

Autenticazione LDAP lenta

Applicabilità

Splunk Enterprise

Descrizione

Le prestazioni degli utenti erano molto lente quando si utilizzava LDAP come metodo di autenticazione.

Indagine

LDAP:

LDAP, o Lightweight Directory Access Protocol, è un protocollo aperto utilizzato per memorizzare e recuperare dati da una struttura di directory gerarchica. Utilizzato comunemente per memorizzare informazioni su un'organizzazione e le relative risorse e utenti, il protocollo LDAP è una soluzione flessibile per la definizione di qualsiasi tipo di entità e delle relative qualità.

Servizio directory:

Un servizio directory viene utilizzato per memorizzare, organizzare e presentare i dati in un formato tipo-valore-chiave. In genere, le directory sono ottimizzate per le ricerche, le ricerche e le operazioni di lettura rispetto alle operazioni di scrittura, pertanto funzionano perfettamente per i dati a cui si fa riferimento spesso ma che vengono modificati raramente.

LDAP, o Lightweight Directory Access Protocol, è un protocollo di comunicazione che definisce i metodi in cui è possibile accedere a un servizio directory. In termini più generali, LDAP definisce il modo in cui i dati all'interno di un servizio di elenco utenti devono essere rappresentati dagli utenti, definisce i requisiti per i componenti utilizzati per creare le voci di dati all'interno di un servizio di elenco utenti e delinea il modo in cui vengono utilizzati diversi elementi di base per comporre le voci. Attributi:

I dati stessi in un sistema LDAP vengono memorizzati principalmente in elementi denominati attributi. Gli attributi sono fondamentalmente coppie chiave-valore.

Voci:

Gli attributi da soli non sono molto utili. Per avere un significato, devono essere associati a qualcosa. In LDAP, gli attributi vengono utilizzati all'interno di una voce. Una voce è fondamentalmente una raccolta di attributi sotto un nome utilizzato per descrivere qualcosa.

Ad esempio, è possibile avere una voce per un utente del sistema o per ciascun articolo di un magazzino. Questa operazione è simile a una riga in un sistema di database relazionale o a una singola pagina in una rubrica (gli attributi qui rappresenterebbero i vari campi in ciascuno di questi modelli). Mentre un attributo definisce una qualità o una caratteristica di un elemento, una voce descrive l'elemento stesso semplicemente raccogliendo questi attributi sotto un nome.

Tutte le voci vengono aggiunte a un sistema LDAP come diramazioni su strutture ad albero chiamate strutture ad albero delle informazioni sui dati, o DIT.

Un DIT rappresenta una struttura organizzativa simile a un file system in cui ogni voce (diversa dalla voce di livello superiore) ha esattamente una voce padre e può avere un numero qualsiasi di voci figlio al di sotto di essa. Poiché le voci di una struttura LDAP possono rappresentare praticamente qualsiasi cosa, alcune voci verranno utilizzate principalmente per scopi organizzativi, simili alle directory all'interno di un file system.

Ad esempio:

```
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

Risoluzione

L'utente dispone di un userBasefilter simile al seguente:

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

Gli utenti che osservavano queste prestazioni lente potrebbero non appartenere a tutti i reparti elencati in userBaseFilter originale. Rimuovere uno o due reparti in modo che ogni volta che si verifica un'autenticazione, le ricerche siano meno ampie in quanto il server LDAP deve controllare solo le voci di un reparto.

Collegamenti correlati

Risposte Splunk:

Perché l'autenticazione LDAP non riesce con errori di "superamento del limite delle dimensioni" usando Splunk 6.2 su Windows 2008 R2?

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).