LDAP用のInsightの設定

OnCommand Insight

NetApp
April 01, 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で使用するように設定する前に、以下の概念を確認し、LDAPドメイン管理者に問い合わせて、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。

> 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リファーラルは、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ラ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、リファーラ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ラ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もあります）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>\SANscreen\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
リファーラル
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。

このタスクについて

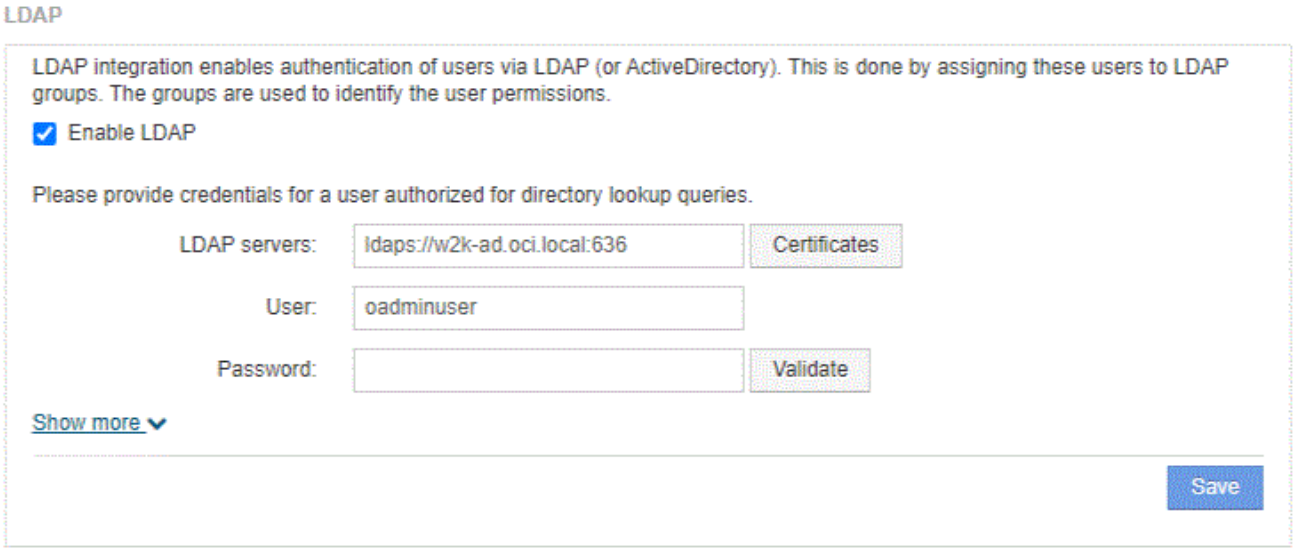
OnCommand Insight は、Microsoft Active Directoryサーバを介したLDAPとLDAPSをサポートしています。その他のLDAP実装でも動作する可能性がありますが、Insightでは確認されていません。この手順 は、Microsoft Active Directoryバージョン2または3のLDAP（Lightweight Directory Access Protocol）を使用していることを前提としています。

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（次の図を参照）。



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。デフォルトはです `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。デフォルトはです `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ーのLDAPグループ。デフォルトはです `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。デフォルトはです `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。デフォルトはです `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。デフォルトはです `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。デフォルトはです `distinguishedName`。

8. [保存（ Save ）] をクリックします。