Configurazione di Insight per LDAP

OnCommand Insight

NetApp
October 24, 2024

Sommario

Configurazione di Insight per LDAP

OnCommand Insight deve essere configurato con le impostazioni LDAP (Lightweight Directory Access Protocol) così come sono configurate nel dominio LDAP aziendale.

Prima di configurare Insight per l'utilizzo con LDAP o LDAP sicuro (LDAPS), prendere nota della configurazione di Active Directory nell'ambiente aziendale. Le impostazioni di Insight devono corrispondere a quelle della configurazione di dominio LDAP dell'organizzazione. Prima di configurare Insight per l'utilizzo con LDAP, consultare i seguenti concetti e rivolgersi all'amministratore di dominio LDAP per conoscere gli attributi appropriati da utilizzare nell'ambiente.

Per tutti gli utenti di Secure Active Directory (ad esempio LDAPS), è necessario utilizzare il nome del server ad esattamente come definito nel certificato. Non è possibile utilizzare l'indirizzo IP per l'accesso ad sicuro.

Se sono state modificate le password *server.keystore* e/o *server.trustore* utilizzando "securityadmin", riavviare il servizio *SANscreen* prima di importare il certificato LDAP.

OnCommand Insight supporta LDAP e LDAPS tramite server Microsoft Active Directory o Azure ad. Ulteriori implementazioni LDAP potrebbero funzionare, ma non sono state qualificate con Insight. Le procedure descritte in queste guide presuppongono l'utilizzo di Microsoft Active Directory versione 2 o 3 LDAP (Lightweight Directory Access Protocol).

User Principal Name Attribute:

L'attributo LDAP User Principal Name (userPrincipalName) è quello che Insight utilizza come attributo Username. Il nome principale dell'utente è garantito per essere univoco a livello globale in una foresta Active Directory (ad), ma in molte grandi organizzazioni il nome principale di un utente potrebbe non essere immediatamente ovvio o noto. L'organizzazione potrebbe utilizzare un'alternativa all'attributo User Principal Name per il nome utente principale.

Di seguito sono riportati alcuni valori alternativi per il campo User Principal Name Attribute (attributo nome principale utente):

- **SAMAccountName**

  Questo attributo utente è il nome utente precedente a Windows 2000 NT legacy, ovvero la maggior parte degli utenti è abituata ad accedere alla propria macchina Windows personale. Non è garantito che questo sia globalmente unico in un insieme di strutture ad.

  SAMAccountName rileva la distinzione tra maiuscole e minuscole per l'attributo User Principal Name.

- **mail**

  Negli ambienti ad con MS Exchange, questo attributo rappresenta l'indirizzo e-mail principale dell'utente finale. A differenza dell'attributo userPrincipalName, questo deve essere univoco a livello globale in un insieme di strutture ad (e familiare anche per gli utenti finali). L'attributo mail non esiste nella maggior parte degli ambienti non MS Exchange.

- **riferimento**

  Un riferimento LDAP è il modo in cui un controller di dominio indica a un'applicazione client che non

dispone di una copia di un oggetto richiesto (o, più precisamente, che non contiene la sezione della struttura di directory in cui si trova l'oggetto, se effettivamente esiste) e che fornisce al client una posizione che è più probabile contenere l'oggetto. A sua volta, il client utilizza il riferimento come base per una ricerca DNS di un controller di dominio. Idealmente, i riferimenti fanno sempre riferimento a un controller di dominio che contiene effettivamente l'oggetto. Tuttavia, è possibile che il controller di dominio indicato generi un altro riferimento, anche se di solito non richiede molto tempo per scoprire che l'oggetto non esiste e per informare il client.

SAMAccountName è generalmente preferito rispetto a User Principal Name. SAMAccountName è univoco nel dominio (anche se potrebbe non essere univoco nella foresta di domini), ma è la stringa utilizzata dagli utenti del dominio per l'accesso (ad esempio,*netapp_Username*). Il nome distinto è il nome univoco nella foresta, ma generalmente non è noto agli utenti.

Nella parte del sistema Windows dello stesso dominio, è sempre possibile aprire un prompt dei comandi e digitare SET per trovare il nome di dominio corretto (USERDOMAIN=). Il nome di accesso OCI sarà quindi `USERDOMAIN\sAMAccountName`.

Per il nome di dominio **mydomain.x.y.z.com**, utilizzare `DC=x,DC=y,DC=z,DC=com` Nel campo dominio di Insight.

Porte:

La porta predefinita per LDAP è 389 e la porta predefinita per LDAPS è 636

URL tipico per LDAPS: `ldaps://<ldap_server_host_name>:636`

I log sono:`\\<install directory>\SANscreen\wildfly\standalone\log\ldap.log`

Per impostazione predefinita, Insight si aspetta i valori annotati nei seguenti campi. Se questi cambiamenti si verificano nell'ambiente Active Directory, assicurarsi di modificarli nella configurazione Insight LDAP.

Attributo ruolo
MemberOf
Attributo mail
mail
Attributo nome distinto
DistinguishedName
Riferimento
segui

Gruppi:

Per autenticare gli utenti con ruoli di accesso diversi nei server OnCommand Insight e DWH, è necessario creare gruppi in Active Directory e immettere i nomi dei gruppi nei server OnCommand Insight e DWH. I nomi dei gruppi riportati di seguito sono solo di esempio; i nomi configurati per LDAP in Insight devono corrispondere a quelli impostati per l'ambiente Active Directory.

Gruppo Insight	Esempio
Gruppo di amministratori del server Insight	insight.server.admins
Gruppo di amministratori di Insight	insight.admins
Gruppo di utenti Insight	insight.users
Gruppo di ospiti Insight	insight.guest
Gruppo di amministratori dei report	insight.report.admins
Gruppo di autori di report pro	insight.report.proauthors
Gruppo di autori di report	insight.report.business.authors
Gruppo di clienti di reporting	insight.report.business.consumer
Gruppo di destinatari dei report	insight.report.destinatari

Configurazione delle definizioni utente mediante LDAP

Per configurare OnCommand Insight (OCI) per l'autenticazione utente e l'autorizzazione da un server LDAP, è necessario definire nel server LDAP l'amministratore del server OnCommand Insight.

Prima di iniziare

È necessario conoscere gli attributi utente e gruppo configurati per Insight nel dominio LDAP.

Per tutti gli utenti di Secure Active Directory (ad esempio LDAPS), è necessario utilizzare il nome del server ad esattamente come definito nel certificato. Non è possibile utilizzare l'indirizzo IP per l'accesso ad sicuro.

Se sono state modificate le password *server.keystore* e/o *server.trustore* utilizzando "securityadmin", riavviare il servizio *SANscreen* prima di importare il certificato LDAP.

A proposito di questa attività

OnCommand Insight supporta LDAP e LDAPS tramite server Microsoft Active Directory. Ulteriori implementazioni LDAP potrebbero funzionare, ma non sono state qualificate con Insight. Questa procedura presuppone che si stia utilizzando Microsoft Active Directory versione 2 o 3 LDAP (Lightweight Directory Access Protocol).

Gli utenti LDAP vengono visualizzati insieme agli utenti definiti localmente nell'elenco **Admin** > **Setup** › **Users**.

Fasi

1. Nella barra degli strumenti Insight, fare clic su **Admin**.
2. Fare clic su **Setup**.
3. Fare clic sulla scheda **utenti**.
4. Scorrere fino alla sezione LDAP.
5. Fare clic su **Enable LDAP** (attiva LDAP) per consentire l'autenticazione e l'autorizzazione dell'utente LDAP.
6. Compilare i campi:

   ◦ `LDAP servers`: Insight accetta un elenco separato da virgole di URL LDAP. Insight tenta di connettersi agli URL forniti senza eseguire la convalida per il protocollo LDAP.

   > Per importare i certificati LDAP, fare clic su **certificati** e importare automaticamente o individuare manualmente i file dei certificati.

   L'indirizzo IP o il nome DNS utilizzato per identificare il server LDAP viene in genere inserito nel seguente formato:

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

   oppure, se si utilizza la porta predefinita:

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

   + Quando si immettono più server LDAP in questo campo, assicurarsi di utilizzare il numero di porta corretto in ciascuna voce.

   ◦ `User name`: Immettere le credenziali di un utente autorizzato per le query di ricerca directory sui server LDAP.

   ◦ `Password`: Inserire la password per l'utente precedente. Per confermare la password sul server LDAP, fare clic su **convalida**.
7. Se si desidera definire questo utente LDAP con maggiore precisione, fare clic su **Mostra altri** e compilare i campi degli attributi elencati.

   Queste impostazioni devono corrispondere agli attributi configurati nel dominio LDAP. In caso di dubbi sui valori da inserire per questi campi, rivolgersi all'amministratore di Active Directory.

   ◦ **Gruppo amministratori**

     Gruppo LDAP per utenti con privilegi Insight Administrator. Il valore predefinito è `insight.admins`.

   ◦ **Gruppo utenti**

     Gruppo LDAP per utenti con privilegi Insight User. Il valore predefinito è `insight.users`.

- **Gruppo ospiti**

  Gruppo LDAP per utenti con privilegi Insight Guest. Il valore predefinito è `insight.guests`.

- Gruppo **Server Admins**

  Gruppo LDAP per utenti con privilegi di amministratore di Insight Server. Il valore predefinito è `insight.server.admins`.

- **Timeout**

  Tempo di attesa di una risposta dal server LDAP prima del timeout, espresso in millisecondi. il valore predefinito è 2,000, che è adeguato in tutti i casi e non deve essere modificato.

- **Dominio**

  Nodo LDAP in cui OnCommand Insight dovrebbe iniziare a cercare l'utente LDAP. In genere si tratta del dominio di primo livello dell'organizzazione. Ad esempio:

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

- **Attributo nome principale utente**

  Attributo che identifica ciascun utente nel server LDAP. Il valore predefinito è `userPrincipalName`, che è unico a livello globale. OnCommand Insight tenta di far corrispondere il contenuto di questo attributo con il nome utente fornito in precedenza.

- **Attributo ruolo**

  Attributo LDAP che identifica la misura dell'utente all'interno del gruppo specificato. Il valore predefinito è `memberOf`.

- **Attributo Mail**

  Attributo LDAP che identifica l'indirizzo e-mail dell'utente. Il valore predefinito è `mail`. Questa opzione è utile se si desidera iscriversi ai report disponibili presso OnCommand Insight. Insight rileva l'indirizzo e-mail dell'utente la prima volta che ciascun utente effettua l'accesso e non lo cerca dopo.

  Se l'indirizzo e-mail dell'utente cambia sul server LDAP, assicurarsi di aggiornarlo in Insight.

- **Attributo nome distinto**

  Attributo LDAP che identifica il nome distinto dell'utente. il valore predefinito è `distinguishedName`.

8. Fare clic su **Save** (Salva).