

LDAP-verificatie verloopt traag

toepasbaarheid

Splunk Enterprise

Beschrijving

Gebruikers hadden zeer trage prestaties bij het gebruik van LDAP als authenticatiemethode.

onderzoek

LDAP:

LDAP, of Lightweight Directory Access Protocol, is een open protocol dat wordt gebruikt om gegevens op te slaan en op te halen uit een hiërarchische directorystructuur. LDAP wordt vaak gebruikt om informatie over een organisatie en haar activa en gebruikers op te slaan en is een flexibele oplossing voor het definiëren van elk type entiteit en haar kwaliteiten.

Directory-service:

Een directoryservice wordt gebruikt om gegevens op te slaan, te organiseren en te presenteren in een sleutelwaardetype. Normaal gesproken zijn mappen geoptimaliseerd voor opzoeken, zoeken en lezen via schrijfbewerkingen, dus ze functioneren zeer goed voor gegevens waarnaar vaak wordt verwezen, maar die zelden worden gewijzigd.

LDAP, of lichtgewicht directory access protocol, is een communicatieprotocol dat de methoden definieert waarin een directory service kan worden benaderd. Meer in het algemeen geeft LDAP vorm aan de manier waarop de gegevens binnen een directoryservice aan gebruikers moeten worden weergegeven, definieert vereisten voor de componenten die worden gebruikt om gegevensinvoer binnen een directoryservice te maken en schetst de manier waarop verschillende primitieve elementen worden gebruikt om items samen te stellen. Attributen:

De gegevens zelf in een LDAP-systeem worden voornamelijk opgeslagen in elementen die attributen worden genoemd. Attributen zijn in principe key-value paren.

Inzendingen:

Attributen op zich zijn niet erg nuttig. Om betekenis te hebben, moeten ze met iets geassocieerd worden. Binnen LDAP gebruikt u attributen binnen een item. Een item is in feite een verzameling attributen onder een naam die wordt gebruikt om iets te beschrijven.

U kunt bijvoorbeeld een vermelding voor een gebruiker in uw systeem of voor elk item in een inventaris hebben. Dit is ongeveer analoog aan een rij in een relationeel databasesysteem of aan een enkele pagina in een adresboek (de attributen hier zouden de verschillende velden in elk van deze modellen vertegenwoordigen). Terwijl een attribuut een kwaliteit of kenmerk van iets definieert, beschrijft een item het item zelf door deze attributen eenvoudigweg onder een naam te verzamelen.

Inzendingen worden allemaal toegevoegd aan een LDAP-systeem als takken op bomen genaamd Data Information Trees, of DIT's.

Een DIT vertegenwoordigt een organisatiestructuur die vergelijkbaar is met een bestandssysteem waarbij elk item (anders dan het bovenste niveau) precies één bovenliggende item heeft en mogelijk een willekeurig aantal onderliggende items eronder heeft. Aangezien vermeldingen in een LDAP-structuur vrijwel alles kunnen vertegenwoordigen, worden sommige vermeldingen voornamelijk gebruikt voor organisatorische doeleinden, vergelijkbaar met mappen binnen een bestandssysteem.

Voorbeeld:

```
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

resolutie

Gebruiker had een userBasefilter als volgt:

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

De gebruikers die deze trage prestaties observeerden, behoorden misschien niet tot alle afdelingen die in de oorspronkelijke userBaseFilter werden vermeld. Verwijder een of twee afdelingen, zodat elke keer dat een verificatie zou gebeuren, de zoekopdrachten minder breed zouden zijn, omdat de LDAP-server alleen de vermeldingen van één afdeling zou hoeven te controleren.

Gerelateerde links

Splunk antwoordt:

Waarom is LDAP-verificatie mislukt met "size limit overschreden" -fouten met Splunk 6.2 op Windows 2008 R2?

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.