Configuration d'Insight pour LDAP(s)

OnCommand Insight

NetApp
October 24, 2024

Sommaire

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**.

Informations sur le copyright

Informations sur les marques commerciales