



Configuration et gestion des comptes utilisateur

OnCommand Insight

NetApp
April 01, 2024

Sommaire

- Configuration et gestion des comptes utilisateur 1
 - Avant de commencer 1
 - Étapes 1
 - Résultats 1
 - Rôles d'utilisateur Insight 2
 - Configuration d'Insight pour LDAP(s) 2
 - Modification des mots de passe utilisateur 7
 - Modification d'une définition utilisateur 8
 - Suppression d'un compte utilisateur 8

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.



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.



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>\SANSscreen\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, veuillez 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 déclarateurs	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.

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, comme illustré ici.

LDAP

LDAP integration enables authentication of users via LDAP (or ActiveDirectory). This is done by assigning these users to LDAP groups. The groups are used to identify the user permissions.

☒ Enable LDAP

Please provide credentials for a user authorized for directory lookup queries.

LDAP servers:

User:

Password:

[Show more](#) ▼

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, veuillez 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**.

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.