

Autenticación LDAP lenta

Aplicabilidad

Splunk Enterprise

Descripción

Los usuarios estaban teniendo un rendimiento muy lento cuando utilizaban LDAP como método de autenticación.

Investigación

LDAP:

LDAP, o protocolo ligero de acceso a directorios, es un protocolo abierto que se utiliza para almacenar y recuperar datos de una estructura jerárquica de directorios. Utilizado habitualmente para almacenar información sobre una organización y sus activos y usuarios, LDAP es una solución flexible para definir cualquier tipo de entidad y sus cualidades.

Servicio de directorio:

Un servicio de directorio se utiliza para almacenar, organizar y presentar datos en un formato de tipo clave-valor. Normalmente, los directorios están optimizados para búsquedas, búsquedas y operaciones de lectura sobre operaciones de escritura, por lo que funcionan muy bien para los datos a los que se hace referencia con frecuencia pero que no cambian con frecuencia.

LDAP, o protocolo ligero de acceso a directorios, es un protocolo de comunicaciones que define los métodos en los que se puede acceder a un servicio de directorio. En términos más generales, LDAP define la forma en que los datos de un servicio de directorio deben representarse ante los usuarios, define los requisitos de los componentes utilizados para crear entradas de datos en un servicio de directorio y describe la forma en que se utilizan los distintos elementos primitivos para crear entradas. Atributos:

Los datos en sí en un sistema LDAP se almacenan principalmente en elementos denominados atributos. Los atributos son básicamente pares clave-valor.

Entradas:

Los atributos por sí mismos no son muy útiles. Para tener significado, deben estar asociados con algo. Dentro de LDAP, se utilizan atributos dentro de una entrada. Una entrada es básicamente una colección de atributos bajo un nombre que se utiliza para describir algo.

Por ejemplo, puede tener una entrada para un usuario del sistema o para cada artículo de un inventario. Esto es más o menos análogo a una fila en un sistema de base de datos relacional o a una sola página dentro de una libreta de direcciones (los atributos aquí representarían los diversos campos en cada uno de estos modelos). Mientras que un atributo define una calidad o característica de algo, una entrada describe el elemento en sí simplemente recopilando estos atributos bajo un nombre.

Todas las entradas se agregan a un sistema LDAP como ramas en árboles denominados Árboles de información de datos, o DITs.

Un DIT representa una estructura organizativa similar a un sistema de archivos en el que cada entrada (distinta de la entrada de nivel superior) tiene exactamente una entrada principal y puede tener cualquier número de entradas secundarias por debajo. Dado que las entradas en un árbol LDAP pueden representar casi cualquier cosa, algunas entradas se utilizarán principalmente con fines organizativos, de manera similar a los directorios dentro de un sistema de archivos.

Por ejemplo:

```
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 e

Resolución

El usuario tenía un filtroBaseUsuario como el siguiente:

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

Es posible que los usuarios que observaban este rendimiento lento no pertenecieran a todos los departamentos enumerados en el userBaseFilter original. Quite uno o dos departamentos para que cada vez que ocurra una autenticación, las búsquedas sean menos amplias porque el servidor LDAP sólo necesitaría verificar las entradas de un departamento.

Enlaces relacionados

Splunk Responde:

¿Por qué falla la autenticación LDAP con errores de "límite de tamaño excedido" al usar Splunk 6.2 en Windows 2008 R2?

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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).