



Administration et autres tâches

Data Infrastructure Insights

NetApp
February 11, 2026

Sommaire

Administration et autres tâches	1
API Data Infrastructure Insights	1
Conditions requises pour l'accès à l'API	1
Documentation de l'API (Swagger)	1
Jetons d'accès API	1
Type d'API	2
Parcours d'inventaire	3
S'agrandit	3
Données de performance	4
Mesures de performance des objets	5
Données d'historique des performances	5
Objets avec attributs de capacité	5
Utiliser la recherche pour rechercher des objets	6
Désactiver ou révoquer un jeton API	6
Rotation des jetons d'accès API expirés	6
Surveiller votre environnement	7
Audit	7
Digital Advisor Active IQ	11

Administration et autres tâches

API Data Infrastructure Insights

L'API Data Infrastructure Insights permet aux clients NetApp et aux fournisseurs de logiciels indépendants (ISV) d'intégrer Data Infrastructure Insights à d'autres applications, telles que CMDB ou d'autres systèmes de billetterie.

Vos Data Infrastructure Insights "rôle de l'ensemble de fonctionnalités" déterminera à quelles API vous pouvez accéder. Les rôles Utilisateur et Invité ont moins de priviléges que le rôle Administrateur. Par exemple, si vous disposez du rôle d'administrateur dans Surveiller et optimiser, mais du rôle d'utilisateur dans Rapports, vous pouvez gérer tous les types d'API à l'exception de l'entrepôt de données.

Conditions requises pour l'accès à l'API

- Un modèle de jeton d'accès API est utilisé pour accorder l'accès.
- La gestion des jetons API est effectuée par les utilisateurs de Data Infrastructure Insights avec le rôle d'administrateur.

Documentation de l'API (Swagger)

Les dernières informations sur l'API sont disponibles en vous connectant à Data Infrastructure Insights et en accédant à **Admin > Accès API**. Cliquez sur le lien **Documentation API**.

[Types d'API]

La documentation de l'API est basée sur Swagger, qui fournit une brève description et des informations d'utilisation de l'API et vous permet de l'essayer dans votre locataire. Selon votre rôle d'utilisateur et/ou votre édition de Data Infrastructure Insights, les types d'API disponibles peuvent varier.

[Exemple d'API Swagger]

Jetons d'accès API

Avant d'utiliser l'API Data Infrastructure Insights, vous devez créer un ou plusieurs **jetons d'accès API**. Les jetons d'accès sont utilisés pour des types d'API spécifiés et peuvent accorder des autorisations de lecture et/ou d'écriture. Vous pouvez également définir l'expiration de chaque jeton d'accès. Toutes les API sous les types spécifiés sont valides pour le jeton d'accès. Chaque jeton est dépourvu de nom d'utilisateur ou de mot de passe.

Pour créer un jeton d'accès :

- Cliquez sur **Admin > Accès API**
- Cliquez sur **+Jeton d'accès API**
 - Entrez le nom du jeton
 - Sélectionnez les types d'API
 - Spécifiez les autorisations accordées pour cet accès API
 - Spécifiez l'expiration du jeton

 Votre jeton ne sera disponible que pour la copie dans le presse-papiers et l'enregistrement pendant le processus de création. Les jetons ne peuvent pas être récupérés après leur création, il est donc fortement recommandé de copier le jeton et de l'enregistrer dans un endroit sûr. Vous serez invité à cliquer sur le bouton **Copier le jeton d'accès API** avant de pouvoir fermer l'écran de création de jeton.

Vous pouvez désactiver, activer et révoquer les jetons. Les jetons désactivés peuvent être activés.

Les jetons accordent un accès général aux API du point de vue du client ; ils gèrent l'accès aux API dans le cadre de leur propre locataire. Les administrateurs clients peuvent accorder et révoquer ces jetons sans intervention directe du personnel back-end de Data Infrastructure Insights .

L'application reçoit un jeton d'accès après qu'un utilisateur s'est authentifié et a autorisé l'accès avec succès, puis transmet le jeton d'accès comme identifiant lorsqu'il appelle l'API cible. Le jeton transmis informe l'API que le porteur du jeton a été autorisé à accéder à l'API et à effectuer des actions spécifiques spécifiées par la portée qui a été accordée lors de l'autorisation.

L'en-tête HTTP où le jeton d'accès est transmis est **X-CloudInsights-ApiKey**:

Par exemple, utilisez ce qui suit pour récupérer les ressources de stockage :

```
curl https://<tenant_host_name>/rest/v1/assets/storages -H 'X-CloudInsights-ApiKey:<API_Access_Token>'
```

Où _<API_Access_Token>_ est le jeton que vous avez enregistré lors de la création de l'accès à l'API.

Consultez les pages Swagger pour des exemples spécifiques à l'API que vous souhaitez utiliser.

Type d'API

L'API Data Infrastructure Insights est basée sur des catégories et contient actuellement les types suivants :

- Le type ASSETS contient des API d'actifs, de requêtes et de recherche.
 - Actifs : énumérer les objets de niveau supérieur et récupérer un objet spécifique ou une hiérarchie d'objets.
 - Requête : récupérez et gérez les requêtes Data Infrastructure Insights .
 - Importer : importer des annotations ou des applications et les affecter à des objets
 - Recherche : localisez un objet spécifique sans connaître l'ID unique ou le nom complet de l'objet.
- Le type COLLECTE DE DONNÉES est utilisé pour récupérer et gérer les collecteurs de données.
- Le type d'INGESTION DE DONNÉES est utilisé pour récupérer et gérer les données d'ingestion et les métriques personnalisées, telles que celles des agents Telegraf
- L'INGESTION DE JOURNAUX est utilisée pour récupérer et gérer les données de journaux

Des types et/ou API supplémentaires peuvent devenir disponibles au fil du temps. Vous pouvez trouver les dernières informations sur l'API dans le "[Documentation de l'API Swagger](#)" .

Notez que les types d'API auxquels un utilisateur a accès dépendent également de la "[Rôle de l'utilisateur](#)" ils ont dans chaque ensemble de fonctionnalités Data Infrastructure Insights (surveillance, sécurité de la charge de travail, reporting).

Parcours d'inventaire

Cette section décrit comment parcourir une hiérarchie d'objets Data Infrastructure Insights .

Objets de niveau supérieur

Les objets individuels sont identifiés dans les requêtes par une URL unique (appelée « self » en JSON) et nécessitent la connaissance du type d'objet et de son identifiant interne. Pour certains objets de niveau supérieur (hôtes, stockages, etc.), l'API REST donne accès à la collection complète.

Le format général d'une URL d'API est :

```
https://<tenant>/rest/v1/<type>/<object>
```

Par exemple, pour récupérer tous les stockages d'un locataire nommé `_mysite.c01.cloudinsights.netapp.com_`, l'URL de la requête est :

```
https://mysite.c01.cloudinsights.netapp.com/rest/v1/assets/storages
```

Enfants et objets apparentés

Les objets de niveau supérieur, tels que le stockage, peuvent être utilisés pour accéder à d'autres enfants et objets associés. Par exemple, pour récupérer tous les disques d'un stockage spécifique, concaténez l'URL « self » du stockage avec « /disks », par exemple :

```
https://<tenant>/rest/v1/assets/storages/4537/disks
```

S'agrandit

De nombreuses commandes API prennent en charge le paramètre **expand**, qui fournit des détails supplémentaires sur l'objet ou les URL des objets associés.

Le seul paramètre d'expansion commun est **expands**. La réponse contient une liste de toutes les extensions spécifiques disponibles pour l'objet.

Par exemple, lorsque vous demandez ce qui suit :

```
https://<tenant>/rest/v1/assets/storages/2782?expand=_expands
```

L'API renvoie toutes les extensions disponibles pour l'objet comme suit :

[développe l'exemple]

Chaque extension contient des données, une URL ou les deux. Le paramètre **expand** prend en charge plusieurs attributs imbriqués, par exemple :

```
https://<tenant>/rest/v1/assets/storages/2782?expand=performance,storageResources.storage
```

Développer vous permet d'intégrer de nombreuses données connexes dans une seule réponse. NetApp vous conseille de ne pas demander trop d'informations à la fois ; cela peut entraîner une dégradation des performances.

Pour décourager cela, les demandes de collections de niveau supérieur ne peuvent pas être étendues. Par exemple, vous ne pouvez pas demander l'extension des données pour tous les objets de stockage à la fois. Les clients doivent récupérer la liste des objets, puis choisir des objets spécifiques à développer.

Données de performance

Les données de performances sont collectées sur de nombreux appareils sous forme d'échantillons distincts. Toutes les heures (par défaut), Data Infrastructure Insights regroupe et résume les échantillons de performances.

L'API permet d'accéder à la fois aux échantillons et aux données résumées. Pour un objet avec des données de performances, un résumé des performances est disponible sous la forme `expand=performance`. Les séries chronologiques de l'historique des performances sont disponibles via `expand=performance.history` imbriqué.

Voici quelques exemples d'objets de données de performance :

- Performances de stockage
- Performances du pool de stockage
- Performances portuaires
- Performances du disque

Une mesure de performance possède une description et un type et contient une collection de résumés de performances. Par exemple, la latence, le trafic et le débit.

Un résumé des performances comporte une description, une unité, une heure de début d'échantillon, une heure de fin d'échantillon et un ensemble de valeurs résumées (actuelles, min, max, moyenne, etc.) calculées à partir d'un seul compteur de performances sur une plage de temps (1 heure, 24 heures, 3 jours, etc.).

[Exemple de performances d'API]

Le dictionnaire de données de performance résultant contient les clés suivantes :

- « self » est l'URL unique de l'objet
- « historique » est la liste des paires d'horodatages et de valeurs de compteurs
- Chaque autre clé du dictionnaire (« diskThroughput » et ainsi de suite) est le nom d'une mesure de performance.

Chaque type d'objet de données de performances possède un ensemble unique de mesures de performances. Par exemple, l'objet de performances de la machine virtuelle prend en charge « diskThroughput » comme mesure de performances. Chaque mesure de performance prise en charge appartient à une certaine « performanceCategory » présentée dans le dictionnaire de mesures. Data Infrastructure Insights prend en charge plusieurs types de mesures de performances répertoriés plus loin dans ce document. Chaque dictionnaire de mesures de performance comportera également le champ « description », qui est une

description lisible par l'homme de cette mesure de performance et un ensemble d'entrées de compteur de résumé de performance.

Le compteur Résumé des performances est le résumé des compteurs de performances. Il présente des valeurs agrégées typiques telles que min, max et moyenne pour un compteur, ainsi que la dernière valeur observée, la plage horaire pour les données résumées, le type d'unité pour le compteur et les seuils pour les données. Seuls les seuils sont facultatifs ; le reste des attributs est obligatoire.

Des résumés de performances sont disponibles pour ces types de compteurs :

- Lecture – Résumé des opérations de lecture
- Écriture – Résumé des opérations d'écriture
- Total – Résumé de toutes les opérations. Elle peut être supérieure à la simple somme des lectures et des écritures ; elle peut inclure d'autres opérations.
- Total Max – Résumé de toutes les opérations. Il s'agit de la valeur totale maximale dans la plage de temps spécifiée.

Mesures de performance des objets

L'API peut renvoyer des métriques détaillées pour les objets de votre locataire, par exemple :

- Mesures de performances de stockage telles que les IOPS (nombre de requêtes d'entrée/sortie par seconde), la latence ou le débit.
- Mesures de performances du commutateur, telles que l'utilisation du trafic, les données BB Credit Zero ou les erreurs de port.

Voir le "[Documentation de l'API Swagger](#)" pour obtenir des informations sur les métriques pour chaque type d'objet.

Données d'historique des performances

Les données d'historique sont présentées dans les données de performances sous la forme d'une liste de paires de cartes d'horodatage et de compteur.

Les compteurs d'historique sont nommés en fonction du nom de l'objet de mesure de performances. Par exemple, l'objet de performance de la machine virtuelle prend en charge « diskThroughput », de sorte que la carte d'historique contiendra des clés nommées « diskThroughput.read », « diskThroughput.write » et « diskThroughput.total ».



L'horodatage est au format horaire UNIX.

Voici un exemple de données de performances JSON pour un disque :

[Performances du disque JSON]

Objets avec attributs de capacité

Les objets avec des attributs de capacité utilisent des types de données de base et CapacityItem pour la représentation.

CapacitéArticle

CapacityItem est une unité logique unique de capacité. Il a une « valeur » et un « seuil élevé » dans les unités définies par son objet parent. Il prend également en charge une carte de répartition facultative qui explique comment la valeur de capacité est construite. Par exemple, la capacité totale d'un pool de stockage de 100 To serait un CapacityItem avec une valeur de 100. La répartition peut montrer 60 To alloués aux « données » et 40 To aux « instantanés ».

Remarque : « highThreshold » représente les seuils définis par le système pour les mesures correspondantes, qu'un client peut utiliser pour générer des alertes ou des repères visuels sur les valeurs qui sont hors des plages configurées acceptables.

L'exemple suivant montre la capacité des StoragePools avec plusieurs compteurs de capacité :

[Exemple de capacité de pool de stockage]

Utiliser la recherche pour rechercher des objets

L'API de recherche est un point d'entrée simple vers le système. Le seul paramètre d'entrée de l'API est une chaîne de forme libre et le JSON résultant contient une liste catégorisée de résultats. Les types sont des types d'actifs différents de l'inventaire, tels que les stockages, les hôtes, les magasins de données, etc. Chaque type contiendrait une liste d'objets du type correspondant aux critères de recherche.

Data Infrastructure Insights est une solution extensible (largement ouverte) qui permet des intégrations avec des systèmes d'orchestration, de gestion d'entreprise, de contrôle des modifications et de billetterie tiers ainsi que des intégrations CMDB personnalisées.

L'API RESTful de Cloud Insight est un point d'intégration principal qui permet un déplacement simple et efficace des données et permet aux utilisateurs d'accéder de manière transparente à leurs données.

Désactiver ou révoquer un jeton API

Pour désactiver temporairement un jeton API, sur la page de liste des jetons API, cliquez sur le menu « trois points » pour l'API et sélectionnez *Désactiver*. Vous pouvez réactiver le jeton à tout moment en utilisant le même menu et en sélectionnant *Activer*.

Pour supprimer définitivement un jeton API, dans le menu, sélectionnez « Révoquer ». Vous ne pouvez pas réactiver un jeton révoqué ; vous devez créer un nouveau jeton.

[Désactiver ou révoquer un jeton API]

Rotation des jetons d'accès API expirés

Les jetons d'accès API ont une date d'expiration. Lorsqu'un jeton d'accès API expire, les utilisateurs doivent générer un nouveau jeton (de type *Data Ingestion* avec des autorisations de lecture/écriture) et reconfigurer Telegraf pour utiliser le jeton nouvellement généré au lieu du jeton expiré. Les étapes ci-dessous détaillent comment procéder.

Kubernetes

Notez que ces commandes utilisent l'espace de noms par défaut « netapp-monitoring ». Si vous avez défini votre propre espace de noms, remplacez cet espace de noms dans ces commandes et fichiers et dans tous les suivants.

Remarque : si vous avez installé la dernière version de NetApp Kubernetes Monitoring Operator et que vous

utilisez un jeton d'accès API renouvelable, les jetons expirant seront automatiquement remplacés par des jetons d'accès API nouveaux/actualisés. Il n'est pas nécessaire d'effectuer les étapes manuelles répertoriées ci-dessous.

- Créez un nouveau jeton API.
- Suivez les étapes pour "[Mise à niveau manuelle](#)" , en sélectionnant le nouveau jeton API.

Remarque : les clients qui gèrent leur NetApp Kubernetes Monitoring Operator avec un outil de gestion de configuration, tel que Kustomize, peuvent suivre les mêmes étapes pour générer et télécharger un ensemble mis à jour de fichiers YAML à envoyer vers leur référentiel.

RHEL/CentOS et Debian/Ubuntu

- Modifiez les fichiers de configuration Telegraf et remplacez toutes les instances de l'ancien jeton API par le nouveau jeton API.

```
sudo sed -i.bkup 's/<OLD_API_TOKEN>/<NEW_API_TOKEN>/g'  
/etc/telegraf/telegraf.d/*.conf  
* Redémarrez Telegraf.
```

```
sudo systemctl restart telegraf
```

Windows

- Pour chaque fichier de configuration Telegraf dans *C:\Program Files\telegraf\telegraf.d*, remplacez toutes les instances de l'ancien jeton API par le nouveau jeton API.

```
cp <plugin>.conf <plugin>.conf.bkup  
(Get-Content <plugin>.conf).Replace('<OLD_API_TOKEN>',  
'<NEW_API_TOKEN>') | Set-Content <plugin>.conf
```

- Redémarrez Telegraf.

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

Surveiller votre environnement

Audit

Pour identifier les modifications attendues (pour le suivi) ou inattendues (pour le dépannage), vous pouvez afficher une piste d'audit des événements système et des activités des utilisateurs de Data Infrastructure Insights .

Affichage des événements audités

Pour afficher la page Audit, cliquez sur **Admin > Audit** dans le menu. La page Audit s'affiche, fournissant les détails suivants pour chaque entrée d'audit :

- **Heure** - Date et heure de l'événement ou de l'activité
- **Utilisateur** - L'utilisateur qui a initié l'activité
- **Rôle** - Le rôle de l'utilisateur dans Data Infrastructure Insights (invité, utilisateur, administrateur)
- **IP** - L'adresse IP associée à l'événement
- **Action** - Type d'activité, par exemple Connexion, Créer, Mettre à jour
- **Catégorie** - La catégorie d'activité
- **Détails** - Détails de l'activité

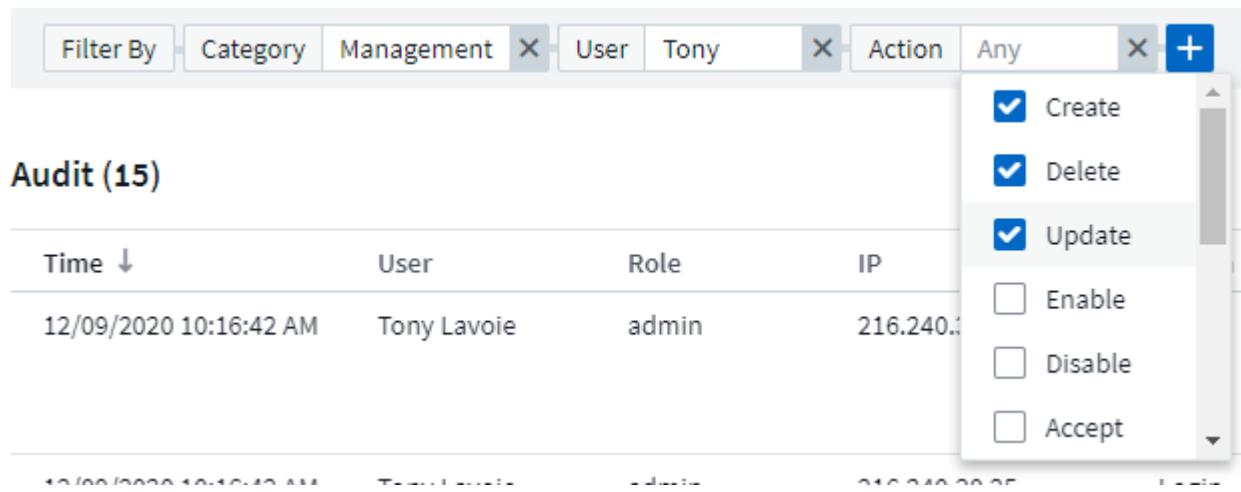
Affichage des entrées d'audit

Il existe plusieurs façons différentes d'afficher les entrées d'audit :

- Vous pouvez afficher les entrées d'audit en choisissant une période particulière (1 heure, 24 heures, 3 jours, etc.).
- Vous pouvez modifier l'ordre de tri des entrées en croissant (flèche vers le haut) ou décroissant (flèche vers le bas) en cliquant sur la flèche dans l'en-tête de la colonne.

Par défaut, le tableau affiche les entrées par ordre chronologique décroissant.

- Vous pouvez utiliser les champs de filtre pour afficher uniquement les entrées que vous souhaitez dans le tableau. Cliquez sur le bouton **[+]** pour ajouter des filtres supplémentaires.



The screenshot shows a table titled "Audit (15)" with columns: Time, User, Role, and IP. Above the table is a filter bar with "Filter By" and "Category Management" dropdowns, and a "User" dropdown set to "Tony". To the right of the table is a dropdown menu titled "Action" with the following options: Create (checked), Delete (checked), Update (checked), Enable (unchecked), Disable (unchecked), and Accept (unchecked).

Time ↓	User	Role	IP
12/09/2020 10:16:42 AM	Tony Lavoie	admin	216.240.1.100

En savoir plus sur le filtrage

Vous pouvez utiliser l'un des éléments suivants pour affiner votre filtre :

Filtre	Ce qu'il fait	Exemple	Résultat

* (Astérisque)	vous permet de rechercher tout ce que vous voulez	vol*rhel	renvoie toutes les ressources commençant par « vol » et se terminant par « rhel »
? (point d'interrogation)	vous permet de rechercher un nombre spécifique de caractères	BOS-PRD??-S12	renvoie BOS-PRD 12 -S12, BOS-PRD 23 -S12, et ainsi de suite
OU	vous permet de spécifier plusieurs entités	FAS2240 OU CX600 OU FAS3270	renvoie l'un des FAS2440, CX600 ou FAS3270
PAS	vous permet d'exclure du texte des résultats de recherche	NON EMC*	renvoie tout ce qui ne commence pas par « EMC »
Aucun	recherche vide/NULL/Aucun dans n'importe quel champ sélectionné	Aucun	renvoie les résultats lorsque le champ cible n'est pas vide
Pas *	comme avec <i>None</i> ci-dessus, mais vous pouvez également utiliser ce formulaire pour rechercher des valeurs NULL dans les champs <i>texte uniquement</i>	Pas *	renvoie les résultats lorsque le champ cible n'est pas vide.
""	recherche une correspondance exacte	"NetApp**"	renvoie des résultats contenant la chaîne littérale exacte <i>NetApp*</i>

Si vous placez une chaîne de filtre entre guillemets doubles, Insight traite tout ce qui se trouve entre le premier et le dernier guillemet comme une correspondance exacte. Tous les caractères spéciaux ou opérateurs à l'intérieur des guillemets seront traités comme des littéraux. Par exemple, le filtrage par « * » renverra des résultats qui sont un astérisque littéral ; l'astérisque ne sera pas traité comme un caractère générique dans ce cas. Les opérateurs OR et NOT seront également traités comme des chaînes littérales lorsqu'ils sont placés entre guillemets.

Événements et actions audités

Les événements et actions audités par Data Infrastructure Insights peuvent être classés dans les grands domaines suivants :

- **Compte utilisateur** : Connexion, déconnexion, changement de rôle, etc.
- **Unité d'acquisition** : créer, supprimer, etc.

Exemple : *Unité d'acquisition AU-Boston-1 supprimée.*

- **Collecteur de données** : ajouter, supprimer, modifier, reporter/reprendre, changer d'unité d'acquisition, démarrer/arrêter, etc.

Exemple : *Datasource * FlexPod Lab* supprimé, fournisseur * NetApp*, modèle * ONTAP Data Management Software*, IP 192.168.106.5.*

- **Application** : ajouter, affecter à un objet, supprimer, etc.

Exemple : *Volume interne ocisedev:t1appSVM01:t1appFlexVol01 ajouté à l'application Test App.*

- **Annotation** : ajouter, attribuer, supprimer, actions de règle d'annotation, modifications de valeur d'annotation, etc.

Exemple : *Valeur d'annotation Boston ajoutée au type d'annotation SalesOffice.*

- **Requête** : ajouter, supprimer, etc.

Exemple : *La requête TL Sales Query est ajoutée.*

- **Moniteur** : ajouter, supprimer, etc.

Exemple : *Surveiller Aggr Size - CI Alerts Notifications Dev mis à jour*

- **Notification** : changement d'email, etc.

Exemple : *Destinataire ci-alerts-notifications-dl créé*

Exportation des événements d'audit

Vous pouvez exporter les résultats de votre affichage d'audit vers un fichier .CSV, ce qui vous permettra d'analyser les données ou de les importer dans une autre application.

Étapes

1. Sur la page Audit, définissez la plage horaire souhaitée et les filtres souhaités. Data Infrastructure Insights exportera uniquement les entrées d'audit qui correspondent au filtrage et à la plage horaire que vous avez définis.
2. Cliquez sur le bouton Exporter  en haut à droite du tableau.

Les événements d'audit affichés seront exportés vers un fichier .CSV, jusqu'à un maximum de 10 000 lignes.

Conservation des données d'audit

La durée pendant laquelle Data Infrastructure Insights conserve les données d'audit dépend de votre abonnement :

- Environnements d'essai : les données d'audit sont conservées pendant 30 jours
- Environnements abonnés : les données d'audit sont conservées pendant 1 an plus 1 jour

Les entrées d'audit plus anciennes que la durée de conservation sont automatiquement purgées. Aucune interaction de l'utilisateur n'est nécessaire.

Les entrées d'audit plus anciennes que la durée de conservation sont automatiquement purgées. Aucune interaction de l'utilisateur n'est nécessaire.

Dépannage

Vous trouverez ici des suggestions pour résoudre les problèmes liés à Audit.

Problème:	Essayez ceci :
------------------	-----------------------

Je vois des messages d'audit m'indiquant qu'un moniteur a été exporté.

L'exportation d'une configuration de moniteur personnalisée est généralement utilisée par les ingénieurs NetApp lors du développement et des tests de nouvelles fonctionnalités. Si vous ne vous attendiez pas à voir ce message, pensez à explorer les actions de l'utilisateur nommé dans l'action auditée ou à contacter le support.

Digital Advisor Active IQ

NetApp "[Digital Advisor Active IQ](#)" (également connu sous le nom de Digital Advisor) fournit une série de visualisations, d'analyses et d'autres services liés au support aux clients NetApp pour leurs systèmes matériels/logiciels. Les données rapportées par Digital Advisor peuvent améliorer la résolution des problèmes système et également fournir un aperçu de l'optimisation et de l'analyse prédictive liées à vos appareils.

Data Infrastructure Insights collecte les **risques** pour tout système de stockage NetApp Clustered Data ONTAP surveillé et signalé par Digital Advisor. Les risques signalés pour les systèmes de stockage sont collectés automatiquement par Data Infrastructure Insights dans le cadre de sa collecte de données à partir de ces appareils. Vous devez ajouter le collecteur de données approprié à Data Infrastructure Insights pour collecter les informations sur les risques de Digital Advisor .

Data Infrastructure Insights n'affichera pas les données de risque pour les systèmes ONTAP qui ne sont pas surveillés et signalés par Digital Advisor.

Les risques signalés sont affichés dans Data Infrastructure Insights sur les pages de destination des actifs *storage* et *storage node*, dans le tableau « Risques ». Le tableau affiche les détails du risque, la catégorie de risque et l'impact potentiel du risque, et fournit également un lien vers la page Digital Advisor résumant tous les risques pour le nœud de stockage (connexion au compte de support NetApp requise).

Risks				
108 items found				
Object ↑	Risk Detail	Category	Potential Impact	Source
 tawny01	The following certificates have expired or are expiring within 30 days: Expired: 53CF9553, 53C504D4, 53D671B4, Expiring within 30 days: None	System Configuration	Clients may not be able to connect to the cluster over secure (SSL based) protocols.	 Active IQ <input checked="" type="checkbox"/>
 tawny01	None of the NIS servers configured for SVM(s) tawny_svm_ocl_mark can be contacted.	CIFS Protocol	Potential CIFS and NFS outages may occur.	 Active IQ <input checked="" type="checkbox"/>
 tawny01	ONTAP version 8.3.2 has entered the Self-Service Support period.	ONTAP	Self-Service Support is the time period where NetApp does not provide support for a version of a software product, but related documentation is still available on the NetApp Support Site.	 Active IQ <input checked="" type="checkbox"/>

Le nombre de risques signalés est également affiché dans le widget Résumé de la page de destination, avec un lien vers la page Digital Advisor appropriée. Sur une page de destination *stockage*, le décompte est la somme des risques de tous les nœuds de stockage sous-jacents.

Storage Summary		
Model: FAS6210	Microcode Version: 8.3.2 clustered Data ONTAP	Management: HTTPS://10.197.143.25:443
Vendor: NetApp	Raw Capacity: 80,024.3 GB	FC Fabrics Connected: 0
Family: FAS6200	Latency - Total: 0.77 ms	Performance Policies:
Serial Number: 1-80-000013	IOPS - Total: 1,819.19 IO/s	Risks: 108 risks detected by  Active IQ 
IP: 10.197.143.25	Throughput - Total: 41.69 MB/s	

Ouverture de la page du Digital Advisor

Lorsque vous cliquez sur le lien vers une page Digital Advisor , si vous n'êtes pas actuellement connecté à votre compte Digital Advisor , vous devez effectuer les étapes suivantes pour afficher la page Digital Advisor du nœud de stockage.

1. Dans le widget Résumé des Data Infrastructure Insights ou dans le tableau Risques, cliquez sur le lien «Digital Advisor».
2. Sign in à votre compte de support NetApp . Vous êtes redirigé directement vers la page du nœud de stockage dans Digital Advisor.

Interrogation sur les risques

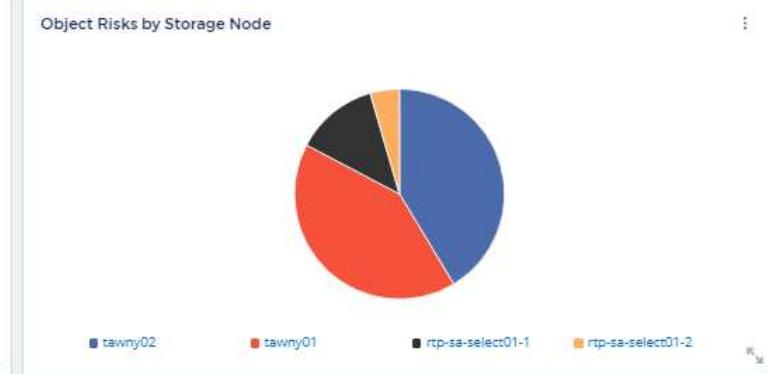
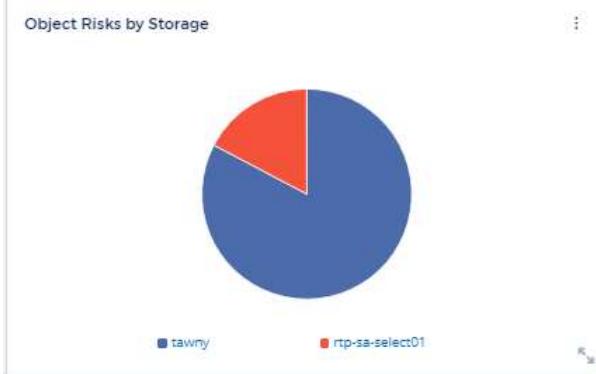
Dans Data Infrastructure Insights, vous pouvez ajouter la colonne **monitoring.count** à une requête de stockage ou de nœud de stockage. Si le résultat renvoyé inclut les systèmes de stockage surveillés par Digital Advisor, la colonne monitoring.count affichera le nombre de risques pour le système de stockage ou le nœud.

Tableaux de bord

Vous pouvez créer des widgets (par exemple, des graphiques à secteurs, des widgets de tableau, des widgets à barres, à colonnes, à nuages de points et à valeur unique) afin de visualiser les risques liés aux objets pour le stockage et les nœuds de stockage pour les systèmes NetApp Clustered Data ONTAP surveillés par Digital Advisor. « Risques d'objet » peut être sélectionné comme colonne ou métrique dans ces widgets où le stockage ou le nœud de stockage est l'objet de concentration.

Object Risks by Array	
12 items found	
Name	Object Risks ↓
tawny	110
rtp-sa-select01	23
rtp-sa-cl02	N/A
rtp-sa-cl07	N/A
oci-phonehome	N/A
durlabprdsfc01	N/A
oci-3070-01	N/A

Object Risks by Node	
25 items found	
Name	Object Risks ↓
tawny02	55
tawny01	55
rtp-sa-select01-1	17
rtp-sa-select01-2	6
tnode02	N/A
rtp-sa-cl06-01	N/A
rtp-sa-cl06-02	N/A



Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUSSANCE, 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.