

Execução lenta da autenticação LDAP

Aplicabilidade

Empresa Splunk

Descrição

O desempenho dos usuários estava muito lento ao usar LDAP como um método de autenticação.

Investigação

LDAP:

LDAP, ou Lightweight Directory Access Protocol, é um protocolo aberto usado para armazenar e recuperar dados de uma estrutura de diretórios hierárquica. Geralmente usado para armazenar informações sobre uma organização e seus ativos e usuários, o LDAP é uma solução flexível para definir qualquer tipo de entidade e suas qualidades.

Serviço de diretório:

Um serviço de diretório é usado para armazenar, organizar e apresentar dados em um formato de tipo chave-valor. Normalmente, os diretórios são otimizados para pesquisas, pesquisas e operações de leitura sobre operações de gravação, de modo que funcionam extremamente bem para dados que são referenciados com frequência, mas mudam com pouca frequência.

O LDAP, ou Lightweight Directory Access Protocol, é um protocolo de comunicação que define os métodos pelos quais um serviço de diretório pode ser acessado. Em termos mais gerais, o LDAP define a forma como os dados em um serviço de diretório devem ser representados para os usuários, define os requisitos dos componentes usados para criar entradas de dados em um serviço de diretório e descreve a forma como diferentes elementos primitivos são usados para compor entradas. Atributos:

Os dados em si em um sistema LDAP são armazenados principalmente em elementos chamados atributos. Os atributos são basicamente pares chave-valor.

Entradas:

Os atributos por si só não são muito úteis. Para ter significado, eles precisam estar associados a algo. No LDAP, você usa atributos em uma entrada. Uma entrada é basicamente uma coleção de atributos sob um nome usado para descrever algo.

Por exemplo, você pode ter uma entrada para um usuário no sistema ou para cada item em um inventário. Isso é aproximadamente análogo a uma linha em um sistema de banco de dados relacional ou a uma única página dentro de um catálogo de endereços (os atributos aqui representariam os vários campos em cada um desses modelos). Enquanto um atributo define uma qualidade ou característica de algo, uma entrada descreve o próprio item simplesmente coletando esses atributos sob um nome.

Todas as entradas são adicionadas a um sistema LDAP como ramificações em árvores chamadas Árvores de Informações de Dados ou DITs.

Uma DIT representa uma estrutura organizacional semelhante a um sistema de arquivos em que cada entrada (diferente da entrada de nível superior) tem exatamente uma entrada pai e pode ter qualquer número de entradas filho abaixo dela. Como as entradas em uma árvore LDAP podem representar praticamente qualquer coisa, algumas entradas serão usadas principalmente para fins organizacionais, semelhantes aos diretórios em um sistema de arquivos.

Por exemplo:

```
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.

Resolução

O usuário tinha um userBasefilter como este:

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

Os usuários que estavam observando esse desempenho lento talvez não pertencessem a todos os departamentos listados no userBaseFilter original. Remova um ou dois departamentos para que cada vez que uma autenticação ocorresse, as pesquisas fossem menos amplas, pois o servidor LDAP só precisaria verificar as entradas de um departamento.

Links relacionados

Respostas de Splunk:

Por que a autenticação LDAP falha com erros de "limite de tamanho excedido" usando Splunk 6.2 no Windows 2008 R2?

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.