Configuration d'Insight

OnCommand Insight

NetApp
October 24, 2024

Sommaire

Configuration d’Insight

Pour configurer Insight, vous devez activer les licences Insight, configurer vos sources de données, définir les utilisateurs et les notifications, activer les sauvegardes et effectuer toutes les étapes de configuration avancée requises.

Une fois le système OnCommand Insight installé, vous devez effectuer les tâches de configuration suivantes :

- Installez vos licences Insight.
- Configurez vos sources de données dans Insight.
- Configurer des comptes utilisateur.
- Configurez votre courrier électronique.
- Définissez vos notifications SNMP, par e-mail ou syslog, si nécessaire.
- Activez des sauvegardes hebdomadaires automatiques de votre base de données Insight.
- Effectuez toutes les étapes de configuration avancées requises, y compris la définition des annotations et des seuils.

Accès à l’interface utilisateur Web

Après avoir installé OnCommand Insight, vous devez installer vos licences, puis configurer Insight pour surveiller votre environnement. Pour ce faire, vous accédez à l’interface utilisateur web d’Insight à l’aide d’un navigateur web.

Étapes

1. Effectuez l’une des opérations suivantes :
    - Ouvrez Insight sur le serveur Insight :

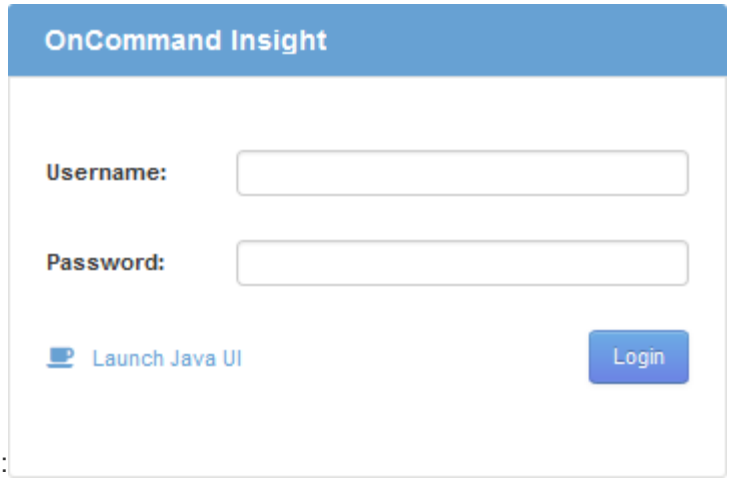
      `https://fqdn`

    - Ouvrez Insight depuis n’importe quel autre emplacement :

      `https://fqdn:port`

      Le numéro de port est 443 ou un autre port configuré lors de l’installation du serveur Insight. Le numéro de port par défaut est 443 si vous ne le spécifiez pas dans l’URL.

   La boîte de dialogue OnCommand Insight s’affiche



:

2. Entrez votre nom d'utilisateur et votre mot de passe, puis cliquez sur **connexion**.

   Si les licences ont été installées, la page de configuration de la source de données s'affiche.

   Une session du navigateur Insight inactive pendant 30 minutes est arrivée à expiration et vous êtes automatiquement déconnecté du système. Pour plus de sécurité, il est recommandé de fermer votre navigateur après vous être déconnecter d'Insight.

Installation de vos licences Insight

Après avoir reçu le fichier de licence contenant les clés de licence Insight de NetApp, vous pouvez utiliser les fonctionnalités d'installation pour installer toutes vos licences en même temps.

Description de la tâche

Les clés de licence Insight sont stockées dans un `.txt` ou `.lcn` fichier.

Étapes

1. Ouvrez le fichier de licence dans un éditeur de texte et copiez le texte.
2. Ouvrez Insight dans votre navigateur.
3. Dans la barre d'outils Insight, cliquez sur **Admin**.
4. Cliquez sur **Configuration**.
5. Cliquez sur l'onglet **licences**.
6. Cliquez sur **mettre à jour la licence**.
7. Copiez le texte de la clé de licence dans la zone de texte **License**.
8. Sélectionnez l'opération **Update (le plus courant)**.
9. Cliquez sur **Enregistrer**.
10. Si vous utilisez le modèle de licence Insight Consumption, vous devez cocher la case **Activer l'envoi des informations d'utilisation à NetApp** dans la section **Envoyer les informations d'utilisation**. Le proxy doit être correctement configuré et activé pour votre environnement.

Une fois que vous avez terminé

Après avoir installé les licences, vous pouvez effectuer les tâches de configuration suivantes :

- Configurer les sources de données.
- Créez des comptes utilisateur OnCommand Insight.

Licences OnCommand Insight

OnCommand Insight fonctionne avec des licences qui activent des fonctionnalités spécifiques sur le serveur Insight.

- **Découverte**

  La fonctionnalité de découverte est la licence Insight de base qui prend en charge l'inventaire. Vous devez disposer d'une licence Discover pour utiliser OnCommand Insight et la licence Discover doit être associée à au moins une des licences assure, Perform ou Plan.

- **Assure**

  Une licence assure prend en charge la fonctionnalité assurance, y compris les règles de chemin SAN et global, ainsi que la gestion des violations. Une licence assure vous permet également d'afficher et de gérer les vulnérabilités.

- **Exécuter**

  Une licence Perform prend en charge la surveillance des performances sur les pages d'actifs, les widgets de tableau de bord, les requêtes, etc., ainsi que la gestion des stratégies de performances et des violations.

- **Plan**

  Une licence Plan prend en charge les fonctions de planification, y compris l'utilisation et l'allocation des ressources.

- **Host Utilization Pack**

  Une licence Host Utilization prend en charge l'utilisation du système de fichiers sur les hôtes et les machines virtuelles.

- **Création de rapports**

  Une licence de création de rapports prend en charge des auteurs supplémentaires pour la création de rapports. Cette licence requiert la licence Plan.

Les modules OnCommand Insight font l'objet d'une licence annuelle ou perpétuelle :

- Par téraoctet de capacité surveillée pour les modules Discover, assure, Plan, Perform
- Par nombre d'hôtes pour le pack d'utilisation d'hôte
- Par nombre d'unités supplémentaires de Cognos pro-auteurs requises pour la création de rapports

Les clés de licence sont un ensemble de chaînes uniques générées pour chaque client. Vous pouvez obtenir les clés de licence auprès de votre représentant OnCommand Insight.

Vos licences installées contrôlent les options suivantes disponibles dans le logiciel :

- **Découverte**

  Acquisition et gestion des stocks (base)

  Surveiller les modifications et gérer les stratégies d'inventaire

- **Assure**

  Affichage et gestion des violations et des stratégies de chemin SAN

  Affichez et gérez les vulnérabilités

  Afficher et gérer les tâches et les migrations

- **Plan**

  Afficher et gérer les demandes

  Afficher et gérer les tâches en attente

  Afficher et gérer les violations de réservation

  Afficher et gérer les violations de l'équilibrage des ports

- **Exécuter**

  Surveillez les données de performances, y compris les données des widgets de tableau de bord, des pages d'actifs et des requêtes

  Affichez et gérez les règles de performances et les violations

Les tableaux suivants fournissent des détails sur les fonctions disponibles avec et sans la licence Perform pour les utilisateurs admin et non-admin.

Fonctionnalité (admin)	Avec licence Perform	Sans licence Perform
Client supplémentaire	Oui.	Pas de données ou de graphiques de performances
Ordinateur virtuel	Oui.	Pas de données ou de graphiques de performances
Hyperviseur	Oui.	Pas de données ou de graphiques de performances
Hôte	Oui.	Pas de données ou de graphiques de performances
Datastore	Oui.	Pas de données ou de graphiques de performances

VMDK	Oui.	Pas de données ou de graphiques de performances
Volume interne	Oui.	Pas de données ou de graphiques de performances
Volumétrie	Oui.	Pas de données ou de graphiques de performances
Pool de stockage	Oui.	Pas de données ou de graphiques de performances
Disque	Oui.	Pas de données ou de graphiques de performances
Stockage	Oui.	Pas de données ou de graphiques de performances
Nœud de stockage	Oui.	Pas de données ou de graphiques de performances
Structure	Oui.	Pas de données ou de graphiques de performances
Port du commutateur	Oui.	Pas de données de performances ni de graphiques ; « erreurs de port » indique « N/A »
Port de stockage	Oui.	Oui.
Port NPV	Oui.	Pas de données ou de graphiques de performances
Commutateur	Oui.	Pas de données ou de graphiques de performances
Commutateur NPV	Oui.	Pas de données ou de graphiques de performances
Qtrees	Oui.	Pas de données ou de graphiques de performances
Quota	Oui.	Pas de données ou de graphiques de performances
Chemin	Oui.	Pas de données ou de graphiques de performances

Zone	Oui.	Pas de données ou de graphiques de performances
Membre de la zone	Oui.	Pas de données ou de graphiques de performances
Périphérique générique	Oui.	Pas de données ou de graphiques de performances
Bande	Oui.	Pas de données ou de graphiques de performances
Masquage	Oui.	Pas de données ou de graphiques de performances
Sessions ISCSI	Oui.	Pas de données ou de graphiques de performances
Portails réseau ICSI	Oui.	Pas de données ou de graphiques de performances
Recherche	Oui.	Oui.
Admin	Oui.	Oui.
Tableau de bord	Oui.	Oui.
Widgets	Oui.	Partiellement disponible (seuls les widgets ASSET, Query et admin sont disponibles)
Tableau de bord des violations	Oui.	Masqué
Tableau de bord des ressources	Oui.	Partiellement disponible (les widgets IOPS de stockage et IOPS de machine virtuelle sont masqués)
Gérer les règles de performance	Oui.	Masqué
Gérer les annotations	Oui.	Oui.
Gérer les règles d’annotation	Oui.	Oui.
Gestion des applications	Oui.	Oui.
Requêtes	Oui.	Oui.

Gérer les entités commerciales	Oui.	Oui.

Fonction	Utilisateur - avec licence Perform	Invité - avec licence Perform	Utilisateur - sans licence Perform	Invité - sans licence d'exécution
Tableau de bord des ressources	Oui.	Oui.	Partiellement disponible (les widgets IOPS de stockage et IOPS de machine virtuelle sont masqués)	Partiellement disponible (les widgets IOPS de stockage et IOPS de machine virtuelle sont masqués)
Tableau de bord personnalisé	Afficher uniquement (pas d'options de création, de modification ou d'enregistrement)	Afficher uniquement (pas d'options de création, de modification ou d'enregistrement)	Afficher uniquement (pas d'options de création, de modification ou d'enregistrement)	Afficher uniquement (pas d'options de création, de modification ou d'enregistrement)
Gérer les règles de performance	Oui.	Masqué	Masqué	Masqué
Gérer les annotations	Oui.	Masqué	Oui.	Masqué
Gestion des applications	Oui.	Masqué	Oui.	Masqué
Gérer les entités commerciales	Oui.	Masqué	Oui.	Masqué
Requêtes	Oui.	Afficher et modifier uniquement (pas d'option d'enregistrement)	Oui.	Afficher et modifier uniquement (pas d'option d'enregistrement)

Configuration et gestion des comptes utilisateur

Les comptes utilisateur, l'authentification utilisateur et l'autorisation utilisateur peuvent être définis et gérés de deux manières : dans le serveur LDAP (Lightweight Directory Access Protocol) Microsoft Active Directory (version 2 ou 3) ou dans une base de données utilisateur OnCommand Insight interne. Le fait d'avoir un compte utilisateur différent pour chaque personne permet de contrôler les droits d'accès, les préférences individuelles et la responsabilité. Utilisez un compte disposant de privilèges d'administrateur pour cette opération.

Avant de commencer

Vous devez avoir effectué les tâches suivantes :

- Installez vos licences OnCommand Insight.
- Attribuez un nom d'utilisateur unique à chaque utilisateur.
- Déterminez les mots de passe à utiliser.
- Attribuez les rôles d'utilisateur appropriés.

Si vous importez un certificat LDAP et que vous avez modifié les mots de passe *Server.keystore* et/ou *Server.trustore* à l'aide de "admin sécurité", redémarrez le service *SANscreen* avant d'importer le certificat LDAP.

Les meilleures pratiques en matière de sécurité exigent que les administrateurs configurent le système d'exploitation hôte pour empêcher la connexion interactive d'utilisateurs non-administrateurs/standard.

Étapes

1. Ouvrez Insight dans votre navigateur.
2. Dans la barre d'outils Insight, cliquez sur **Admin**.
3. Cliquez sur **Configuration**.
4. Sélectionnez l'onglet **utilisateurs**.
5. Pour créer un nouvel utilisateur, cliquez sur le bouton **actions** et sélectionnez **Ajouter un utilisateur**.

   Entrez l'adresse **Nom**, **Mot de passe**, **E-mail** et sélectionnez l'un des utilisateurs **rôles** en tant qu'administrateur, utilisateur ou invité.

6. Pour modifier les informations d'un utilisateur, sélectionnez-le dans la liste et cliquez sur le symbole **Modifier le compte utilisateur** à droite de la description de l'utilisateur.
7. Pour supprimer un utilisateur du système OnCommand Insight, sélectionnez-le dans la liste et cliquez sur **Supprimer le compte utilisateur** à droite de la description de l'utilisateur.

Résultats

Lorsqu'un utilisateur se connecte à OnCommand Insight, le serveur tente d'abord de s'authentifier via LDAP, si LDAP est activé. Si OnCommand Insight ne parvient pas à localiser l'utilisateur sur le serveur LDAP, il recherche dans la base de données Insight locale.

Rôles d'utilisateur Insight

Chaque compte utilisateur se voit attribuer l'un des trois niveaux d'autorisation possibles.

- Le client vous permet de vous connecter à Insight et d'afficher les différentes pages.
- L'utilisateur autorise tous les privilèges de niveau invité, ainsi que l'accès aux opérations Insight, telles que la définition de règles et l'identification d'appareils génériques. Le type de compte utilisateur ne vous permet pas d'effectuer des opérations de source de données, ni d'ajouter ou de modifier des comptes utilisateur autres que le vôtre.

- Administrator vous permet d'effectuer n'importe quelle opération, y compris l'ajout de nouveaux utilisateurs et la gestion des sources de données.

Meilleure pratique : Limitez le nombre d'utilisateurs disposant d'autorisations d'administrateur en créant la plupart des comptes pour les utilisateurs ou les invités.

Configuration d'Insight pour LDAP(s)

OnCommand Insight doit être configuré avec les paramètres LDAP (Lightweight Directory Access Protocol), tels qu'ils sont configurés dans votre domaine LDAP d'entreprise.

Avant de configurer Insight pour une utilisation avec LDAP ou LDAP sécurisé (LDAPS), notez la configuration Active Directory dans votre environnement d'entreprise. Les paramètres Insight doivent correspondre à ceux de la configuration de domaine LDAP de votre entreprise. Lisez les concepts ci-dessous avant de configurer Insight pour une utilisation avec LDAP, et vérifiez auprès de votre administrateur de domaine LDAP les attributs appropriés à utiliser dans votre environnement.

Pour tous les utilisateurs de Secure Active Directory (LDAPS, par exemple), vous devez utiliser le nom du serveur AD tel qu'il est défini dans le certificat. Vous ne pouvez pas utiliser l'adresse IP pour la connexion AD sécurisée.

Si vous avez modifié les mots de passe *Server.keystore* et/ou *Server.trustore* à l'aide de "admin sécurité", redémarrez le service *SANscreen* avant d'importer le certificat LDAP.

OnCommand Insight prend en charge le protocole LDAP et LDAPS via le serveur Microsoft Active Directory ou Azure AD. D'autres implémentations LDAP peuvent fonctionner, mais n'ont pas été qualifiées à Insight. Les procédures décrites dans ces guides supposent que vous utilisez Microsoft Active Directory version 2 ou 3 LDAP (Lightweight Directory Access Protocol).

Nom principal de l'utilisateur attribut :

L'attribut Nom principal de l'utilisateur LDAP (userPrincipalName) est utilisé par Insight comme attribut username. Le nom principal de l'utilisateur est garanti pour être globalement unique dans une forêt Active Directory (AD), mais dans de nombreuses grandes organisations, le nom principal d'un utilisateur peut ne pas être immédiatement évident ou connu pour eux. Votre organisation peut utiliser une alternative à l'attribut Nom principal de l'utilisateur pour le nom d'utilisateur principal.

Voici quelques valeurs alternatives pour le champ d'attribut Nom principal d'utilisateur :

- **SAMAccountName**

  Cet attribut utilisateur est le nom d'utilisateur hérité pré-Windows 2000 NT - c'est ce que la plupart des utilisateurs sont habitués à se connecter à leur machine Windows personnelle. Cela n'est pas garanti pour être unique dans le monde entier dans une forêt d'AD.

  SAMAccountName est sensible à la casse pour l'attribut Nom principal de l'utilisateur.

- **mail**

  Dans les environnements AD avec MS Exchange, cet attribut est l'adresse e-mail principale de l'utilisateur final. Ceci devrait être globalement unique dans une forêt AD, (et également familier pour les utilisateurs finaux), contrairement à leur attribut userPrincipalName. L'attribut de courrier n'existera pas dans la plupart des environnements non MS Exchange.

- **référence**

  Une référence LDAP est une façon pour un contrôleur de domaine d'indiquer à une application client qu'elle ne dispose pas d'une copie d'un objet demandé (ou, plus précisément, qu'il ne contient pas la section de l'arborescence de répertoires où cet objet serait, s'il existe en fait) et donnant au client un emplacement qui est plus susceptible de contenir l'objet. Le client utilise à son tour la référence comme base de la recherche DNS d'un contrôleur de domaine. Idéalement, les référencements font toujours référence à un contrôleur de domaine qui détient effectivement l'objet. Cependant, il est possible que le contrôleur de domaine référencé génère encore une autre référence, bien qu'il ne prenne généralement pas de temps à découvrir que l'objet n'existe pas et à informer le client.

SAMAccountName est généralement préféré au nom principal de l'utilisateur. SAMAccountName est unique dans le domaine (bien qu'il ne soit pas unique dans la forêt de domaines), mais il s'agit de la chaîne que les utilisateurs du domaine utilisent généralement pour la connexion (par exemple,*netapp\username*). Le nom unique est le nom unique de la forêt, mais il n'est généralement pas connu des utilisateurs.

Dans la partie système Windows du même domaine, vous pouvez toujours ouvrir une invite de commande et saisir SET pour trouver le nom de domaine correct (USERDOMAIN=). Le nom de connexion OCI sera alors `USERDOMAIN\sAMAccountName`.

Pour le nom de domaine **mydomain.x.y.z.com**, utilisez `DC=x,DC=y,DC=z,DC=com` Dans le champ domaine de Insight.

Ports :

Le port par défaut pour LDAP est 389 et le port par défaut pour LDAPS est 636

URL type pour LDAPS : `ldaps://<ldap_server_host_name>:636`

Les journaux sont à :`\\<install directory>\SANscreen\wildfly\standalone\log\ldap.log`

Par défaut, Insight attend les valeurs notées dans les champs suivants. Si ces modifications sont apportées à votre environnement Active Directory, veillez à les modifier dans la configuration d'Insight LDAP.

Attribut de rôle
Membre
Attribut de courrier
e-mail
Attribut de nom unique
DistinguishedName
Référence

suivez

Groupes:

Pour authentifier les utilisateurs ayant des rôles d'accès différents dans les serveurs OnCommand Insight et DWH, vous devez créer des groupes dans Active Directory et entrer ces noms de groupe dans les serveurs OnCommand Insight et DWH. Les noms de groupe ci-dessous sont fournis à titre d'exemple uniquement. Les noms que vous configurez pour LDAP dans Insight doivent correspondre à ceux configurés pour votre environnement Active Directory.

Groupe Insight	Exemple
Groupe d'administrateurs du serveur Insight	insight.server.admins
Groupe d'administrateurs Insight	insight.administrateurs
Groupe d'utilisateurs Insight	insight.users
Groupe de clients Insight	insight.invités
Groupe d'administrateurs de rapports	insight.report.administrateurs
Groupe d'auteurs professionnels	insight.report.proauthors
Groupe d'auteurs de rapports	insight.report.business.authors
Groupe consommateurs déclareux	insight.report.business.consommateurs
Groupe de destinataires du rapport	insight.report.destinataires

Configuration des définitions utilisateur à l'aide de LDAP

Pour configurer le logiciel OnCommand Insight (OCI) pour l'authentification et l'autorisation des utilisateurs à partir d'un serveur LDAP, vous devez être défini dans le serveur LDAP en tant qu'administrateur du serveur OnCommand Insight.

Avant de commencer

Vous devez connaître les attributs d'utilisateur et de groupe qui ont été configurés pour Insight dans votre domaine LDAP.

Pour tous les utilisateurs de Secure Active Directory (LDAPS, par exemple), vous devez utiliser le nom du serveur AD tel qu'il est défini dans le certificat. Vous ne pouvez pas utiliser l'adresse IP pour la connexion AD sécurisée.

Si vous avez modifié les mots de passe *Server.keystore* et/ou *Server.trustore* à l'aide de "admin sécurité", redémarrez le service *SANscreen* avant d'importer le certificat LDAP.

Description de la tâche

OnCommand Insight prend en charge LDAP et LDAPS via le serveur Microsoft Active Directory. D'autres implémentations LDAP peuvent fonctionner, mais n'ont pas été qualifiées à Insight. Cette procédure suppose que vous utilisez Microsoft Active Directory version 2 ou 3 LDAP (Lightweight Directory Access Protocol).

Les utilisateurs LDAP s'affichent avec les utilisateurs définis localement dans la liste **Admin** > **Setup** › **Users**.

Étapes

1. Dans la barre d'outils Insight, cliquez sur **Admin**.
2. Cliquez sur **Configuration**.
3. Cliquez sur l'onglet **utilisateurs**.
4. Faites défiler jusqu'à la section LDAP.
5. Cliquez sur **Activer LDAP** pour autoriser l'authentification et l'autorisation de l'utilisateur LDAP.
6. Renseignez les champs suivants :

   - `LDAP servers`: Insight accepte une liste séparée par des virgules d'URL LDAP. Insight tente de se connecter aux URL fournies sans valider le protocole LDAP.

     Pour importer les certificats LDAP, cliquez sur **Certificates** et importez ou localisez automatiquement les fichiers de certificat.

     L'adresse IP ou le nom DNS utilisé pour identifier le serveur LDAP est généralement saisi dans ce format :

     ```
     ldap://<ldap-server-address>:port
     ```

     ou, si vous utilisez le port par défaut :

     ```
     ldap://<ldap-server-address>
     ```

     + Lorsque vous entrez plusieurs serveurs LDAP dans ce champ, assurez-vous que le numéro de port correct est utilisé dans chaque entrée.

   - `User name`: Saisissez les informations d'identification d'un utilisateur autorisé pour les requêtes de recherche d'annuaire sur les serveurs LDAP.
   - `Password`: Entrez le mot de passe de l'utilisateur ci-dessus. Pour confirmer ce mot de passe sur le serveur LDAP, cliquez sur **Valider**.
7. Si vous souhaitez définir cet utilisateur LDAP plus précisément, cliquez sur **Afficher plus** et remplissez les champs des attributs répertoriés.

   Ces paramètres doivent correspondre aux attributs configurés dans votre domaine LDAP. Vérifiez auprès de votre administrateur Active Directory si vous n'êtes pas sûr des valeurs à saisir pour ces champs.

   - **Groupe administrateurs**

     Groupe LDAP pour les utilisateurs disposant de privilèges d'administrateur Insight. La valeur par défaut

est `insight.admins`.

- **Groupe d'utilisateurs**

  Groupe LDAP pour les utilisateurs disposant de privilèges Insight User. La valeur par défaut est `insight.users`.

- **Groupe invités**

  Groupe LDAP pour les utilisateurs disposant de privilèges Insight Guest. La valeur par défaut est `insight.guests`.

- **Groupe d'administrateurs de serveurs**

  Groupe LDAP pour les utilisateurs disposant de privilèges d'administrateur Insight Server. La valeur par défaut est `insight.server.admins`.

- **Temporisation**

  Délai d'attente d'une réponse du serveur LDAP avant expiration, en millisecondes. la valeur par défaut est 2,000, ce qui est adéquat dans tous les cas et ne doit pas être modifié.

- **Domaine**

  Nœud LDAP sur lequel OnCommand Insight doit commencer à rechercher l'utilisateur LDAP. Il s'agit généralement du domaine de premier niveau de l'organisation. Par exemple :

  ```
  DC=<enterprise>,DC=com
  ```

- **Nom principal utilisateur attribut**

  Attribut qui identifie chaque utilisateur dans le serveur LDAP. La valeur par défaut est `userPrincipalName`, qui est globalement unique. OnCommand Insight tente de faire correspondre le contenu de cet attribut avec le nom d'utilisateur fourni ci-dessus.

- **Attribut de rôle**

  Attribut LDAP qui identifie l'adéquation de l'utilisateur au sein du groupe spécifié. La valeur par défaut est `memberOf`.

- **Attribut Mail**

  Attribut LDAP identifiant l'adresse e-mail de l'utilisateur. La valeur par défaut est `mail`. Ceci est utile si vous souhaitez vous abonner aux rapports disponibles auprès de OnCommand Insight. Insight récupère l'adresse e-mail de l'utilisateur la première fois que chaque utilisateur se connecte et ne la recherche pas après cela.

  > Si l'adresse e-mail de l'utilisateur change sur le serveur LDAP, veillez à la mettre à jour dans Insight.

- **Attribut de nom unique**

  Attribut LDAP identifiant le nom distinctif de l'utilisateur. la valeur par défaut est `distinguishedName`.

8. Cliquez sur **Enregistrer**.

Modification des mots de passe utilisateur

Un utilisateur disposant de privilèges d'administrateur peut modifier le mot de passe de tout compte d'utilisateur OnCommand Insight défini sur le serveur local.

Avant de commencer

Les éléments suivants doivent avoir été remplis :

- Notifications à toute personne se connectant au compte utilisateur que vous modifiez.
- Nouveau mot de passe à utiliser après cette modification.

Description de la tâche

Lorsque vous utilisez cette méthode, vous ne pouvez pas modifier le mot de passe d'un utilisateur validé via LDAP.

Étapes

1. Connectez-vous avec des privilèges d'administrateur.
2. Dans la barre d'outils Insight, cliquez sur **Admin**.
3. Cliquez sur **Configuration**.
4. Cliquez sur l'onglet **utilisateurs**.
5. Recherchez la ligne qui affiche le compte utilisateur que vous souhaitez modifier.
6. À droite des informations utilisateur, cliquez sur **Modifier le compte utilisateur**.
7. Saisissez le nouveau **Mot de passe**, puis saisissez-le à nouveau dans le champ de vérification.
8. Cliquez sur **Enregistrer**.

Modification d'une définition utilisateur

Un utilisateur disposant de privilèges d'administrateur peut modifier un compte d'utilisateur pour modifier l'adresse e-mail ou les rôles pour OnCommand Insight ou DWH et les fonctions de génération de rapports.

Avant de commencer

Déterminez le type de compte utilisateur (OnCommand Insight, DWH ou une combinaison) à modifier.

Description de la tâche

Pour les utilisateurs LDAP, vous ne pouvez modifier l'adresse e-mail qu'à l'aide de cette méthode.

Étapes

1. Connectez-vous avec des privilèges d'administrateur.
2. Dans la barre d'outils Insight, cliquez sur **Admin**.

3. Cliquez sur **Configuration**.
4. Cliquez sur l'onglet **utilisateurs**.
5. Recherchez la ligne qui affiche le compte utilisateur que vous souhaitez modifier.
6. À droite des informations utilisateur, cliquez sur l'icône **Modifier le compte utilisateur**.
7. Apportez les modifications nécessaires.
8. Cliquez sur **Enregistrer**.

Suppression d'un compte utilisateur

Tout utilisateur disposant de privilèges d'administrateur peut supprimer un compte utilisateur, soit lorsqu'il n'est plus utilisé (pour une définition d'utilisateur local), soit pour forcer OnCommand Insight à redécouvrir les informations utilisateur la prochaine fois que l'utilisateur se connecte (pour un utilisateur LDAP).

Étapes

1. Connectez-vous à OnCommand Insight avec des privilèges d'administrateur.
2. Dans la barre d'outils Insight, cliquez sur **Admin**.
3. Cliquez sur **Configuration**.
4. Cliquez sur l'onglet **utilisateurs**.
5. Recherchez la ligne qui affiche le compte utilisateur que vous souhaitez supprimer.
6. À droite des informations utilisateur, cliquez sur l'icône **Supprimer le compte utilisateur "x"**.
7. Cliquez sur **Enregistrer**.

Définition d'un message d'avertissement de connexion

OnCommand Insight permet aux administrateurs de définir un message texte personnalisé qui s'affiche lorsque les utilisateurs se connectent.

Étapes

1. Pour définir le message dans le serveur OnCommand Insight :
   a. Accédez au **Admin › Dépannage › Dépannage avancé › Paramètres avancés**.
   b. Saisissez votre message de connexion dans la zone de texte.
   c. Cochez la case **le client affiche le message d'avertissement de connexion**.
   d. Cliquez sur **Enregistrer**.

   Le message s'affiche lors de la connexion pour tous les utilisateurs.
2. Pour définir le message dans l'entrepôt de données (DWH) et le reporting (Cognos) :
   a. Accédez à **informations système** et cliquez sur l'onglet **Avertissement de connexion**.
   b. Saisissez votre message de connexion dans la zone de texte.
   c. Cliquez sur **Enregistrer**.

Le message s'affiche lors de la connexion à DWH et Cognos Reporting pour tous les utilisateurs.

Outil SecurityAdmin

OnCommand Insight fournit des fonctionnalités qui permettent aux environnements Insight de fonctionner avec une sécurité renforcée. Ces fonctionnalités comprennent le cryptage, le hachage de mot de passe et la possibilité de modifier les mots de passe des utilisateurs internes et les paires de clés qui chiffrent et déchiffrent les mots de passe. Vous pouvez gérer ces fonctionnalités sur tous les serveurs de l'environnement Insight à l'aide de **SecurityAdmin Tool**.

Qu'est-ce que l'outil SecurityAdmin ?

L'outil d'administration de la sécurité prend en charge les modifications apportées au contenu des coffres-forts ainsi que les modifications coordonnées apportées à l'installation de OnCommand Insight.

Les principales utilisations de l'outil SecurityAdmin sont **Backup** et **Restore** de la configuration de la sécurité (c'est-à-dire du coffre-fort) et des mots de passe. Par exemple, vous pouvez sauvegarder le coffre-fort sur une unité d'acquisition locale et le restaurer sur une unité d'acquisition distante, assurant ainsi la coordination des mots de passe dans l'ensemble de votre environnement. Ou si votre environnement comporte plusieurs serveurs OnCommand Insight, vous pouvez effectuer une sauvegarde du coffre-fort du serveur et le restaurer sur d'autres serveurs pour conserver les mêmes mots de passe. Ce ne sont que deux exemples de la façon dont SecurityAdmin peut être utilisé pour assurer la cohésion dans vos environnements.

Il est fortement recommandé de **sauvegarder le coffre-fort** chaque fois que vous sauvegardez une base de données OnCommand Insight. Le non-respect de cette consigne peut entraîner une perte d'accès.

L'outil fournit à la fois les modes **interactif** et **ligne de commande**.

De nombreuses opérations de l'outil SecurityAdmin modifient le contenu du coffre-fort et modifient également l'installation, en s'assurant que le coffre-fort et l'installation restent synchronisés.

Par exemple :

- Lorsque vous modifiez le mot de passe d'un utilisateur Insight, l'entrée de l'utilisateur dans le tableau SANscreen.users est mise à jour avec le nouveau hachage.
- Lorsque vous modifiez le mot de passe d'un utilisateur MySQL, l'instruction SQL appropriée est exécutée pour mettre à jour le mot de passe de l'utilisateur dans l'instance MySQL.

Dans certains cas, plusieurs modifications seront apportées à l'installation :

- Lorsque vous modifiez l'utilisateur MySQL dwh, en plus de mettre à jour le mot de passe dans la base de données MySQL, plusieurs entrées de registre pour ODBC seront également mises à jour.

Dans les sections suivantes, le terme « changements coordonnés » est utilisé pour décrire ces changements.

Modes d'exécution

- Fonctionnement normal/par défaut - le service serveur SANscreen doit être en cours d'exécution

Pour le mode d'exécution par défaut, l'outil SecurityAdmin requiert que le service **SANscreen Server** soit en cours d'exécution. Le serveur est utilisé pour l'authentification et de nombreuses modifications coordonnées de l'installation sont effectuées en appelant le serveur.

- Fonctionnement direct - le service serveur SANscreen peut être en cours d'exécution ou arrêté.

  Lorsqu'il est exécuté sur une installation d'OCI Server ou DWH, l'outil peut également être exécuté en mode « direct ». Dans ce mode, l'authentification et les modifications coordonnées sont effectuées à l'aide de la base de données. Le service serveur n'est pas utilisé.

  Le fonctionnement est le même que le mode normal, à l'exception des cas suivants :

- L'authentification est prise en charge uniquement pour les utilisateurs non administrateurs de domaine. (Utilisateurs dont le mot de passe et les rôles sont dans la base de données, et non LDAP).
- L'opération « remplacer les clés » n'est pas prise en charge.
- L'étape de re-chiffrement de la restauration du coffre-fort est ignorée.
- Mode de récupération l'outil peut également être exécuté même si l'accès au serveur et à la base de données n'est pas possible (par exemple parce que le mot de passe racine dans le coffre-fort est incorrect).

  Lorsqu'elle est exécutée dans ce mode, l'authentification n'est pas possible et, par conséquent, aucune opération avec une modification coordonnée de l'installation ne peut être effectuée.

  Le mode de récupération peut être utilisé pour :

- déterminez les entrées du coffre-fort incorrectes (à l'aide de l'opération de vérification)
- remplacez le mot de passe root incorrect par la valeur correcte. (Ceci ne modifie pas le mot de passe. L'utilisateur doit saisir le mot de passe actuel.)

> ⓘ Si le mot de passe root du coffre-fort est incorrect et que le mot de passe n'est pas connu et qu'il n'y a pas de sauvegarde du coffre-fort avec le mot de passe root correct, l'installation ne peut pas être récupérée à l'aide de l'outil SecurityAdmin. La seule façon de récupérer l'installation est de réinitialiser le mot de passe de l'instance MySQL en suivant la procédure décrite à https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html. Après avoir effectué la procédure de réinitialisation, utilisez l'opération correct-stocké-password pour entrer le nouveau mot de passe dans le coffre-fort.

Commandes

Commandes non restreintes

Les commandes non restreintes modifient l'installation de manière coordonnée (sauf les magasins de confiance). Des commandes non restreintes peuvent être exécutées sans authentification de l'utilisateur.

Commande	Description

archivage sécurisé	Créez un fichier zip contenant le coffre-fort. Le chemin relatif vers les fichiers du coffre-fort correspond au chemin du coffre-fort par rapport à la racine d'installation. • wildfly/standalone/configuration/vault/* • acq/conf/vault/* Notez qu'il est fortement recommandé de sauvegarder le coffre-fort chaque fois que vous sauvegardez une base de données OnCommand Insight.
vérifiez-les-clés-par-défaut	Vérifiez si les clés du coffre-fort correspondent à celles du coffre-fort par défaut utilisé dans les instances antérieures à 7.3.16.
mot de passe-stocké-correct	Remplacez un mot de passe (incorrect) stocké dans le coffre-fort par le mot de passe correct connu de l'utilisateur. Ceci peut être utilisé lorsque le coffre-fort et l'installation ne sont pas cohérents. **Notez qu'il ne modifie pas le mot de passe réel dans l'installation.**
	Changer-confiance-mot-de-passe-magasin modifiez le mot de passe utilisé pour un magasin de confiance et stockez le nouveau mot de passe dans le coffre-fort. Le mot de passe actuel du magasin de confiance doit être « connu ».
vérifier-keystore	vérifiez si les valeurs dans le coffre-fort sont correctes: • Pour les utilisateurs d'OCI, le hachage du mot de passe correspond-t-il à la valeur de la base de données • Pour les utilisateurs de MySQL, une connexion à la base de données peut-elle être établie • pour les magasins de clés, le magasin de clés peut-il être chargé et ses clés (le cas échéant) peuvent-elles être lues
touches de liste	répertorier les entrées dans le coffre-fort (sans afficher la valeur stockée)

Commandes restreintes

L'authentification est requise pour toute commande non masquée qui apporte des modifications coordonnées à l'installation :

Commande	Description

restauration-archivage-sauvegarde	Remplace le coffre-fort actuel par le coffre-fort contenu dans le fichier de sauvegarde de coffre-fort spécifié. Exécute toutes les actions coordonnées pour mettre à jour l'installation en fonction des mots de passe du coffre-fort restauré : • Mettez à jour les mots de passe des utilisateurs de communication OCI • Mettez à jour les mots de passe utilisateur MySQL, y compris root • pour chaque magasin de clés, si le mot de passe du magasin de clés est « connu », mettez à jour le magasin de clés à l'aide des mots de passe du coffre-fort restauré. Lorsqu'elle est exécutée en mode normal, elle lit également chaque valeur chiffrée de l'instance, la décrypte à l'aide du service de cryptage du coffre-fort actuel, la re-crypte à l'aide du service de cryptage du coffre-fort restauré et stocke la valeur de nouveau cryptage.
synchroniser-avec-coffre-fort	Exécute toutes les actions coordonnées pour mettre à jour l'installation en fonction des mots de passe utilisateur dans le coffre-fort restauré : • Met à jour les mots de passe des utilisateurs de communication OCI • Met à jour les mots de passe utilisateur MySQL, y compris root
changer-mot-de-passe	Modifie le mot de passe dans le coffre-fort et exécute les actions coordonnées.
remplacer les clés	Créez un nouveau coffre-fort vide (qui aura des clés différentes de celles du coffre-fort existant). Copiez ensuite les entrées du coffre-fort actuel dans le nouveau coffre-fort. Lit ensuite chaque valeur chiffrée de l'instance, la déchiffre à l'aide du service de cryptage du coffre-fort actuel, la recrypte à l'aide du service de cryptage du coffre-fort restauré et stocke la valeur re-chiffrée.

Actions coordonnées

Coffre-fort du serveur

_interne	mettre à jour le hachage du mot de passe pour l'utilisateur dans la base de données
acquisition	mettre à jour le hachage du mot de passe pour l'utilisateur dans la base de données si le coffre-fort d'acquisition est présent, mettez également à jour l'entrée dans le coffre-fort d'acquisition
dwh_interne	mettre à jour le hachage du mot de passe pour l'utilisateur dans la base de données

cognos_admin	mettre à jour le hachage du mot de passe pour l'utilisateur dans la base de données Si DWH et Windows, mettez à jour SANscreen/cognos/analytics/configuration/SANscreenAP.properties pour définir la propriété cognos.admin sur le mot de passe.
racine	Exécutez SQL pour mettre à jour le mot de passe utilisateur dans l'instance MySQL
inventaire	Exécutez SQL pour mettre à jour le mot de passe utilisateur dans l'instance MySQL
dwh	Exécutez SQL pour mettre à jour le mot de passe utilisateur dans l'instance MySQL Si DWH et Windows, mettez à jour le registre Windows pour définir les entrées liées ODBC suivantes sur le nouveau mot de passe : • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Capacity\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Capacity_Efficiency\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_fs_util\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Inventory\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_performance\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_ports\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_sa\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Cloud_Cost\PWD
dwhuser	Exécutez SQL pour mettre à jour le mot de passe utilisateur dans l'instance MySQL

hôtes	Exécutez SQL pour mettre à jour le mot de passe utilisateur dans l'instance MySQL
keystore_password	réécrivez le magasin de clés avec le nouveau mot de passe : wildfly/standalone/configuration/server.keystore
truststore_password	réécrivez le magasin de clés avec le nouveau mot de passe : wildfly/standalone/configuration/server.trustore
mot_de_passe_clé	réécrivez le magasin de clés avec le nouveau mot de passe : wildfly/standalone/configuration/sso.jks
cognos_archive	Aucune

Coffre-fort d'acquisition

acquisition	Aucune
truststore_password	réécrivez le magasin de clés avec le nouveau mot de passe (s'il existe) - acq/conf/cert/client.keystore

Exécution de l'outil d'administration de sécurité - ligne de commande

La syntaxe pour exécuter l'outil sa en mode ligne de commande est la suivante :

```
securityadmin [-s | -au] [-db] [-lu <user> [-lp <password>]] <additional-
options>

where

-s                      selects server vault
-au                     selects acquisition vault

-db                     selects direct operation mode

-lu <user>              user for authentication
-lp <password>          password for authentication
<addition-options>      specifies command and command arguments as
described below
```

Remarques :

- L'option "-i" peut ne pas être présente sur la ligne de commande (car cela sélectionne le mode interactif).
- pour les options "-s" et "-au" :

- "-s" n’est pas autorisé sur un RAU
- "-au" n’est pas autorisé sur DWH
- si aucune n’est présente, alors
  - Le coffre-fort du serveur est sélectionné sur Server, DWH et Dual
  - Le coffre-fort d’acquisition est sélectionné sur RAU

- Les options -lu et -lp sont utilisées pour l’authentification utilisateur.
  - Si <user> est spécifié et que <password> n’est pas, l’utilisateur est invité à entrer le mot de passe.
  - Si <user> n’est pas fourni et que l’authentification est requise, l’utilisateur est invité à entrer <user> et <password>.

Commandes :

Commande	Du stockage
mot de passe-stocké-correct	`securityadmin [-s`
-au] [-db] -pt <key> [<value>] `where` -pt specifies the command ("put") <key> is the key <value> is the value. If not present, user will be prompted for value ` `	archivage sécurisé
`securityadmin [-s`	-au] [-db] -b [<backup-dir>] where -b specified command <backup-dir> is the output directory. If not present, default location of SANscreen/backup/vault is used The backup file will be named ServerSecurityBackup-yyyy-MM-dd-HH-mm.zip ` `
archivage sécurisé	`securityadmin [-s`

-au] [-db] -ub <backup-file> where -ub specified command ("upgrade-backup") <backup-file> The location to write the backup file ```	touches de liste
`` securityadmin [-s ```	-au] [-db] -l where -l specified command ```
touches de vérification	``` securityadmin [-s ```
-au] [-db] -ck where -ck specified command exit code: 1 error 2 default key(s) 3 unique keys ```	vérifier-keystore (serveur)
`` securityadmin [-s] [-db] -v where -v specified command ```	mise à niveau

`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -u where -u specified command For server vault, if -lu is not present, then authentication will be performed for <user> =_internal and <password> = _internal's password from vault. For acquisition vault, if -lu is not present, then no authentication will be attempted ``
remplacer les clés	`securityadmin [-s`
-au] [-db] [-lu <user>] [-lp <password>] -rk where -rk specified command ``	restauration-archivage-sauvegarde
`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -r <backup-file> where -r specified command <backup-file> the backup file location ``
modifier le mot de passe (serveur)	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -up -un <user> -p [<password>] [-sh]` `where` `-up specified command ("update-password")` `-un <user> entry ("user") name to update` `-p <password> new password. If <password not supplied, user will be prompted.` `-sh for mySQL user, use strong hash`

modifier le mot de passe de l'utilisateur d'acquisition (acquisition)	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -up -p [<password>]` `where` `-up specified command ("update-password") -p <password> new password. If <password not supplied, user will be prompted.`
change-password for truststore-_password (acquisition)	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -utp -p [<password>]` `where` `-utp specified command ("update-truststore-password") -p <password> new password. If <password not supplied, user will be prompted.`
synchroniser-avec-vault (serveur)	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -sv <backup-file>` `where` `-sv specified command`

Exécution de l'outil d'administration de sécurité - mode interactif

Interactif - Menu principal

Pour exécuter l'outil sa en mode interactif, entrez la commande suivante :

```
 securityadmin -i
Sur un serveur ou une installation double, SecurityAdmin invite
l'utilisateur à sélectionner le serveur ou l'unité d'acquisition locale.
```

Nœuds de serveur et d'unité d'acquisition détectés ! Sélectionnez le nœud dont la sécurité doit être reconfigurée :

```
1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:
```

Sur DWH, "serveur" est automatiquement sélectionné. Sur un au distant, « unité d'acquisition » est automatiquement sélectionné.

Interactive - Server : récupération du mot de passe root

En mode serveur, l'outil SecurityAdmin vérifie d'abord que le mot de passe root enregistré est correct. Si ce n'est pas le cas, l'outil affiche l'écran de récupération du mot de passe racine.

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

Si l'option 1 est sélectionnée, l'utilisateur est invité à entrer le mot de passe correct.

```
 Enter password (blank = don't change)
 Enter correct password for 'root':
Si le mot de passe correct est saisi, le message suivant s'affiche.
```

```
 Password verified.  Vault updated
Appuyez sur entrée pour afficher le menu sans restriction du serveur.
```

Si le mot de passe saisi est incorrect, le message suivant s'affiche

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Appuyez sur ENTER pour revenir au menu de récupération.
```

Si l'option 2 est sélectionnée, l'utilisateur est invité à fournir le nom d'un fichier de sauvegarde à partir duquel

lire le mot de passe correct :

```
 Enter Backup File Location:
Si le mot de passe de la sauvegarde est correct, le message suivant
s'affiche.
```

```
 Password verified.  Vault updated
Appuyez sur entrée pour afficher le menu sans restriction du serveur.
```

Si le mot de passe de la sauvegarde est incorrect, le message suivant s'affiche

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Appuyez sur ENTER pour revenir au menu de récupération.
```

Interactive - serveur : mot de passe correct

L'action « Mot de passe correct » est utilisée pour modifier le mot de passe stocké dans le coffre-fort afin qu'il corresponde au mot de passe réel requis par l'installation. Cette commande est utile dans les situations où une modification de l'installation a été faite par quelque chose d'autre que l'outil securityadmin. Voici quelques exemples :

- Le mot de passe d'un utilisateur SQL a été modifié par l'accès direct à MySQL.
- Un magasin de clés est remplacé ou le mot de passe d'un magasin de clés est modifié à l'aide de keytool.
- Une base de données OCI a été restaurée et cette base de données a des mots de passe différents pour les utilisateurs internes

« Mot de passe correct » invite d'abord l'utilisateur à sélectionner le mot de passe pour enregistrer la valeur correcte.

```
Replace incorrect stored password with correct password.  (Does not change
the required password)
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

Après avoir sélectionné l'entrée à corriger, l'utilisateur est invité à indiquer la façon dont il souhaite fournir la valeur.

```
1 - Enter {user} password

2 - Get {user} password from vault backup

9 - Exit

Enter your choice:
```

Si l’option 1 est sélectionnée, l’utilisateur est invité à entrer le mot de passe correct.

```
 Enter password (blank = don't change)
 Enter correct password for '{user}':
Si le mot de passe correct est saisi, le message suivant s'affiche.
```

```
 Password verified.  Vault updated
Appuyez sur entrée pour revenir au menu sans restriction du serveur.
```

Si le mot de passe saisi est incorrect, le message suivant s’affiche

```
Password verification failed - {additional information}
Vault entry not updated.
```

Appuyez sur entrée pour revenir au menu sans restriction du serveur.

Si l’option 2 est sélectionnée, l’utilisateur est invité à fournir le nom d’un fichier de sauvegarde à partir duquel lire le mot de passe correct :

```
 Enter Backup File Location:
Si le mot de passe de la sauvegarde est correct, le message suivant
s'affiche.
```

```
 Password verified.  Vault updated
Appuyez sur entrée pour afficher le menu sans restriction du serveur.
```

Si le mot de passe de la sauvegarde est incorrect, le message suivant s’affiche

```
Password verification failed - {additional information}
Vault entry not updated.
```

Appuyez sur entrée pour afficher le menu sans restriction du serveur.

Interactive - serveur : vérifiez le contenu du coffre-fort

Vérifier le contenu du coffre-fort vérifiera si le coffre-fort a des clés qui correspondent au coffre-fort par défaut distribué avec les versions antérieures d’OCI et vérifiera si chaque valeur du coffre-fort correspond à l’installation.

Les résultats possibles pour chaque clé sont les suivants :

OK	La valeur du coffre-fort est correcte

Non cochée	La valeur ne peut pas être vérifiée par rapport à l'installation
MAUVAIS	La valeur ne correspond pas à l'installation
Manquant	Une entrée attendue est manquante.

```
Encryption keys secure: unique, non-default encryption keys detected

             cognos_admin: OK
                    hosts: OK
             dwh_internal: OK
                inventory: OK
                  dwhuser: OK
        keystore_password: OK
                      dwh: OK
      truststore_password: OK
                     root: OK
                _internal: OK
          cognos_internal: Not Checked
             key_password: OK
              acquisition: OK
           cognos_archive: Not Checked
 cognos_keystore_password: Missing


Press enter to continue
```

Interactive - serveur : sauvegarde

Backup demande le répertoire dans lequel le fichier zip de sauvegarde doit être stocké. Le répertoire doit déjà exister et le nom du fichier sera ServerSecurityBackup-yyyy-mm-DD-hh-mm.zip.

```
Enter backup directory location [C:\Program Files\SANscreen\backup\vault]
:

Backup Succeeded!   Backup File: C:\Program
Files\SANscreen\backup\vault\ServerSecurityBackup-2024-08-09-12-02.zip
```

Interactive - serveur : connexion

L'action de connexion permet d'authentifier un utilisateur et d'accéder aux opérations qui modifient l'installation. L'utilisateur doit avoir admin Privileges. Lors de l'exécution avec le serveur, tout utilisateur administrateur peut être utilisé ; lors de l'exécution en mode direct, l'utilisateur doit être un utilisateur local plutôt qu'un utilisateur LDAP.

```
Authenticating via server. Enter user and password

UserName: admin

Password:
```

ou

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:
```

Si le mot de passe est correct et que l'utilisateur est un utilisateur admin, le menu restreint s'affiche.

Si le mot de passe est incorrect, le message suivant s'affiche :

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:

Login Failed!
```

Si l'utilisateur n'est pas un administrateur, les informations suivantes s'affichent :

```
Authenticating via server. Enter user and password

UserName: user

Password:

User 'user' does not have 'admin' role!
```

Interactive - serveur : menu restreint

Une fois l'utilisateur connecté, l'outil affiche le menu restreint.

```
Logged in as: admin
Select Action:

2 - Change Password

3 - Verify Vault Contents

4 - Backup

5 - Restore

6 - Change Encryption Keys

7 - Fix installation to match vault

9 - Exit

Enter your choice:
```

Interactive - serveur : modification du mot de passe

L’action « Modifier le mot de passe » permet de modifier un mot de passe d’installation en une nouvelle valeur.

« Modifier le mot de passe » invite d’abord l’utilisateur à sélectionner le mot de passe à modifier.

```
Change Password
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

Après avoir sélectionné l'entrée à corriger, si l'utilisateur est un utilisateur MySQL, l'utilisateur sera invité à confirmer le hachage du mot de passe

```
MySQL supports SHA-1 and SHA-256 password hashes. SHA-256 is stronger but
requires all clients use SSL connections

Use strong password hash? (Y/n): y
```

Ensuite, l'utilisateur est invité à entrer le nouveau mot de passe.

```
New Password for '{user}':
If the password is empty, the operation is cancelled.

Password is empty - cancelling operation
```

Si un mot de passe non vide est saisi, l'utilisateur est invité à confirmer le mot de passe.

```
New Password for '{user}':

Confirm New Password for '{user}':

Password successfully updated for 'dwhuser'!
```

Si la modification échoue, l'erreur ou l'exception s'affiche.

Interactive - serveur : restauration

Interactive - serveur : modification des clés de cryptage

L'action Modifier les clés de cryptage remplace la clé de cryptage utilisée pour crypter les entrées du coffre-fort et remplace la clé de cryptage utilisée pour le service de cryptage du coffre-fort. Comme la clé du service de chiffrement est modifiée, les valeurs cryptées dans la base de données sont à nouveau chiffrées ; elles sont lues, déchiffrées avec la clé actuelle, cryptées avec la nouvelle clé et enregistrées à nouveau dans la base de données.

Cette action n'est pas prise en charge en mode direct car le serveur fournit l'opération de re-chiffrement pour certains contenus de base de données.

```
Replace encryption key with new key and update encrypted database values

Confirm (y/N): y

Change Encryption Keys succeeded! Restart 'Server' Service!
```

Interactive - serveur : installation fixe

L'action réparer l'installation mettra à jour l'installation. Tous les mots de passe d'installation modifiables via l'outil securityadmin, à l'exception de root, seront définis sur les mots de passe du coffre-fort.

- Les mots de passe des utilisateurs internes d'OCI seront mis à jour.
- Les mots de passe des utilisateurs MySQL, sauf root, seront mis à jour.
- Les mots de passe des keystores seront mis à jour.

```
Fix installation - update installation passwords to match values in vault

Confirm:  (y/N): y

Installation update succeeded! Restart 'Server' Service.
```

L'action s'arrête à la première mise à jour ayant échoué et affiche l'erreur ou l'exception.

Gestion de la sécurité sur le serveur Insight

Le `securityadmin` Cet outil vous permet de gérer les options de sécurité sur le serveur Insight. La gestion de la sécurité inclut la modification des mots de passe, la génération de nouvelles clés, l'enregistrement et la restauration des configurations de sécurité que vous créez ou la restauration des configurations par défaut.

Description de la tâche

Vous utilisez le `securityadmin` outil de gestion de la sécurité :

- Vitres - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux : `/bin/oci-securityadmin.sh`

Pour plus d'informations, reportez-vous à la "Admin sécurité"documentation.

Gestion de la sécurité sur l'unité d'acquisition locale

Le `securityadmin` L'outil vous permet de gérer les options de sécurité de l'utilisateur d'acquisition local (LAU). 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 avoir `admin` privilèges permettant d'effectuer des tâches de configuration de la sécurité.

Description de la tâche

Vous utilisez le `securityadmin` outil de gestion de la sécurité :

- Vitres - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux : `/bin/oci-securityadmin.sh`

Pour plus d'informations, reportez-vous aux "Outil SecurityAdmin"instructions.

Gestion de la sécurité sur un RAU

Le `securityadmin` L'outil vous permet de gérer les options de sécurité sur Raus. Vous

devrez peut-être sauvegarder ou restaurer une configuration de coffre-fort, modifier les clés de cryptage ou mettre à jour les mots de passe des unités d'acquisition.

Description de la tâche

Vous utilisez le `securityadmin` outil de gestion de la sécurité :

- Vitres - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux : `/bin/oci-securityadmin.sh`

Un scénario de mise à jour de la configuration de sécurité pour le LAU/RAU consiste à mettre à jour le mot de passe utilisateur d'acquisition lorsque le mot de passe de cet utilisateur a été modifié sur le serveur. Le LAU et tous les Raus utilisent le même mot de passe que celui de l'utilisateur d'acquisition du serveur pour communiquer avec le serveur.

L'utilisateur 'acquisition' n'existe que sur le serveur Insight. Le RAU ou LAU se connecte en tant qu'utilisateur lorsqu'il se connecte au serveur.

Pour plus d'informations, reportez-vous aux "Outil SecurityAdmin"instructions.

Gestion de la sécurité dans l'entrepôt de données

Le `securityadmin` L'outil vous permet de gérer les options de sécurité sur le serveur Data Warehouse. La gestion de la sécurité inclut la mise à jour des mots de passe internes des utilisateurs internes sur le serveur DWH, la création de sauvegardes de la configuration de sécurité ou la restauration des configurations par défaut.

Description de la tâche

Vous utilisez le `securityadmin` outil de gestion de la sécurité :

- Vitres - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux : `/bin/oci-securityadmin.sh`

Pour plus d'informations, reportez-vous à la "Admin sécurité"documentation.

Modification des mots de passe des utilisateurs internes OnCommand Insight

Les stratégies de sécurité peuvent vous obliger à modifier les mots de passe dans votre environnement OnCommand Insight. Certains mots de passe d'un serveur existent sur un serveur différent dans l'environnement, ce qui nécessite que vous modifiiez le mot de passe sur les deux serveurs. Par exemple, lorsque vous modifiez le mot de passe utilisateur « Inventory » sur le serveur Insight Server, vous devez faire correspondre le mot de passe utilisateur « Inventory » sur le connecteur du serveur Data Warehouse configuré pour ce serveur Insight Server.

Avant de commencer

Vous devez comprendre les dépendances des comptes d'utilisateur avant de modifier les mots de passe. Si vous ne mettez pas à jour les mots de passe sur tous les serveurs requis, les problèmes de communication entre les composants Insight seront à l'origine de ces échecs.

Description de la tâche

Le tableau suivant répertorie les mots de passe des utilisateurs internes pour Insight Server et répertorie les composants Insight qui ont des mots de passe dépendants qui doivent correspondre au nouveau mot de passe.

Mots de passe du serveur Insight	Modifications requises
_interne	
acquisition	LAU, RAU
dwh_interne	Entrepôt de données
hôtes	
inventaire	Entrepôt de données
racine	

Le tableau suivant répertorie les mots de passe des utilisateurs internes pour l'entrepôt de données et répertorie les composants Insight qui ont des mots de passe dépendants qui doivent correspondre au nouveau mot de passe.

Mots de passe d'entrepôt de données	Modifications requises
cognos_admin	
dwh	
dwh_Internal (modifié à l'aide de l'interface utilisateur de configuration du connecteur du serveur)	Serveur Insight
dwhuser	
hôtes	
Inventaire (modifié à l'aide de l'interface utilisateur de configuration de Server Connector)	Serveur Insight
racine	

Modification des mots de passe dans l'interface utilisateur de configuration de la connexion au serveur DWH

Le tableau suivant répertorie le mot de passe utilisateur POUR LAU et répertorie les composants Insight qui ont des mots de passe dépendants qui doivent correspondre au nouveau mot de passe.

Mots de passe LAU	Modifications requises
acquisition	Insight Server, RAU

Modification des mots de passe “Inventory” et “dwh_Internal” à l’aide de l’interface utilisateur Server Connection Configuration

Si vous devez modifier les mots de passe « Inventory » ou « dwh_Internal » pour qu’ils correspondent à ceux du serveur Insight, vous utilisez l’interface utilisateur Data Warehouse.

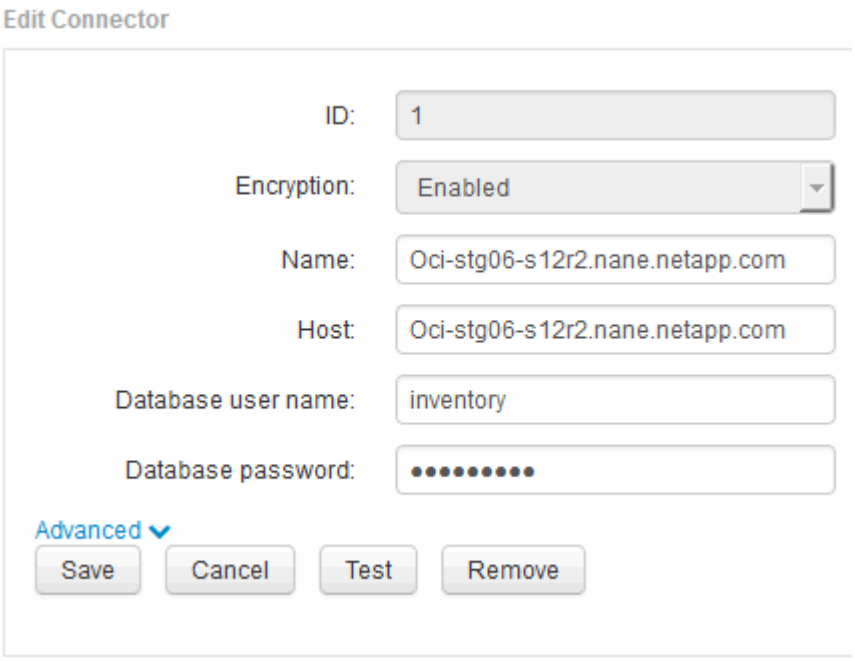
Avant de commencer

Vous devez être connecté en tant qu’administrateur pour effectuer cette tâche.

Étapes

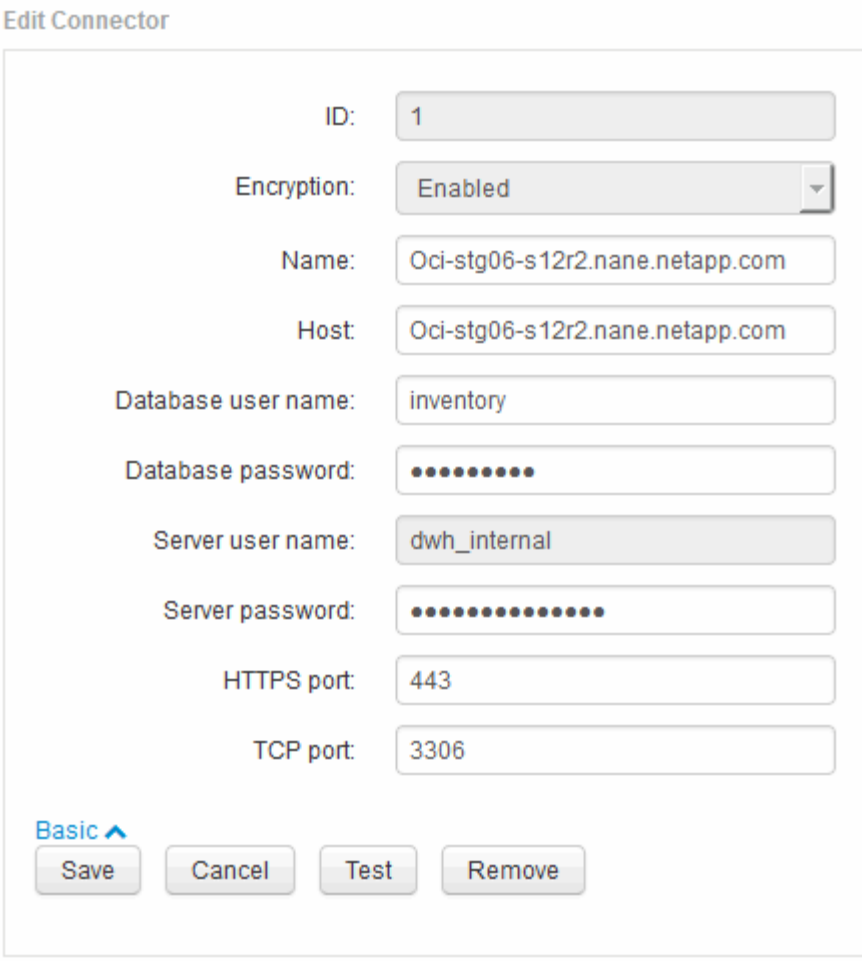
1. Connectez-vous au portail Data Warehouse à l’adresse https://hostname/dwh, Où hostname est le nom du système sur lequel est installé l’entrepôt de données OnCommand Insight.
2. Dans le volet de navigation de gauche, cliquez sur **connecteurs**.

   L’écran **Edit Connector** s’affiche.



3. Entrez un nouveau mot de passe « inventaire » pour le champ **Mot de passe de la base de données**.
4. Cliquez sur **Enregistrer**
5. Pour modifier le mot de passe "dwh_Internal", cliquez sur **Avancé.**

   L’écran Editer connecteur avancé s’affiche.



6. Entrez le nouveau mot de passe dans le champ **Mot de passe du serveur** :
7. Cliquez sur enregistrer.

Modification du mot de passe dwh à l'aide de l'outil d'administration ODBC

Lorsque vous modifiez le mot de passe sur pour l'utilisateur dwh sur le serveur Insight, le mot de passe doit également être modifié sur le serveur Data Warehouse. Vous utilisez l'outil Administrateur de source de données ODBC pour modifier le mot de passe de l'entrepôt de données.

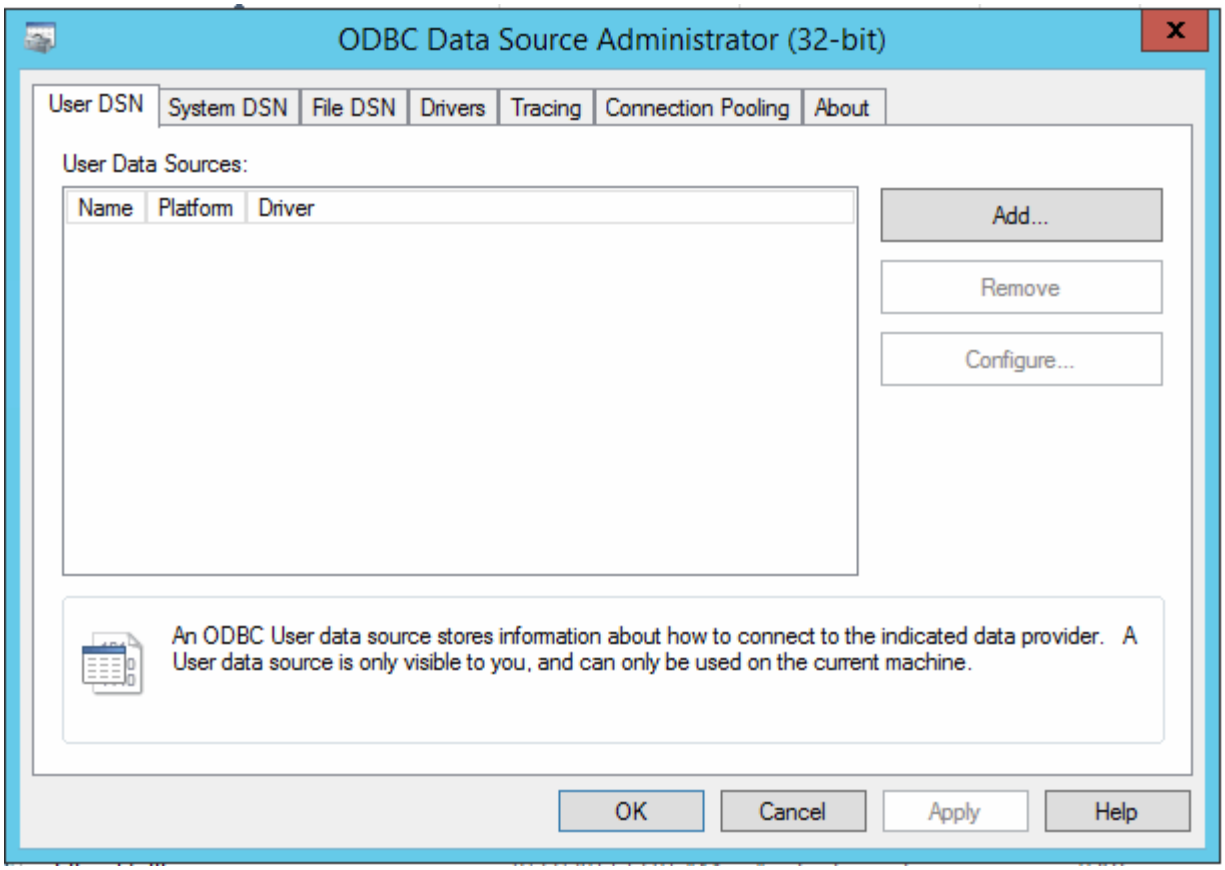
Avant de commencer

Vous devez ouvrir une session à distance sur le serveur Data Warehouse à l'aide d'un compte disposant de privilèges d'administrateur.

Étapes

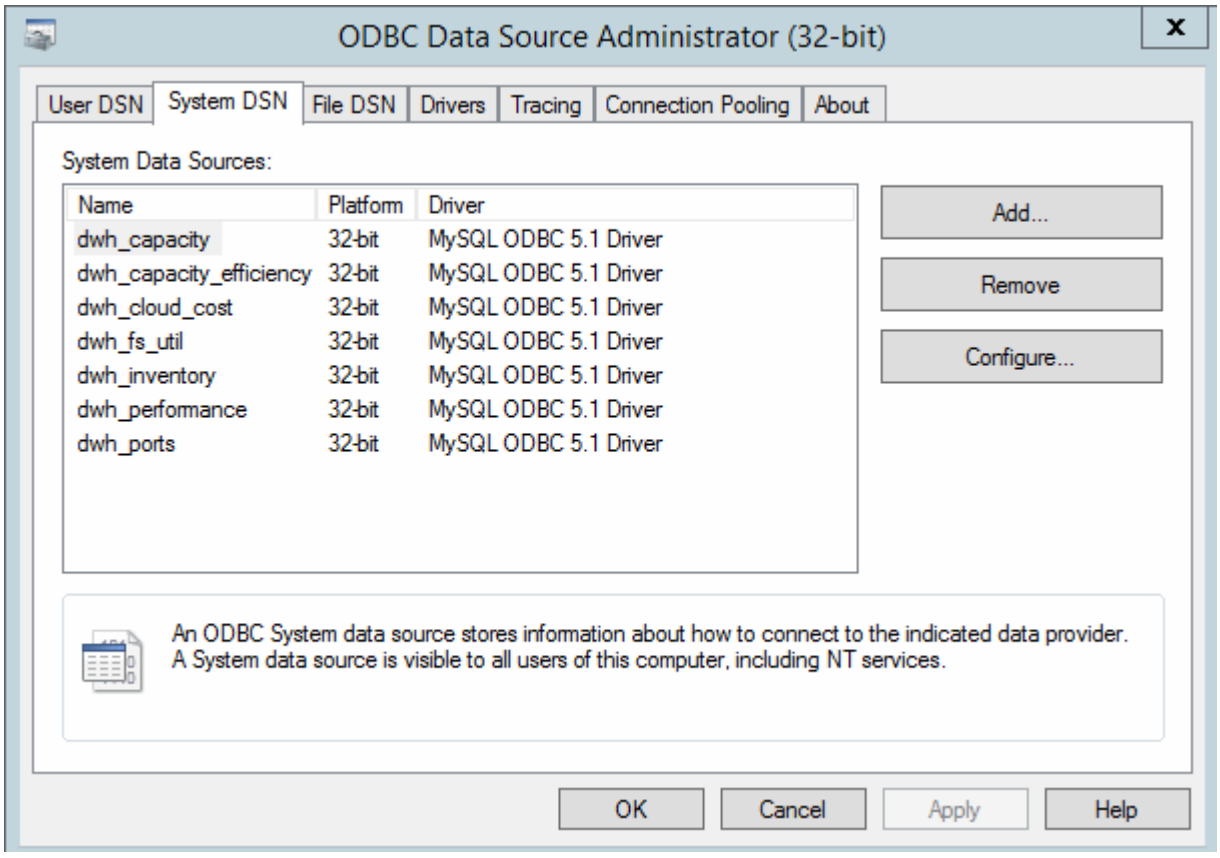
1. Effectuez une connexion à distance au serveur hébergeant cet entrepôt de données.
2. Accédez à l'outil d'administration ODBC à l'adresse `C:\Windows\SysWOW64\odbcad32.exe`

   Le système affiche l'écran Administrateur de source de données ODBC.



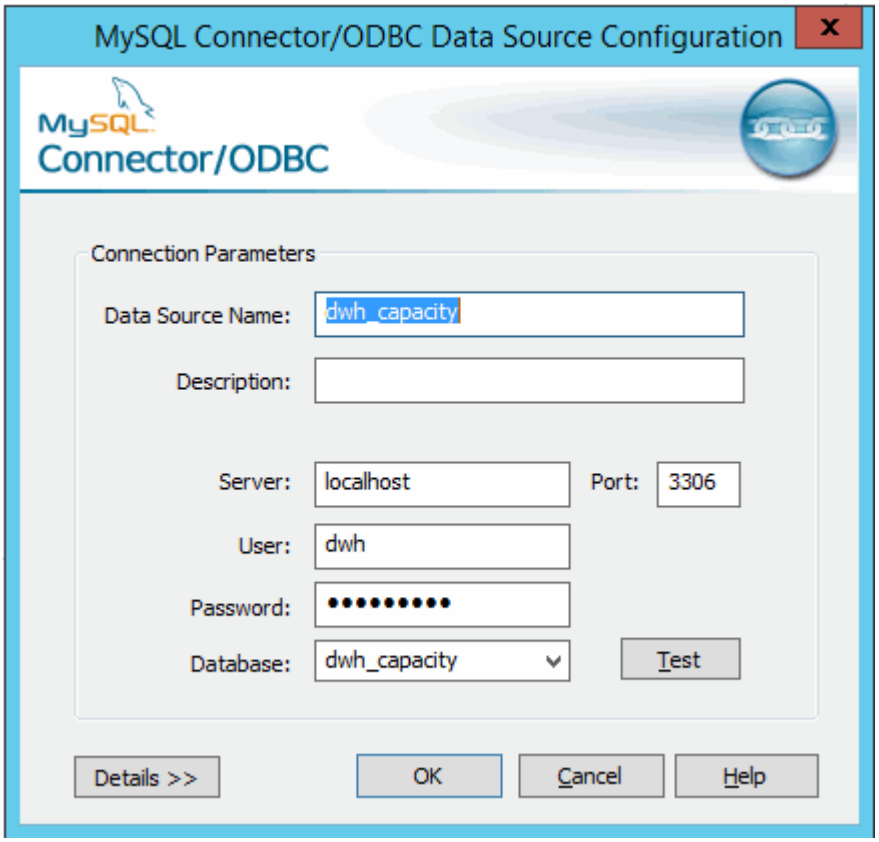
3. Cliquez sur **DSN système**

   Les sources de données système s'affichent.



4. Sélectionnez une source de données OnCommand Insight dans la liste.
5. Cliquez sur **configurer**

   L'écran Configuration de la source de données s'affiche.



6. Entrez le nouveau mot de passe dans le champ **Mot de passe**.

Prise en charge de la connexion par carte à puce et certificat

OnCommand Insight prend en charge l'utilisation de cartes à puce (CAC) et de certificats pour authentifier les utilisateurs qui se connectent aux serveurs Insight. Vous devez configurer le système pour activer ces fonctions.

Après avoir configuré le système pour prendre en charge le contrôle d'admission des appels et les certificats, la navigation vers une nouvelle session de OnCommand Insight entraîne l'affichage d'une boîte de dialogue native qui fournit à l'utilisateur une liste de certificats personnels à choisir. Ces certificats sont filtrés en fonction de l'ensemble des certificats personnels émis par les autorités de certification approuvées par le serveur OnCommand Insight. Le plus souvent, il y a un seul choix. Par défaut, Internet Explorer ignore cette boîte de dialogue s'il n'y a qu'une seule option.

Pour les utilisateurs CAC, les cartes à puce contiennent plusieurs certificats, dont un seul peut correspondre à l'autorité de certification approuvée. Le certificat CAC pour `identification` doit être utilisé.

Pour obtenir les instructions les plus récentes sur les cartes CAC et les certificats, consultez les articles suivants de la base de connaissances (connexion au support requise) :

- "Comment configurer l'authentification CAC (Common Access Card) pour OnCommand Insight"
- "Comment configurer l'authentification CAC (Common Access Card) pour l'entrepôt de données OnCommand Insight"
- "Comment créer et importer un certificat signé d'autorité de certification dans OnComand Insight et l'entrepôt de données OnCommand Insight 7.3.x."
- "Comment créer un certificat auto-signé dans OnCommand Insight 7.3.X installé sur un hôte Windows"
- "Importation d'un certificat signé par l'autorité de certification Cognos dans l'entrepôt de données OnCommand 7.3.3 et versions ultérieures"

Configuration des hôtes pour la connexion par carte à puce et certificat

Vous devez apporter des modifications à la configuration de l'hôte OnCommand Insight pour prendre en charge les connexions par carte à puce (CAC) et certificat.

Avant de commencer

- LDAP doit être activé sur le système.
- Le LDAP `User principal account name` L'attribut doit correspondre au champ LDAP qui contient l'ID d'un utilisateur.

Si vous avez modifié les mots de passe *Server.keystore* et/ou *Server.trustore* à l'aide de "admin sécurité", redémarrez le service *SANscreen* avant d'importer le certificat LDAP.

Pour obtenir les instructions les plus récentes sur les cartes CAC et les certificats, consultez les articles suivants de la base de connaissances (connexion au support requise) :

- "Comment configurer l'authentification CAC (Common Access Card) pour OnCommand Insight"
- "Comment configurer l'authentification CAC (Common Access Card) pour l'entrepôt de données OnCommand Insight"
- "Comment créer et importer un certificat signé d'autorité de certification dans OnComand Insight et l'entrepôt de données OnCommand Insight 7.3.x."
- "Comment créer un certificat auto-signé dans OnCommand Insight 7.3.X installé sur un hôte Windows"
- "Importation d'un certificat signé par l'autorité de certification Cognos dans l'entrepôt de données OnCommand 7.3.3 et versions ultérieures"

Étapes

1. Utilisez le `regedit` utilitaire permettant de modifier les valeurs de registre dans `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`:

a. Modifiez JVM_option `DclientAuth=false` à `DclientAuth=true.`

2. Sauvegardez le fichier du magasin de clés : `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. Ouvrez une invite de commande en spécifiant `Run as administrator`
4. Supprimez le certificat généré automatiquement : `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. Générer un nouveau certificat : `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "alias_name" -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -dname "CN=commonName,OU=orgUnit,O=orgName,L=localityNameI,S=stateName,C=countryName"`
6. Générer une requête de signature de certificat (CSR) : `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -sigalg SHA1withRSA -alias "alias_name" -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file C:\temp\server.csr"`
7. Une fois la CSR renvoyée à l'étape 6, importez le certificat, puis exportez-le au format base-64 et placez-le dans `"C:\temp" named servername.cer`.
8. Extrayez le certificat du magasin de clés :`C:\Program Files\SANscreen\java64\bin\keytool.exe -v -importkeystore -srckeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srcalias "alias_name" -destkeystore "C:\temp\file.p12" -deststoretype PKCS12`
9. Extraire une clé privée du fichier p12 : `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`
10. Fusionnez le certificat base-64 que vous avez exporté à l'étape 7 avec la clé privée : `openssl pkcs12 -export -in "<folder>\<certificate>.cer" -inkey "C:\temp\servername.private.pem" -out "C:\temp\servername.new.p12" -name "servername.abc.123.yyy.zzz"`
11. Importez le certificat fusionné dans le magasin de clés : `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -destkeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias_name"`
12. Importer le certificat racine : `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file "C:\<root_certificate>.cer" -trustcacerts -alias "alias_name"`
13. Importez le certificat racine dans le serveur.trustore : `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<email_certificate>.cer" -trustcacerts -alias "alias_name"`
14. Importer le certificat intermédiaire : `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file`

```
"C:\<intermediate_certificate>.cer" -trustcacerts -alias "alias_name"
```

Répétez cette étape pour tous les certificats intermédiaires.

15. Spécifiez le domaine dans LDAP pour correspondre à cet exemple.
16. Redémarrez le serveur.

Configuration d'un client pour prendre en charge la connexion par carte à puce et certificat

Les ordinateurs clients nécessitent un middleware et des modifications aux navigateurs pour permettre l'utilisation des cartes à puce et la connexion au certificat. Les clients qui utilisent déjà des cartes à puce ne doivent pas nécessiter de modifications supplémentaires sur leurs ordinateurs clients.

Avant de commencer

Pour obtenir les instructions les plus récentes sur les cartes CAC et les certificats, consultez les articles suivants de la base de connaissances (connexion au support requise) :

- "Comment configurer l'authentification CAC (Common Access Card) pour OnCommand Insight"
- "Comment configurer l'authentification CAC (Common Access Card) pour l'entrepôt de données OnCommand Insight"
- "Comment créer et importer un certificat signé d'autorité de certification dans OnComand Insight et l'entrepôt de données OnCommand Insight 7.3.x."
- "Comment créer un certificat auto-signé dans OnCommand Insight 7.3.X installé sur un hôte Windows"
- "Importation d'un certificat signé par l'autorité de certification Cognos dans l'entrepôt de données OnCommand 7.3.3 et versions ultérieures"

Description de la tâche

Les exigences de configuration client courantes sont les suivantes :

- Installation d'un middleware de carte à puce, tel qu'ActivClient (voir
- Modification du navigateur IE (voir
- Modification du navigateur Firefox (voir

Activation de CAC sur un serveur Linux

Certaines modifications sont nécessaires pour activer le contrôle d'accès aux appels sur un serveur OnCommand Insight Linux.

L'autorité de certification racine doit être importée dans le magasin de confiance.

Étapes

1. Accédez à `/opt/netapp/oci/conf/`
2. Modifier `wildfly.properties` et modifiez la valeur de `CLIENT_AUTH_ENABLED` Sur « vrai »
3. Importez le « certificat racine » qui existe sous `/opt/netapp/oci/wildfly/standalone/configuration/server.truststore`
4. Redémarrez le serveur

Configuration de Data Warehouse pour la connexion par carte à puce et certificat

Vous devez modifier la configuration de l'entrepôt de données OnCommand Insight pour prendre en charge les connexions par carte à puce (CAC) et certificat.

Avant de commencer

- LDAP doit être activé sur le système.
- Le LDAP `User principal account name` L'attribut doit correspondre au champ LDAP qui contient le numéro d'identification du gouvernement d'un utilisateur.

  Le nom commun (CN) stocké dans les PCA émises par le gouvernement est normalement dans le format suivant : `first.last.ID`. Pour certains champs LDAP, tels que `sAMAccountName`, ce format est trop long. Pour ces champs, OnCommand Insight extrait uniquement le numéro d'ID du CNS.

Si vous avez modifié les mots de passe *Server.keystore* et/ou *Server.trustore* à l'aide de "admin sécurité", redémarrez le service *SANscreen* avant d'importer le certificat LDAP.

Pour obtenir les instructions les plus récentes sur les cartes CAC et les certificats, consultez les articles suivants de la base de connaissances (connexion au support requise) :

- "Comment configurer l'authentification CAC (Common Access Card) pour OnCommand Insight"
- "Comment configurer l'authentification CAC (Common Access Card) pour l'entrepôt de données OnCommand Insight"
- "Comment créer et importer un certificat signé d'autorité de certification dans OnComand Insight et l'entrepôt de données OnCommand Insight 7.3.x."
- "Comment créer un certificat auto-signé dans OnCommand Insight 7.3.X installé sur un hôte Windows"
- "Importation d'un certificat signé par l'autorité de certification Cognos dans l'entrepôt de données OnCommand 7.3.3 et versions ultérieures"

Étapes

1. Utilisez regedit pour modifier les valeurs de registre dans `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. Modifiez JVM_option `-DclientAuth=false` à `-DclientAuth=true`.

Pour Linux, modifiez le `clientAuth` paramètre dans `/opt/netapp/oci/scripts/wildfly.server`

2. Ajoutez des autorités de certification (CA) au magasin de données :
   a. Dans une fenêtre de commande, accédez à `..\SANscreen\wildfly\standalone\configuration`.
   b. Utilisez `keytool` l'utilitaire pour répertorier les autorités de certification de confiance : `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass <password>` + consultez "Admin sécurité"la documentation pour plus d'informations sur la définition ou la modification du mot de passe de Server_trustore.

      Le premier mot de chaque ligne indique l'alias de l'autorité de certification.

   c. Si nécessaire, fournissez un fichier de certificat d'autorité de certification, généralement un `.pem` fichier. Pour inclure les autorités de certification du client avec les autorités de certification de l'entrepôt de données approuvées, rendez-vous sur `..\SANscreen\wildfly\standalone\configuration` et utiliser le `keytool` commande d'importation : `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      My_alias est généralement un alias qui identifie facilement l'autorité de certification dans le`keytool -list` fonctionnement.

3. Sur le serveur OnCommand Insight, le `wildfly/standalone/configuration/standalone-full.xml` Le fichier doit être modifié en mettant à jour VERIFY-client sur « REQUEST » dans `/subsystem=undertow/server=default-server/https-listener=default-https`Pour activer CAC. Connectez-vous au serveur Insight et exécutez la commande appropriée :

OS	Script
Répertoires de base	<install dir>\SANscreen\Wildfly\bin\enableCACforRemoteEJB.bat
Linux	/Opt/netapp/oci/Wildfly/bin/enableCACforRemoteEJB.sh

   Après avoir exécuté le script, attendez la fin du rechargement du serveur WildFly avant de passer à l'étape suivante.

4. Redémarrez le serveur OnCommand Insight.

Configuration de Cognos pour la connexion par carte à puce et certificat (OnCommand Insight 7.3.10 et versions ultérieures)

Vous devez modifier la configuration de l'entrepôt de données OnCommand Insight pour prendre en charge les connexions de carte à puce (CAC) et de certificat pour le serveur Cognos.

Avant de commencer

Cette procédure concerne les systèmes exécutant OnCommand Insight 7.3.10 et versions ultérieures.

Pour obtenir les instructions les plus récentes sur les cartes CAC et les certificats, consultez les articles suivants de la base de connaissances (connexion au support requise) :

- "Comment configurer l'authentification CAC (Common Access Card) pour OnCommand Insight"
- "Comment configurer l'authentification CAC (Common Access Card) pour l'entrepôt de données OnCommand Insight"
- "Comment créer et importer un certificat signé d'autorité de certification dans OnComand Insight et l'entrepôt de données OnCommand Insight 7.3.x."
- "Comment créer un certificat auto-signé dans OnCommand Insight 7.3.X installé sur un hôte Windows"
- "Importation d'un certificat signé par l'autorité de certification Cognos dans l'entrepôt de données OnCommand 7.3.3 et versions ultérieures"

Étapes

1. Ajoutez des autorités de certification (AC) au magasin de certificats Cognos.
   a. Dans une fenêtre de commande, accédez à `..\SANscreen\cognos\analytics\configuration\certs\`
   b. Utilisez `keytool` l'utilitaire pour répertorier les autorités de certification de confiance : `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass <password>`

      Le premier mot de chaque ligne indique l'alias de l'autorité de certification.

   c. S'il n'existe aucun fichier approprié, fournissez un fichier de certificat d'autorité de certification, généralement un `.pem` fichier.
   d. Pour inclure les autorités de certification du client avec des autorités de certification OnCommand Insight approuvées, rendez-vous sur `..\SANscreen\cognos\analytics\configuration\certs\`.
   e. Utilisez le `keytool` utilitaire d'importation de `.pem` fichier : `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` Est généralement un alias qui identifie facilement l'autorité de certification dans l'`keytool -list`opération.

   f. Lorsque vous êtes invité à entrer un mot de passe, entrez le mot de passe du fichier */SANscreen/bin/cognos_info.dat*.
   g. Réponse `yes` lorsque vous êtes invité à approuver le certificat.
2. Pour activer le mode CAC, procédez comme suit :
   a. Configurez la page de déconnexion CAC en procédant comme suit :
      - Se connecter au portail Cognos (l'utilisateur doit faire partie du groupe administrateurs système, c'est-à-dire cognos_admin)

- (Uniquement pour 7.3.10 et 7.3.11) cliquez sur gérer -> Configuration -> système -> sécurité
- (Uniquement pour 7.3.10 et 7.3.11) Entrez cacLogout.html en regard de l'URL de redirection de déconnexion -> appliquer
- Fermez le navigateur.

b. L'exécution `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

c. Démarrez le service IBM Cognos. Attendez que le service Cognos démarre.

3. Pour désactiver le mode CAC, procédez comme suit :

a. L'exécution `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

b. Démarrez le service IBM Cognos. Attendez que le service Cognos démarre.

c. (Uniquement pour 7.3.10 et 7.3.11) Déconfigurer la page de déconnexion CAC, en procédant comme suit :

- Se connecter au portail Cognos (l'utilisateur doit faire partie du groupe administrateurs système, c'est-à-dire cognos_admin)
- Cliquez sur gérer -> Configuration -> système -> sécurité
- Saisissez cacLogout.html par rapport à l'URL de redirection de déconnexion -> appliquer
- Fermez le navigateur.

Importation de certificats SSL signés par une autorité de certification pour Cognos et DWH (Insight 7.3.10 et versions ultérieures)

Vous pouvez ajouter des certificats SSL pour activer l'authentification et le chiffrement améliorés pour votre environnement Data Warehouse et Cognos.

Avant de commencer

Cette procédure concerne les systèmes exécutant OnCommand Insight 7.3.10 et versions ultérieures.

Pour obtenir les instructions les plus récentes sur les cartes CAC et les certificats, consultez les articles suivants de la base de connaissances (connexion au support requise) :

- "Comment configurer l'authentification CAC (Common Access Card) pour OnCommand Insight"
- "Comment configurer l'authentification CAC (Common Access Card) pour l'entrepôt de données OnCommand Insight"
- "Comment créer et importer un certificat signé d'autorité de certification dans OnComand Insight et l'entrepôt de données OnCommand Insight 7.3.x."
- "Comment créer un certificat auto-signé dans OnCommand Insight 7.3.X installé sur un hôte Windows"
- "Importation d'un certificat signé par l'autorité de certification Cognos dans l'entrepôt de données OnCommand 7.3.3 et versions ultérieures"

Description de la tâche

Vous devez disposer de privilèges d'administrateur pour effectuer cette procédure.

Étapes

1. Arrêtez Cognos à l'aide de l'outil de configuration IBM Cognos. Fermer Cognos.
2. Créer des sauvegardes du `..\SANScreen\cognos\analytics\configuration` et `..\SANScreen\cognos\analytics\temp\cam\freshness` dossiers.
3. Générez une demande de cryptage de certificat à partir de Cognos. Dans une fenêtre Admin CMD, exécutez :
   a. cd "`\Program Files\sanscreen\cognos\analytics\bin`"
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p <password> -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress"`. Note: Ici -H et -i sont d'ajouter subjectAltNames comme dns et ipaddress.
   c. Pour <password>, utilisez le mot de passe du fichier */SANscreen/bin/cognos_info.dat*.
4. Ouvrez le `c:\temp\encryptRequest.csr` classez et copiez le contenu généré.
5. Entrez le contenu encryptRequest.csr et générez un certificat à l'aide du portail de signature CA.
6. Téléchargez les certificats de chaîne en incluant le certificat racine en utilisant le format PKCS7

   Ceci téléchargera le fichier fqdn.p7b
7. Obtenez un certificat au format .p7b auprès de votre autorité de certification. Utilisez un nom qui le marque comme certificat pour le serveur Web Cognos.
8. ThirdPartyCertificateTool.bat ne parvient pas à importer l'ensemble de la chaîne ; plusieurs étapes sont donc nécessaires pour exporter tous les certificats. Divisez la chaîne en les exportant individuellement comme suit :
   a. Ouvrez le certificat .p7b dans « Crypto Shell Extensions ».
   b. Naviguez dans le volet de gauche jusqu'à "certificats"".
   c. Cliquez avec le bouton droit de la souris sur CA racine > toutes les tâches > Exporter.
   d. Sélectionnez sortie Base64.
   e. Entrez un nom de fichier identifiant celui-ci comme certificat racine.
   f. Répétez les étapes 8a à 8e pour exporter tous les certificats séparément dans des fichiers .cer.
   g. Nommez les fichiers intermediateX.cer et cognos.cer.
9. Ignorez cette étape si vous n'avez qu'un seul certificat CA, sinon fusionnez root.cer et intermediateX.cer en un seul fichier.
   a. Ouvrez root.cer avec le Bloc-notes et copiez le contenu.
   b. Ouvrez intermediate.cer avec le Bloc-notes et ajoutez le contenu à partir de 9a (intermédiaire en premier et racine en suivant).
   c. Enregistrez le fichier sous chain.cer.
10. Importez les certificats dans le magasin de clés Cognos à l'aide de l'invite Admin CMD :
    a. cd « Program Files\sanscreen\cognos\analytics\bin »
    b. ThirdPartyCertificateTool.bat -Java:local -i -T -r c:\temp\root.cer
    c. ThirdPartyCertificateTool.bat -Java:local -i -T -r c:\temp\intermediate.cer
    d. ThirdPartyCertificateTool.bat -Java:local -i -e -r c:\temp\cognos.cer -t c:\temp\chain.cer

11. Ouvrez la configuration IBM Cognos.
    a. Sélectionnez Configuration locale→ sécurité -→ cryptographie -→ Cognos
    b. Modifier « utiliser une autorité de certification tierce ? » Sur vrai.
    c. Enregistrez la configuration.
    d. Redémarrez Cognos
12. Exportez le dernier certificat Cognos dans cognos.crt à l'aide de l'invite Admin CMD :
    a. cd « C:\Program Files\SANscreen »
    b. java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\analytics\configuration\certs\CAMKeystore -storetype PKCS12 -storepass <password> -alias Encryption
    c. Pour <password>, utilisez le mot de passe du fichier */SANscreen/bin/cognos_info.dat*.
13. Sauvegardez le serveur DWH trustore sur`..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. Importez « c:\temp\cognos.crt » dans DWH trustore pour établir une communication SSL entre Cognos et DWH, à l'aide de la fenêtre d'invite Admin CMD.
    a. cd « C:\Program Files\SANscreen »
    b. java\bin\keytool.exe -importcert -file c:\temp\cognos.crt -keystore wildfly\standalone\configuration\server.trustore -storepass <password> -alias cogoss3rdca
    c. Pour <password>, utilisez le mot de passe du fichier */SANscreen/bin/cognos_info.dat*.
15. Redémarrez le service SANscreen.
16. Effectuez une sauvegarde de DWH pour vous assurer que DWH communique avec Cognos.
17. Les étapes suivantes doivent être effectuées même lorsque seul le "sl certificate" est modifié et que les certificats Cognos par défaut restent inchangés. Dans le cas contraire, Cognos peut se plaindre du nouveau certificat SANscreen ou être incapable de créer une sauvegarde DWH.
    a. `cd "%SANSCREEN_HOME%cognos\analytics\bin\"`
    b. `"%SANSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sanscreen.cer" -keystore "%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass <password> -alias "ssl certificate"`
    c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sanscreen.cer"`

    Généralement, ces étapes sont effectuées dans le cadre du processus d'importation de certificat Cognos décrit dans "Importation d'un certificat signé par l'autorité de certification Cognos dans l'entrepôt de données OnCommand 7.3.3 et versions ultérieures"

Importation de certificats SSL

Vous pouvez ajouter des certificats SSL pour activer l'authentification et le cryptage améliorés afin d'améliorer la sécurité de votre environnement OnCommand Insight.

Avant de commencer

Vous devez vous assurer que votre système répond au niveau de bit minimum requis (1024 bits).

Description de la tâche

Il est fortement recommandé de sauvegarder le coffre-fort avant la mise à niveau.

Reportez-vous aux "Outil SecurityAdmin" instructions pour plus d'informations sur le coffre-fort et la gestion des mots de passe.

Étapes

1. Créez une copie du fichier de stockage de clés d'origine : `cp c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore.old`
2. Répertoriez le contenu du magasin de clés : `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -v -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   Le système affiche le contenu du magasin de clés. Il doit y avoir au moins un certificat dans le magasin de clés, `"ssl certificate"`.

3. Supprimez le `"ssl certificate"`: `keytool -delete -alias "ssl certificate" -keystore c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
4. Générer une nouvelle clé : `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "ssl certificate" -keyalg RSA -keysize 2048 -validity 365 -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
   a. Lorsque vous êtes invité à entrer le prénom et le nom de famille, entrez le nom de domaine complet (FQDN) que vous souhaitez utiliser.
   b. Fournissez les informations suivantes sur votre organisation et votre structure organisationnelle :
      - Pays : abréviation ISO à deux lettres pour votre pays (par exemple, États-Unis)
      - État ou province : nom de l'État ou de la province où se trouve le siège social de votre organisation (par exemple, Massachusetts)
      - Localité : nom de la ville où se trouve le siège social de votre organisation (Waltham, par exemple)
      - Nom de l'organisation : nom de l'organisation qui possède le nom de domaine (par exemple, NetApp)
      - Nom de l'unité organisationnelle : nom du service ou du groupe qui utilisera le certificat (par exemple, support)
      - Nom de domaine/Nom commun : nom de domaine complet utilisé pour les recherches DNS de votre serveur (par exemple, www.example.com). Le système répond avec des informations similaires à ce qui suit : `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`
   c. Entrez `Yes` Lorsque le nom commun (CN) est égal au nom de domaine complet.
   d. Lorsque vous êtes invité à saisir le mot de passe de la clé, entrez le mot de passe ou appuyez sur la touche entrée pour utiliser le mot de passe existant de la base de stockage de clés.
5. Générer un fichier de demande de certificat : `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -alias "ssl certificate" -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file`

`c:\localhost.csr`

Le `c:\localhost.csr` fichier est le fichier de demande de certificat qui vient d'être généré.

6. Soumettre le `c:\localhost.csr` Soumettez-le à votre autorité de certification pour approbation.

   Une fois le fichier de demande de certificat approuvé, vous souhaitez que le certificat vous soit renvoyé dans `.der` format. Il se peut que le fichier soit renvoyé en tant que `.der` fichier. Le format de fichier par défaut est `.cer` Pour les services CA de Microsoft.

   La plupart des autorités de certification des entreprises utilisent un modèle de chaîne de confiance, y compris une autorité de certification racine, qui est souvent hors ligne. Il a signé les certificats pour quelques AC enfants seulement, connues sous le nom d'AC intermédiaires.

   Vous devez obtenir la clé publique (certificats) pour l'ensemble de la chaîne de confiance - le certificat de l'autorité de certification qui a signé le certificat pour le serveur OnCommand Insight, et tous les certificats entre cette autorité de certification de signature jusqu'à l'autorité de certification racine de l'organisation.

   Dans certaines organisations, lorsque vous soumettez une demande de signature, vous pouvez recevoir l'une des réponses suivantes :

   - Fichier PKCS12 contenant votre certificat signé et tous les certificats publics de la chaîne de confiance
   - A `.zip` dossier contenant des fichiers individuels (y compris votre certificat signé) et tous les certificats publics de la chaîne de confiance
   - Seul votre certificat signé

     Vous devez obtenir les certificats publics.

7. Importez le certificat approuvé pour Server.keystore : `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   a. Lorsque vous y êtes invité, entrez le mot de passe de la base de stockage de clés.

      Le message suivant s'affiche : `Certificate reply was installed in keystore`

8. Importez le certificat approuvé pour Server.trustore : `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore"`

   a. Lorsque vous y êtes invité, entrez le mot de passe trustore.

      Le message suivant s'affiche : `Certificate reply was installed in trustore`

9. Modifiez le `SANscreen\wildfly\standalone\configuration\standalone-full.xml` fichier :

   Remplacez la chaîne d'alias suivante : `alias="cbc-oci-02.muccbc.hq.netapp.com"`. Par exemple :

   ```
   <keystore path="server.keystore" relative-to="jboss.server.config.dir"
   keystore-password="${VAULT::HttpsRealm::keystore_password::1}" alias="cbc-oci-
   02.muccbc.hq.netapp.com" key-
   ```

```
password="${VAULT::HttpsRealm::key_password::1}"/>
```

10. Redémarrez le service du serveur SANscreen.

    Une fois Insight en cours d'exécution, vous pouvez cliquer sur l'icône du cadenas pour afficher les certificats installés sur le système.

    Si vous voyez un certificat contenant des informations « émis à » correspondant aux informations « émis par », un certificat auto-signé est toujours installé. Les certificats auto-signés générés par le programme d'installation Insight ont une expiration de 100 ans.

    NetApp ne peut pas garantir que cette procédure supprimera les avertissements de certificat numérique. NetApp ne peut pas contrôler la configuration des postes de travail des utilisateurs. Prenez en compte les scénarios suivants :

    - Microsoft Internet Explorer et Google Chrome utilisent tous deux la fonctionnalité native de certificat de Microsoft sous Windows.

      Cela signifie que si vos administrateurs Active Directory poussent les certificats CA de votre entreprise dans les magasins de certificats de l'utilisateur final, les utilisateurs de ces navigateurs verront disparaître les avertissements de certificat lorsque les certificats auto-signés OnCommand Insight ont été remplacés par ceux signés par l'infrastructure CA interne.

    - Java et Mozilla Firefox ont leurs propres magasins de certificats.

      Si vos administrateurs système n'automatisent pas l'ingestion des certificats CA dans les magasins de certificats approuvés de ces applications, l'utilisation du navigateur Firefox peut continuer à générer des avertissements de certificat en raison d'un certificat non approuvé, même lorsque le certificat auto-signé a été remplacé. La mise en place de la chaîne de certificats de votre organisation dans la trustore est une exigence supplémentaire.

Configuration de sauvegardes hebdomadaires de votre base de données Insight

Vous pouvez configurer des sauvegardes hebdomadaires automatiques pour votre base de données Insight afin de protéger vos données. Ces sauvegardes automatiques écrasent les fichiers du répertoire de sauvegarde spécifié.

Description de la tâche

Meilleure pratique : lorsque vous configurez la sauvegarde hebdomadaire de la base de données OCI, vous devez stocker les sauvegardes sur un serveur différent de celui utilisé par Insight, en cas de défaillance du serveur. Ne stockez pas de sauvegardes manuelles dans le répertoire de sauvegarde hebdomadaire car chaque sauvegarde hebdomadaire écrase les fichiers du répertoire.

Le fichier de sauvegarde contient les éléments suivants :

- Données d'inventaire
- Jusqu'à 7 jours de données de performances

Étapes

1. Dans la barre d'outils Insight, cliquez sur **Admin** > **Setup**.
2. Cliquez sur l'onglet **sauvegarde et archivage**.
3. Dans la section sauvegarde hebdomadaire, sélectionnez **Activer la sauvegarde hebdomadaire**.
4. Entrez le chemin d'accès à l'emplacement **Backup**. Il peut se trouver sur le sur le serveur Insight local ou sur un serveur distant accessible à partir du serveur Insight.

> Le paramètre d'emplacement de sauvegarde est inclus dans la sauvegarde elle-même. Si vous restaurez la sauvegarde sur un autre système, sachez que l'emplacement du dossier de sauvegarde peut être incorrect sur le nouveau système. Vérifiez les paramètres de votre emplacement de sauvegarde après la restauration d'une sauvegarde.

5. Sélectionnez l'option **Cleanup** pour conserver les deux dernières sauvegardes ou les cinq dernières.
6. Cliquez sur **Enregistrer**.

Résultats

Vous pouvez également accéder à **Admin** > **Troubleshooting** pour créer une sauvegarde à la demande.

Éléments inclus dans la sauvegarde

Des sauvegardes hebdomadaires et à la demande peuvent être utilisées pour résoudre les problèmes ou migrer.

La sauvegarde hebdomadaire ou à la demande comprend les éléments suivants :

- Données d'inventaire
- Données de performances (si elles sont sélectionnées pour être incluses dans la sauvegarde)
- Sources de données et paramètres de source de données
- Packs d'intégration
- Unités d'acquisition à distance
- Paramètres ASUP/proxy
- Paramètres d'emplacement de sauvegarde
- Paramètres d'emplacement d'archivage
- Paramètres de notification
- Utilisateurs
- Règles de performance
- Entités commerciales et applications
- Règles et paramètres de résolution du périphérique
- Tableaux de bord et widgets
- Tableaux de bord et widgets personnalisés de la page des ressources
- Requêtes
- Annotations et règles d'annotation

La sauvegarde hebdomadaire ne comprend pas :

- Paramètres de l'outil de sécurité/informations du coffre-fort (sauvegardés via un processus CLI distinct)
- Journaux (peuvent être enregistrés dans un fichier .zip à la demande)
- Données de performances (si cette option n'est pas sélectionnée pour être incluse dans la sauvegarde)
- Licences

Si vous choisissez d'inclure les données de performances à la sauvegarde, les données des sept derniers jours sont sauvegardées. Les données restantes seront dans l'archive si cette fonction est activée.

Archivage des données de performance

Avec OnCommand Insight 7.3, vous pouvez désormais archiver les données de performances au quotidien. Cela complète les sauvegardes de données de configuration et de performances limitées.

OnCommand Insight conserve jusqu'à 90 jours de données de performances et de violation. Toutefois, lors de la création d'une sauvegarde de ces données, seules les informations les plus récentes sont incluses dans la sauvegarde. L'archivage vous permet d'enregistrer le reste de vos données de performances et de les charger si nécessaire.

Une fois l'emplacement d'archivage configuré et l'archivage activé, une fois par jour, Insight archive les données de performances de tous les objets du jour précédent dans l'emplacement d'archivage. Les archives de chaque jour sont conservées dans le dossier d'archive dans un fichier distinct. L'archivage s'effectue en arrière-plan et se poursuit tant qu'Insight est en cours d'exécution.

Les 90 derniers jours d'archives sont conservés ; les fichiers d'archives de plus de 90 jours sont supprimés lorsque de nouveaux sont créés.

Activation de l'archivage des performances

Pour activer l'archivage des données de performances, procédez comme suit.

Étapes

1. Dans la barre d'outils, cliquez sur **Admin** > **Setup**.
2. Sélectionnez l'onglet **sauvegarde et archivage**.
3. Dans la section Archives de performances, assurez-vous que la case **Activer l'archive de performances** est cochée.
4. Spécifiez un emplacement d'archive valide.

   Vous ne pouvez pas spécifier de dossier sous le dossier d'installation d'Insight.

   Meilleure pratique : ne spécifiez pas le même dossier pour l'archivage que l'emplacement de sauvegarde Insight.

5. Cliquez sur **Enregistrer**.

   Le processus d'archivage est géré en arrière-plan et n'interfère pas avec d'autres activités Insight.

Chargement de l'archive de performance

Pour charger l'archive des données de performances, procédez comme suit.

Avant de commencer

Avant de charger l'archive des données de performances, vous devez restaurer une sauvegarde hebdomadaire ou manuelle valide.

Étapes

1. Dans la barre d'outils, cliquez sur **Admin** > **Dépannage**.
2. Dans la section Restaurer, sous **Charger l'archive de performances**, cliquez sur **Charger**.

> Le chargement de l'archive est géré en arrière-plan. Le chargement de l'archive complète peut prendre beaucoup de temps car les données de performances archivées de chaque jour sont renseignées dans Insight. L'état du chargement de l'archive s'affiche dans la section archive de cette page.

Configuration de votre courrier électronique

Vous devez configurer OnCommand Insight pour qu'il accède à votre système de messagerie de sorte que le serveur OnCommand Insight puisse utiliser votre messagerie pour générer des rapports auxquels vous êtes abonné, et transporter les informations de support à des fins de dépannage vers le support technique NetApp.

Configuration de la messagerie requise

Avant de configurer OnCommand Insight pour accéder à votre système de messagerie, vous devez détecter le nom d'hôte ou l'adresse IP pour identifier le serveur de messagerie (SMTP ou Exchange) et attribuer un compte de messagerie pour les rapports OnCommand Insight.

Demandez à votre administrateur de messagerie de créer un compte de messagerie pour OnCommand Insight. Vous aurez besoin des informations suivantes :

- Nom d'hôte ou adresse IP permettant d'identifier le serveur de messagerie (SMTP ou Exchange) utilisé par votre organisation. Vous trouverez ces informations dans l'application que vous utilisez pour lire votre courrier électronique. Dans Microsoft Outlook, par exemple, vous pouvez trouver le nom du serveur en affichant la configuration de votre compte : Outils - comptes de messagerie - Afficher ou modifier le compte de messagerie existant.
- Nom du compte de messagerie par lequel OnCommand Insight enverra des rapports réguliers. Le compte doit être une adresse e-mail valide dans votre organisation. (La plupart des systèmes de messagerie n'envoient pas de messages à moins qu'ils ne soient envoyés par un utilisateur valide.) Si le serveur de messagerie a besoin d'un nom d'utilisateur et d'un mot de passe pour envoyer du courrier, demandez ces informations à votre administrateur système.

Configuration de votre messagerie pour Insight

Si vos utilisateurs souhaitent recevoir des rapports Insight dans leurs comptes de messagerie, vous devez configurer votre serveur de messagerie pour activer cette fonctionnalité.

Étapes

1. Dans la barre d'outils Insight, cliquez sur **Admin** et sélectionnez **Notifications**.
2. Faites défiler jusqu'à la section **Email** de la page.
3. Dans la zone **Server**, entrez le nom de votre serveur SMTP dans votre organisation, identifié à l'aide d'un nom d'hôte ou d'une adresse IP (*nnn.nnn.nnn* format).

   Si vous spécifiez un nom d'hôte, assurez-vous que ce nom peut être résolu via DNS.
4. Dans la zone **Nom d'utilisateur**, entrez votre nom d'utilisateur.
5. Dans la zone **Mot de passe**, entrez le mot de passe d'accès au serveur de messagerie, requis uniquement si votre serveur SMTP est protégé par un mot de passe. Il s'agit du même mot de passe que celui que vous utilisez pour vous connecter à l'application qui vous permet de lire votre courrier électronique. Si un mot de passe est requis, vous devez le saisir une deuxième fois pour vérification.
6. Dans la zone **adresse e-mail de l'expéditeur**, entrez le compte de messagerie de l'expéditeur qui sera identifié comme expéditeur dans tous les rapports OnCommand Insight.

   Ce compte doit être un compte de messagerie valide au sein de votre organisation.
7. Dans la zone **Signature de l'e-mail**, entrez le texte que vous souhaitez insérer dans chaque e-mail envoyé.
8. Dans la zone destinataires, cliquez sur ✚, Entrez une adresse e-mail et cliquez sur **OK**.

   Pour modifier une adresse e-mail, sélectionnez-la et cliquez sur ✎. Pour supprimer une adresse e-mail, sélectionnez-la et cliquez sur ✖.
9. Pour envoyer un e-mail de test à des destinataires spécifiés, cliquez sur ✔.
10. Cliquez sur **Enregistrer**.

Configuration des notifications SNMP

OnCommand Insight prend en charge les notifications SNMP en cas de modification de la configuration et des règles de chemin global ainsi que de violation. Par exemple, des notifications SNMP sont envoyées lorsque les seuils des sources de données sont dépassés.

Avant de commencer

Les éléments suivants doivent avoir été remplis :

- Identification de l'adresse IP du serveur qui consolide les interruptions pour chaque type d'événement.

  Vous devrez peut-être consulter votre administrateur système pour obtenir ces informations.

- Identification du numéro de port par lequel la machine désignée obtient des interruptions SNMP, pour chaque type d'événement.

  Le port par défaut des interruptions SNMP est 162.

- Compilation de la MIB sur votre site.

  La base MIB propriétaire est fournie avec le logiciel d'installation pour prendre en charge les interruptions OnCommand Insight. La MIB NetApp est compatible avec tous les logiciels de gestion SNMP standard et peut être trouvée sur le serveur Insight dans `<install dir>\SANscreen\MIBS\sanscreen.mib`.

Étapes

1. Cliquez sur **Admin** et sélectionnez **Notifications**.
2. Faites défiler jusqu'à la section **SNMP** de la page.
3. Cliquez sur **actions** et sélectionnez **Ajouter une source d'interruption**.
4. Dans la boîte de dialogue **Ajouter des destinataires de trap SNMP**, entrez les valeurs suivantes :
   - **IP**

     Adresse IP à laquelle OnCommand Insight envoie des messages d'interruption SNMP.

   - **Port**

     Numéro de port auquel OnCommand Insight envoie des messages d'interruption SNMP.

   - **Chaîne de communauté**

     Utilisez « public » pour les messages d'interruption SNMP.
5. Cliquez sur **Enregistrer**.

Activation de la fonction syslog

Vous pouvez identifier un emplacement pour le journal des violations OnCommand Insight et des alertes de performances, ainsi que des messages d'audit, et activer le processus de journalisation.

Avant de commencer

- Vous devez disposer de l'adresse IP du serveur sur lequel stocker le journal système.
- Vous devez connaître le niveau de l'établissement correspondant au type de programme qui enregistre le message, tel QUE LOCAL1 ou USER.

Description de la tâche

Le syslog comprend les types d'informations suivants :

- Messages de violation
- Alertes de performance

- Éventuellement, messages du journal d'audit

Les unités suivantes sont utilisées dans le syslog :

- Mesures d'utilisation : pourcentage
- Mesures de trafic : Mo
- Débit de trafic : Mo/s.

Étapes

1. Dans la barre d'outils Insight, cliquez sur **Admin** et sélectionnez **Notifications**.
2. Faites défiler jusqu'à la section **Syslog** de la page.
3. Cochez la case **Activer syslog**.
4. Si vous le souhaitez, cochez la case **Envoyer audit**. Les nouveaux messages du journal d'audit seront envoyés à syslog en plus d'être affichés sur la page Audit. Notez que les messages du journal d'audit déjà existants ne seront pas envoyés à syslog ; seuls les nouveaux messages de journal seront envoyés.
5. Dans le champ **Server**, entrez l'adresse IP du serveur de journaux.

   Vous pouvez spécifier un port personnalisé en l'ajoutant après deux-points à la fin de l'adresse IP du serveur (par exemple serveur:port). Si le port n'est pas spécifié, le port syslog par défaut de 514 est utilisé.
6. Dans le champ **Facility**, sélectionnez le niveau de l'établissement correspondant au type de programme qui enregistre le message.
7. Cliquez sur **Enregistrer**.

Contenu des syslog Insight

Vous pouvez activer un syslog sur un serveur pour collecter des messages d'alerte de violation Insight et de performance incluant des données d'utilisation et de trafic.

Types de message

Insight syslog répertorie trois types de messages :

- Violations du chemin SAN
- Violations générales
- Alertes de performance

Données fournies

Les descriptions des violations incluent les éléments impliqués, l'heure de l'événement et la gravité ou la priorité relative de la violation.

Les alertes de performance incluent les données suivantes :

- Pourcentages d'utilisation
- Types de trafic
- Débit de trafic mesuré en Mo

Configuration des notifications de performances et de violation garantie

OnCommand Insight prend en charge les notifications de performances et assure les violations. Par défaut, Insight n'envoie pas de notifications pour ces violations ; vous devez configurer Insight pour envoyer des e-mails, envoyer des messages syslog au serveur syslog ou pour envoyer des notifications SNMP en cas de violation.

Avant de commencer

Vous devez avoir configuré les méthodes d'envoi par e-mail, syslog et SNMP pour les violations.

Étapes

1. Cliquez sur **Admin** > **Notifications**.
2. Cliquez sur **Evénements**.
3. Dans la section **événements de violation des performances** ou **assurer les événements de violation**, cliquez sur la liste de la méthode de notification (**Email**, **Syslog** ou **SNMP**) de votre choix, puis sélectionnez le niveau de gravité (**Avertissement et supérieur** ou **critique**) de la violation.
4. Cliquez sur **Enregistrer**.

Configuration des notifications d'événements au niveau du système

OnCommand Insight prend en charge les notifications d'événements au niveau du système, tels que les pannes d'unité d'acquisition ou les erreurs de source de données. Pour recevoir des notifications, vous devez configurer Insight pour envoyer des e-mails lorsqu'un ou plusieurs de ces événements se produisent.

Avant de commencer

Vous devez avoir configuré les destinataires des e-mails pour recevoir des notifications dans **Admin** > **Notifications** > **méthodes d'envoi**.

Étapes

1. Cliquez sur **Admin** > **Notifications**.
2. Cliquez sur **Evénements**.
3. Dans la section **événements d'alerte système** E-mail, sélectionnez le niveau de gravité (**Avertissement et supérieur** ou **critique**) pour la notification, ou choisissez **ne pas envoyer** si vous ne souhaitez pas recevoir de notifications d'événements de niveau système.
4. Cliquez sur **Enregistrer**.
5. Cliquez sur **Admin** > **alertes système** pour configurer les alertes elles-mêmes.
6. Pour ajouter une nouvelle alerte, cliquez sur **+Ajouter** et donnez à l'alerte un **Nom** unique. Vous pouvez également cliquer sur l'icône de droite pour **modifier** une alerte existante.

7. Choisissez le **Type d'événement** sur lequel vous souhaitez être averti, par exemple *défaillance de l'unité d'acquisition*.
8. Choisissez un intervalle **Snooze** pour supprimer les notifications sur les événements en double du type sélectionné pour l'intervalle de temps sélectionné. Si vous sélectionnez *Never*, vous recevrez des notifications répétées une fois par minute jusqu'à ce que l'événement ne se produise plus.
9. Choisissez une **gravité** (Avertissement ou critique) pour la notification d'événement.
10. Les notifications par e-mail seront envoyées par défaut à la liste mondiale des destinataires par e-mail, ou vous pouvez cliquer sur le lien fourni pour remplacer la liste globale et envoyer des notifications à des destinataires spécifiques.
11. Cliquez sur Enregistrer pour ajouter l'alerte.

Configuration du traitement ASUP

Tous les produits NetApp sont dotés de fonctionnalités automatisées pour fournir le meilleur support possible aux clients. Le support automatisé (ASUP) envoie régulièrement des informations prédéfinies et spécifiques au support client. Vous pouvez contrôler les informations à transmettre à NetApp et leur fréquence d'envoi.

Avant de commencer

Vous devez configurer OnCommand Insight pour transférer des données avant qu'elles ne soient envoyées.

Description de la tâche

Les données ASUP sont transmises via le protocole HTTPS.

Étapes

1. Dans la barre d'outils Insight, cliquez sur **Admin**.
2. Cliquez sur **Configuration**.
3. Cliquez sur l'onglet **ASUP & Proxy**.
4. Dans la section **ASUP**, sélectionnez **Activer ASUP** pour activer la fonction ASUP.
5. Si vous souhaitez modifier vos informations d'entreprise, mettez à jour les champs suivants :
   - **Nom de la société**
   - **Nom du site**
   - **Qu'envoyer**: Journaux, données de configuration, données de performances
6. Cliquez sur **Tester la connexion** pour vous assurer que la connexion que vous avez spécifiée fonctionne.
7. Cliquez sur **Enregistrer**.
8. Dans la section **Proxy**, choisissez **Activer le proxy** et indiquez les informations relatives à votre proxy **host**, **port** et **user**.
9. Cliquez sur **Tester la connexion** pour vous assurer que le proxy que vous avez spécifié fonctionne.
10. Cliquez sur **Enregistrer**.

Éléments inclus dans le pack AutoSupport (ASUP

Le package AutoSupport contient la sauvegarde de la base de données ainsi que des informations détaillées.

Le pack AutoSupport comprend les éléments suivants :

- Données d'inventaire
- Données de performance (si sélectionnées pour inclusion dans ASUP)
- Sources de données et paramètres de source de données
- Packs d'intégration
- Unités d'acquisition à distance
- Paramètres ASUP/proxy
- Paramètres d'emplacement de sauvegarde
- Paramètres d'emplacement d'archivage
- Paramètres de notification
- Utilisateurs
- Règles de performance
- Entités commerciales et applications
- Règles et paramètres de résolution du périphérique
- Tableaux de bord et widgets
- Tableaux de bord et widgets personnalisés de la page des ressources
- Requêtes
- Annotations et règles d'annotation
- Journaux
- Licences
- État de la source d'acquisition/de données
- Statut MySQL
- Informations système

Le package AutoSupport n'inclut pas :

- Paramètres de l'outil de sécurité/informations du coffre-fort (sauvegardés via un processus CLI distinct)
- Données de performance (si cette option n'est pas sélectionnée pour être incluse dans ASUP)

> Si vous choisissez d'inclure les données de performances dans ASUP, elles incluent les sept derniers jours de données. Les données restantes seront dans l'archive si cette fonction est activée. ASUP n'inclut pas les données d'archive.

Définition des applications

Si vous souhaitez suivre les données associées à des applications spécifiques

s’exécutant dans votre environnement, vous devez définir ces applications.

Avant de commencer

Si vous souhaitez associer l’application à une entité métier, vous devez avoir déjà créé l’entité métier.

Description de la tâche

Vous pouvez associer des applications aux ressources suivantes : hôtes, machines virtuelles, volumes, volumes internes, qtrees, les partages et les hyperviseurs.

Étapes

1. Connectez-vous à l’interface utilisateur Web de OnCommand Insight.
2. Cliquez sur **gérer** et sélectionnez **applications**.

   Après avoir défini une application, la page applications affiche le nom de l’application, sa priorité et, le cas échéant, l’entité métier associée à l’application.

3. Cliquez sur **Ajouter**.

   La boîte de dialogue Ajouter une application s’affiche.

4. Entrez un nom unique pour l’application dans la zone **Nom**.
5. Cliquez sur **priorité** et sélectionnez la priorité (critique, élevée, moyenne ou faible) de l’application dans votre environnement.
6. Si vous prévoyez d’utiliser cette application avec une entité métier, cliquez sur **entité commerciale** et sélectionnez l’entité dans la liste.
7. **Facultatif** : si vous n’utilisez pas le partage de volume, désactivez la case **Valider le partage de volume**.

   Ceci nécessite la licence assure. Définissez cette option pour vous assurer que chaque hôte a accès aux mêmes volumes dans un cluster. Par exemple, les hôtes des clusters haute disponibilité doivent souvent être masqués pour les mêmes volumes afin de permettre le basculement. Cependant, les hôtes d’applications non liées n’ont généralement pas besoin d’accéder aux mêmes volumes physiques. En outre, les stratégies réglementaires peuvent vous obliger à interdire explicitement aux applications non liées d’accéder aux mêmes volumes physiques pour des raisons de sécurité.

8. Cliquez sur **Enregistrer**.

   L’application s’affiche dans la page applications. Si vous cliquez sur le nom de l’application, Insight affiche la page de ressources de l’application.

Une fois que vous avez terminé

Après avoir défini une application, vous pouvez accéder à une page de ressources pour l’hôte, la machine virtuelle, le volume, le volume interne ou l’hyperviseur afin d’affecter une application à une ressource.

Affectation d’applications aux ressources

Après avoir défini des applications avec ou sans entités métier, vous pouvez les associer à des ressources.

Étapes

1. Connectez-vous à l'interface utilisateur Web de OnCommand Insight.
2. Recherchez la ressource (hôte, machine virtuelle, volume ou volume interne) à laquelle vous souhaitez appliquer l'application en effectuant l'une des opérations suivantes :
   - Cliquez sur **Tableau de bord**, sélectionnez **Tableau de bord des actifs**, puis cliquez sur la ressource.
   - Cliquez sur Dans la barre d'outils pour afficher la zone **Rechercher des actifs**, tapez le nom de la ressource, puis sélectionnez la ressource dans la liste.
3. Dans la section **données utilisateur** de la page de ressource, placez votre curseur sur le nom de l'application actuellement affectée à l'actif (si aucune application n'est affectée, **aucune** s'affiche à la place), puis cliquez sur (Modifier l'application).

   La liste des applications disponibles pour l'actif sélectionné s'affiche. Les applications actuellement associées à l'actif sont précédées d'une coche.
4. Vous pouvez taper dans la zone de recherche pour filtrer les noms d'applications ou faire défiler la liste vers le bas.
5. Sélectionnez les applications que vous souhaitez associer à la ressource.

   Vous pouvez attribuer plusieurs applications à l'hôte, à la machine virtuelle et au volume interne ; cependant, vous ne pouvez affecter qu'une seule application au volume.
6. Cliquez sur pour affecter l'application ou les applications sélectionnées à la ressource.

   Les noms des applications apparaissent dans la section données utilisateur ; si l'application est associée à une entité métier, le nom de l'entité métier apparaît également dans cette section.

Modification d'applications

Vous pouvez modifier la priorité d'une application, l'entité métier associée à une application ou l'état du partage de volumes.

Étapes

1. Connectez-vous à l'interface utilisateur Web de OnCommand Insight.
2. Cliquez sur **gérer** et sélectionnez **applications**.
3. Placez le curseur sur l'application que vous souhaitez modifier et cliquez sur .

   La boîte de dialogue Modifier l'application s'affiche.
4. Effectuez l'une des opérations suivantes :
   - Cliquez sur **priorité** et sélectionnez une autre priorité.

     Vous ne pouvez pas modifier le nom de l'application.
   - Cliquez sur **entité commerciale** et sélectionnez une autre entité commerciale à associer à l'application ou sélectionnez **aucune** pour supprimer l'association de l'application à l'entité métier.
   - Cliquez pour effacer ou sélectionner **Valider le partage de volume**.

Cette option n’est disponible que si vous disposez de la licence assure.

5. Cliquez sur **Enregistrer**.

Suppression d’applications

Vous pouvez supprimer une application lorsque celle-ci ne répond plus à un besoin de votre environnement.

Étapes

1. Connectez-vous à l’interface utilisateur Web Insight.
2. Cliquez sur **gérer** et sélectionnez **applications**.
3. Placez le curseur sur l’application à supprimer et cliquez sur .

   Une boîte de dialogue de confirmation s’affiche, vous demandant si vous souhaitez supprimer l’application.

4. Cliquez sur **OK**.

La hiérarchie de vos entités commerciales

Vous pouvez définir des entités métier pour assurer le suivi des données de votre environnement et générer des rapports à un niveau plus granulaire.

Dans OnCommand Insight, la hiérarchie des entités métier contient les niveaux suivants :

- **Tenant** est principalement utilisé par les fournisseurs de services pour associer des ressources à un client, par exemple NetApp.
- **Secteur d’activité (LOB)** est un secteur d’activité ou une gamme de produits au sein d’une entreprise, par exemple, le stockage de données.
- **Unité commerciale** représente une unité commerciale traditionnelle telle que juridique ou Marketing.
- **Le projet** est souvent utilisé pour identifier un projet spécifique au sein d’une unité commerciale pour lequel vous souhaitez une refacturation de capacité. Par exemple, « brevets » peut être un nom de projet pour l’unité commerciale juridique et « événements de vente » peut être un nom de projet pour l’unité commerciale Marketing. Notez que les noms de niveau peuvent inclure des espaces.

Vous n’êtes pas tenu d’utiliser tous les niveaux dans la conception de votre hiérarchie d’entreprise.

Conception de la hiérarchie de vos entités commerciales

Vous devez comprendre les éléments de votre structure d’entreprise et ce qui doit être représenté dans les entités commerciales car ils deviennent une structure fixe dans votre base de données OnCommand Insight. Vous pouvez utiliser les informations suivantes pour configurer vos entités commerciales. N’oubliez pas que vous n’avez pas besoin d’utiliser tous les niveaux hiérarchiques pour collecter des données dans ces catégories.

Étapes

1. Examinez chaque niveau de la hiérarchie des entités métier pour déterminer si ce niveau doit être inclus dans la hiérarchie des entités métiers de votre entreprise :
   - **Le niveau locataire** est nécessaire si votre entreprise est un FAI et que vous voulez suivre l'utilisation des ressources par le client.
   - **Secteur d'activité (LOB)** est nécessaire dans la hiérarchie si les données des différentes gammes de produits doivent être suivies.
   - **L'unité commerciale** est requise si vous devez effectuer le suivi des données pour différents services. Ce niveau de la hiérarchie est souvent utile pour séparer une ressource qu'un ministère utilise et que les autres ministères n'utilisent pas.
   - **Le niveau projet** peut être utilisé pour le travail spécialisé au sein d'un ministère. Ces données peuvent être utiles pour déterminer, définir et surveiller les besoins technologiques d'un projet distinct par rapport à d'autres projets d'une entreprise ou d'un service.
2. Créez un graphique montrant chaque entité commerciale avec les noms de tous les niveaux au sein de l'entité.
3. Vérifiez les noms dans la hiérarchie pour vous assurer qu'ils seront explicites dans les vues et rapports OnCommand Insight.
4. Identifiez toutes les applications associées à chaque entité business.

Création d'entités commerciales

Après avoir conçu la hiérarchie des entités métier pour votre société, vous pouvez configurer des applications, puis associer les entités métier aux applications. Ce processus crée la structure des entités métier dans votre base de données OnCommand Insight.

Description de la tâche

L'association d'applications à des entités commerciales est facultative ; cependant, il s'agit d'une meilleure pratique.

Étapes

1. Connectez-vous à l'interface utilisateur Web Insight.
2. Cliquez sur **gérer** et sélectionnez **entités commerciales**.

   La page entités commerciales s'affiche.
3. Cliquez sur 

pour commencer à construire une nouvelle entité.

   La boîte de dialogue **Ajouter une entité métier** s'affiche.
4. Pour chaque niveau d'entité (locataire, secteur d'activité, entité commerciale et projet), vous pouvez effectuer l'une des opérations suivantes :
   - Cliquez sur la liste de niveau d'entité et sélectionnez une valeur.
   - Saisissez une nouvelle valeur et appuyez sur entrée.
   - Laissez la valeur de niveau d'entité N/A si vous ne souhaitez pas utiliser le niveau d'entité pour l'entité métier.

5. Cliquez sur **Enregistrer**.

Affectation d'entités commerciales à des actifs

Vous pouvez attribuer une entité métier à une ressource (hôte, port, stockage, commutateur, machine virtuelle, qtree, share, volume, or internal volume) sans avoir associé l'entité business à une application. cependant, les entités business sont attribuées automatiquement à une ressource si cette ressource est associée à une application associée à une entité business.

Avant de commencer

Vous devez avoir déjà créé une entité métier.

Description de la tâche

Bien que vous puissiez affecter des entités métier directement à des actifs, il est recommandé d'affecter des applications à des actifs, puis d'affecter des entités métier à des actifs.

Étapes

1. Connectez-vous à l'interface utilisateur Web de OnCommand Insight.
2. Recherchez la ressource à laquelle vous souhaitez appliquer l'entité commerciale en effectuant l'une des actions suivantes :
   - Cliquez sur la ressource dans le tableau de bord des ressources.
   - Cliquez sur Dans la barre d'outils pour afficher la zone **Rechercher des actifs**, tapez le nom de la ressource, puis sélectionnez la ressource dans la liste.
3. Dans la section **données utilisateur** de la page de la ressource, placez votre curseur sur **aucune** en regard de **entités commerciales**, puis cliquez sur .

   La liste des entités commerciales disponibles s'affiche.

4. Saisissez la case **Rechercher** pour filtrer la liste d'une entité spécifique ou faites défiler la liste vers le bas ; sélectionnez une entité métier dans la liste.

   Si l'entité métier que vous choisissez est associée à une application, le nom de l'application s'affiche. Dans ce cas, le mot « sérived » apparaît à côté du nom de l'entité commerciale. Si vous souhaitez maintenir l'entité uniquement pour l'actif et non pour l'application associée, vous pouvez remplacer manuellement l'affectation de l'application.

5. Pour remplacer une application dérivée d'une entité commerciale, placez votre curseur sur le nom de l'application et cliquez sur , sélectionnez une autre entité métier et sélectionnez une autre application dans la liste.

Affectation d'entités commerciales à des entités commerciales ou suppression de plusieurs ressources

Vous pouvez affecter ou supprimer des entités métier de plusieurs actifs en utilisant une requête au lieu de devoir les affecter ou les supprimer manuellement.

Avant de commencer

Vous devez avoir déjà créé les entités métier que vous souhaitez ajouter aux ressources souhaitées.

Étapes

1. Créez une nouvelle requête ou ouvrez une requête existante.
2. Si vous le souhaitez, filtrez les actifs auxquels vous souhaitez ajouter des entités métier.
3. Sélectionnez les ressources souhaitées dans la liste ou cliquez sur ☐ ▾ | Pour sélectionner **tout**.

   Le bouton **actions** s'affiche.

4. Pour ajouter une entité métier aux actifs sélectionnés, cliquez sur Actions ▾. Si le type d'actif sélectionné peut avoir des entités métier qui lui sont attribuées, vous verrez le choix de menu **Ajouter une entité métier**. Sélectionnez cette option.
5. Sélectionnez l'entité métier souhaitée dans la liste et cliquez sur **Enregistrer**.

   Toute nouvelle entité métier que vous attribuez remplace toutes les entités métier qui ont déjà été affectées à la ressource. L'affectation d'applications à des actifs remplacera également les entités métier affectées de la même manière. L'affectation d'entités commerciales à comme ressource peut également remplacer toutes les applications affectées à cette ressource.

6. Pour supprimer une entité métier affectée aux actifs, cliquez sur Actions ▾ Et sélectionnez **Supprimer l'entité commerciale**.
7. Sélectionnez l'entité métier souhaitée dans la liste et cliquez sur **Supprimer**.

Définition des annotations

Lors de la personnalisation de OnCommand Insight pour suivre les données selon les exigences de votre entreprise, vous pouvez définir les annotations spécialisées nécessaires pour obtenir une vue d'ensemble de vos données : par exemple, la fin de vie des ressources, le data Center, l'emplacement du bâtiment, le niveau de stockage ou le volume des ressources, et le niveau de service du volume interne.

Étapes

1. Répertoriez toute terminologie de l'industrie à laquelle les données d'environnement doivent être associées.
2. Répertoriez la terminologie de l'entreprise à laquelle les données d'environnement doivent être associées, qui n'est pas déjà suivie à l'aide des entités métier.
3. Identifiez tout type d'annotation par défaut que vous pouvez utiliser.
4. Identifiez les annotations personnalisées que vous devez créer.

Utilisation des annotations pour surveiller votre environnement

Lorsque vous personnalisez OnCommand Insight pour suivre les données en fonction des besoins de votre entreprise, vous pouvez définir des notes spécialisées, appelées

annotations, et les affecter à vos ressources. Par exemple, vous pouvez annoter les ressources avec des informations telles que la fin de vie des ressources, le data Center, l'emplacement du bâtiment, le niveau de stockage ou le niveau de service 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.
- Utilisation de l'utilitaire d'importation d'annotations pour importer des annotations.
- Filtrer les ressources par leurs annotations.
- Regroupement des données dans des rapports en fonction des annotations et génération de ces rapports.

  Pour plus d'informations sur les rapports, reportez-vous au *Guide de création de rapports OnCommand Insight*.

Gestion des types d'annotation

OnCommand Insight fournit certains types d'annotations par défaut, comme le cycle de vie des ressources (date d'anniversaire ou fin de vie), l'emplacement du bâtiment ou du data Center et le niveau, que vous pouvez personnaliser pour afficher dans vos rapports. Vous pouvez définir des valeurs pour les types d'annotation par défaut ou créer vos propres types d'annotation personnalisés. Vous pouvez modifier ces valeurs ultérieurement.

Types d'annotation par défaut

OnCommandInsight fournit certains types d'annotations par défaut. Ces annotations peuvent être utilisées pour filtrer ou regrouper des données et filtrer les rapports de 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'annotation par défaut. Vous pouvez modifier n'importe lequel de ces noms d'annotation en fonction de vos besoins.

Types d’annotation	Description	Type
Alias	Nom convivial d’une ressource.	Texte
Anniversaire	Date à laquelle le périphérique a été ou sera mis en ligne.	Date
Bâtiment	Emplacement physique de l’hôte, du stockage, du commutateur et des ressources sur bande.	Liste
Ville	Emplacement municipal des ressources d’hôte, de stockage, de commutateur et de bande.	Liste
Calculer le groupe de ressources	Affectation de groupe utilisée par la source de données Host et VM Filesystems.	Liste
Continent américain	Emplacement géographique de l’hôte, du stockage, des commutateurs et des bandes	Liste
Pays	Emplacement national des ressources d’hôte, de stockage, de commutateur et de bande.	Liste
Data Center	Emplacement physique de la ressource et disponible pour les hôtes, les baies de stockage, les commutateurs et les bandes.	Liste
Directement attaché	Indique (Oui ou non) si une ressource de stockage est connectée directement aux hôtes.	Booléen
Fin de vie	Date à laquelle un périphérique sera mis hors ligne, par exemple, si le bail a expiré ou si le matériel est retiré.	Date
Alias de la structure	Nom convivial d’un tissu.	Texte
Plancher	Emplacement d’un dispositif sur un étage d’un bâtiment. Peut être défini pour les hôtes, les baies de stockage, les commutateurs et les bandes.	Liste

Chaud	Appareils déjà utilisés régulièrement ou au seuil de capacité.	Booléen
Remarque	Commentaires que vous souhaitez associer à une ressource.	Texte
Rack	Rack dans lequel réside la ressource.	Texte
Chambre	Salle dans un bâtiment ou autre emplacement des ressources hôte, de stockage, de commutateur et de bande.	Liste
SAN	Partition logique du réseau. Disponible sur les hôtes, les baies de stockage, les bandes, les commutateurs et les applications.	Liste
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
État/province	État ou province dans lequel la ressource est située.	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	Inclut des options prédéfinies pour la configuration de catégories pour les commutateurs. En général, ces désignations restent pour la durée de vie de l'appareil, bien que vous puissiez les modifier, si nécessaire. 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, Switch Level, Service Level, Tier et violation Severity sont des annotations au niveau du système, que vous ne pouvez pas supprimer ou renommer ; vous pouvez modifier uniquement les valeurs qui leur sont attribuées.

Mode d'affectation des annotations

Vous pouvez affecter des annotations manuellement ou automatiquement à l'aide des règles d'annotation. OnCommand Insight attribue également automatiquement certaines annotations lors de l'acquisition des actifs et par héritage. Toutes les annotations que vous attribuez à une ressource apparaissent dans la section données utilisateur de la page ressource.

Les annotations sont attribuées de la manière suivante :

- Vous pouvez affecter une annotation manuellement à une ressource.

  Si une annotation est affectée directement à une ressource, elle apparaît sous la forme d'un texte normal sur une page de ressource. Les annotations attribuées manuellement ont toujours priorité sur les annotations héritées ou affectées par des règles d'annotation.

- Vous pouvez créer une règle d'annotation pour affecter automatiquement des annotations aux actifs du même type.

  Si l'annotation est affectée par une règle, Insight affiche le nom de la règle en regard du nom de l'annotation sur une page de ressource.

- Insight associe automatiquement un niveau à un modèle de niveau de stockage pour accélérer l'affectation des annotations de stockage à vos ressources lors de l'acquisition des ressources.

  Certaines ressources de stockage sont automatiquement associées à un niveau prédéfini (tiers 1 et 2). Par exemple, le niveau de stockage Symmetrix est basé sur la famille Symmetrix et VMAX et est associé au

niveau 1. Vous pouvez modifier les valeurs par défaut pour les adapter à vos exigences de niveau. Si l'annotation est affectée par Insight (par exemple, Tier), vous voyez « défini par le système » lorsque vous placez votre curseur sur le nom de l'annotation sur une page d'actif.

- Quelques ressources (enfants d'une ressource) peuvent dériver l'annotation de niveau prédéfinie de leur ressource (parent).

  Par exemple, si vous attribuez une annotation à un stockage, l'annotation de niveau est dérivée de tous les pools de stockage, des volumes internes, des volumes, des qtrees et des partages appartenant au stockage. Si une annotation différente est appliquée à un volume interne du stockage, l'annotation est ensuite dérivée de tous les volumes, qtrees et partages. "derived" apparaît à côté du nom de l'annotation sur une page de ressource.

Association de coûts à des annotations

Avant d'exécuter des rapports sur les coûts, vous devez associer les coûts aux annotations au niveau du système niveau de service, niveau de commutateur et niveau. Cela permet de refacturer les utilisateurs du stockage en fonction de leur utilisation réelle de la capacité de production et répliquée. Par exemple, pour le niveau, vous pouvez avoir des valeurs de niveau Gold et Silver et attribuer un coût plus élevé au niveau Gold que au niveau Silver.

Étapes

1. Connectez-vous à l'interface utilisateur Insigtweb.
2. Cliquez sur gérer et sélectionnez **Annotations**.

   La page Annotation s'affiche.

3. Placez le curseur sur l'annotation niveau de service, niveau de commutation ou niveau, puis cliquez sur  .

   La boîte de dialogue Editer l'annotation s'affiche.

4. Entrez les valeurs de tous les niveaux existants dans le champ **coût**.

   Les annotations de niveau et de niveau de service ont respectivement des valeurs de hiérarchisation automatique et de stockage objet que vous ne pouvez pas supprimer.

5. Cliquez sur 

pour ajouter des niveaux supplémentaires.
6. Cliquez sur **Enregistrer** lorsque vous avez terminé.

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 OnCommand Insight propose un ensemble d'annotations par défaut, vous pouvez voir les données de différentes manières. 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 Insight.

Étapes

1. Connectez-vous à l'interface utilisateur Web Insight.
2. Cliquez sur **gérer** et sélectionnez **Annotations**.

   La page Annotations affiche la liste des annotations.

3. Cliquez sur  .

   La boîte de dialogue **Ajouter une annotation** s'affiche.

4. Entrez un nom et une description dans les champs **Nom** et **Description**.

   Ces champs peuvent comporter jusqu'à 255 caractères.

   Noms d'annotation commençant ou se terminant par un point « ». ne sont pas pris en charge.

5. Cliquez sur **Type**, puis sélectionnez l'une des options suivantes qui représente le type de données autorisé dans cette annotation :

   - Booléen

     Cela crée une liste déroulante avec les choix de oui et non Par exemple, l'annotation "Direct attached" est booléenne.

   - Date

     Ceci crée un champ contenant une date. Par exemple, si l'annotation est une date, sélectionnez cette option.

   - Liste

     Ceci peut créer l'une des situations suivantes :

     - Liste déroulante fixe

       Lorsque d'autres personnes sont affectées à ce type d'annotation sur un périphérique, elles ne peuvent pas ajouter de valeurs supplémentaires à la liste.

     - 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

     Cela crée un champ dans lequel l'utilisateur qui affecte l'annotation peut entrer un nombre. Par exemple, si le type d'annotation est ""Floor""", l'utilisateur peut sélectionner la valeur Type de ""number"" et entrer le numéro d'étage.

   - Texte

Cela crée un champ qui permet le texte libre. Par exemple, vous pouvez entrer « 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.

6. Si vous sélectionnez **List**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 un nom dans les champs **valeur** et **Description**.
   c. Cliquez sur + Add pour ajouter des valeurs supplémentaires.
   d. Cliquez sur pour supprimer une valeur.
7. Cliquez sur **Enregistrer**.

Vos annotations apparaissent dans la liste de la page Annotations.

Informations connexes

"Importation et exportation des données utilisateur"

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 affecter automatiquement des annotations aux actifs d'un type particulier, vous pouvez, à l'aide des règles d'annotation, affecter des annotations à une ressource individuelle en utilisant sa page d'actif.

Avant de commencer

Vous devez avoir créé l'annotation que vous souhaitez attribuer.

Étapes

1. Connectez-vous à l'interface utilisateur Web de OnCommand Insight.
2. Recherchez la ressource à laquelle vous souhaitez appliquer l'annotation en procédant de l'une des manières suivantes :
   - Cliquez sur la ressource dans le tableau de bord des ressources.
   - Cliquez sur Dans la barre d'outils pour afficher la zone **Rechercher des actifs**, saisissez le type

ou le nom de la ressource, puis sélectionnez la ressource dans la liste qui s'affiche.

La page ASSET s'affiche.

3. Dans la section **données utilisateur** de la page de la ressource, cliquez sur + Add.

   La boîte de dialogue Ajouter une annotation s'affiche.

4. Cliquez sur **Annotation** et sélectionnez une annotation dans la liste.
5. Cliquez sur **valeur** et effectuez l'une des opérations suivantes, selon le type d'annotation 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.
6. Cliquez sur **Enregistrer**.
7. Si vous souhaitez modifier la valeur de l'annotation après l'avoir attribuée, cliquez sur et sélectionnez une autre valeur.

   Si l'annotation est de type liste pour laquelle l'option **Ajouter des valeurs dynamiquement lors de l'affectation d'annotation** est sélectionnée, vous pouvez taper pour ajouter une nouvelle valeur en plus de sélectionner une valeur existante.

Modification des annotations

Vous pouvez modifier le nom, la description ou les valeurs d'une annotation ou supprimer une annotation que vous ne souhaitez plus utiliser.

Étapes

1. Connectez-vous à l'interface utilisateur OnCommand Insigtweb.
2. Cliquez sur **gérer** et sélectionnez **Annotations**.

   La page Annotations s'affiche.

3. Placez le curseur sur l'annotation à modifier et cliquez sur .

   La boîte de dialogue **Modifier l'annotation** s'affiche.

4. Vous pouvez apporter les modifications suivantes à une annotation :

   a. Modifiez le nom, la description ou les deux.

      Notez toutefois que vous pouvez entrer un maximum de 255 caractères pour le nom et la description, et que vous ne pouvez pas modifier le type d'une annotation. En outre, pour les annotations au niveau du système, vous ne pouvez pas modifier le nom ou la description ; cependant, vous pouvez ajouter ou supprimer des valeurs si l'annotation est un type de liste.

      Si une annotation personnalisée est publiée dans l'entrepôt de données et que vous la renommez, vous perdrez les données historiques.

   a. Pour ajouter une autre valeur à une annotation de type liste, cliquez sur + Add.
   b. Pour supprimer une valeur d'une annotation de type liste, cliquez sur .

Vous ne pouvez pas supprimer une valeur d'annotation si cette valeur est associée à une annotation contenue dans une règle d'annotation, une requête ou une règle de performance.

5. Cliquez sur **Enregistrer** lorsque vous avez terminé.

Une fois que vous avez terminé

Si vous allez utiliser des annotations dans l'entrepôt de données, vous devez forcer une mise à jour des annotations dans l'entrepôt de données. Reportez-vous au *Guide d'administration de l'entrepôt de données OnCommand Insight*.

Suppression d'annotations

Vous pouvez supprimer une annotation que vous ne souhaitez plus utiliser. Il est impossible de supprimer une annotation au niveau du système ou une annotation utilisée dans une règle d'annotation, une requête ou une règle de performance.

Étapes

1. Connectez-vous à l'interface utilisateur Web de OnCommand Insight.
2. Cliquez sur **gérer** et sélectionnez **Annotations**.

   La page Annotations s'affiche.

3. Placez le curseur sur l'annotation à supprimer, puis cliquez sur .

   Une boîte de dialogue de confirmation s'affiche.

4. Cliquez sur **OK**.

Affectation d'annotations à des actifs 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. OnCommand Insight affecte les annotations aux ressources en fonction de ces règles. Insight 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.

Règles d'annotation de stockage par défaut

Pour accélérer l'affectation des annotations de stockage à vos ressources, OnCommand Insight inclut 21 règles d'annotation par défaut, qui associent un niveau de Tier à un modèle de hiérarchisation du stockage. Toutes vos ressources de stockage sont automatiquement associées à un niveau lors de l'acquisition des ressources de votre environnement.

Les règles d'annotation par défaut appliquent les annotations de niveau de la manière suivante :

- Niveau 1, qualité du stockage

  L'annotation de niveau 1 est appliquée aux fournisseurs suivants et à leurs familles spécifiées : EMC (Symmetrix), HDS (HDS9500V, HDS9900, HDS9900V, R600, R700, USP r, USP V), IBM (DS8000),

NetApp (FAS6000 ou FAS6200) et Violin (mémoire).

- Niveau 2, qualité du stockage

  L'annotation de niveau 2 s'applique aux fournisseurs suivants et à leurs familles spécifiques : HP (3PAR StoreServ ou EVA), EMC (CLARiiON), HDS (AMS ou D800), IBM (XIV) et NetApp (FAS3000, FAS3100 et FAS3200).

Vous pouvez modifier les paramètres par défaut de ces règles pour les adapter à vos exigences de niveau, ou vous pouvez les supprimer si vous n'en avez pas besoin.

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. Connectez-vous à l'interface utilisateur Web de OnCommand Insight.
2. Cliquez sur **gérer** et sélectionnez **règles d'annotation**.

   La page règles d'annotation affiche la liste des règles d'annotation existantes.

3. Cliquez sur + Add.

   La boîte de dialogue Ajouter une règle s'affiche.

4. 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 **requête** et sélectionnez la requête que OnCommand Insight doit utiliser pour appliquer l'annotation aux actifs.
   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.

5. Cliquez sur **Enregistrer**.
6. Cliquez sur **Exécuter toutes les règles** si vous souhaitez exécuter toutes les règles immédiatement ; sinon, les règles sont exécutées à un intervalle planifié régulièrement.

Définition de la priorité des règles d'annotation

Par défaut, OnCommand Insight évalue les règles d'annotation de manière séquentielle. Toutefois, vous pouvez configurer l'ordre dans lequel OnCommand Insight évalue les règles d'annotation si vous souhaitez qu'Insight évalue les règles dans un ordre spécifique.

Étapes

1. Connectez-vous à l'interface utilisateur Insigtweb.
2. Cliquez sur **gérer** et sélectionnez **règles d'annotation**.

   La page règles d'annotation affiche la liste des règles d'annotation existantes.

3. Placez le curseur sur une règle d'annotation.

   Les flèches de priorité apparaissent à droite de la règle.

4. Pour déplacer une règle vers le haut ou vers le bas dans la liste, cliquez sur la flèche vers le haut ou vers le bas.

   Par défaut, les nouvelles règles sont ajoutées séquentiellement à la liste des règles. 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.

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. Connectez-vous à l'interface utilisateur OnCommand Insigtweb.
2. Cliquez sur **gérer** et sélectionnez **règles d'annotation**.

   La page règles d'annotation affiche la liste des règles d'annotation existantes.

3. Recherchez la règle à modifier :
   - Sur la page règles d'annotation, vous pouvez filtrer les règles d'annotation en entrant une valeur dans la zone de filtre.
   - Cliquez sur un numéro de page pour parcourir les règles d'annotation par page s'il y a plus de règles que d'ajustement sur une page.
4. Effectuez l'une des opérations suivantes pour afficher la boîte de dialogue **Modifier la règle** :
   - Si vous vous trouvez sur la page règles d'annotation, placez le curseur sur la règle d'annotation et cliquez sur  .

◦ Si vous vous trouvez sur une page de ressource, placez votre curseur sur l'annotation associée à la règle, placez votre curseur sur le nom de la règle lorsqu'elle s'affiche, puis cliquez sur le nom de la règle.

5. Effectuez les modifications requises et cliquez sur **Enregistrer**.

Suppression de règles d'annotation

Vous pouvez supprimer une règle d'annotation lorsque celle-ci n'est plus nécessaire pour surveiller les objets de votre réseau.

Étapes

1. Connectez-vous à l'interface utilisateur OnCommand Insigtweb.
2. Cliquez sur **gérer** et sélectionnez **règles d'annotation**.

   La page règles d'annotation affiche la liste des règles d'annotation existantes.

3. Recherchez la règle à supprimer :
   ◦ Sur la page règles d'annotation, vous pouvez filtrer les règles d'annotation en entrant une valeur dans la zone de filtre.
   ◦ Cliquez sur un numéro de page pour parcourir les règles d'annotation par page s'il y a plus de règles que d'ajustement sur une seule page.
4. Pointez le curseur sur la règle à supprimer, puis cliquez sur 🗑.

   Un message de confirmation s'affiche, vous invitant à supprimer la règle.

5. Cliquez sur **OK**.

Importation de valeurs d'annotation

Si vous conservez des annotations sur des objets SAN (tels que le stockage, les hôtes et les machines virtuelles) dans un fichier CSV, vous pouvez importer ces informations dans OnCommand Insight. Vous pouvez importer des applications, des entités commerciales ou des annotations telles que des niveaux et des constructions.

Description de la tâche

Les règles suivantes s'appliquent :

- Si une valeur d'annotation est vide, cette annotation est supprimée de l'objet.
- Lors de l'annotation de volumes ou de volumes internes, le nom de l'objet est une combinaison du nom du stockage et du nom du volume utilisant le séparateur tiret et flèche (->) :

```
<storage_name>-><volume_name>
```

- Lorsque le stockage, les commutateurs ou les ports sont annotés, la colonne application est ignorée.
- Les colonnes tenant, Line_of_Business, Business_Unit et Project constituent une entité métier.

  Toutes les valeurs peuvent rester vides. Si une application est déjà associée à une entité métier différente

des valeurs d'entrée, elle est affectée à la nouvelle entité métier.

L'utilitaire d'importation prend en charge les types d'objet et les clés suivants :

Type	Clé
Hôte	`id-><id>` ou `<Name>` ou `<IP>`
VM	`id-><id>` ou `<Name>`
Pool de stockage	`id-><id>` ou `<Storage_name>-><Storage_Pool_name>`
Volume interne	`id-><id>` ou `<Storage_name>-><Internal_volume_name>`
Volumétrie	`id-><id>` ou `<Storage_name>-><Volume_name>`
Stockage	`id-><id>` ou `<Name>` ou `<IP>`
Commutateur	`id-><id>` ou `<Name>` ou `<IP>`
Port	`id-><id>` ou `<WWN>`
Partagez	`id-><id>` ou `<Storage Name>-><Internal Volume Name>-><Share Name>-><Protocol>` `<Qtree>` est facultatif s'il existe un qtree par défaut.
Qtree	`id-><id>` ou `<Storage Name>-><Internal Volume Name>-><Qtree Name>`

Le fichier CSV doit utiliser le format suivant :

```
, , <Annotation Type> [, <Annotation Type> ...]
[, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]

<Object Type Value 1>, <Object Key 1>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]

...

<Object Type Value N>, <Object Key N>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]
```

Étapes

1. Connectez-vous à l'interface utilisateur Web Insight.
2. Cliquez sur **Admin** et sélectionnez **Dépannage**.

   La page Dépannage s'affiche.
3. Dans la section **autres tâches** de la page, cliquez sur le lien **Portail OnCommand Insight**.
4. Cliquez sur **API Insight Connect**.
5. Connectez-vous au portail.
6. Cliquez sur **Utilitaire d'importation d'annotations**.
7. Enregistrez le `.zip` fichier, décompressez-le et lisez le `readme.txt` pour obtenir des informations et des exemples supplémentaires.
8. Placez le fichier CSV dans le même dossier que le `.zip` fichier.
9. Dans la fenêtre de ligne de commande, entrez les informations suivantes :

   ```
   java -jar rest-import-utility.jar [-uusername] [-ppassword]
   [-aserver name or IP address] [-bbatch size] [-ccase
   sensitive:true/false]
   [-lextra logging:true/false] csv filename
   ```

   L'option -l, qui active la journalisation supplémentaire, et l'option -c, qui active la sensibilité à la casse, sont définies sur false par défaut. Par conséquent, vous devez les spécifier uniquement lorsque vous voulez utiliser les fonctions.

   Il n'y a pas d'espace entre les options et leurs valeurs.

Les mots-clés suivants sont réservés et empêchent les utilisateurs de les spécifier comme noms d'annotation : - application - priorité_application - locataire - ligne_de_métier - unité_commerciale - des erreurs de projet sont générées si vous essayez d'importer un type d'annotation à l'aide d'un des mots-clés réservés. Si vous avez créé des noms d'annotations à l'aide de ces mots clés, vous devez les modifier pour que l'utilitaire d'importation fonctionne correctement.

L'utilitaire d'importation d'annotations nécessite Java 8 ou Java 11. Assurez-vous que l'une de ces installations est installée avant d'exécuter l'utilitaire d'importation. Il est recommandé d'utiliser la dernière version d'OpenJDK 11.

Affectation d'annotations à plusieurs ressources à l'aide d'une requête

L'affectation d'une annotation à un groupe de ressources vous permet d'identifier et d'utiliser plus facilement ces ressources associées dans des requêtes ou des tableaux de bord.

Avant de commencer

Les annotations que vous souhaitez affecter aux actifs doivent avoir été créées au préalable.

Description de la tâche

Vous pouvez simplifier l'affectation d'une annotation à plusieurs actifs à l'aide d'une requête. Par exemple, si vous souhaitez attribuer une annotation d'adresse personnalisée à toutes vos baies à un emplacement de data Center spécifique.

Étapes

1. Créez une nouvelle requête pour identifier les actifs sur lesquels vous souhaitez affecter une annotation. Cliquez sur **requêtes** > **+Nouvelle requête**.
2. Dans la liste déroulante **Rechercher…**, choisissez **stockage**. Vous pouvez définir des filtres pour affiner davantage la liste des stockages affichés.
3. Dans la liste des stockages affichés, sélectionnez-en un ou plusieurs en cochant la case en regard du nom du stockage. Vous pouvez également sélectionner tous les stockages affichés en cliquant sur la case principale en haut de la liste.
4. Lorsque vous avez sélectionné tous les stockages souhaités, cliquez sur **actions** > **Modifier l'annotation**.

   Le système affiche la boîte de dialogue Ajouter une annotation.

5. Sélectionnez les options **Annotation** et **valeur** que vous souhaitez affecter aux stockages et cliquez sur **Enregistrer**.

   Si vous affichez la colonne de cette annotation, elle apparaît sur tous les stockages sélectionnés.

6. Vous pouvez désormais utiliser l'annotation pour filtrer les stockages dans un widget ou une requête. Dans un widget, vous pouvez effectuer les opérations suivantes :

   a. Créez un tableau de bord ou ouvrez-en un existant. Ajoutez une **variable** et choisissez l'annotation que vous avez définie sur les stockages ci-dessus. La variable est ajoutée au tableau de bord.

   b. Dans le champ de variable que vous venez d'ajouter, cliquez sur **Any** et entrez la valeur appropriée à

filtrer. Cliquez sur la coche pour enregistrer la valeur de la variable.

c. Ajouter un widget. Dans la requête du widget, cliquez sur le bouton **Filtrer par+**et sélectionnez l'annotation appropriée dans la liste.

d. Cliquez sur **Any** et sélectionnez la variable d'annotation que vous avez ajoutée ci-dessus. Les variables que vous avez créées commencent par "$" et sont affichées dans la liste déroulante.

e. Définissez tous les autres filtres ou champs que vous désirez, puis cliquez sur **Enregistrer** lorsque le widget est personnalisé à votre goût.

Le widget du tableau de bord affiche uniquement les données des stockages auxquels vous avez attribué l'annotation.

Interrogation des ressources

Les requêtes vous permettent de surveiller et de dépanner votre réseau en recherchant les ressources de votre environnement à un niveau granulaire, en fonction de critères sélectionnés par l'utilisateur (annotations et mesures de performances). En outre, les règles d'annotation, qui attribuent automatiquement des annotations aux ressources, nécessitent une requête.

Ressources utilisées dans les requêtes et les tableaux de bord

Les requêtes Insight et les widgets de tableau de bord peuvent être utilisés avec un large éventail de types de ressources

Les types de ressources suivants peuvent être utilisés dans les requêtes, les widgets de tableau de bord et les pages de ressources personnalisées. 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
- Commutateur
- Bande
- VMDK
- Ordinateur virtuel
- Volumétrie
- Zone
- Membre de la zone

Création d'une requête

Vous pouvez créer une requête pour effectuer des recherches granulaires sur les ressources de votre environnement. Les requêtes vous permettent de découper les données en ajoutant des filtres, puis en triant les résultats pour afficher les données d'inventaire et de performances dans une seule vue.

Description de la tâche

Par exemple, vous pouvez créer une requête pour des volumes, ajouter un filtre pour rechercher des stockages particuliers associés au volume sélectionné, ajouter un filtre pour rechercher une annotation particulière, telle que Tier 1, sur les stockages sélectionnés, Enfin, ajoutez un autre filtre pour rechercher tous les stockages avec les E/S (IOPS) supérieures à 25. Lorsque les résultats sont affichés, vous pouvez trier les colonnes d'informations associées à la requête dans l'ordre croissant ou décroissant.

Lors de l'ajout d'une nouvelle source de données qui acquiert des ressources ou des affectations d'annotation ou d'application, vous pouvez interroger ces ressources, annotations ou applications après l'indexation des requêtes, qui se produit à un intervalle planifié régulier.

Étapes

1. Connectez-vous à l'interface utilisateur Web de OnCommand Insight.
2. Cliquez sur **requêtes** et sélectionnez **+ Nouvelle requête**.
3. Cliquez sur **Sélectionner le type de ressource** et sélectionnez un type d'actif.

   Lorsqu'une ressource est sélectionnée pour une requête, un certain nombre de colonnes par défaut s'affichent automatiquement ; vous pouvez supprimer ces colonnes ou en ajouter de nouvelles à tout moment.

4. Dans la zone de texte **Nom**, tapez le nom de la ressource ou une partie du texte à filtrer par les noms de la ressource.

   Vous pouvez utiliser l'une des options suivantes, seule ou combinée, pour affiner votre recherche dans n'importe quelle zone de texte de la page Nouvelle requête :

   - 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.

5. Cliquez sur  pour afficher les actifs.
6. Pour ajouter un critère, cliquez sur 

et effectuez l'une des opérations suivantes :
   - Tapez pour rechercher un critère spécifique, puis sélectionnez-le.
   - Faites défiler la liste et sélectionnez un critère.
   - Entrez une plage de valeurs si vous choisissez une mesure de performance comme IOPS - lecture (E/S). Les annotations par défaut fournies par Insight sont indiquées par ; il est possible d'avoir des annotations avec des noms en double.

   Une colonne est ajoutée à la liste des résultats de la requête pour les critères et les résultats de la requête dans la liste sont mis à jour.
7. Vous pouvez également cliquer sur pour supprimer une annotation ou une mesure de performance des résultats de la requête.

   Par exemple, si votre requête affiche la latence maximale et le débit maximal pour les datastores et que vous souhaitez afficher uniquement la latence maximale dans la liste des résultats de la requête, cliquez sur ce bouton et décochez la case **débit - Max**. La colonne débit - maximum (Mo/s) est supprimée de la liste des résultats de la requête.

   Selon le nombre de colonnes affichées dans le tableau des résultats de la requête, il se peut que vous ne puissiez pas afficher d'autres colonnes ajoutées. Vous pouvez supprimer une ou plusieurs colonnes jusqu'à ce que les colonnes souhaitées deviennent visibles.
8. Cliquez sur **Enregistrer**, entrez un nom pour la requête, puis cliquez à nouveau sur **Enregistrer**.

   Si vous disposez d'un compte avec un rôle d'administrateur, vous pouvez créer des tableaux de bord personnalisés. Un tableau de bord personnalisé peut comprendre n'importe lequel des widgets de la bibliothèque de widgets, dont plusieurs, vous permettent de représenter les résultats de la requête dans un tableau de bord personnalisé. Pour plus d'informations sur les tableaux de bord personnalisés, reportez-vous au *Guide de mise en route OnCommand Insight*.

Informations connexes

"Importation et exportation des données utilisateur"

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 l'interface utilisateur Web de OnCommand Insight.
2. Cliquez sur **requêtes** et sélectionnez **Afficher toutes les requêtes**.
3. Vous pouvez modifier l'affichage des requêtes en effectuant l'une des actions suivantes :
   - Vous pouvez saisir du texte dans la zone **filter** pour rechercher des requêtes spécifiques.
   - 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.
   - 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.
   - 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, n'oubliez pas que les résultats peuvent changer car Insight interroge automatiquement vos sources 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 d'une requête dans un fichier .CSV pour importer les données dans une autre application.

Étapes

1. Connectez-vous à l'interface utilisateur Web de OnCommand Insight.
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 `.CSV` fichier.
5. Effectuez l'une des opérations suivantes :
   - Cliquez sur **Ouvrir avec**, puis sur **OK** pour ouvrir le fichier avec Microsoft Excel et enregistrer le fichier à un emplacement spécifique.
   - Cliquez sur **Enregistrer le fichier**, puis sur **OK** pour enregistrer le fichier dans votre dossier Téléchargements. Seuls les attributs des colonnes affichées seront exportés. Certaines colonnes affichées, en particulier celles faisant partie de relations imbriquées complexes, ne sont pas exportées.

     Lorsqu'une virgule apparaît dans un nom de ressource, l'exportation entre guillemets le nom de la ressource et le format .csv approprié.

     + lors de l'exportation des résultats de la requête, n'oubliez pas que **toutes les** lignes de la table de résultats seront exportées, pas seulement celles sélectionnées ou affichées à l'écran, jusqu'à un maximum de 10,000 lignes.

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 :

+

```
-   Open a new sheet in Excel.
-   On the "Data" tab, choose "From Text".
-   Locate the desired .CSV file and click "Import".
-   In the Import wizard, choose "Delimited" and click Next.
-   Choose "Comma" for the delimiter and click Next.
-   Select the desired columns and choose "Text" for the column data
format.
-   Click Finish.
Your objects should show in Excel in the proper format.
```

+

Modification des requêtes

Vous pouvez modifier les critères qui sont associés à une requête lorsque vous voulez modifier les critères de recherche des ressources que vous interrogez.

Étapes

1. Connectez-vous à l'interface utilisateur Insigtweb.
2. Cliquez sur **requêtes** et sélectionnez **Afficher toutes les requêtes**.

   La page requêtes s'affiche.

3. Cliquez sur le nom de la requête.
4. Pour supprimer un critère de la requête, cliquez sur .
5. Pour ajouter un critère à la requête, cliquez sur 

, et sélectionnez un critère dans la liste.
6. Effectuez l'une des opérations suivantes :
   - Cliquez sur **Enregistrer** pour enregistrer la requête avec le nom qui a été utilisé initialement.
   - Cliquez sur **Enregistrer sous** pour enregistrer la requête sous un autre nom.
   - Cliquez sur **Renommer** pour modifier le nom de la requête que vous avez utilisée initialement.
   - Cliquez sur **Revert** pour redéfinir le nom de la requête sur celui que vous avez utilisé initialement.

Suppression de requêtes

Vous pouvez supprimer des requêtes lorsqu'elles ne recueillent plus d'informations utiles sur vos ressources. Vous ne pouvez pas supprimer une requête si elle est utilisée dans une règle d'annotation.

Étapes

1. Connectez-vous à l'interface utilisateur Insigtweb.
2. Cliquez sur **requêtes** et sélectionnez **Afficher toutes les requêtes**.

   La page requêtes s'affiche.

3. Placez le curseur sur la requête à supprimer et cliquez sur .

   Un message de confirmation s'affiche, vous demandant si vous souhaitez supprimer la requête.

4. Cliquez sur **OK**.

Attribution ou suppression de plusieurs applications à des ressources ou à des applications multiples

Vous pouvez affecter plusieurs applications à ou supprimer plusieurs applications des ressources en utilisant une requête au lieu de devoir les affecter ou les supprimer manuellement.

Avant de commencer

Vous devez avoir déjà créé une requête qui trouve toutes les ressources à modifier.

Étapes

1. Cliquez sur **requêtes** et sélectionnez **Afficher toutes les requêtes**.

   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 Pour sélectionner **tout**.

   Le bouton **actions** s'affiche.

4. Pour ajouter une application aux ressources sélectionnées, cliquez sur Actions, Et sélectionnez **Modifier l'application**.
   a. Cliquez sur **application** et sélectionnez une ou plusieurs applications.

      Vous pouvez sélectionner plusieurs applications pour les hôtes, les volumes internes et les machines virtuelles ; cependant, vous ne pouvez sélectionner qu'une seule application pour un volume.

   b. Cliquez sur **Enregistrer**.

5. Pour supprimer une application affectée aux actifs, cliquez sur Actions Et sélectionnez **Supprimer l'application**.

   a. Sélectionnez l'application ou les applications que vous souhaitez supprimer.

   b. 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.

Modification ou suppression de plusieurs annotations des actifs

Vous pouvez modifier plusieurs annotations pour les ressources ou supprimer plusieurs annotations des ressources en utilisant une requête au lieu de les modifier ou de les supprimer manuellement.

Avant de commencer

Vous devez avoir déjà créé une requête qui trouve tous les actifs que vous souhaitez modifier.

Étapes

1. Cliquez sur **requêtes** et sélectionnez **Afficher toutes les requêtes**.

   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 ☐ Pour sélectionner **tout**.

   Le bouton **actions** s'affiche.

4. Pour ajouter une annotation aux actifs ou modifier la valeur d'une annotation affectée aux actifs, cliquez sur Actions, Et sélectionnez **Modifier l'annotation**.

   a. Cliquez sur **Annotation** et sélectionnez une annotation pour laquelle vous souhaitez modifier la valeur, ou sélectionnez une nouvelle annotation pour l'affecter à tous les actifs.

   b. Cliquez sur **valeur** et sélectionnez une valeur pour l'annotation.

   c. Cliquez sur **Enregistrer**.

5. Pour supprimer une annotation affectée aux actifs, cliquez sur Actions, Et sélectionnez **Supprimer une annotation**.

   a. Cliquez sur **Annotation** et sélectionnez l'annotation que vous souhaitez supprimer des actifs.

   b. Cliquez sur **Supprimer**.

Copie des valeurs de table

Vous pouvez copier des valeurs dans des tableaux pour les utiliser dans des zones de recherche ou d'autres applications.

Description de la tâche

Vous pouvez utiliser deux méthodes pour copier des valeurs à partir de tables ou de résultats de requête.

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 dont la longueur dépasse la largeur de la colonne du tableau, indiquée par des points de suspension (…), passez la souris sur le champ et cliquez sur l'icône du presse-papiers. 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. Notez également que seuls les champs contenant des valeurs uniques (c'est-à-dire des non-listes) ont l'icône de copie.

Gestion des règles de performance

OnCommand Insight vous permet de créer des règles de performance afin de surveiller votre réseau et d'augmenter les alertes lorsque ces seuils sont franchis. Les règles de performances vous permettent de détecter immédiatement une violation d'un seuil, d'identifier les implications et d'analyser l'impact et la cause profonde du problème de manière à permettre une correction rapide et efficace.

Une règle de performances vous permet de définir des seuils sur tous les objets (datastore, disque, hyperviseur, volume interne, port, Stockage, nœud de stockage, pool de stockage, VMDK, machine virtuelle, Et volume) avec des compteurs de performances rapportés (par exemple, IOPS totales). Lorsqu'une violation d'un seuil se produit, Insight le détecte et le signale dans la page de ressources associée, en affichant un cercle rouge continu, une alerte par e-mail, si elle est configurée, et dans le tableau de bord des violations ou tout tableau de bord personnalisé signalant des violations.

Insight fournit des règles de performances par défaut, que vous pouvez modifier ou supprimer si elles ne sont pas applicables à votre environnement, pour les objets suivants :

- Hyperviseur

  Il existe des règles d'échange ESX et d'utilisation ESX.

- Volume et volume internes

  Il existe deux règles de latence pour chaque ressource, l'une annotée pour le niveau 1 et l'autre pour le niveau 2.

- Port

  Il existe une politique pour le crédit BB zéro.

- Nœud de stockage

  Une règle d'utilisation des nœuds est définie.

- Ordinateur virtuel

  Il existe des règles relatives à la permutation des ordinateurs virtuels et à l'UC et à la mémoire ESX.

- Volumétrie

  La latence est constatée par Tier et les règles de volume sont mal alignées.

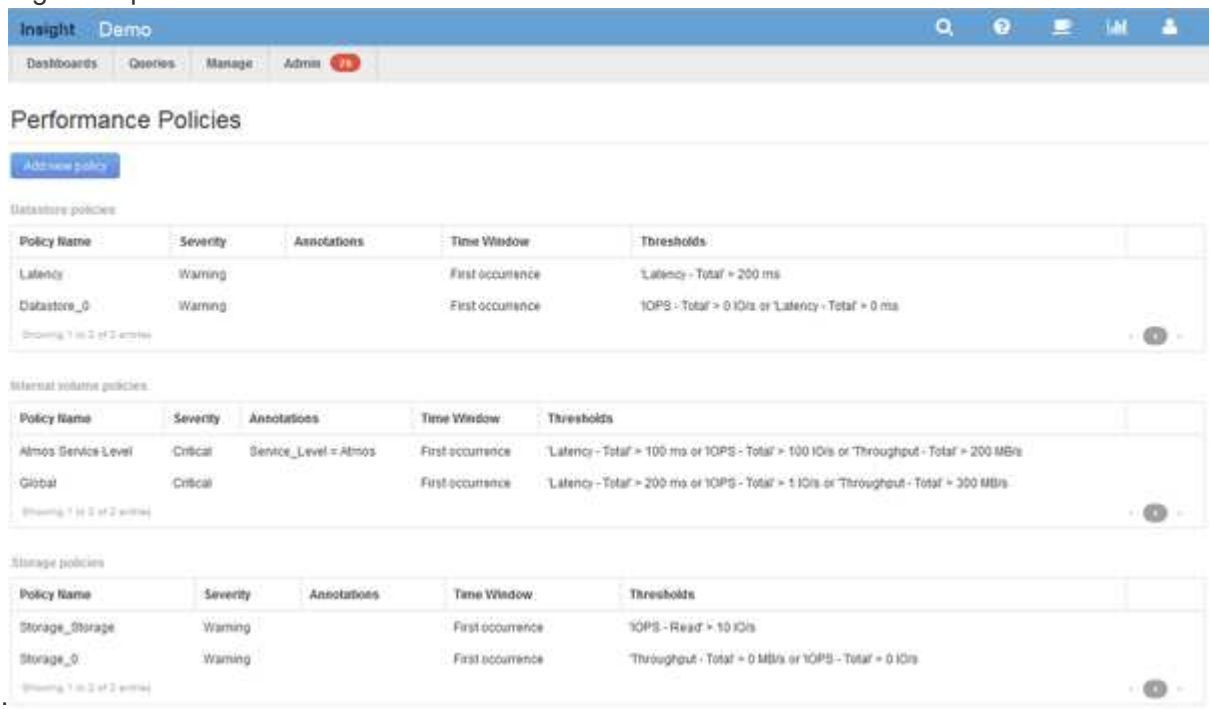
Création de règles de performance

Vous créez des stratégies de performances pour définir des seuils qui déclenchent des alertes pour vous informer des problèmes liés aux ressources de votre réseau. Par exemple, vous pouvez créer une règle de performance qui vous alerte lorsque l'utilisation totale des pools de stockage est supérieure à 60 %.

Étapes

1. Ouvrez OnCommand Insight dans votre navigateur.
2. Sélectionnez **gérer** > **politiques de performances**.

   La page règles de performance



   s'affiche.

   Les règles sont organisées par objet et sont évaluées dans l'ordre dans lequel elles apparaissent dans la liste pour cet objet.

3. Cliquez sur **Ajouter une nouvelle stratégie**.

   La boîte de dialogue Ajouter une stratégie s'affiche.

4. Dans le champ **Policy name**, entrez un nom pour la stratégie.

   Vous devez utiliser un nom différent de tous les autres noms de stratégie pour l'objet. Par exemple, vous ne pouvez pas avoir deux politiques nommées « latence » pour un volume interne. Vous pouvez toutefois avoir une règle de « latence » pour un volume interne et une autre règle de « latence » pour un volume différent. La meilleure pratique consiste à toujours utiliser un nom unique pour n'importe quelle règle, quel que soit le type d'objet.

5. Dans la liste **appliquer aux objets de type**, sélectionnez le type d'objet auquel la stratégie s'applique.
6. Dans la liste **avec annotation**, sélectionnez un type d'annotation, le cas échéant, et entrez une valeur pour l'annotation dans la zone **valeur** pour appliquer la règle uniquement aux objets qui ont cet ensemble d'annotations particulier.
7. Si vous avez sélectionné **Port** comme type d'objet, dans la liste **connecté à**, sélectionnez le port auquel il est connecté.
8. Dans la liste **appliquer après une fenêtre de**, sélectionnez lorsqu'une alerte est émise pour indiquer une violation de seuil.

   L'option première occurrence déclenche une alerte lorsqu'un seuil est dépassé sur le premier échantillon de données. Toutes les autres options déclenchent une alerte lorsque le seuil est franchi une fois et est traversé en continu pendant au moins la durée spécifiée.

9. Dans la liste **avec gravité**, sélectionnez la gravité de la violation.
10. Par défaut, des alertes par e-mail sur les violations de stratégie sont envoyées aux destinataires de la liste de messagerie globale. Vous pouvez remplacer ces paramètres afin que les alertes d'une stratégie donnée soient envoyées à des destinataires spécifiques.
    - Cliquez sur le lien pour ouvrir la liste des destinataires, puis cliquez sur le bouton **+** pour ajouter des destinataires. Les alertes de violation pour cette stratégie seront envoyées à tous les destinataires de la liste.
11. Cliquez sur le lien **any** dans la section **Create ALERT si l'une des situations suivantes est vraie** pour contrôler le déclenchement des alertes :
    - **tous**

      Il s'agit du paramètre par défaut qui crée des alertes lorsque l'un des seuils associés à une règle est dépassé.

    - **tous**

      Ce paramètre crée une alerte lorsque tous les seuils d'une règle sont dépassés. Lorsque vous sélectionnez **All**, le premier seuil que vous créez pour une stratégie de performances est appelé règle primaire. Vous devez vous assurer que le seuil de la règle principale est la violation dont vous êtes le plus préoccupé par la stratégie de performances.

12. Dans la section **Créer une alerte IF**, sélectionnez un compteur de performances et un opérateur, puis entrez une valeur pour créer un seuil.
13. Cliquez sur **Ajouter un seuil** pour ajouter d'autres seuils.
14. Pour supprimer un seuil, cliquez sur l'icône de la corbeille.
15. Cochez la case **Arrêter le traitement d'autres stratégies si une alerte est générée** si vous souhaitez que la stratégie arrête le traitement lorsqu'une alerte se produit.

    Par exemple, si vous avez quatre règles pour les datastores et que la deuxième règle est configurée pour

arrêter le traitement lorsqu'une alerte se produit, les troisième et quatrième règles ne sont pas traitées tant qu'une violation de la deuxième règle est active.

16. Cliquez sur **Enregistrer**.

    La page règles de performance s'affiche, et la règle de performance s'affiche dans la liste des règles pour le type d'objet.

Priorité de l'évaluation de la politique de performances

La page règles de performance regroupe les règles par type d'objet et Insight évalue les règles dans l'ordre dans lequel elles apparaissent dans la liste des règles de performance de l'objet. Vous pouvez modifier l'ordre dans lequel Insight évalue les stratégies afin d'afficher les informations les plus importantes pour vous sur votre réseau.

Insight évalue toutes les règles applicables à un objet de manière séquentielle lorsque des échantillons de données de performance sont prélevés dans le système pour cet objet. Cependant, en fonction des annotations, toutes les règles ne s'appliquent pas à un groupe d'objets. Par exemple, supposons que le volume interne possède les règles suivantes :

- Règle 1 (la règle par défaut fournie par Insight)
- Règle 2 (avec une annotation de « niveau de service = Silver » avec l'option **Arrêter le traitement d'autres stratégies si une alerte est générée**
- Politique 3 (avec une annotation de « niveau de service = Gold »)
- Politique 4

Pour un niveau de volume interne avec une annotation Gold, Insight évalue la règle 1, ignore la règle 2, puis évalue la règle 3 et la règle 4. Pour un niveau non annoté, Insight évalue par ordre des règles. Ainsi, Insight n'évalue que la règle 1 et la règle 4. Pour un niveau de volume interne avec une annotation Silver, Insight évalue la règle 1 et la règle 2 ; Toutefois, si une alerte est déclenchée lorsque le seuil de la règle est franchi une fois et est continuellement franchi pour la fenêtre de temps spécifiée dans la règle, Insight n'évalue plus les autres règles de la liste pendant qu'il évalue les compteurs actuels de l'objet. Lorsque Insight capture l'ensemble suivant d'exemples de performances pour l'objet, il commence à nouveau à évaluer les règles de performance pour l'objet par filtrage, puis par ordre.

Modification de la priorité d'une règle de performances

Par défaut, Insight évalue les règles d'un objet de manière séquentielle. Vous pouvez configurer l'ordre dans lequel Insight évalue les règles de performances. Par exemple, si une règle est configurée pour arrêter le traitement en cas de violation de stockage de niveau Gold, vous pouvez placer cette règle en premier dans la liste et éviter de voir d'autres violations génériques pour le même actif de stockage.

Étapes

1. Ouvrez Insight dans votre navigateur.
2. Dans le menu **gérer**, sélectionnez **politiques de performances**.

   La page règles de performance s'affiche.

3. Placez le curseur de la souris sur le nom d'une règle dans la liste des règles de performances d'un type d'objet.

   Les flèches de priorité apparaissent à droite de la règle.

4. Pour déplacer une stratégie vers le haut de la liste, cliquez sur la flèche vers le haut ; pour la déplacer vers le bas de la liste, cliquez sur la flèche vers le bas.

   Par défaut, les nouvelles règles sont ajoutées séquentiellement à la liste des règles d'un objet.

Modification des règles de performances

Vous pouvez modifier les règles de performance existantes et par défaut pour modifier la façon dont Insight surveille les conditions qui vous intéressent sur votre réseau. Par exemple, vous pouvez modifier le seuil d'une règle.

Étapes

1. Ouvrez Insight dans votre navigateur.
2. Dans le menu **gérer**, sélectionnez **politiques de performances**.

   La page règles de performance s'affiche.

3. Placez le curseur de la souris sur le nom d'une règle dans la liste des règles de performances d'un objet.
4. Cliquez sur .

   La boîte de dialogue Modifier la stratégie s'affiche.

5. Apportez les modifications requises.

   Si vous modifiez une option autre que le nom de la règle, Insight supprime toutes les violations existantes pour cette règle.

6. Cliquez sur **Enregistrer.**

Suppression des règles de performance

Vous pouvez supprimer une règle de performances si vous pensez qu'elle ne s'applique plus à la surveillance des objets de votre réseau.

Étapes

1. Ouvrez Insight dans votre navigateur.
2. Dans le menu **gérer**, sélectionnez **politiques de performances**.

   La page règles de performance s'affiche.

3. Positionnez le curseur de votre souris sur le nom d'une règle dans la liste des règles de performances d'un objet.
4. Cliquez sur .

Un message s'affiche, vous demandant si vous souhaitez supprimer la stratégie.

5. Cliquez sur **OK**.

Importation et exportation des données utilisateur

Les fonctions d'importation et d'exportation vous permettent d'exporter dans un fichier des annotations, des règles d'annotation, des requêtes, des règles de performance et des tableaux de bord personnalisés. Ce fichier peut ensuite être importé sur différents serveurs OnCommand Insight.

Les fonctions d'exportation et d'importation sont prises en charge uniquement entre les serveurs qui exécutent la même version de OnCommand Insight.

Pour exporter ou importer des données utilisateur, cliquez sur **Admin** et sélectionnez **Setup**, puis choisissez l'onglet **Importer/Exporter des données utilisateur**.

Lors de l'importation, des données sont ajoutées, fusionnées ou remplacées, en fonction des objets et des types d'objets en cours d'importation.

- Types d'annotations
  - Ajoute une annotation si aucune annotation du même nom n'existe 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.

  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.

- Règles d'annotation
  - Ajoute une règle d'annotation si aucune règle d'annotation portant le même nom n'existe dans le système cible.
  - Remplace une règle d'annotation si une règle d'annotation portant le même nom existe dans le système cible.

  Les règles d'annotation dépendent à la fois des requêtes et des annotations. Vous devez vérifier la précision de toutes les règles d'annotation une fois l'opération d'importation terminée.

- Stratégies
  - Ajoute une règle si aucune règle portant le même nom n'existe dans le système cible.
  - Remplace une règle si une règle portant le même nom existe dans le système cible.

Les politiques peuvent être hors service une fois l'opération d'importation terminée. Vous devez vérifier l'ordre des polices après l'importation. Les règles qui dépendent des annotations peuvent échouer si elles sont incorrectes. Vous devez vérifier toutes les dépendances d'annotation après l'importation.

+

- Requêtes
  - Ajoute une requête si aucune requête portant le même nom n'existe dans le système cible.
  - Remplace une requête si une requête portant le même nom existe dans le système cible, même si le type de ressource de la requête est différent.

Si le type de ressource d'une requête est différent, après l'importation, les widgets de tableau de bord qui utilisent cette requête peuvent afficher des résultats indésirables ou incorrects. Vous devez vérifier l'exactitude de tous les widgets basés sur des requêtes après l'importation. Les requêtes qui dépendent des annotations peuvent échouer si les annotations sont incorrectes. Vous devez vérifier toutes les dépendances d'annotation après l'importation.

+

- Tableaux de bord
  - Ajoute un tableau de bord si aucun tableau de bord portant le même nom n'existe dans le système cible.
  - Remplace un tableau de bord si un tableau de bord portant le même nom existe dans le système cible, même si le type de ressource de la requête est différent.

Vous devez vérifier l'exactitude de tous les widgets basés sur des requêtes dans les tableaux de bord après l'importation. Si le serveur source possède plusieurs tableaux de bord portant le même nom, ils sont tous exportés. Cependant, seul le premier sera importé vers le serveur cible. Pour éviter les erreurs lors de l'importation, vous devez vous assurer que vos tableaux de bord ont des noms uniques avant de les exporter.

+

Informations sur le copyright

Informations sur les marques commerciales