



# LDAP用のInsightの設定

## OnCommand Insight

NetApp  
October 24, 2024

# 目次

LDAP用のInsightの設定 .....	1
LDAPを使用したユーザ定義の設定 .....	3

# LDAP用のInsightの設定

OnCommand Insight は、Lightweight Directory Access Protocol (LDAP) 設定を使用して、社内のLDAPドメインで設定する必要があります。

LDAPまたはSecure LDAP (LDAPS) で使用するようにInsightを設定する前に、社内環境でのActive Directoryの設定をメモしておいてください。Insightの設定は、組織のLDAPドメイン設定と一致している必要があります。InsightをLDAPで使用する前に、以下の概念を確認し、LDAPドメイン管理者に問い合わせ、環境で使用する適切な属性を確認してください。

すべてのSecure Active Directory (LDAPS) ユーザに対して、ADサーバ名は証明書で定義されているとおり、に正確に使用する必要があります。セキュアADログインにIPアドレスを使用することはできません。



を使用して\_server.keystore\_and/or\_server.truststore\_passwordsを変更した場合は"securityadmin"、SANSscreen証明書をインポートする前に\_ldap\_serviceを再起動してください。



OnCommand Insight は、Microsoft Active DirectoryサーバまたはAzure AD経由でLDAPとLDAPSをサポートしています。その他のLDAP実装でも動作する可能性がありますが、Insightでは確認されていません。これらのマニュアルの手順は、Microsoft Active Directoryバージョン2または3 LDAP (Lightweight Directory Access Protocol) を使用していることを前提としています。

ユーザープリンシパル名属性：

Insightでは、LDAPのUser PrincipalName属性 (userPrincipalName) をユーザ名属性として使用します。ユーザープリンシパル名は、Active Directory(AD)フォレスト内でグローバルに一意であることが保証されていますが、多くの大規模な組織では、ユーザーのプリンシパル名がすぐにはわかりません。組織では、プライマリユーザー名に[ユーザープリンシパル名]属性の代わりに使用することがあります。

次に'ユーザープリンシパル名属性フィールドの代替値を示します

- \* sAMAccountName \*

このユーザー属性は、Windows 2000 NT以前のレガシーユーザー名です。これは、ほとんどのユーザーが個人用Windowsマシンにログインするのに慣れているものです。これは、ADフォレスト全体でグローバルに一意であることが保証されていません。



sAMAccountNameは'ユーザープリンシパル名属性では大文字と小文字が区別されます

- メール

MS Exchangeを使用するAD環境では、この属性はエンドユーザーのプライマリ電子メールアドレスです。これは、userPrincipalName属性とは異なり、ADフォレスト全体でグローバルに一意である必要があります（エンドユーザーにも馴染みがあります）。メール属性は、MS Exchange以外のほとんどの環境には存在しません。

- 紹介

LDAPリファラールは、要求されたオブジェクト（より正確には、オブジェクトが存在するディレクトリ

ツリーのセクションを保持せず、オブジェクトを保持する可能性が高い場所をクライアントに与えます。次に、クライアントはこのリファールをドメインコントローラのDNS検索のベースとして使用します。理想的には、リファールは常にオブジェクトを保持するドメインコントローラを参照する。ただし、参照先ドメインコントローラが別のリファールを生成することは可能ですが、通常はオブジェクトが存在しないことを検出してクライアントに通知するのに時間はかかりません。



通常、ユーザプリンシパル名よりもsAMAccountNameが推奨されます。sAMAccountNameは、ドメイン内で一意です（ただし、ドメインフォレスト内で一意ではない場合があります）が、通常、ログインに使用するドメインユーザの文字列です（例：*NetApp\username*）。識別名はフォレスト内で一意の名前ですが、通常はユーザによって認識されません。



同じドメインのWindowsシステム部分では、いつでもコマンドプロンプトを開き、setと入力して適切なドメイン名(USERDOMAIN=)を検索できます。OCIログイン名はになります  
USERDOMAIN\sAMAccountName。

ドメイン名\* mydomain.x.y.z.com \*には、を使用します DC=x, DC=y, DC=z, DC=com をクリックします。

• ポート \* :

LDAPのデフォルトポートは389、LDAPSのデフォルトポートは636です

LDAPSの一般的なURL : ldaps://<ldap\_server\_host\_name>:636

ログは次の場所にあります。\\<install  
directory>\SANSscreen\wildfly\standalone\log\ldap.log

デフォルトでは、次のフィールドに値が表示されます。Active Directory環境でこれらの変更が発生した場合は、InsightのLDAP設定で変更してください。

ロール属性
所属グループ
Mail属性
メール
Distinguished Name属性
distinguishedName
リファール
ついて来い

グループ :

OnCommand Insight サーバとDWHサーバで異なるアクセスロールを持つユーザを認証するには、Active Directoryでグループを作成し、OnCommand Insight サーバとDWHサーバでそれらのグループ名を入力する必要があります。以下のグループ名は一例です。InsightでLDAP用に設定する名前は、Active Directory環境用に設定した名前と一致している必要があります。

Insight Groupの略	例
Insight Server管理者グループ	insight.server.admins
Insight管理者グループ	insight.admins
Insightユーザグループ	insight.users
Insightゲストグループ	インサイトゲスト
Reporting Administrator Groupの略	insight.report.admins
Reporting Pro Authorsグループ	insight.report.proauthors
レポート作成者グループ	insight.report.business.authors
レポートコンシューマグループ	洞察力レポートビジネス消費者
レポート受信者グループ	インサイトレポート受信者

## LDAPを使用したユーザ定義の設定

LDAPサーバからのユーザ認証と許可にOnCommand Insight（OCI）を設定するには、LDAPサーバでOnCommand Insight サーバ管理者として定義されている必要があります。

### 作業を開始する前に

LDAPドメインでInsight用に設定されているユーザとグループの属性を確認しておく必要があります。

すべてのSecure Active Directory（LDAPS）ユーザに対して、ADサーバ名は証明書で定義されているとおりに正確に使用する必要があります。セキュアADログインにIPアドレスを使用することはできません。



を使用して\_server.keystore\_and/or\_server.truststore\_passwordsを変更した場合は"securityadmin"、SANscreen証明書をインポートする前に\_ldap\_serviceを再起動してください。

### このタスクについて

OnCommand Insight は、Microsoft Active Directoryサーバを介したLDAPとLDAPSをサポートしています。その他のLDAP実装でも動作する可能性がありますが、Insightでは確認されていません。この手順 は、Microsoft

Active Directoryバージョン2または3のLDAP（Lightweight Directory Access Protocol）を使用していることを前提としています。

LDAPユーザは、ローカルで定義されたユーザとともに\*Admin\*>メニューのSetup [ Users ]リストに表示されます。

## 手順

1. Insightのツールバーで、\*[Admin]\*をクリックします。
2. [設定]\*をクリックします。
3. [ユーザー]タブをクリックします。
4. [LDAP]セクションまでスクロールします。
5. [LDAPを有効にする]\*をクリックして、LDAPユーザの認証と許可を許可します。
6. 次のフィールドに入力します。

- LDAP servers：Insightでは、LDAP URLをカンマで区切ったリストを使用できます。LDAPプロトコルを検証せずに、指定されたURLに接続しようとします。



LDAP証明書をインポートするには、\*[証明書]\*をクリックし、証明書ファイルを自動的にインポートするか、手動で検索します。

LDAPサーバの識別に使用するIPアドレスまたはDNS名は、通常次の形式で入力します。

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

または、デフォルトのポートを使用している場合：

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

+ このフィールドに複数のLDAPサーバを入力する場合は、各エントリで正しいポート番号が使用されていることを確認してください。

- User name：LDAPサーバでディレクトリ検索クエリを許可されたユーザのクレデンシャルを入力します。
- Password：上記のユーザのパスワードを入力します。LDAPサーバでこのパスワードを確認するには、\*[検証]\*をクリックします。

7. このLDAPユーザをより正確に定義する場合は、\*[詳細を表示]\*をクリックし、表示された属性のフィールドに入力します。

これらの設定は、LDAPドメインで設定されている属性と一致する必要があります。これらのフィールドに入力する値が不明な場合は、Active Directory管理者に確認してください。

- 管理者グループ

Insight管理者の権限を持つユーザのLDAPグループ。デフォルトはです `insight.admins`。

- ユーザーグループ

Insightユーザの権限を持つユーザのLDAPグループ。デフォルトは `insight.users`。

- ゲストグループ

Insight Guest権限を持つユーザのLDAPグループ。デフォルトは `insight.guests`。

- サーバー管理者グループ

Insight Server管理者権限を持つユーザのLDAPグループ。デフォルトは `insight.server.admins`。

- タイムアウト

タイムアウトするまでにLDAPサーバからの応答を待機する時間（ミリ秒）。デフォルトは2,000です。これはすべてのケースで適切なため、変更しないでください。

- ドメイン

OnCommand Insight がLDAPユーザの検索を開始するLDAPノード。通常、これは組織のトップレベルドメインです。例：

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

- ユーザープリンシパル名属性

LDAPサーバ内の各ユーザを識別する属性。デフォルトは `userPrincipalName`。世界的にユニークなものです。OnCommand Insight は、この属性の内容を上記で指定したユーザ名と照合しようとします。

- ロール属性

指定したグループ内でのユーザの適合性を識別するLDAP属性。デフォルトは `memberOf`。

- メール属性

ユーザのEメールアドレスを識別するLDAP属性。デフォルトは `mail`。これは、OnCommand Insight から利用可能なレポートをサブスクライブする場合に便利です。Insightでは、各ユーザが初めてログインしたときにユーザのEメールアドレスが取得され、それ以降は検索されません。



LDAPサーバでユーザのEメールアドレスが変更された場合は、Insightでそのアドレスを更新してください。

- 識別名属性

ユーザの識別名を識別するLDAP属性。デフォルトは `distinguishedName`。

8. [ 保存 ( Save ) ] をクリックします。

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。