

LDAP認証の実行が遅い

適用性

Splunkエンタープライズ

説明

LDAPを認証方式として使用すると、ユーザのパフォーマンスが非常に低下していました。

調査

LDAP :

LDAP(Lightweight Directory Access Protocol)は、階層ディレクトリ構造のデータの保存と取得に使用されるオープンプロトコルです。LDAPは、組織とその資産およびユーザに関する情報を保存するために一般的に使用され、あらゆるタイプのエンティティとその品質を定義するための柔軟なソリューションです。

ディレクトリ サービス:

ディレクトリサービスは、キー値型の形式でデータを格納、整理、および提示するために使用されます。通常、ディレクトリは書き込み操作に対するルックアップ、検索、読み取り操作に最適化されているため、頻繁に参照されるが頻繁に変更されないデータに対しては非常に適切に機能します。

LDAP(Lightweight Directory Access Protocol)は、ディレクトリサービスにアクセスする方法を定義する通信プロトコルです。より広い意味では、LDAPはディレクトリサービス内のデータをユーザに対して表現する方法を形成し、ディレクトリサービス内でデータエントリを作成するために使用されるコンポーネントの要件を定義し、さまざまなプリミティブ要素を使用してエントリを構成する方法の概要を示します。属性:

LDAPシステムのデータ自体は主に 属性と呼ばれる要素に保存されます。アトリビュートは基本的にキーと値のペアです。

Entries:

アトリビュート自体はあまり役に立ちません。意味を持つためには、何かに 関連付けられている必要があります。LDAPでは、 エントリ内の属性を使用します。エントリは、基本的には何かを説明するために使用される名前の下属性の集合です。

たとえば、システム内のユーザまたはインベントリ内の各項目に対してエントリを設定できます

。これは、リレーショナルデータベースシステムの1行またはアドレス帳の1ページに似ています (この属性は、各モデルのさまざまなフィールドを表します)。属性は何かの品質や特性を定義しますが、エントリは単に名前の下でこれらの属性を収集することによってアイテム自体を説明します。

エントリはすべて、データ情報ツリー(DIT)と呼ばれるツリー上のブランチとしてLDAPシステムに追加されます。

DITは、各エントリ (最上位のエントリを除く) がちょうど1つの親エントリを持ち、その下に任意の数の子エントリを持つ、ファイルシステムに似た組織構造を表します。LDAPツリーのエントリはほぼすべてを表すことができるため、ファイルシステム内のディレクトリと同様に、一部のエントリは主に組織的な目的で使用されます。

以下に、いくつかの例を示します。

```
dn: sn=Ellingwood,ou=people,dc=digitalocean,dc=com
```

This line is called the entry's distinguished name (more on this later) and is used to identify the entry. It functions like a full

LDAP authentication in Splunk in the end is querying a database and this query could be very broad if you don't set the right authentication.conf In the authentication.conf specification you can find out the following:

```
userBaseFilter = <string>
* OPTIONAL
* This is the LDAP search filter you wish to use when searching for users.
* Highly recommended, especially when there are many entries in your LDAP
  user subtrees
* When used properly, search filters can significantly speed up LDAP queries
* Example that matches users in the IT or HR department:
  * userBaseFilter = (&(department=IT)(department=HR))
  * See RFC 2254 for more detailed information on search filter syntax
* This defaults to no filtering.
```

This in turn allows to narrow down the amount of entries that the query needs to search on because it filters allows to look only into certain e

解決方法

ユーザには、次のようなuserBasefilterがあります。

```
userBaseFilter = (|(department=VP30)(department=VPIN)(department=VA02))
```

このパフォーマンスの低下を観察していたユーザは、元のuserBaseFilterにリストされているすべての部門に属していたとは限りません。LDAPサーバでは1つの部門のエントリだけをチェックすればよいので、認証が行われるたびに検索範囲が狭くなるように、1つまたは2つの部門を削除します。

関連リンク

Splunkの回答：

Windows 2008 R2でSplunk 6.2を使用すると、「size limit exceeded」エラーによってLDAP認証が失敗するのはなぜですか。

<https://answers.splunk.com/answers/179797/why-is-ldap-authentication-failing-with-size-limit.html>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。