Konfigurieren von Insight für LDAP(s)

OnCommand Insight

NetApp
September 03, 2024

This PDF was generated from https://docs.netapp.com/de-de/oncommand-insight/config-admin/configuring-user-definitions-using-ldap.html on September 03, 2024. Always check docs.netapp.com for the latest.

Inhalt

Konfigurieren von Insight für LDAP(s) 1
Konfigurieren von Benutzerdefinitionen mithilfe von LDAP 3

Konfigurieren von Insight für LDAP(s)

OnCommand Insight muss mit LDAP-Einstellungen (Lightweight Directory Access Protocol) konfiguriert werden, da diese in Ihrer LDAP-Domäne des Unternehmens konfiguriert sind.

Bevor Sie Insight für die Verwendung mit LDAP oder Secure LDAP (LDAPS) konfigurieren, notieren Sie sich die Active Directory-Konfiguration in Ihrer Unternehmensumgebung. Insight-Einstellungen müssen mit denen in der LDAP-Domänenkonfiguration Ihres Unternehmens übereinstimmen. Lesen Sie die folgenden Konzepte, bevor Sie Insight für die Verwendung mit LDAP konfigurieren, und wenden Sie sich an Ihren LDAP-Domänenadministrator, um die richtigen Attribute für Ihre Umgebung zu ermitteln.

Für alle Secure Active Directory (d. h. LDAPS)-Benutzer müssen Sie den AD-Servernamen genau so verwenden, wie er im Zertifikat definiert ist. Sie können die IP-Adresse nicht für die sichere AD-Anmeldung verwenden.

> OnCommand Insight unterstützt LDAP und LDAPS über Microsoft Active Directory Server oder Azure AD. Zusätzliche LDAP-Implementierungen funktionieren möglicherweise, wurden aber nicht für Insight qualifiziert. Die Verfahren in diesen Handbüchern gehen davon aus, dass Sie Microsoft Active Directory Version 2 oder 3 LDAP (Lightweight Directory Access Protocol) verwenden.

User Principal Name Attribut:

Das Attribut LDAP User Principal Name (userPrincipalName) wird von Insight als Attribut username verwendet. Der Hauptname des Benutzers ist in einer Active Directory (AD)-Gesamtstruktur garantiert global eindeutig, aber in vielen großen Unternehmen ist der Hauptname eines Benutzers möglicherweise nicht sofort ersichtlich oder bekannt. Ihr Unternehmen kann für den primären Benutzernamen eine Alternative zum Attribut User Principal Name verwenden.

Im Folgenden finden Sie einige alternative Werte für das Attributfeld User Principal Name:

- **SAMAccountName**

  Dieses Benutzerattribut ist der alte Benutzername vor Windows 2000 NT - das ist es, was die meisten Benutzer gewohnt sind, sich auf ihrem persönlichen Windows-Rechner anzumelden. Dies ist nicht garantiert weltweit einzigartig in einer AD-Gesamtstruktur.

  > SAMAccountName berücksichtigt Groß- und Kleinschreibung für das Attribut User Principal Name.

- **Mail**

  In AD-Umgebungen mit MS Exchange ist dieses Attribut die primäre E-Mail-Adresse für den Endbenutzer. Dies sollte global einzigartig in einer AD-Gesamtstruktur sein (und auch für Endbenutzer bekannt), im Gegensatz zu ihrem userPrincipalName-Attribut. Das Mail-Attribut ist in den meisten nicht-MS Exchange-Umgebungen nicht vorhanden.

- **Empfehlung**

  Eine LDAP-Weiterleitung ist die Art und Weise eines Domänencontrollers, einer Client-Anwendung zu zeigen, dass sie keine Kopie eines angeforderten Objekts hat (genauer gesagt: Dass es nicht den Abschnitt des Verzeichnisbaums enthält, in dem das Objekt sein würde, wenn es tatsächlich existiert) und

dem Client einen Speicherort gibt, der das Objekt wahrscheinlicher enthält. Der Client wiederum verwendet die Weiterleitung als Grundlage für eine DNS-Suche nach einem Domänencontroller. Im Idealfall verweisen Verweise immer auf einen Domänencontroller, der das Objekt tatsächlich enthält. Es ist jedoch möglich, dass der verwies Domänencontroller eine weitere Empfehlung generiert, obwohl es in der Regel nicht lange dauert, zu erkennen, dass das Objekt nicht existiert und den Client zu informieren.

SAMAccountName wird im Allgemeinen dem Hauptnamen des Benutzers vorgezogen. SAMAccountName ist in der Domain eindeutig (obwohl er in der Domänenstruktur nicht eindeutig ist), aber es ist die String-Domain, die Benutzer normalerweise für die Anmeldung verwenden (z. B.,*netapp\username*).der Distinguished Name ist der eindeutige Name in der Gesamtstruktur, ist aber in der Regel von den Benutzern nicht bekannt.

Auf dem Windows-Systemteil derselben Domäne können Sie immer eine Eingabeaufforderung öffnen und SET eingeben, um den richtigen Domänennamen zu finden (USERDOMAIN=). Der OCI-Anmeldename lautet dann `USERDOMAIN\sAMAccountName`.

Verwenden Sie für den Domainnamen **mydomain.x.y.z.com** `DC=x,DC=y,DC=z,DC=com` Geben Sie in Insight im Feld Domain ein.

Ports:

Der Standardport für LDAP ist 389, und der Standardport für LDAPS ist 636

Typische URL für LDAPS: `ldaps://<ldap_server_host_name>:636`

Protokolle befinden sich bei:`\\<install directory>\SANscreen\wildfly\standalone\log\ldap.log`

Standardmäßig erwartet Insight die in den folgenden Feldern angegebenen Werte. Wenn sich diese Änderungen in Ihrer Active Directory-Umgebung ändern, müssen Sie sie in der Insight LDAP-Konfiguration ändern.

Rollenattribut
Mitgliedschafts
Mail-Attribut
E-Mail
Attribut Distinguished Name
Name wird unterschieden
Empfehlung
Folgen

Gruppen:

Um Benutzer mit unterschiedlichen Zugriffsrollen auf den OnCommand Insight- und DWH-Servern zu authentifizieren, müssen Sie Gruppen in Active Directory erstellen und diese Gruppennamen auf OnCommand Insight- und DWH-Servern eingeben. Die folgenden Gruppennamen sind nur Beispiele. Die Namen, die Sie für LDAP in Insight konfigurieren, müssen mit denen übereinstimmen, die für Ihre Active Directory-Umgebung eingerichtet wurden.

Insight Group	Beispiel
Insight Server Administratorgruppe	insight.server.admins
Insight Administratoren	Insight.Administratoren
Insight Benutzergruppe	insight.users
Insight Gästegruppe	Insight.Gäste
Administratorgruppe für Berichte	Insight.Report.Administratoren
Gruppe der pro-Autoren berichten	insight.report.proauthors
Gruppe „Verfasser von Berichten“	insight.report.business.authors
Gruppe der meldesstattenen Verbraucher	Insight.Report.Business.Consumers
Gruppe der Reporting-Empfänger	Insight.Report.Empfänger

Konfigurieren von Benutzerdefinitionen mithilfe von LDAP

Um OnCommand Insight (OCI) für die Benutzerauthentifizierung und -Autorisierung von einem LDAP-Server zu konfigurieren, müssen Sie auf dem LDAP-Server als OnCommand Insight-Serveradministrator definiert sein.

Bevor Sie beginnen

Sie müssen die Benutzer- und Gruppenattribute kennen, die für Insight in Ihrer LDAP-Domäne konfiguriert wurden.

Für alle Secure Active Directory (d. h. LDAPS)-Benutzer müssen Sie den AD-Servernamen genau so verwenden, wie er im Zertifikat definiert ist. Sie können die IP-Adresse nicht für die sichere AD-Anmeldung verwenden.

Über diese Aufgabe

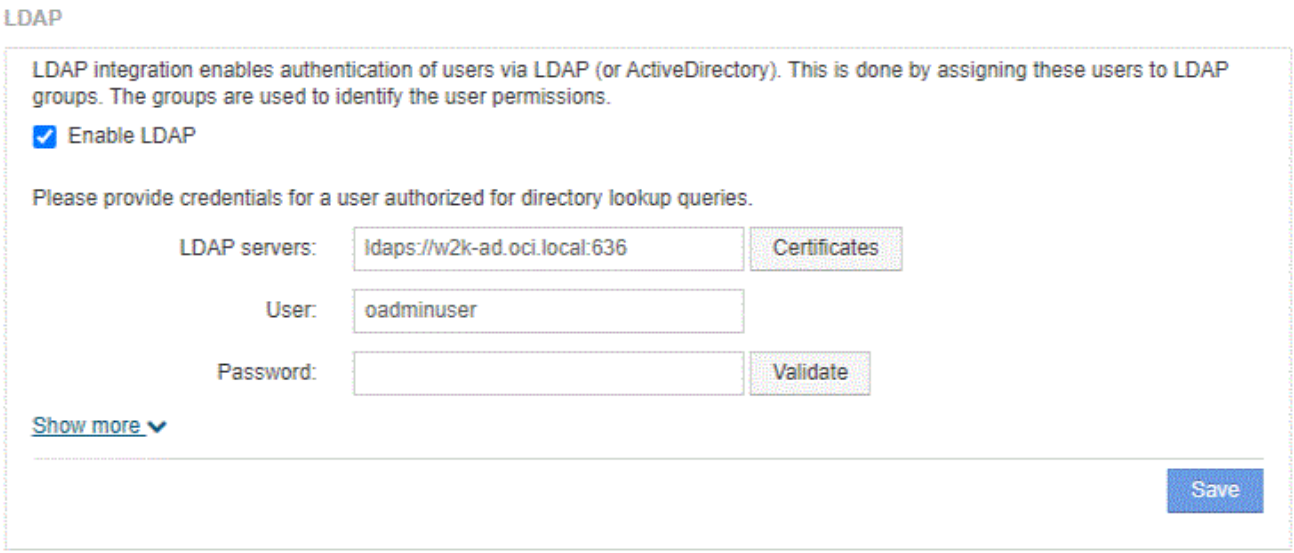
OnCommand Insight unterstützt LDAP und LDAPS über Microsoft Active Directory Server. Zusätzliche LDAP-Implementierungen funktionieren möglicherweise, wurden aber nicht für Insight qualifiziert. Bei diesem Verfahren wird davon ausgegangen, dass Sie Microsoft Active Directory Version 2 oder 3 LDAP (Lightweight Directory Access Protocol) verwenden.

LDAP-Benutzer werden zusammen mit den lokal definierten Benutzern in der Liste **Admin** > **Setup** › **Users**

angezeigt.

Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
2. Klicken Sie Auf **Setup**.
3. Klicken Sie auf die Registerkarte **Users**.
4. Scrollen Sie zum LDAP-Abschnitt, wie hier gezeigt.



5. Klicken Sie auf **LDAP aktivieren**, um die LDAP-Benutzerauthentifizierung und -Autorisierung zu ermöglichen.
6. Füllen Sie die Felder aus:

   - `LDAP servers`: Insight akzeptiert eine kommagetrennte Liste von LDAP-URLs. Insight versucht, eine Verbindung zu den bereitgestellten URLs herzustellen, ohne das LDAP-Protokoll zu überprüfen.

     > Um die LDAP-Zertifikate zu importieren, klicken Sie auf **Zertifikate** und importieren oder suchen Sie die Zertifikatdateien automatisch.

     Die IP-Adresse oder der DNS-Name, der zur Identifizierung des LDAP-Servers verwendet wird, wird in der Regel in diesem Format eingegeben:

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

     Oder, wenn Sie den Standardport verwenden:

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

+ Stellen Sie bei der Eingabe mehrerer LDAP-Server in dieses Feld sicher, dass bei jedem Eintrag die richtige Portnummer verwendet wird.

- `User name`: Geben Sie die Anmeldeinformationen für einen Benutzer ein, der für Anfragen zur Verzeichnissuche auf den LDAP-Servern autorisiert ist.
- `Password`: Geben Sie das Passwort für den oben genannten Benutzer ein. Um dieses Passwort auf dem LDAP-Server zu bestätigen, klicken Sie auf **Validieren**.

7. Wenn Sie diesen LDAP-Benutzer genauer definieren möchten, klicken Sie auf **Mehr anzeigen** und füllen Sie die Felder für die aufgelisteten Attribute aus.

   Diese Einstellungen müssen mit den in Ihrer LDAP-Domäne konfigurierten Attributen übereinstimmen. Wenden Sie sich an Ihren Active Directory-Administrator, wenn Sie sich nicht sicher sind, welche Werte für diese Felder eingegeben werden müssen.

   - **Admins-Gruppe**

     LDAP-Gruppe für Benutzer mit Insight Administrator-Berechtigungen. Standard ist `insight.admins`.

   - **Benutzergruppe**

     LDAP-Gruppe für Benutzer mit Insight-Benutzerberechtigungen. Standard ist `insight.users`.

   - **Gästegruppe**

     LDAP-Gruppe für Benutzer mit Insight Gastberechtigungen. Standard ist `insight.guests`.

   - **Server Admins-Gruppe**

     LDAP-Gruppe für Benutzer mit Insight Server Administrator-Berechtigungen. Standard ist `insight.server.admins`.

   - **Timeout**

     Dauer der Wartezeit auf eine Antwort vom LDAP-Server vor der Zeitüberschreitung in Millisekunden. Der Standardwert ist 2,000, was in allen Fällen angemessen ist und nicht geändert werden sollte.

   - **Domäne**

     LDAP-Knoten, auf dem OnCommand Insight nach dem LDAP-Benutzer suchen soll. Dies ist in der Regel die Domäne der obersten Ebene für das Unternehmen. Beispiel:

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

   - **Attribut des Hauptnamens des Benutzers**

     Attribut, das jeden Benutzer im LDAP-Server identifiziert. Standard ist `userPrincipalName`, Die weltweit einzigartig ist. OnCommand Insight versucht, den Inhalt dieses Attributs mit dem oben angegebenen Benutzernamen abzugleichen.

   - **Rollenattribut**

     LDAP-Attribut, das die Passung des Benutzers innerhalb der angegebenen Gruppe identifiziert. Standard ist `memberOf`.

   - **Mail-Attribut**

LDAP-Attribut, das die E-Mail-Adresse des Benutzers identifiziert. Standard ist `mail`. Dies ist nützlich, wenn Sie Berichte von OnCommand Insight abonnieren möchten. Insight erfasst die E-Mail-Adresse des Benutzers bei der ersten Anmeldung und sucht danach nicht mehr.

> Wenn sich die E-Mail-Adresse des Benutzers auf dem LDAP-Server ändert, müssen Sie sie in Insight aktualisieren.

- **Distinguished Name Attribut**

  LDAP-Attribut, das den Distinguished Name des Benutzers identifiziert. Der Standardwert ist `distinguishedName`.

8. Klicken Sie Auf **Speichern**.

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.