

LDAP 身份验证执行缓慢

适用范围

Splunk企业

描述

使用LDAP作为身份验证方法时，用户的性能非常低。

调查

LDAP:

LDAP（轻量级目录访问协议）是一种开放式协议，用于存储和检索分层目录结构中的数据。LDAP通常用于存储有关组织及其资产和用户的信息，是一种用于定义任何类型的实体及其特性的灵活解决方案。

目录服务:

目录服务用于以键值类型格式存储、组织和显示数据。通常，目录针对查找、搜索和读取操作（而不是写入操作）进行了优化，因此对于经常引用但不常更改的数据来说，它们非常有效。

LDAP（轻量级目录访问协议）是一种通信协议，定义了访问目录服务的方法。更广泛地说，LDAP决定了向用户呈现目录服务内的数据的方式，定义了用于创建目录服务内数据条目的组件的要求，并概述了使用不同基元元素合成条目的方式。Attributes:
LDAP系统中的数据本身主要存储在称为 attributes的元素中。属性基本上是键值对。

条目：

属性本身并不是很有用。为了有意义，它们必须与某物相关联。在LDAP中，可以使用条目中的属性。一个条目基本上是一个属性集合，其名称用于描述某事物。

例如，您可以为系统中的用户或资产中的每个项目设置一个条目。这大致类似于关系数据库系统中的行或通讯簿中的单个页（这里的属性将代表这些模型中的各个字段）。当属性定义某物的质量或特征时，条目通过简单地收集名称下的这些属性来描述项目本身。

所有条目都作为树上的分支添加到LDAP系统，这些树称为 数据信息树，或 DIT。

DIT表示类似于文件系统的组织结构，其中每个条目（除顶级条目外）只有一个父条目，并且其下可以有任意数量的子条目。由于LDAP树中的条目几乎可以代表任何内容，因此某些条目将主要用

于组织目的，类似于文件系统内的目录。

例如：

```
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

分辨率

用户的userBasefilter如下所示：

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

观察到此性能缓慢的用户可能不属于原始userBaseFilter中列出的所有部门。删除一个或两个部门，这样每次进行身份验证时，搜索范围会变小，因为LDAP服务器只需要检查一个部门的条目。

相关链接

Splunk答案：

为什么在Windows 2008 R2上使用Splunk 6.2时，LDAP身份验证失败，出现“超出大小限制”错误？
<https://answers.splunk.com/answers/179797/why-is-ldap-authentication-failing-with-size-limit.html>

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。