sessions nombre total de requêtes nombre de réécritures

Objet :	Identifiants :	Attributs :	Points de données :
Serveur HAProxy	Serveur proxy d'adresse d'espace de noms	Nœud Nom du nœud IP heure de vérification de la vérification de la configuration de chute Vérification de la valeur de l'état Vérification de l'état de l'état ID du proxy dernière modification de la dernière session mode de l'heure de la dernière session ID du processus ID du serveur poids de l'état	Serveurs actifs serveurs de sauvegarde octets en octets hors octets Vérification Downs échec client liaisons connexion temps moyen d'arrêt Total réponses refusées erreurs de connexion réponses 1xx réponses 2xx réponses 3xx réponses 4xx réponses 5xx autres réponses serveur sélectionné File d'attente totale de la file d'attente actuelle durée moyenne des sessions par Seconde sessions par seconde Max Connection Reuse temps de réponse sessions moyennes sessions Max Server Transfer interrompt sessions Total sessions Total Time moyenne demandes rerépartit les demandes nouvelles tentatives réécritures

Objet :	Identifiants :	Attributs :	Points de données :
Système back-end HANProxy	Proxy d'adresse d'espace de noms	Noeud IP Nom de noeud ID proxy dernière modification heure dernière session mode temps processus ID de serveur sessions limite poids d'état	Serveurs actifs serveurs de sauvegarde octets en octets en octets en octets en cache Hits cache recherches cache Check Downs client abandonne les octets de compression ignorés octets de compression réponses de compression connexions temps moyen de connexion nombre de demandes refusées par des problèmes de sécurité réponses refusées par des problèmes de sécurité erreurs de connexion réponses aux erreurs de réponse 1xx réponses 2xx réponses 3xx réponses 4xx réponses 5xx autres réponses serveur sélectionné File d'attente totale file d'attente actuelle maximale file d'attente moyenne sessions par seconde nombre max demandes durée moyenne de la connexion réutilisation nombre total de sessions nombre moyen de sessions transfert serveur nombre total de sessions nombre total de sessions nombre total de sessions nombre total de fois nombre de requêtes redistribue les demandes de nouvelles Réécrit

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données JVM

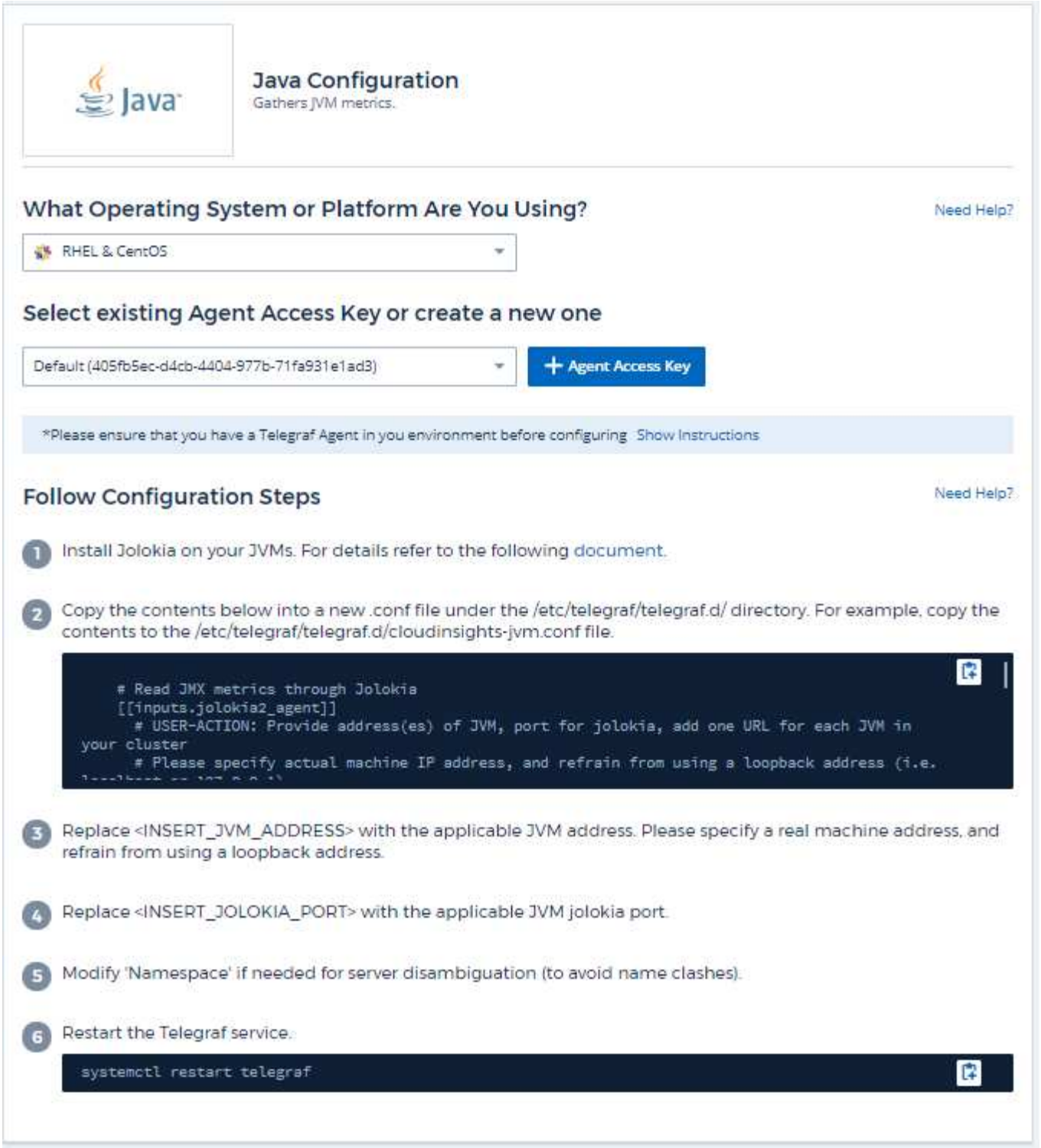
Data Infrastructure Insights utilise ce collecteur de données pour collecter des mesures à partir de JVM.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez JVM.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un 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 les "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 à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
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 utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans "Documentation de l'JVM".

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
JVM	JVM d’espace de noms	Architecture OS Nom OS version OS spécification d’exécution spécification d’exécution version spécification d’exécution Vendor version Uptime Runtime Nom VM Runtime VM Runtime version vendeur Nom du nœud IP	Classe chargée Total de la mémoire non chargée de la classe chargée mémoire vive mémoire vive mémoire vive mémoire vive mémoire vive utilisée mémoire maximale mémoire vive mémoire vive mémoire non mémoire non résolue mémoire non Heap mémoire non mémoire non mémoire vive objets de mémoire non utilisée en attente Finalisation processeurs OS disponibles taille de mémoire virtuelle OS non résolue Taille de la mémoire physique espace libre du système d’exploitation taille de l’espace libre du système d’exploitation nombre de descripteurs de fichier ouverts du système d’exploitation nombre de descripteurs de fichier du processeur du système d’exploitation charge du système d’exploitation CPU du système d’exploitation charge système d’exploitation taille moyenne de la mémoire physique totale du système d’exploitation nombre total de threads nombre de pics de threads Thread Count Thread Total Started Count Garbage Collector Copy Count Garbage Collector Copy collecte Time Garbage Collector Mark-balayage Collection Count Garbage Collector Mark-balayage collecte temps collecteur d’ordures G1 Old Generation Collection temps collecteur d’ordures ancien génération G1 Young Generation Collection Count Garbage

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données Kafka

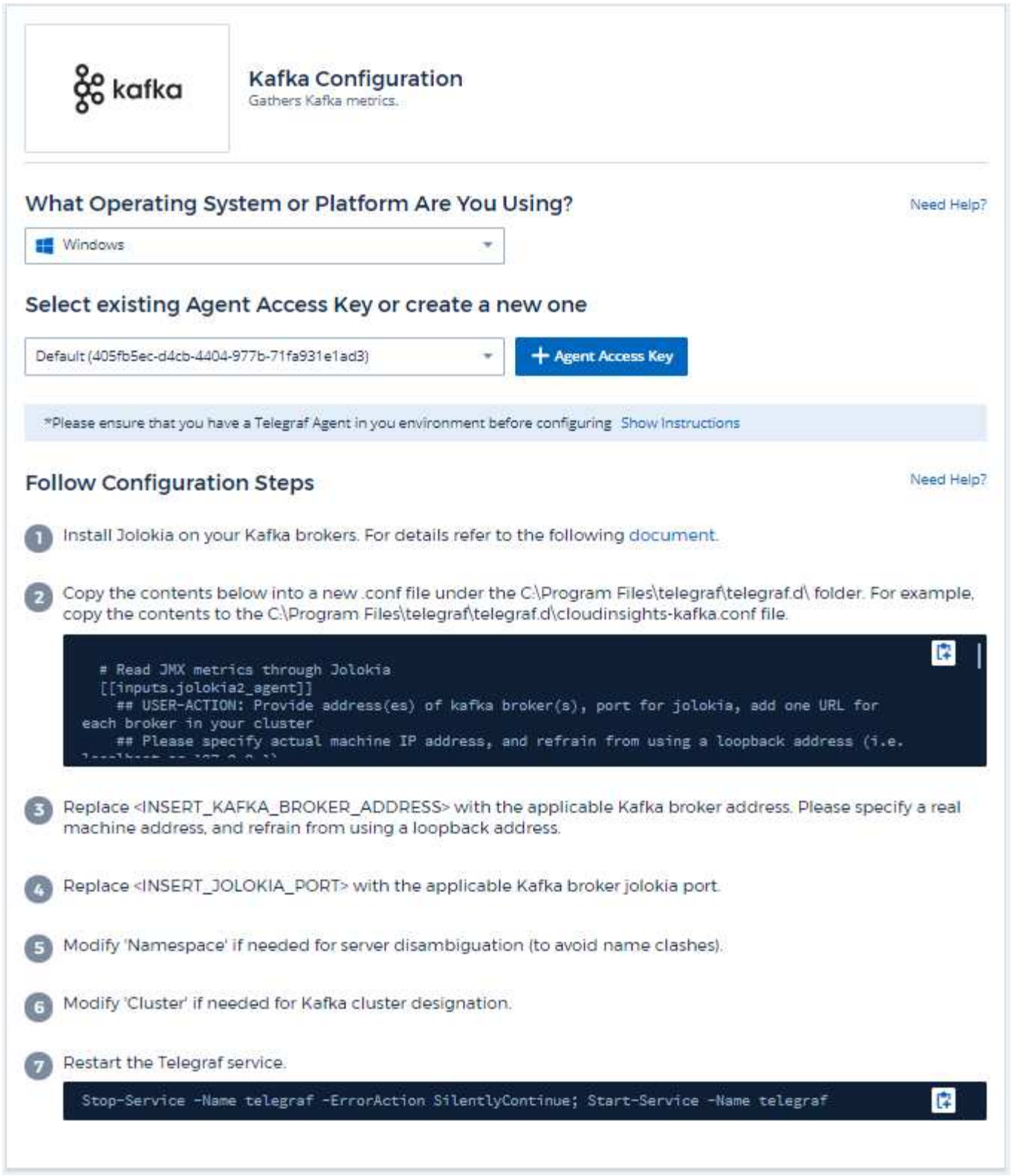
Data Infrastructure Insights utilise ce collecteur de données pour collecter les metrics de Kafka.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Kafka.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un 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 les "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 à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
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 utilisé pour collecter des données.



Configuration

Le plug-in Kafka est basé sur le plug-in Jolokia de telegraf. Par exemple, pour recueillir des 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 par rapport à Kafka version 0.11.0.2.

Configuration

Toutes les instructions ci-dessous supposent que votre emplacement d'installation pour kafka est '/opt/kafka'. Vous pouvez adapter les instructions ci-dessous en fonction de votre emplacement d'installation.

Bol d'agent Jolokia

Une version le 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/'.

Kafka Brokers

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 plusieurs machines IP, vous devez modifier cette configuration pour recueillir l'IP sur laquelle vous vous prenez en charge pour les connexions RMI.

Vous pouvez choisir un autre port pour JMX (9999 ci-dessus) et Jolokia (8778). Si vous avez un IP interne pour verrouiller Jolokia sur vous pouvez remplacer le 0.0.0.0 "tout capturer" par votre propre IP. Notez que cette adresse IP doit être accessible à partir du plug-in telegraf. Vous pouvez utiliser l'option -Dcom.sun.management.jmxremote.authenticate=false' si vous ne souhaitez pas vous authentifier. Utilisation 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	IP du nœud de nom de nœud

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données Kibana

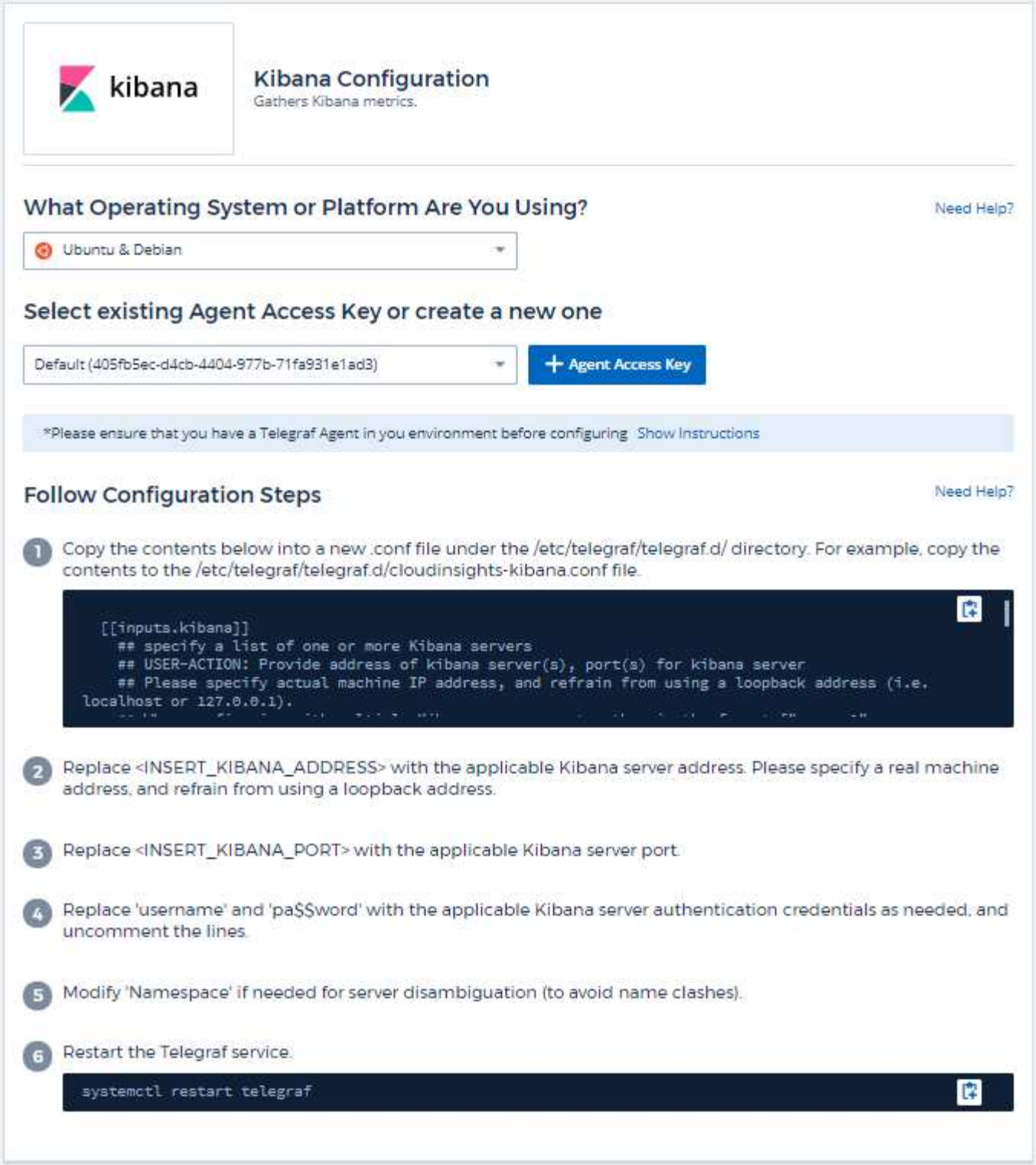
Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir de Kibana.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Kibana.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un 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 les "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 à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
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 utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans le "Documentation 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	État de la version du nom de nœud IP du nœud	Connexions simultanées Heap Max Heap utilisait des requêtes par seconde temps de réponse moyen temps de réponse maximum disponibilité

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

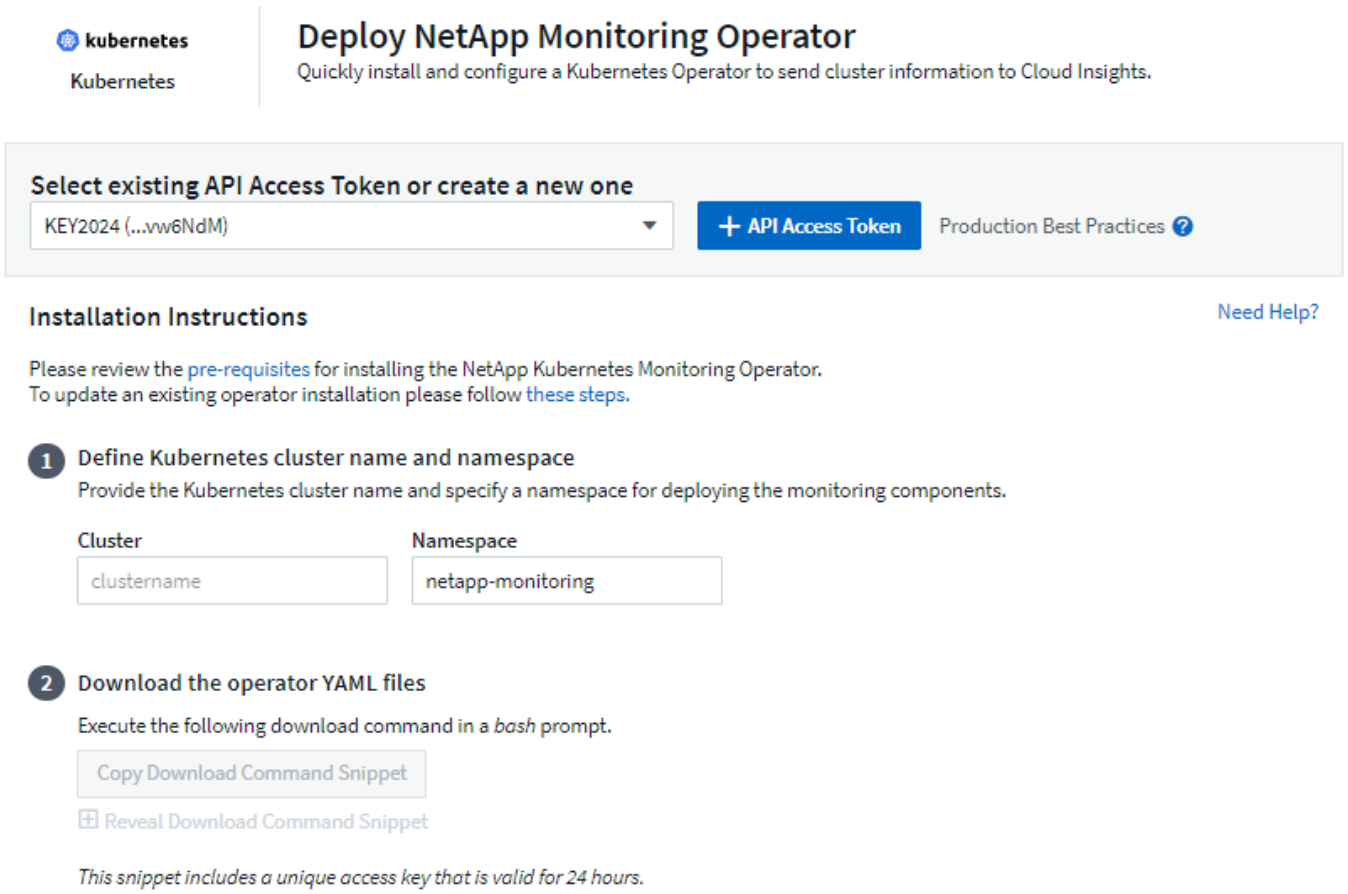
Installation et configuration de l'opérateur de contrôle Kubernetes

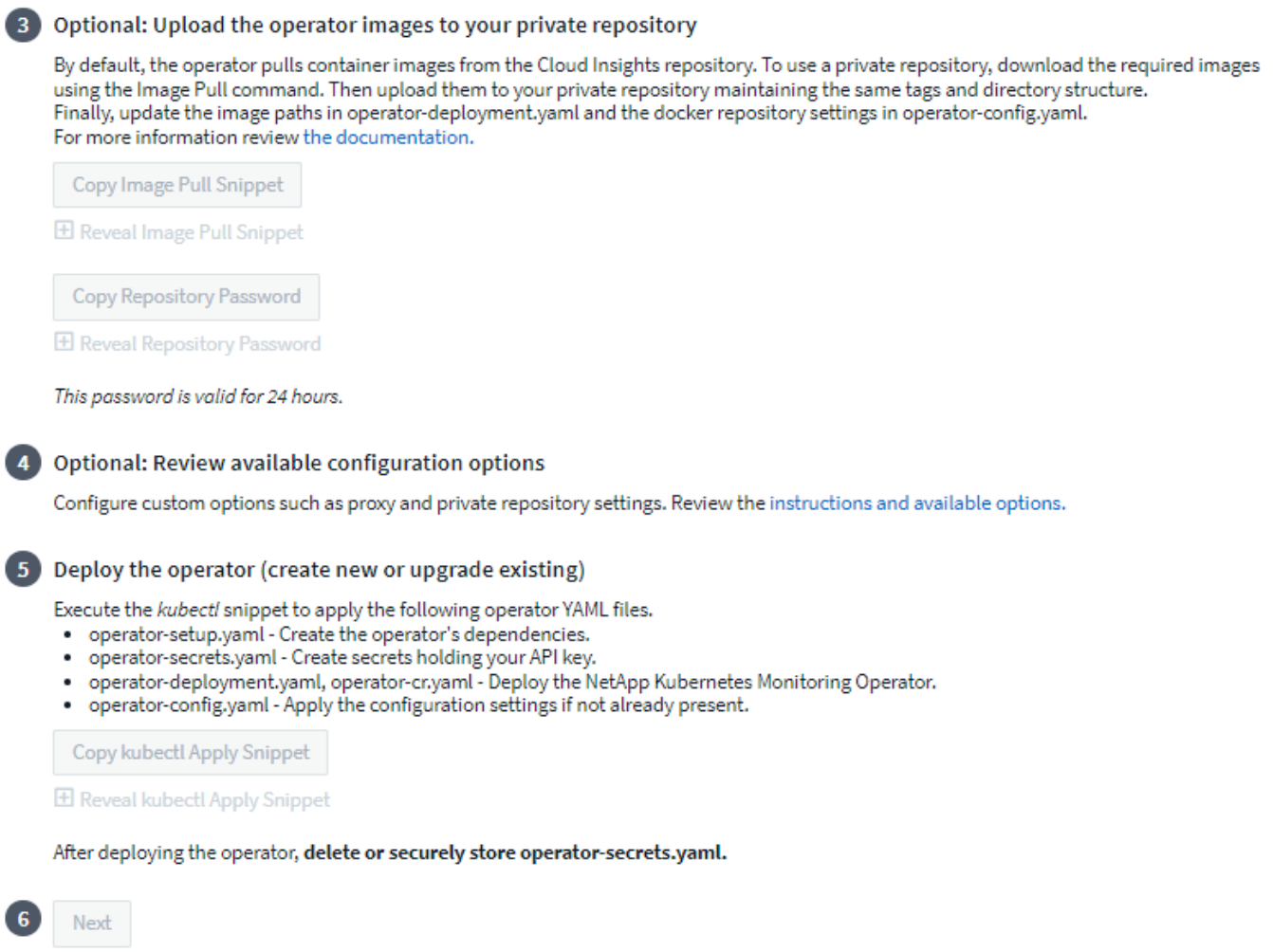
Data Infrastructure Insights propose l'opérateur **Kubernetes Monitoring Operator** pour la collecte Kubernetes. Accédez à **Kubernetes > Collectors > +Kubernetes Collector** pour déployer un nouvel opérateur.

Avant d'installer l'opérateur de surveillance Kubernetes

Consultez "Conditions préalables"la documentation avant d'installer ou de mettre à niveau l'opérateur de surveillance Kubernetes.

Installation de l'opérateur de surveillance Kubernetes





Étapes d'installation de l'agent opérateur de surveillance Kubernetes sur Kubernetes :

1. Entrez un nom de cluster et un espace de noms uniques. Si vous mise à niveauutilisez un opérateur Kubernetes précédent, utilisez le même nom de cluster et le même espace de noms.
2. Une fois ces données saisies, vous pouvez copier le fragment de commande de téléchargement dans le presse-papiers.
3. Collez le fragment dans une fenêtre *bash* et exécutez-le. Les fichiers d'installation de l'opérateur seront téléchargés. Notez que l'extrait de code possède une clé unique et est valide pendant 24 heures.
4. Si vous disposez d'un référentiel personnalisé ou privé, copiez le fragment facultatif image Pull, 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, passez en revue 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 le fragment kubectl Apply, en le téléchargeant et en l'exécutant.
7. L'installation se poursuit 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 propos de à l'aide d'un référentiel docker

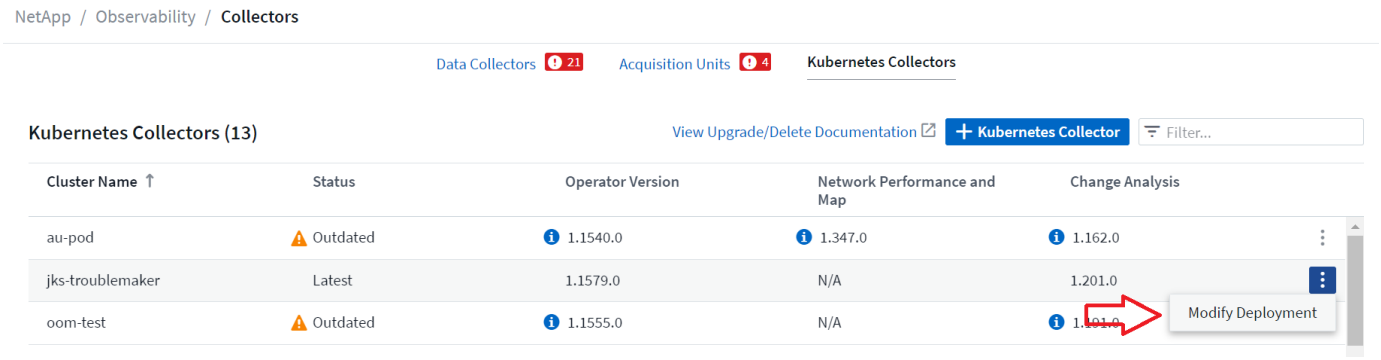
personnalisé/privé.

Composants de surveillance Kubernetes

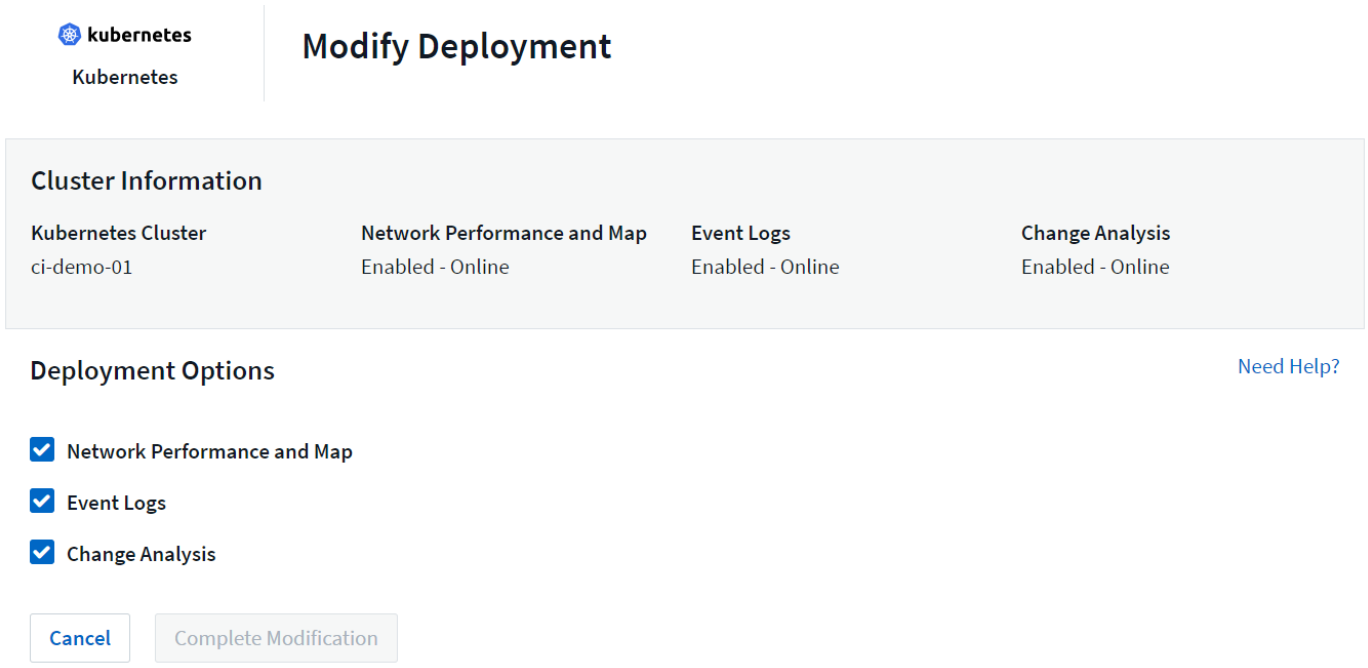
La surveillance Kubernetes de Data Infrastructure Insights comprend quatre composants de surveillance :

- Metrics du cluster
- Carte et performances réseau (en option)
- Journaux d'événements (facultatif)
- Analyse des modifications (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 > Collectors** et en sélectionnant *Modify Deployment* 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 pour ce collecteur selon vos besoins.



Mise à niveau vers le dernier opérateur de surveillance Kubernetes

Mises à niveau DII à bouton-poussoir

Vous pouvez mettre à niveau l'opérateur de surveillance Kubernetes à partir de la page collecteurs Kubernetes DII. Cliquez sur le menu en regard du cluster que vous souhaitez mettre à niveau et sélectionnez *Upgrade*. L'opérateur vérifie les signatures d'image, effectue un instantané de votre installation actuelle et effectue la mise à niveau. Dans quelques minutes, vous devriez voir l'état de l'opérateur progression de la mise à niveau en cours vers la dernière. Si vous rencontrez une erreur, vous pouvez sélectionner l'état d'erreur pour plus de détails et vous reporter au tableau Dépannage des mises à niveau par bouton-poussoir ci-dessous.

Mises à niveau à l'aide de référentiels privés par simple pression

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 les images manquantes, ajoutez-les simplement à votre référentiel et réessayez la mise à niveau. Pour télécharger les signatures d'images dans votre référentiel, utilisez l'outil de cosignature comme suit, en vous assurant de télécharger les signatures pour toutes les images spécifiées sous 3 Facultatif : chargez 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>
```

Retour à une version précédente

Si vous avez effectué une mise à niveau à l'aide de la fonction de mise à niveau par bouton-poussoir et que vous rencontrez des difficultés avec la version actuelle de l'opérateur dans les sept jours suivant la mise à niveau, vous pouvez revenir à la version précédente en utilisant l'instantané créé pendant le processus de mise à niveau. Cliquez sur le menu en regard du cluster que vous souhaitez restaurer et sélectionnez *Retour arrière*.

Mises à niveau manuelles

Déterminez si une configuration d'agentConfiguration existe avec l'opérateur existant (si votre espace de noms n'est pas le *netapp-monitoring* par défaut, remplacez l'espace de noms approprié) :

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-ci-monitoring-
configuration
Si une configuration d'agentConfiguration existe :
```

- Installez Dernier opérateur par rapport à l'opérateur existant.
  - Assurez-vous que vous extraction des dernières images du conteneurutilisez un référentiel personnalisé.

Si AgentConfiguration n'existe pas :

- Notez le nom de votre cluster tel qu'il a été reconnu par les informations d'infrastructure de données (si

votre namespace n'est pas le contrôle NetApp par défaut, remplacez l'espace de noms approprié) :

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* Créer une sauvegarde de l'opérateur existant (si votre namespace n'est
pas la surveillance netapp par défaut, remplacez le namespace 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,Installez>> Le dernier
opérateur.
```

- Utilisez le même nom de cluster.
- Après avoir téléchargé les derniers fichiers Operator YAML, porter toutes les personnalisations trouvées dans agent_backup.yaml à l'opérateur-config.yaml téléchargé avant le déploiement.
- Assurez-vous que vous extraction des dernières images du conteneurutilisez 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 de l'opérateur de surveillance Kubernetes est « netapp-monitoring ». Si vous avez défini votre propre espace de noms, remplacez-le dans ces commandes et tous les fichiers suivants.

Les nouvelles versions de l'opérateur de surveillance peuvent être désinstallées à l'aide des 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, supprimer l'espace de noms :

```
 kubectl delete ns <NAMESPACE>
Remarque : si la première commande renvoie "aucune ressource trouvée",
suivez les instructions ci-dessous pour désinstaller les anciennes
versions de l'opérateur de surveillance.
```

Exécutez chacune des commandes suivantes dans l'ordre indiqué. Selon votre installation actuelle, certaines de ces commandes peuvent renvoyer des messages « objet introuvable ». 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 des indicateurs Kube-State

L'opérateur de surveillance NetApp Kubernetes installe ses propres metrics kube-State pour éviter les conflits avec d'autres instances.

Pour plus d'informations sur Kube-State-Metrics, reportez-vous à "cette page"la section .

Configuration/personnalisation de l'opérateur

Ces sections contiennent des informations sur la personnalisation de la configuration de votre opérateur,

l'utilisation du 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 contient des exemples de paramètres commentés. Voir la liste des pour la version la plus récente de "paramètres disponibles"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 du support de proxy

Vous pouvez utiliser un proxy sur votre locataire à deux endroits pour installer l'opérateur Kubernetes Monitoring. Il peut s'agir de systèmes proxy identiques ou distincts :

- Proxy nécessaire lors de l'exécution de l'extrait de code d'installation (à l'aide de « curl ») pour connecter le système sur lequel l'extrait de code 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'une ou l'autre de ces opérations, ou pour les deux, 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 que vous 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 le moniteur d'exploitation Kubernetes, avant d'installer l'opérateur, définissez les variables d'environnement *http_proxy/https_proxy*. Pour certains environnements proxy, il peut être nécessaire de définir la variable *no_proxy Environment*.

Pour définir la ou les variable(s), effectuez les opérations suivantes sur votre système **avant** installation de l'opérateur de surveillance Kubernetes :

1. Définissez les variables d'environnement *https_proxy* et/ou *http_proxy* pour l'utilisateur actuel :
    a. Si le proxy en cours de configuration n'a 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 la
commande suivante :
```

```
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 l'opérateur de surveillance Kubernetes après avoir lu toutes ces instructions.

Configurez la section proxy d'AgentConfiguration dans Operator-config.yaml avant de déployer l'opérateur de surveillance 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
  ...
...
```

À l'aide d'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 utilisez un cluster Kubernetes comme cible pour la surveillance et que ce cluster est configuré pour extraire uniquement les 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 requis par l'opérateur de surveillance Kubernetes.

Exécutez l'extrait de code image dans la mosaïque d'installation de NetApp Monitoring Operator. Cette commande permet de se connecter au référentiel Data Infrastructure Insights, d'extraire toutes les dépendances d'image pour l'opérateur et de se déconnecter du référentiel Data Infrastructure Insights. Lorsque vous y êtes invité, saisissez le mot de passe temporaire du référentiel fourni. Cette commande permet de télécharger toutes les images utilisées par l'opérateur, y compris pour les fonctions facultatives. Voir ci-dessous pour connaître les caractéristiques auxquelles ces images sont utilisées.

Fonctionnalités centrales de l'opérateur et surveillance Kubernetes

- surveillance netapp
- proxy ci-kube-rbac
- ci-ksm
- ci-telegraf
- utilisateur-root-distroless

Journal des événements

- bit fluide ci
- ci-kubernetes-exportateur-événements

Performances et carte réseau

- ci-net-observateur

Envoyez l'image de docker de l'opérateur à votre référentiel docker privé, local ou d'entreprise, conformément aux règles de votre entreprise. Assurez-vous que les balises d'image et les chemins de répertoire vers 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 la configuration d'agentConfiguration dans Operator-config.yaml pour refléter le nouvel emplacement docker repo. Créez une nouvelle imagePullSecret pour votre référentiel privé. Pour plus de détails, voir *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
```

Instructions OpenShift

Si vous exécutez sur OpenShift 4.6 ou une version ultérieure, vous devez modifier la configuration d'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 tainations

Les *netapp-ci-telegraf-ds*, *netapp-ci-Fluent-bit-ds* et *netapp-ci-net-observateur-l4-ds* Demonsets 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 certains **taints** bien connus. Si vous avez configuré des fichiers d'accès personnalisés sur vos nœuds, empêchant ainsi les modules de s'exécuter sur chaque nœud, vous pouvez créer une **tolérance** pour ces fichiers d'accès "Dans *AgentConfiguration*". Si vous avez appliqué des rejets personnalisés 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 opérateur.

En savoir plus sur Kubernetes "Teintes et tolérances".

Revenir au **"Page installation de l'opérateur de surveillance NetApp Kubernetes"**

Remarque sur les secrets

Pour supprimer l'autorisation pour l'opérateur de surveillance Kubernetes d'afficher les secrets à l'échelle du cluster, supprimez les ressources suivantes du fichier *Operator-setup.yaml* avant d'installer :

```
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'option analyse des modifications est activée, modifiez *AgentConfiguration* ou *Operator-config.yaml* pour annuler le commentaire de la section de gestion des modifications et incluez *kindsToIgnoreFromWatch: '"secrets"'* dans la section de gestion des modifications. 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'images 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 co-signer 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 : télécharger les images de l'opérateur dans votre référentiel privé > clé publique de signature d'image*

Pour vérifier manuellement une signature d'image, effectuez les opérations suivantes :

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 du cosigne. Reportez-vous à l'exemple suivant d'utilisation des coenseignes

```
$ 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

Voici quelques points à essayer en cas de problème lors de la configuration de l'opérateur de surveillance Kubernetes :

Problème :	**Essayer :**
Je ne vois pas de lien hypertexte/connexion entre mon volume persistant Kubernetes et le périphérique de stockage back-end correspondant. Mon volume persistant Kubernetes est configuré en utilisant le nom d'hôte du serveur de stockage.	Procédez comme suit pour désinstaller l'agent Telegraf existant, puis réinstaller l'agent Telegraf le plus récent. Vous devez utiliser Telegraf version 2.0 ou ultérieure et le stockage de votre cluster Kubernetes doit être activement surveillé par Data Infrastructure Insights.
Je vois des messages dans les journaux qui ressemblent à ce qui suit : E0901 15 352:21:39.962145 178 1 Reflector.Go:178] k8s.io/kube-state-metrics/Internal/store/Builder.Go:43.168161 : échec de la liste *v1.MutatingWebhookio Configuration : le serveur n'a pas pu trouver la ressource demandée E0901 15:21/352/Reflector.s.Go.so	Ces messages peuvent se produire si vous exécutez des metrics d'état kube version 2.0.0 ou supérieure avec les versions Kubernetes inférieures à 1.20. Pour obtenir la version Kubernetes : *kubectl version* pour obtenir la version kube-state-metrics : *kubectl get deployment/kube-state-metrics -o jsonpath='{..image}'* pour éviter que ces messages se produisent, les utilisateurs peuvent modifier leur déploiement de metrics kube-state-metrics pour désactiver les baux suivants : *hookingwebconfigurations*. Ressources=certificats,demandes persistantes,configmaps,cronjobs,demonets, déploiements,noeuds finaux,horizontalepodpodscalers,ingresources,details, resuts,undats,depositionsstatees,depositigmats,defiees,resottes,depositionssecuts,defiees,dees,depositionunedats,delimantees,delimantees,deficedats,dees,delimantees,delimantees,delimantees,deficedats,delimantees,deficedats,delimantees,deficedats,deficedats,dees,delimantees,delimantees,dees,delimantees,deficedats,dees,delimantees,delimantees,delimantees,delimantees,de vaillewebconfiguration,v'

Problème :	Essayer :
Je vois des messages d'erreur de Telegraf ressemblant aux messages suivants, mais Telegraf démarre et s'exécute : oct 11 14:23:41 ip-172-31-39-47 systemd[1] : lancé l'agent serveur piloté par des plug-ins pour signaler des mesures dans InfluxDB. Oct 11 14:23:41 ip-172-31-39-47 telegraf[1827] : heure="2021-10-11T14:23:41Z" level=erreur msg="Impossible de créer le répertoire de cache. /Etc/telegraf/.cache/flocon de neige, err : mkdir /etc/telegraf/.ca che : permission refusée. Ignored\n » func="nowgosflake.(*defaultLogger).Errorf" file="log.Go:10" Oct 1827 23:2021:39-47 ip-172-31-41 telegraf[11 14] : échec de l'ouverture:23:120. Ignoré. Ouvrir /etc/telegraf/.cache/flocon/ocsp_Response_cache.jso n : pas de fichier ou répertoire\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.Go:120 10" Oct 23:2021:39-47 ip-1827-31 telegraf[172]: 23-41-11 14:11Z! Démarrage de Telegraf 1.19.3	Il s'agit d'un problème connu. Voir "Article GitHub"pour plus de détails. Tant que Telegraf est opérationnel, les utilisateurs peuvent ignorer ces messages d'erreur.
Sur Kubernetes, mes coffee pad(s) Telegraf ont signalé l'erreur suivante : "erreur lors du traitement des informations de mountstats : échec de l'ouverture du fichier mountstats: /Hostfs/proc/1/mountstats, erreur: Ouvrir /hostfs/proc/1/mountstats: Permission refusée"	Si SELinux est activé et applique, il empêche probablement le ou les pod(s) Telegraf d'accéder au fichier /proc/1/mountstats sur le nœud Kubernetes. Pour contourner cette restriction, modifiez la configuration d'agentconfiguration 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 plug-in : impossible de charger keypair /etc/kubernetes/pki/ETcd/Server.crt:/etc/kubernetes/pki/ETcd/Server.key : ouvrir /etc/kubernetes/pki/ETcd/Server.crt : aucun fichier ni répertoire	Le pod Télégraf ReplicaSet est conçu pour 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 obtenez ces erreurs. Vérifiez si vos nœuds maître/ETCD ont des astuces sur eux. S'ils le font, ajoutez les tolérances nécessaires à Telegraf ReplicaSet, telegraf-RS. Par exemple, modifiez le ReplicaSet… kubectl edit RS telegraf-RS …et ajoutez les tolérances appropriées à la spécification. Redémarrez ensuite le pod ReplicaSet.

Problème :	Essayer :
J'ai un environnement PSP/PSA. Cela affecte-t-il mon opérateur de surveillance ?	Si votre cluster Kubernetes s'exécute avec la règle de sécurité Pod (PSP) ou l'admission de sécurité Pod (PSA) sur place, vous devez effectuer la mise à niveau vers l'opérateur de surveillance Kubernetes le plus récent. Procédez comme suit pour mettre à niveau vers l'opérateur actuel avec la prise en charge de PSP/PSA : 1. Désinstaller le précédent opérateur de surveillance : kubectl delete 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-cluster-agent-roleadmin-binding-cluster-2-agent-binding. Installez dernière version de l'opérateur de surveillance.
J'ai rencontré des problèmes lors de la tentative de déploiement de l'opérateur, et j'ai utilisé PSP/PSA.	1. Modifiez l'agent à l'aide de la commande suivante : kubectl -n <name-space> edit agent 2. Marquez « Security-policy-enabled » comme « false ». Ceci désactivera les stratégies de sécurité du Pod et l'admission de sécurité du Pod et permettra à l'opérateur de déployer. Confirmez en utilisant les commandes suivantes : kubectl get psp (devrait afficher Pod Security Policy supprimé) kubectl get all -n <namespace>
grep -i psp (doit montrer que rien n'a été trouvé)	Erreurs « ImagePullBackoff » détectées
Ces erreurs peuvent se produire si vous disposez d'un référentiel docker personnalisé ou privé et que vous n'avez pas encore configuré l'opérateur de surveillance Kubernetes pour qu'il le reconnaisse correctement. En savoir plus a propos de la configuration pour 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.

Capturer ou noter le résultat des commandes suivantes et contacter 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-observateur (Workload Map) de l'espace de noms de l'opérateur se trouvent dans CrashLoopBackOff

Problème :	Essayer :
Ces pods correspondent au collecteur de données Workload Map pour l'observabilité réseau. Essayez : • Vérifiez les journaux de l'un des modules pour confirmer la version minimale du noyau. Par exemple : --- {"ci-tenant-ID":"votre-tenant-ID","collectionneur-cluster":"votre-k8s-cluster-name","Environment":"prod","level":"error","msg":"échec de la validation. Raison : la version 3.10.0 du noyau est inférieure à la version minimale du noyau de 4.18.0","Time":"2022-11-09T08:23:08Z"} ---- • les pods Net-observateur requièrent 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'ils sont >= 4.18.0	Les pods s'exécutent dans l'espace de noms Operator (par défaut : surveillance netapp), mais aucune donnée n'est affichée dans l'interface pour la carte des workloads ou les metrics Kubernetes dans les requêtes
Vérifiez le réglage de l'heure sur les nœuds du cluster K8S. Pour un audit et un reporting précis des données, il est vivement recommandé de synchroniser l'heure sur l'ordinateur de l'agent à l'aide du protocole NTP (Network Time Protocol) ou SNTP (simple Network Time Protocol).	Certains des pods net-observateur dans l'espace de noms de l'opérateur sont à l'état en attente
Net-observateur est un DemonSet et exécute un pod dans chaque nœud du cluster k8s. • Notez le pod qui est à l'état en attente et vérifiez s'il rencontre un problème de ressource 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 l'opérateur de surveillance Kubernetes : [inputs.prometheus] erreur dans le plug-in : erreur lors de la demande HTTP vers http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics : get http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics : Dial tcp: kube-state-metrics.<namespace>.svc.cluster.local : pas de recherche d'hôte
Ce message n'apparaît généralement que lorsqu'un nouvel opérateur est installé et que le module *telegraf-RS* est en marche avant que le module *ksm* ne soit en marche. Ces messages doivent s'arrêter une fois que tous les modules sont en cours d'exécution.	Je ne vois aucun indicateur collecté pour les cronjobs Kubernetes qui existent dans mon cluster.
Vérifiez votre version de Kubernetes (c'est-à-dire `kubectl version`). S'il est v1.20.x ou inférieur, il s'agit d'une limitation attendue. La version de kube-state-metrics déployée avec l'opérateur de surveillance Kubernetes ne prend en charge que v1.cronjob. Avec Kubernetes 1.20.x et versions antérieures, la ressource cronjob est à v1beta.cronjob. Par conséquent, les indicateurs d'état kube ne peuvent pas trouver la ressource cronjob.	Après l'installation de l'opérateur, les modules telegraf-ds entrent dans CrashLoopBackOff et les journaux du pod indiquent « su: Authentication failure ».

Problème :	Essayer :
Modifiez la section telegraf dans *AgentConfiguration* et définissez *dockerMetricCollectionEnabled* sur FALSE. Pour plus de détails, reportez-vous au "options de configuration"manuel de l'opérateur . … spec: … telegraf: … - Nom: docker run-mode : - DemonSet substitutions: - Key: DOCKER_UNIX_SOCK_PLACEHOLDER valeur: unix:///run/docker.sock … …	Je vois des messages d'erreur récurrents ressemblant à ce qui suit dans mes journaux Telegraf: E! [Agent] erreur d'écriture dans outputs.http: Post "https://<tenant_url>/REST/v1/Lake/iningt/influxdb": Délai de contexte dépassé (client. Dépassement du délai d'attente des en-têtes)
Modifiez la section telegraf dans *AgentConfiguration* et augmentez *outputTimeout* à 10 s. Pour plus de détails, reportez-vous au "options de configuration"manuel de l'opérateur .	Il me manque des données *involvedobject* pour certains journaux d'événements.
Assurez-vous d'avoir suivi les étapes de la "Autorisations" section ci-dessus.	Pourquoi deux modules d'opérateurs de surveillance s'exécutent, l'un nommé netapp-ci-monitoring-Operator-<pod> et l'autre Monitoring-Operator-<pod> ?
Depuis le 12 octobre 2023, Data Infrastructure Insights a été décidé de réorganiser l'opérateur pour mieux répondre aux besoins de nos utilisateurs. Pour que ces changements soient entièrement adoptés, vous devez retirez l'ancien opérateur et installez le nouveau.	Mes événements kubernetes ont cessé de générer des rapports à Data Infrastructure Insights de manière inattendue.
Récupérer le nom du pod Event-exportateur : `kubectl -n netapp-monitoring get pods`	grep event-exporter

Problème :	Essayer :
awk '{print $1}'	sed 's/event-exporter./event-exporter/'` Il doit être « netapp-ci-event-exportatrice » ou « event-exportatrice ». Ensuite, modifiez l'agent de surveillance `kubectl -n netapp-monitoring edit agent` et définissez la valeur de LOG_FILE pour qu'elle reflète 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-exportatrice.log » ou «/var/log/containers/event-exportatrice*.log ». …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. Sinon, on peut aussi désinstaller et réinstallez l'agent.
J'constate que le ou les pods déployés par l'opérateur de surveillance Kubernetes sont en panne en raison de ressources insuffisantes.	Reportez-vous à l'opérateur de surveillance Kubernetes "options de configuration"pour augmenter les limites de processeur et/ou de mémoire selon les besoins.
Si une image manquante ou une configuration non valide a entraîné l'échec du démarrage ou de la préparation des pods de metrics d'état de netapp-ci-kube. L'état StatefulSet est bloqué et les modifications de configuration ne sont pas appliquées aux pods de metrics netapp-ci-kube-state.	StatefulSet est dans un "cassé" état. Après avoir résolu tout problème de configuration, utilisez les pods de metrics netapp-ci-kube-état.
les pods de metrics d'état-ci-kube-netapp ne parviennent pas à démarrer après l'exécution d'une mise à niveau d'opérateur Kubernetes, et lancent ErrImagePull (échec de l'extraction de l'image).	Essayez de réinitialiser les modules manuellement.
Des messages « événement ignoré comme étant plus ancien que maxEventAgeSeconds » sont observés pour mon cluster Kubernetes sous analyse du journal.	Modifiez l'opérateur *agentconfiguration* et augmentez les valeurs *event-exportatrice-maxEventAgeSeconds* (c.-à-d. à 60 s), *event-exportatrice-kubeQPS* (c.-à-d. à 100) et *event-exportatrice-kubeBurst* (c.-à-d. à 500). Pour plus de détails sur ces options de configuration, reportez-vous à la "options de configuration" page.

Problème :	Essayer :
Telegraf avertit ou se bloque en raison 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'agentNKMO et définissez *Unprotected* sur *true*. Cela indique 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 disque, il permet une exécution dans des environnements où il est impossible de réserver de la mémoire verrouillée. Pour plus de détails sur les options de configuration *Unprotected*, 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 lors de la lecture de /dev/vdc : pas de fichier ou de répertoire	Pour l'opérateur de surveillance Kubernetes, ces messages d'avertissement sont bénins et peuvent être ignorés en toute sécurité. Vous pouvez également modifier la section telegraf dans AgentConfiguration et définir *runDsPrivileged* sur TRUE. Pour plus de détails, reportez-vous au "options de configuration de l'opérateur".

Problème :	Essayer :

Mon pod Fluent-bit échoue avec les erreurs suivantes : [2024/10/16 14 23:16:23] [erreur] [/src/fluent-bit/plugins/In_tail/tail_fs_inotify.c:360 errno=10/16 14] trop de fichiers ouverts [2024/10/16 14:16:23] [erreur] échec de l'initialisation de l'entrée tail.0 [2024/24:16] [erreur d'initialisation du moteur]	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 lors des redémarrages de 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 :	Essayer :
Les pods telegraf DS signalent des erreurs liées au plug-in d’entrée kubernetes qui ne parviennent pas à faire de requêtes HTTP en raison de l’incapacité à valider le certificat TLS. Par exemple : E! [Inputs.kubernetes] erreur dans le plug-in : erreur lors de la demande HTTP pour "<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 la vérification du certificat : x509 : impossible de valider le certificat pour <kubelet_IP> car il ne contient pas de 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 des certificats *Subject alternative Name*. Pour résoudre ce problème, l'utilisateur peut modifier le "configuration de l'agent", et définir *telegraf:insecureK8sSkipVerify* sur *true*. Cela va configurer le plug-in d'entrée telegraf pour ignorer la vérification. Sinon, l'utilisateur peut configurer le kubelet pour "ServerTLSBootstrap", qui déclenchera une demande de certificat à partir de l'API 'certificates.k8s.io'.

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données Memcached

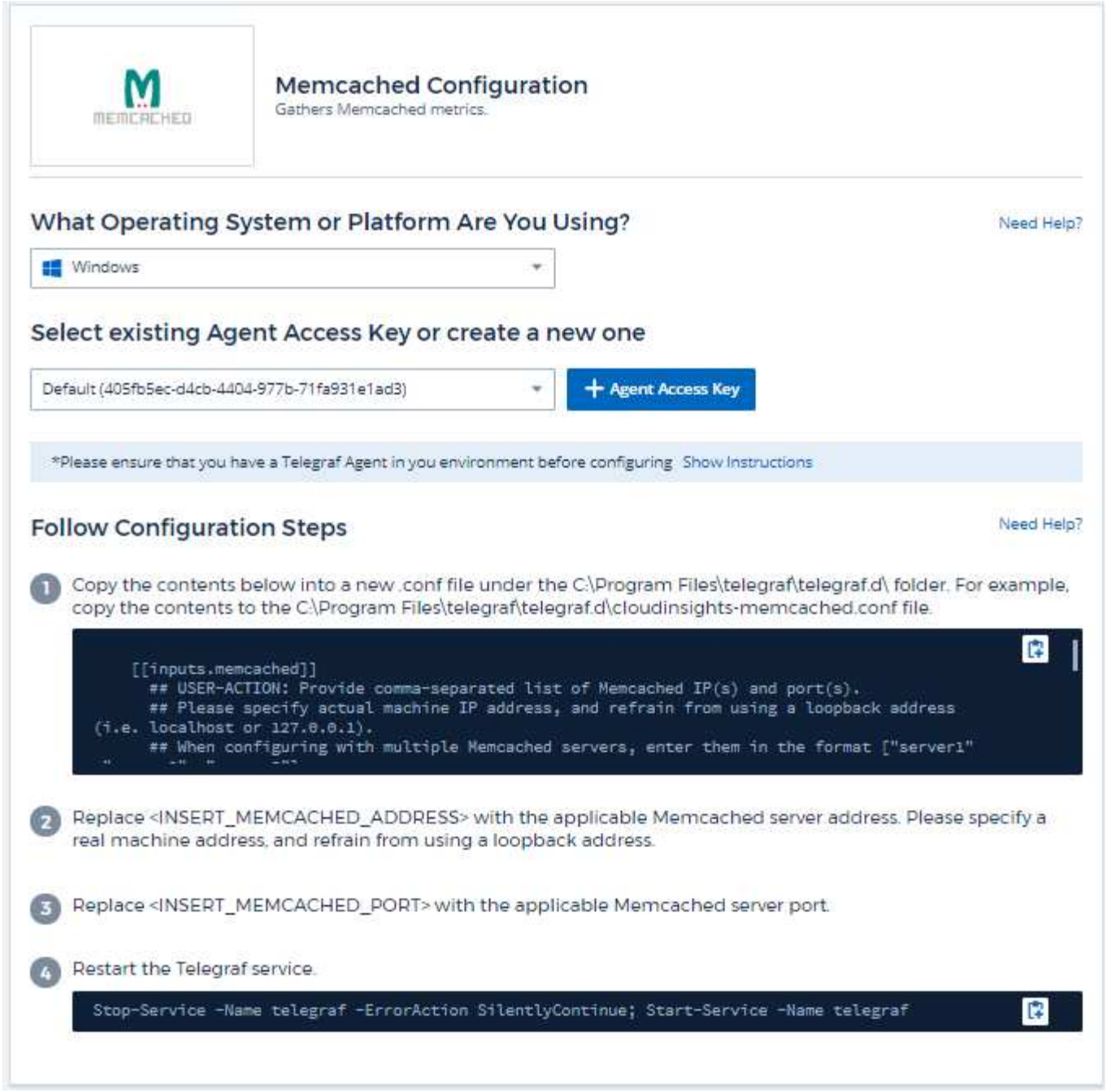
Data Infrastructure Insights utilise ce collecteur de données pour collecter des mesures à partir de Memcached.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Sélectionnez Memcached.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un 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 les "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 à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
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 utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans le "Wiki Memcached".

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
Mise en mémoire cache	Serveur d’espace de noms	Nom du nœud IP du nœud	Acceptation des connexions traitées demandes d’authentification échouées octets utilisés octets lus (par seconde) octets écrits (par seconde) cas Banval cas Hits cas échecs rinçage cas demandes (par seconde) get Reqs (par seconde) set Reqs (par seconde) Touch Reqs (par seconde) rendements de connexion (par seconde) Structures de connexion Open Connections éléments stockés actuels demandes décr Hits (par seconde) demandes décr Hits (par seconde) demandes de suppression Hits (par seconde) demandes de suppression d’échecs (par seconde) éléments expulsés nombre d’expulsions valides nombre d’éléments expirés obtenir Hits (par seconde) échecs (par seconde) Hachage en octets utilisés le hachage est en train d’étendre le Hash Power Level Incr Requests (par seconde) demandes d’incr Hits (par seconde) nombre max octets d’écoute du serveur nombre de threads de travail récupérés Num désactivé nombre total de connexions ouvertes nombre total d’éléments stockés Touch Hits Touch Touch échecs du serveur Uptime

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données MongoDB

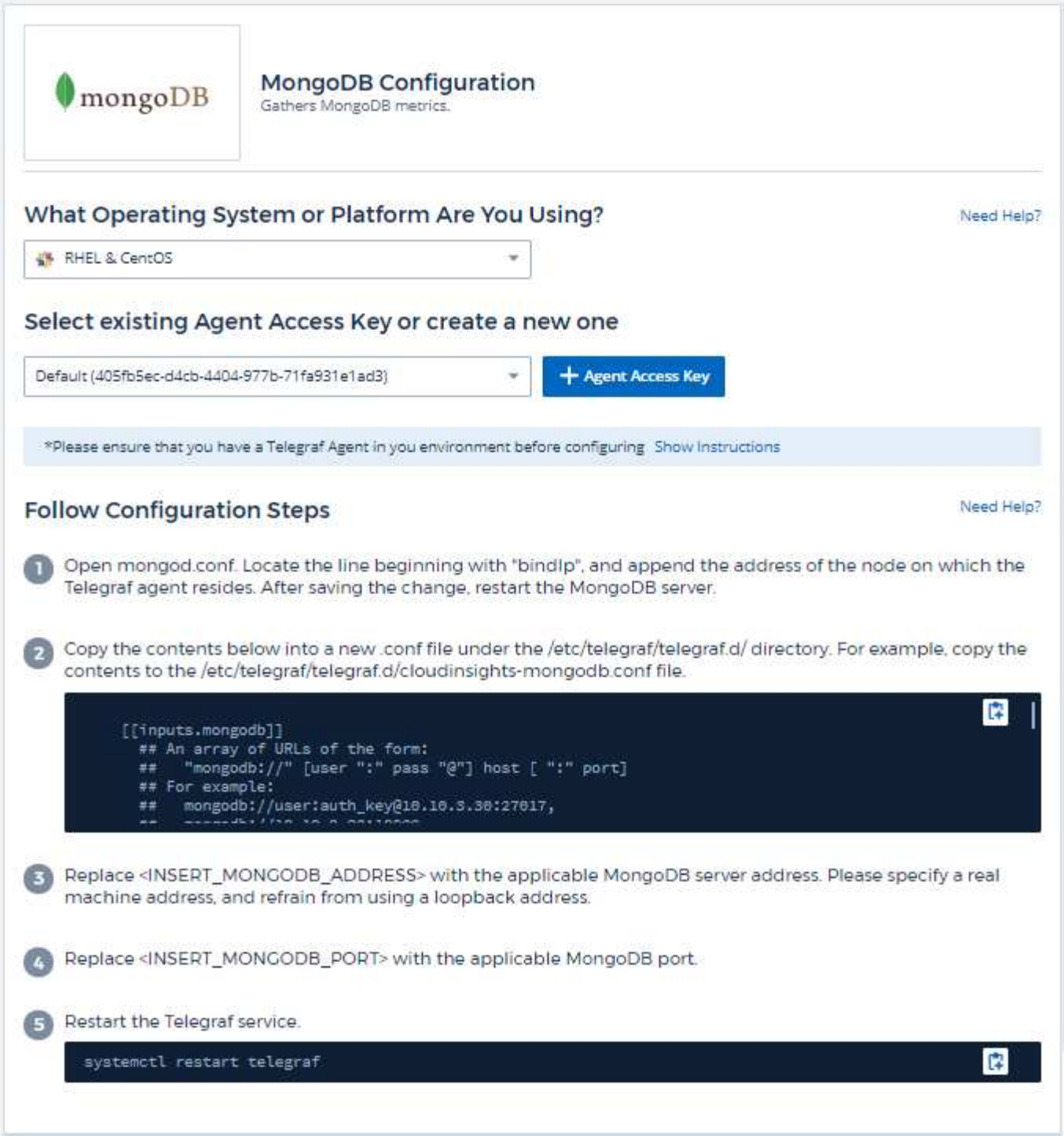
Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir de MongoDB.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez MongoDB.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un 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 les "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 à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
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 utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans le "Documentation MongoDB".

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
MongoDB	Nom d'hôte du namespace		
Base de données MongoDB	Nom d'hôte de l'espace de noms Nom de la		

Dépannage

Vous trouverez des informations à partir de la "Assistance" page.

Collecteur de données MySQL

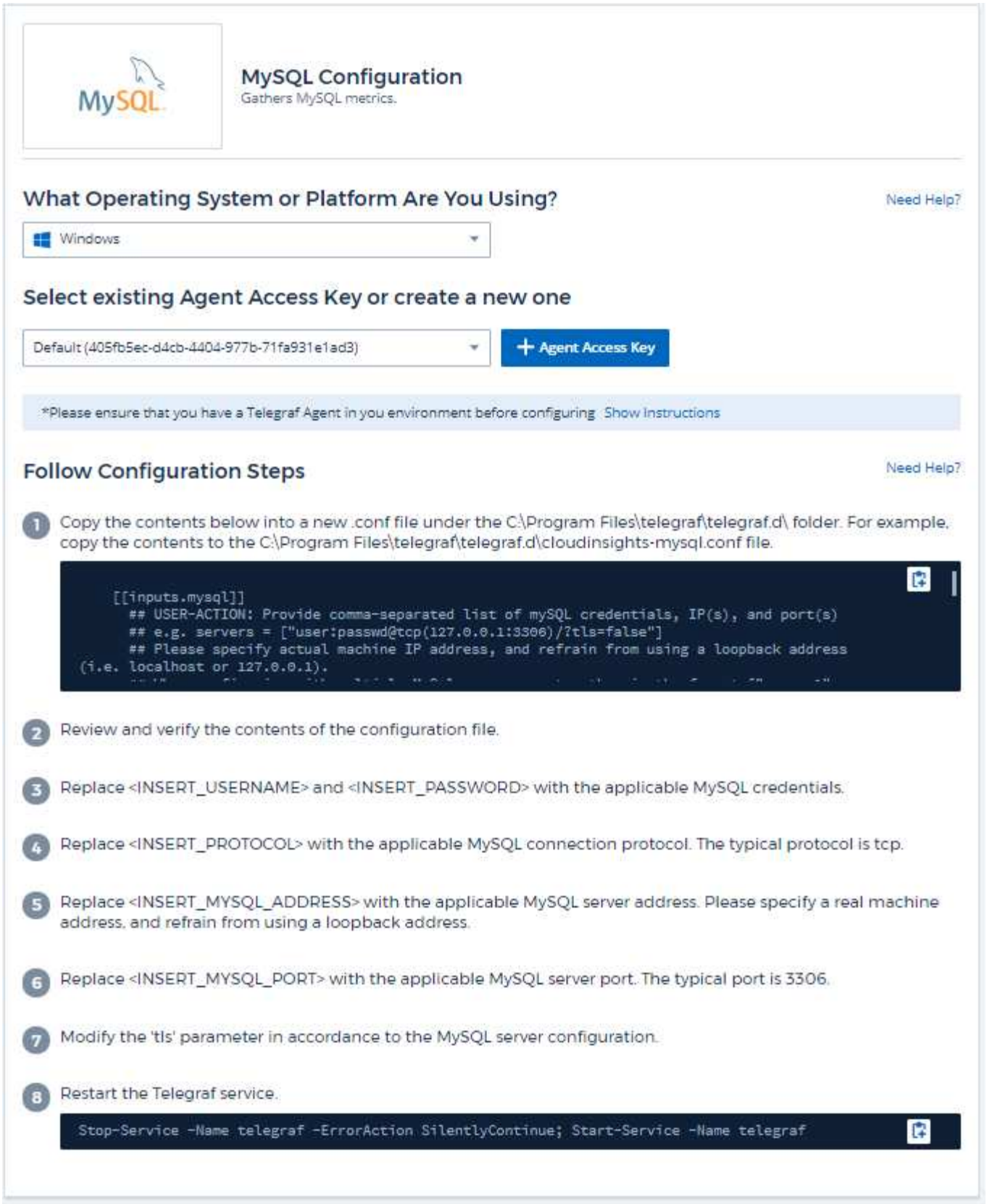
Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics de MySQL.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez MySQL.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un 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 les "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 à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
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 utilisé pour collecter des données.



Configuration

Vous trouverez des informations 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 serveur MySQL	Nom du nœud IP du nœud	Clients abandonnés (par seconde) connexions abandonnées (par seconde) RX Bytes (par seconde) TX Bytes (par seconde) commandes Admin (par seconde) Commandes ALTER Event commandes ALTER fonction commandes ALTER instance commandes ALTER procédure commandes ALTER Server commandes ALTER Table commandes ALTER Tablespace commandes ALTER User commandes Analyze commandes Assign to Keycache commandes Begin log procédure commandes change DB commandes change DB commandes change Master change Repl Filter commandes Check commandes Commandes de la somme de contrôle commandes d'archivage commandes de création de bases de données commandes de création d'événements commandes de création d'index commandes de procédure création de commandes de création de tableaux commandes de déclenchement création de commandes UDF création de commandes d'affichage commandes de DEALLOC erreurs de connexion SQL acceptent les tables de disques tmp erreurs retardées commandes de rinçage Gestionnaire de validation InnoDB tampon octets de pool de données blocs de clés non vidés clés demandes de lecture clés demandes d'écriture clé durée d'exécution max. Dépassée

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données netstat

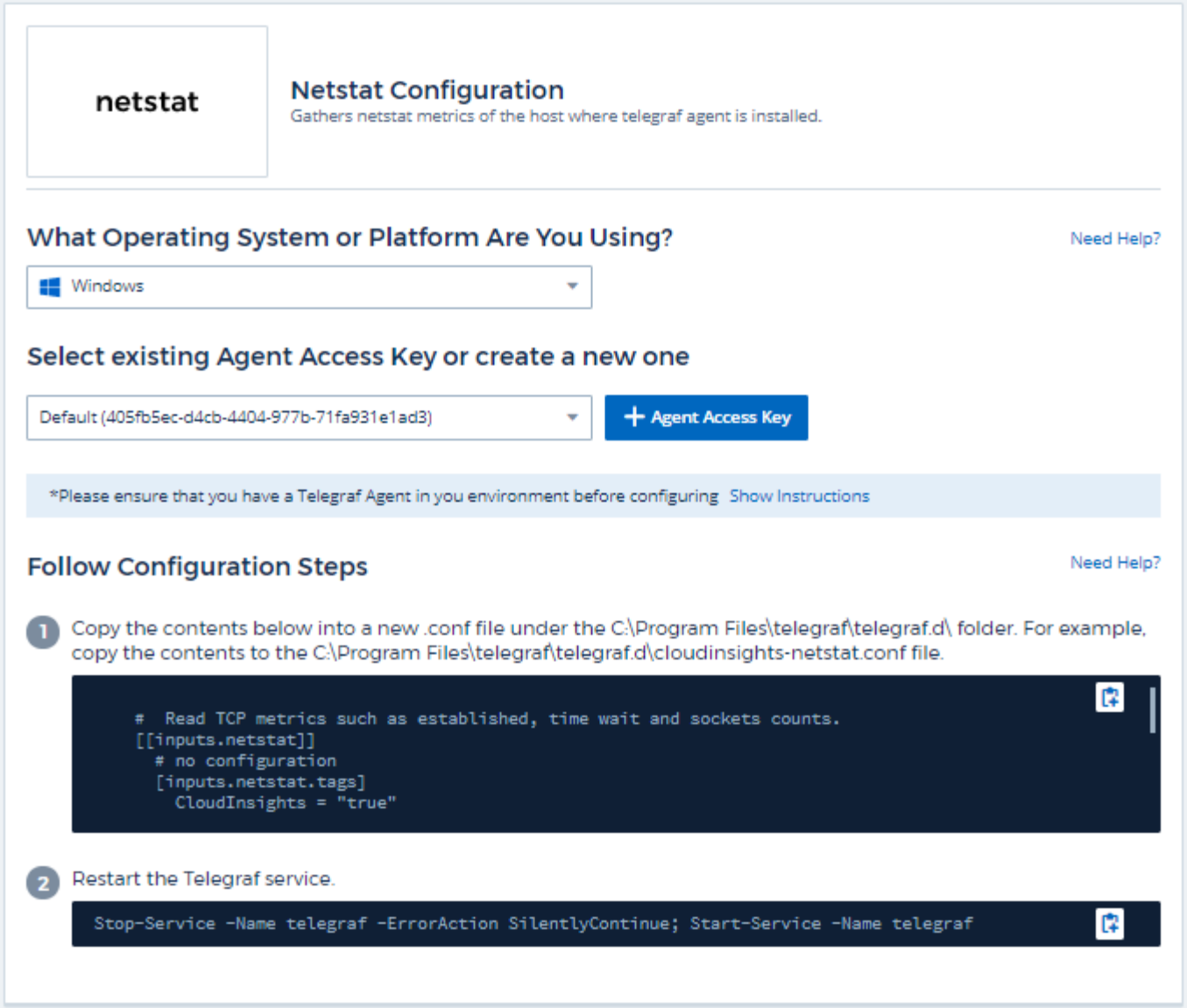
Data Infrastructure Insights utilise ce collecteur de données pour collecter les metrics Netstat.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Netstat.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un 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 les "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 à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
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 utilisé pour collecter des données.



Configuration

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
Netstat	UUID du nœud	Nom du nœud IP du nœud	

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données Nginx

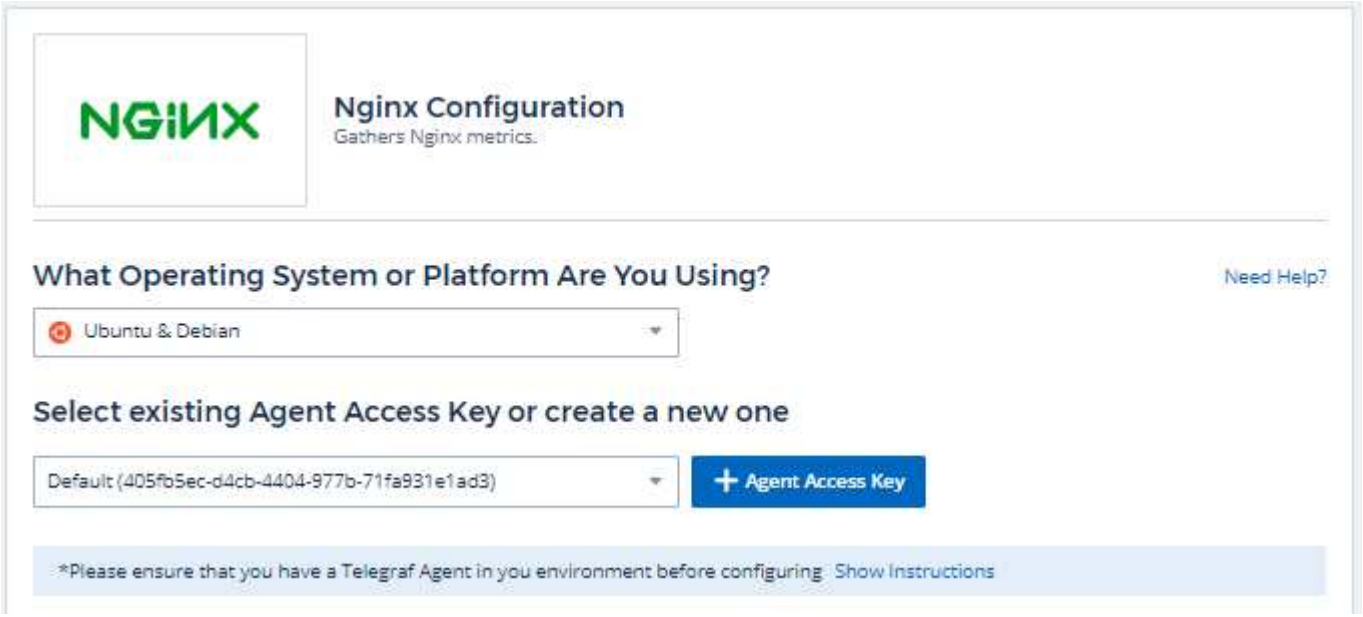
Data Infrastructure Insights utilise ce collecteur de données pour collecter les metrics de ce dernier.

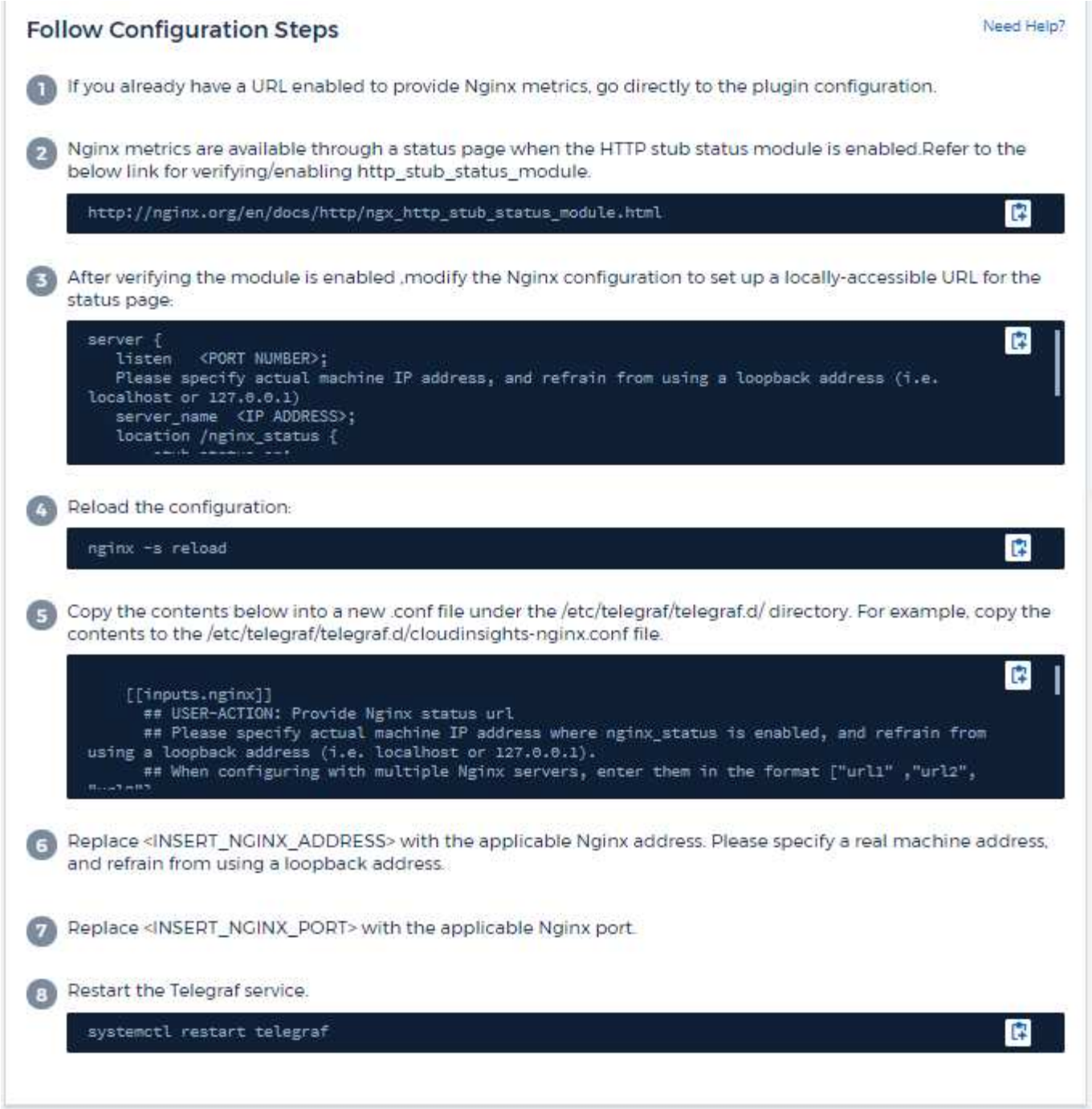
Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Nginx.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un 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 les "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 à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
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 utilisé pour collecter des données.





Configuration

La collecte des mesures NGINX requiert l'"http_stub_status_module"activation de ce dernier.

Vous trouverez des informations supplémentaires 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	Port du nom de nœud IP du nœud	Accepte les demandes de lecture traitées actives en attente d'écriture

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données PostgreSQL

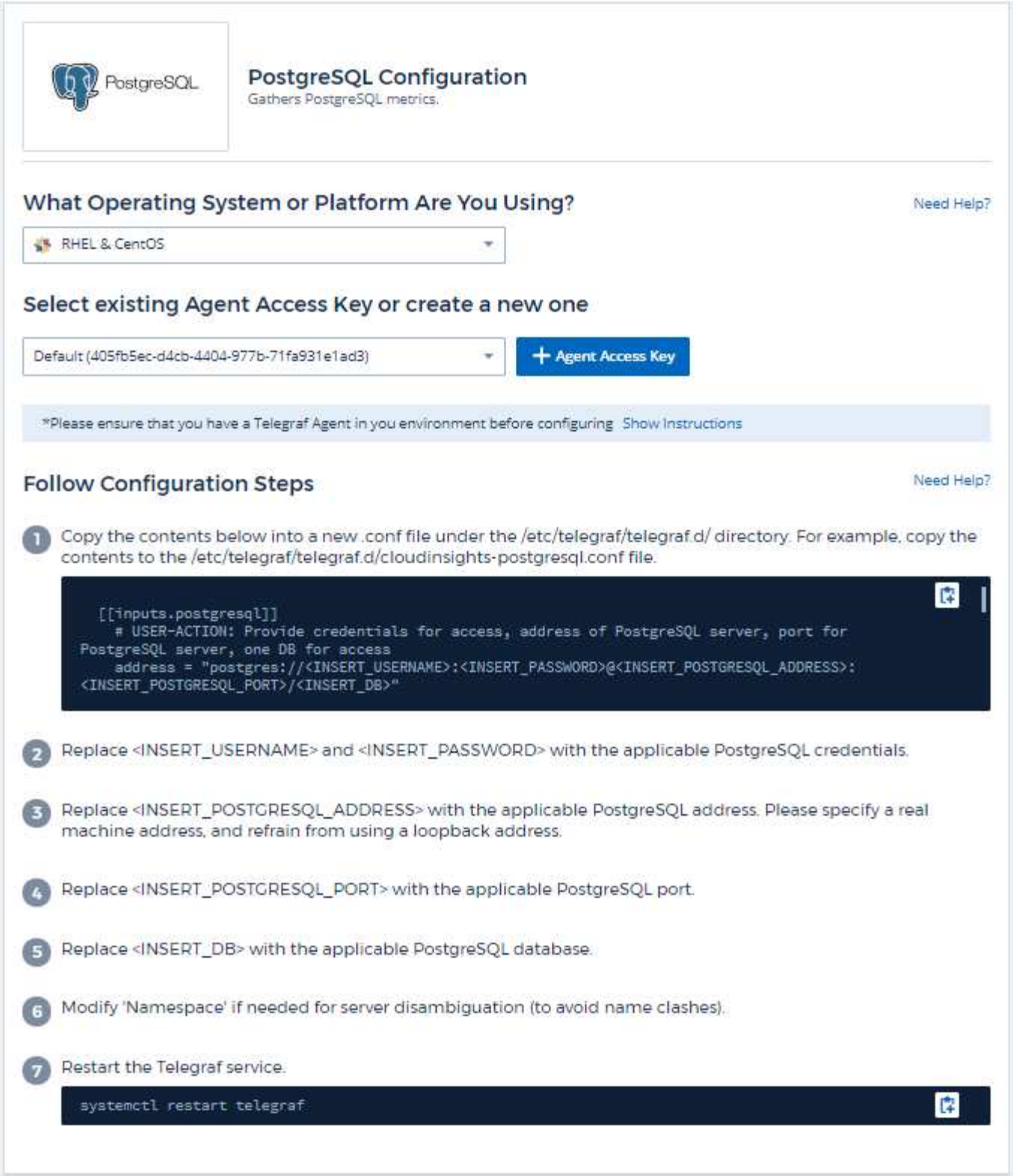
Data Infrastructure Insights utilise ce collecteur de données pour collecter les metrics de PostgreSQL.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez PostgreSQL.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un 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 les "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 à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
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 utilisé pour collecter des données.



Configuration

Vous trouverez des informations 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	IP du nœud de nom de nœud	Tampons alloués tampons tampons Backend Buffers Backend File Sync tampons point de contrôle tampon nettoyage points de contrôle temps de synchronisation points de contrôle temps d'écriture demandes points de contrôle délai maximum écriture nettoyage
Base de données PostgreSQL	Serveur de base de données d'espace de noms	ID objet de la base de données Nom du nœud IP	Blocs blocs de temps de lecture blocs de temps d'écriture nombre de blocs de lectures nombre de conflits nombre de fichiers temporaires octets fichiers temporaires nombre de lignes supprimées lignes extraites lignes extraites lignes retournées lignes retournées transactions mises à jour validées Rollened transactions

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données Puppet Agent

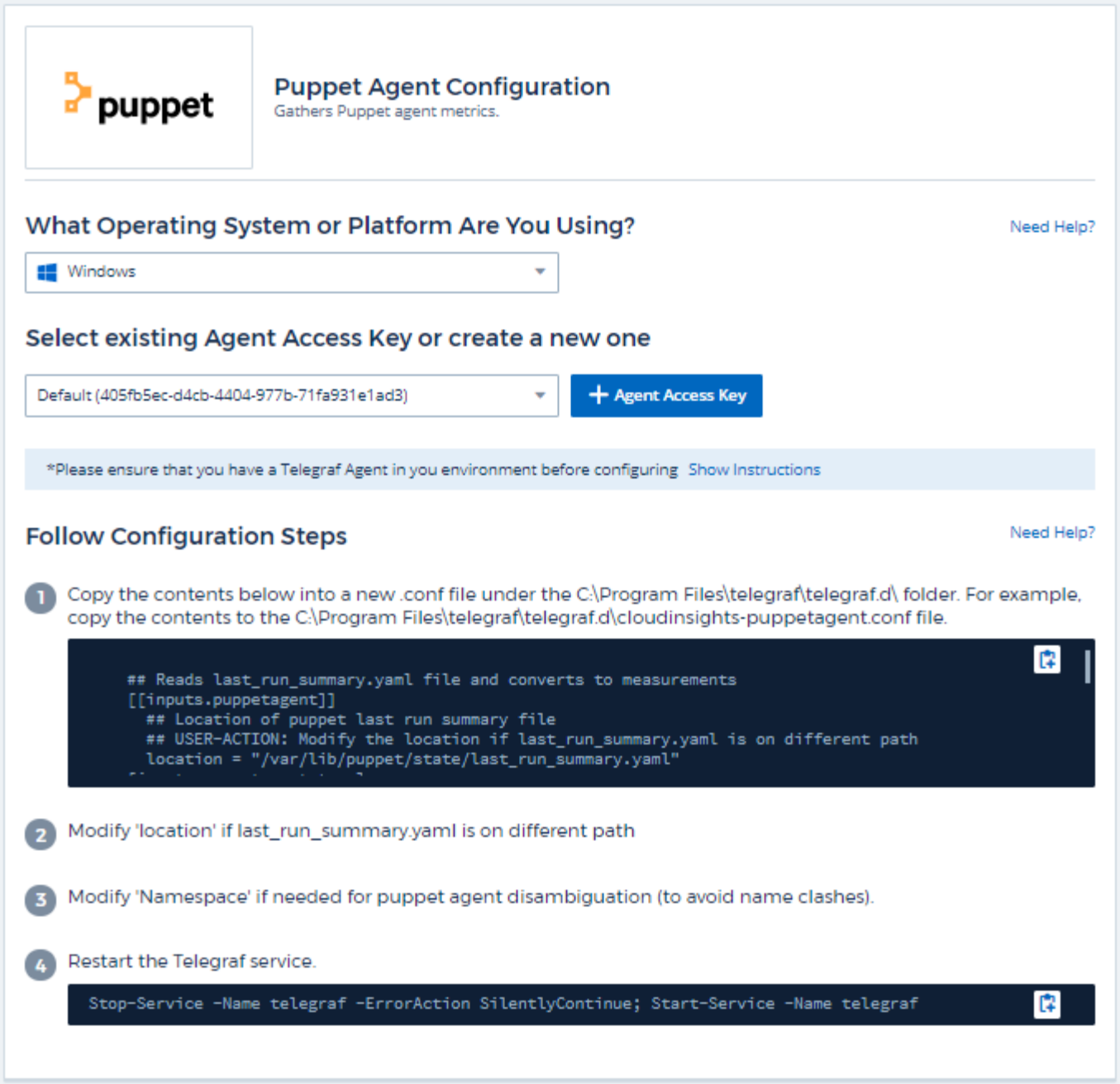
Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir de l'agent Puppet.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Puppet.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un 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 les "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 à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
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 utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans le "Documentation Puppet"

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :

Agent Puppet	UUID de nœud de namespace	Nom du nœud emplacement nœud version IP de la chaîne de configuration version Puppet	Changements Total des événements échec événements succès événements Total des ressources modifiées Ressources non modifiées Ressources non activées redémarrer les ressources désync Ressources redémarrées Ressources planifiées Ressources ignorées Ressources Total temps d'ancrage temps d'extraction temps d'extraction Cron Time Exec Time File Time Filebucket Time LASTRUN temps temps du temps du temps du temps de service Sshauthorizedkey Time Total Utilisateur de temps

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Redis Data Collector

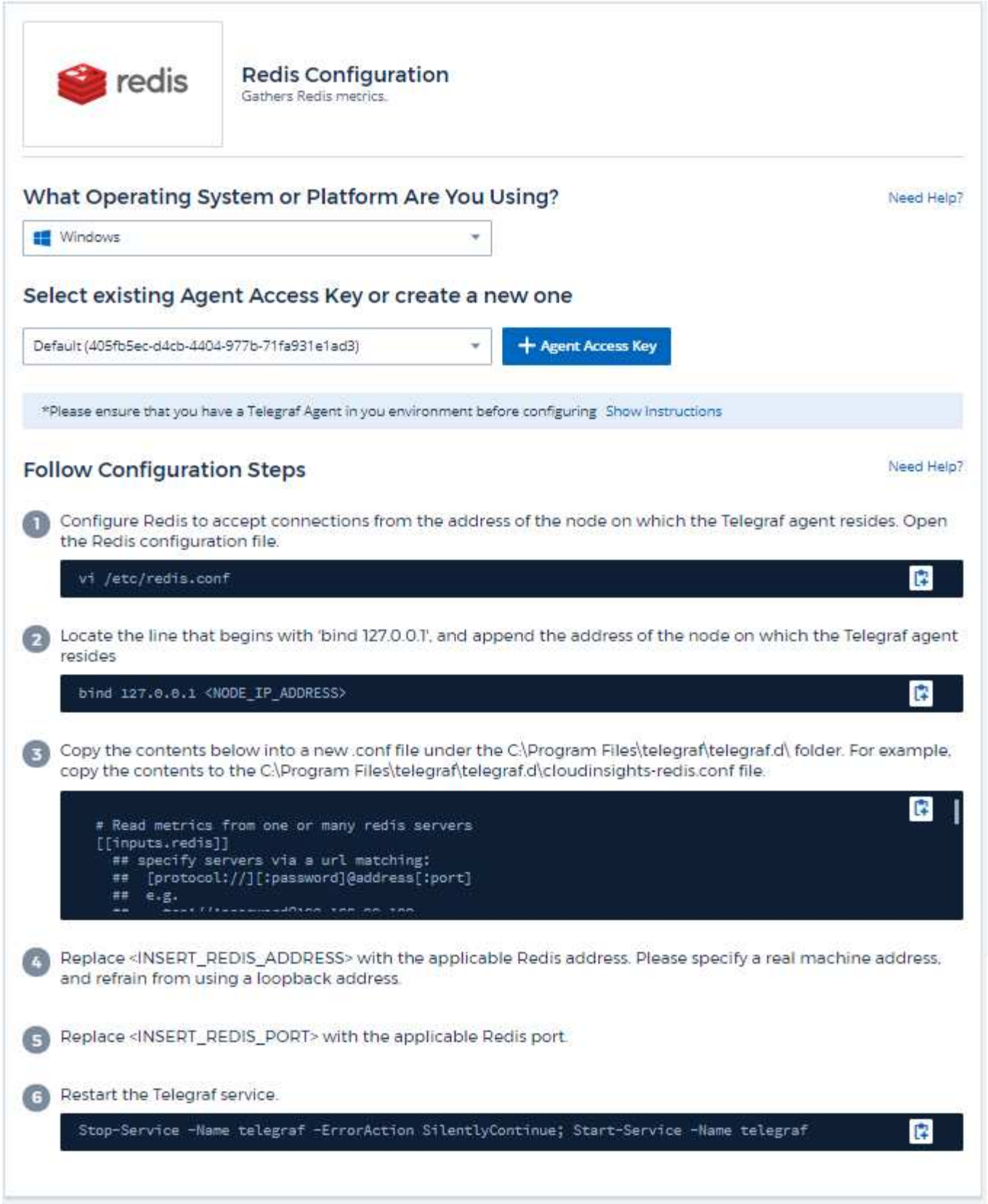
Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir de Redis. Redis est un magasin de structure de données in-memory open source utilisé comme base de données, cache, et courtier en messages, prenant en charge les structures de données suivantes : chaînes, hachages, listes, jeux, etc.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Redis.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un 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 les "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 à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
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 utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans le "Redis documentation".

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
Redis	Serveur d'espace de noms		

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

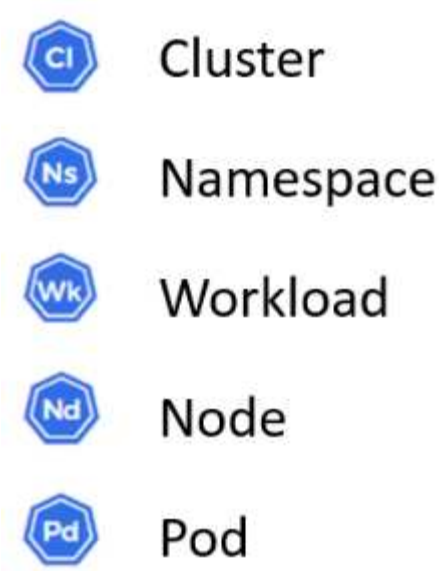
Référence de l'icône d'objet

Icônes d'objet utilisées dans Data Infrastructure Insights.

Icônes d'infrastructure :



Icônes Kubernetes :



Contrôle des performances du réseau Kubernetes et icônes de carte :



Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

Droits d’auteur

"https://www.netapp.com/company/legal/copyright/"

Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

"https://www.netapp.com/company/legal/trademarks/"

Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l’adresse suivante :

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politique de confidentialité

"https://www.netapp.com/company/legal/privacy-policy/"

Inclure:https://raw.githubusercontent.com/NetAppDocs/common/main/_include/open-source-notice-intro.adoc[]

"Avis concernant les informations concernant l’infrastructure de données (anciennement Cloud Insights)"

"Remarque concernant la sécurité des charges de travail (anciennement Cloud Secure)"

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.