

Lenteur de l'authentification LDAP

Applicabilité

Splunk Enterprise

Description

Les performances des utilisateurs étaient très faibles lors de l'utilisation de LDAP comme méthode d'authentification.

Enquête

LDAP :

Le protocole LDAP (Lightweight Directory Access Protocol) est un protocole ouvert utilisé pour stocker et récupérer des données à partir d'une structure de répertoires hiérarchique.

Généralement utilisé pour stocker des informations sur une organisation, ses ressources et ses utilisateurs, le protocole LDAP est une solution flexible permettant de définir n'importe quel type d'entité et ses qualités.

Service d'annuaire :

Un service d'annuaire est utilisé pour stocker, organiser et présenter des données dans un format de type clé-valeur. Généralement, les répertoires sont optimisés pour les recherches, les recherches et les opérations de lecture sur les opérations d'écriture. Ils fonctionnent donc très bien pour les données qui sont souvent référencées mais qui changent peu fréquemment.

Le protocole LDAP (Lightweight Directory Access Protocol) est un protocole de communication qui définit les méthodes d'accès à un service d'annuaire. De manière plus générale, le protocole LDAP définit la manière dont les données d'un service d'annuaire doivent être représentées aux utilisateurs, définit les exigences des composants utilisés pour créer des entrées de données dans un service d'annuaire et décrit la manière dont différents éléments primitifs sont utilisés pour composer des entrées. Attributs :

Les données elles-mêmes dans un système LDAP sont principalement stockées dans des éléments appelés attributs. Les attributs sont essentiellement des paires clé-valeur.

Entrées :

Les attributs en eux-mêmes ne sont pas très utiles. Pour avoir un sens, ils doivent être associés à quelque chose. Dans LDAP, vous utilisez des attributs dans une entrée. Une entrée est

essentiellement une collection d'attributs sous un nom utilisé pour décrire quelque chose.

Par exemple, vous pouvez avoir une entrée pour un utilisateur de votre système ou pour chaque article d'un inventaire. Ceci est à peu près similaire à une ligne dans un système de base de données relationnelle ou à une seule page dans un carnet d'adresses (les attributs ici représenteraient les différents champs dans chacun de ces modèles). Alors qu'un attribut définit une qualité ou une caractéristique de quelque chose, une entrée décrit l'élément lui-même en collectant simplement ces attributs sous un nom.

Les entrées sont toutes ajoutées à un système LDAP en tant que branches sur des arborescences appelées arborescences d'informations de données, ou DIT.

Un DIT représente une structure organisationnelle similaire à un système de fichiers où chaque entrée (autre que l'entrée de niveau supérieur) a exactement une entrée parent et peut avoir un nombre quelconque d'entrées enfant sous elle. Étant donné que les entrées d'une arborescence LDAP peuvent représenter à peu près n'importe quoi, certaines entrées seront principalement utilisées à des fins d'organisation, comme les répertoires d'un système de fichiers.

Exemple :

```
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 path in a file system.

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 filters. 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 entries.

Résolution

L'utilisateur avait un userBasefilter comme suit :

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

Les utilisateurs qui observaient cette lenteur des performances n'appartenaient peut-être pas à tous les services répertoriés dans le userBaseFilter d'origine. Supprimez un ou deux services de sorte que chaque fois qu'une authentification se produirait, les recherches seraient moins larges car le serveur LDAP n'aurait besoin de vérifier que les entrées d'un seul service.

Liens connexes

Réponses du Splunk :

Pourquoi l'authentification LDAP échoue-t-elle avec des erreurs « taille limite dépassée » à l'aide de Splunk 6.2 sur Windows 2008 R2 ?

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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.