

LDAP 身份驗證執行緩慢

適用性

Splunk企業版

說明

使用LDAP作為身份驗證方法時，使用者的效能非常低。

調查

LDAP:

LDAP（輕量型目錄訪問協定）是一種開放式協定，用於儲存和檢索分層目錄結構中的資料。LDAP通常用於儲存有關組織及其資產和使用者的資訊，它是用於定義任何型別的實體及其特性的靈活解決方案。

目錄服務：

目錄服務用於以鍵值型別格式儲存、組織和顯示資料。通常，目錄針對查詢、搜尋和讀取操作（而不是寫入操作）進行了最佳化，因此對於經常引用但不經常更改的資料來說，它們非常有效。

LDAP（輕量級目錄訪問協定）是一種通訊協定，定義訪問目錄服務的方法。更廣義地說，LDAP決定了應該向使用者呈現目錄服務中的資料的方式，定義了用於在目錄服務中建立資料條目的元件的要求，並概述了使用不同基元元素來構成條目的方式。屬性：

LDAP系統中的資料本身主要儲存在稱為 attributes的元素中。屬性基本上是鍵值對。

條目：

屬性本身並不是很有用。為了有意義，它們必須與某物相關聯。在LDAP中，可以在條目中使用屬性。一個條目基本上是一個屬性集合，其名稱用於描述某事物。

例如，您可以為系統中的使用者或清單中的每個專案設定一個條目。這大致類似於關聯式資料庫系統中的行或通訊簿中的單個頁（這裡的屬性將表示這些模型中的各個欄位）。屬性定義某物的品質或特徵，而條目描述專案本身的簡單方式是收集名稱下的這些屬性。

所有條目都作為樹上的分支新增到LDAP系統，這些樹稱為 資料資訊樹(DITs)。

DIT表示類似於檔案系統的組織結構，其中每個條目（頂級條目除外）只有一個父條目，並且其下可以有任意數量的子條目。由於LDAP樹中的條目幾乎可以代表任何內容，因此某些條目將主要用

於組織目的，類似於檔案系統內的目錄。

舉例來說：

```
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

解析

使用者的userBasefilter如下所示：

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

觀察此緩慢效能的使用者可能不屬於原始userBaseFilter中列出的所有部門的成員。刪除一個或兩個部門，這樣每次進行身份驗證時，搜尋範圍會變小，因為LDAP伺服器只需要檢查一個部門的條目

。

相關連結

Splunk答案：

為什麼在Windows 2008 R2上使用Splunk 6.2時LDAP身份驗證失敗，出現「超出大小限制」錯誤？

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。