Configuring Insight for LDAP(s)

OnCommand Insight

NetApp
October 24, 2024

Table of Contents

Configuring Insight for LDAP(s)

OnCommand Insight must be configured with Lightweight Directory Access Protocol (LDAP) settings as they are configured in your corporate LDAP domain.

Before configuring Insight for use with LDAP or secure LDAP (LDAPs), make note of the Active Directory configuration in your corporate environment. Insight settings must match those in your organization's LDAP domain configuration. Review the concepts below before configuring Insight for use with LDAP, and check with your LDAP domain administrator for the proper attributes to use in your environment.

For all Secure Active Directory (i.e. LDAPS) users, you must use the AD server name exactly as it is defined in the certificate. You can not use IP address for secure AD login.

If you changed *server.keystore* and/or *server.trustore* passwords using securityadmin, restart the *sanscreen* service before importing the LDAP certificate.

OnCommand Insight supports LDAP and LDAPS via Microsoft Active Directory server or Azure AD. Additional LDAP implementations may work but have not been qualified with Insight. The procedures in these guides assume that you are using Microsoft Active Directory Version 2 or 3 LDAP (Lightweight Directory Access Protocol).

User Principal Name attribute:

The LDAP User Principal Name attribute (userPrincipalName) is what Insight uses as the username attribute. User Principal Name is guaranteed to be globally unique in an Active Directory (AD) forest, but in many large organizations, a user's principal name may not be immediately obvious or known to them. Your organization might use an alternative to the User Principal Name attribute for primary user name.

Following are some alternative values for the User Principal Name attribute field:

- **sAMAccountName**

  This user attribute is the legacy pre-Windows 2000 NT username - this is what most users are accustomed to logging into their personal Windows machine. This is not guaranteed to be globally unique throughout an AD forest.

  sAMAccountName is case-sensitive for the User Principal Name attribute.

- **mail**

  In AD environments with MS Exchange, this attribute is the primary e-mail address for the end user. This should be globally unique throughout an AD forest, (and also familiar for end users), unlike their userPrincipalName attribute. The mail attribute will not exist in most non-MS Exchange environments.

- **referral**

  An LDAP referral is a domain controller's way of indicating to a client application that it does not have a copy of a requested object (or, more precisely, that it does not hold the section of the directory tree where that object would be, if in fact it exists) and giving the client a location that is more likely to hold the object. The client in turn uses the referral as the basis for a DNS search for a domain controller. Ideally, referrals always reference a domain controller that indeed holds the object. However, it is possible for the referred-to domain controller to generate yet another referral, although it usually does not take long to discover that

the object does not exist and to inform the client.

sAMAccountName is generally preferred over User Principal Name. sAMAccountName is unique in the domain (though it may not be unique in the domain forest), but it is the string domain users typically use for login (For example,*netapp\username*).The Distinguished Name is the unique name in the forest, but is generally not known by the users.

On the Windows system part of the same domain, you can always open a command prompt and type SET to find the proper domain name (USERDOMAIN=). The OCI login name will then be `USERDOMAIN\sAMAccountName`.

For the domain name **mydomain.x.y.z.com**, use `DC=x,DC=y,DC=z,DC=com` in the Domain field in Insight.

Ports:

The default port for LDAP is 389, and the default port for LDAPs is 636

Typical URL for LDAPs: `ldaps://<ldap_server_host_name>:636`

Logs are at:`\\<install directory>\SANscreen\wildfly\standalone\log\ldap.log`

By default, Insight expects the values noted in the following fields. If these change in your Active Directory environment, be sure to change them in the Insight LDAP configuration.

Role attribute
memberOf
Mail attribute
mail
Distinguished Name attribute
distinguishedName
Referral
follow

Groups:

To authenticate users with different access roles in the OnCommand Insight and DWH servers, you must create groups in Active Directory and enter those group names in OnCommand Insight and DWH servers. The group names below are examples only; the names you configure for LDAP in Insight must match the ones set up for your Active Directory environment.

Insight Group	Example

Insight server administrator group	insight.server.admins
Insight administrators group	insight.admins
Insight users group	insight.users
Insight guests group	insight.guests
Reporting administrator group	insight.report.admins
Reporting pro authors group	insight.report.proauthors
Reporting authors group	insight.report.business.authors
Reporting consumers group	insight.report.business.consumers
Reporting recipients group	insight.report.recipients

Configuring user definitions using LDAP

To configure OnCommand Insight (OCI) for user authentication and authorization from an LDAP server, you must be defined in the LDAP server as the OnCommand Insight server administrator.

Before you begin

You must know the user and group attributes that have been configured for Insight in your LDAP domain.

For all Secure Active Directory (i.e. LDAPS) users, you must use the AD server name exactly as it is defined in the certificate. You can not use IP address for secure AD login.

If you changed *server.keystore* and/or *server.trustore* passwords using securityadmin, restart the *sanscreen* service before importing the LDAP certificate.

About this task

OnCommand Insight supports LDAP and LDAPS via Microsoft Active Directory server. Additional LDAP implementations may work but have not been qualified with Insight. This procedure assumes that you are using Microsoft Active Directory Version 2 or 3 LDAP (Lightweight Directory Access Protocol).

LDAP users display along with the locally defined users in the **Admin** > **Setup** › **Users** list.

Steps

1. On the Insight toolbar, click **Admin**.
2. Click **Setup**.

3. Click the **Users** tab.
4. Scroll to the LDAP section.

1. Click **Enable LDAP** to allow the LDAP user authentication and authorization.
2. Fill in the fields:
   - `LDAP servers`: Insight accepts a comma-separated list of LDAP URLs. Insight attempts to connect to the provided URLs without validating for LDAP protocol.

     To import the LDAP certificates, click **Certificates** and automatically import or manually locate the certificate files.

     The IP address or DNS name used to identify the LDAP server is typically entered in this format:

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

     or, if using the default port:

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

     When entering multiple LDAP servers in this field, ensure that the correct port number is used in each entry.

   - `User name`: Enter the credentials for a user authorized for directory lookup queries on the LDAP servers.
   - `Password`: Enter the password for the above user. To confirm this password on the LDAP server, click **Validate**.
3. If you want to define this LDAP user more precisely, click **Show more** and fill in the fields for the listed attributes.

   These settings must match the attributes configured in your LDAP domain. Check with your Active Directory administrator if you are unsure of the values to enter for these fields.

   - **Admins group**

     LDAP group for users with Insight Administrator privileges. Default is `insight.admins`.

   - **Users group**

     LDAP group for users with Insight User privileges. Default is `insight.users`.

   - **Guests group**

     LDAP group for users with Insight Guest privileges. Default is `insight.guests`.

   - **Server admins group**

     LDAP group for users with Insight Server Administrator privileges. Default is `insight.server.admins`.

- **Timeout**

  Length of time to wait for a response from the LDAP server before timing out, in milliseconds. default is 2,000, which is adequate in all cases and should not be modified.

- **Domain**

  LDAP node where OnCommand Insight should start looking for the LDAP user. Typically this is the top-level domain for the organization. For example:

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

- **User principal name attribute**

  Attribute that identifies each user in the LDAP server. Default is `userPrincipalName`, which is globally unique. OnCommand Insight attempts to match the contents of this attribute with the username that has been supplied above.

- **Role attribute**

  LDAP attribute that identifies the user's fit within the specified group. Default is `memberOf`.

- **Mail attribute**

  LDAP attribute that identifies the user's email address. Default is `mail`. This is useful if you want to subscribe to reports available from OnCommand Insight. Insight picks up the user's email address the first time each user logs in and does not look for it after that.

  If the user's email address changes on the LDAP server, be sure to update it in Insight.

- **Distinguished name attribute**

  LDAP attribute that identifies the user's distinguished name. default is `distinguishedName`.

4. Click **Save**.

Copyright information

Trademark information