

LDAP-Authentifizierung langsam

Geltungsbereich

Splunk Enterprise

Beschreibung

Die Verwendung von LDAP als Authentifizierungsmethode kam nur sehr langsam voran.

Untersuchung

LDAP:

LDAP (Lightweight Directory Access Protocol) ist ein offenes Protokoll zum Speichern und Abrufen von Daten aus einer hierarchischen Verzeichnisstruktur. LDAP wird häufig verwendet, um Informationen über eine Organisation und ihre Ressourcen und Benutzer zu speichern. Es ist eine flexible Lösung, um jegliche Art von Entität und ihre Qualitäten zu definieren.

Verzeichnisdienst:

Ein Verzeichnisdienst wird verwendet, um Daten in einem Schlüsselwerttypformat zu speichern, zu organisieren und darzustellen. In der Regel sind Verzeichnisse für Suchvorgänge, Suchen und Lesevorgänge im Vergleich zu Schreibvorgängen optimiert, sodass sie für Daten, auf die häufig verwiesen wird, aber selten geändert wird, sehr gut funktionieren.

LDAP (Lightweight Directory Access Protocol) ist ein Kommunikationsprotokoll, das die Methoden für den Zugriff auf einen Verzeichnisdienst definiert. Allgemeiner formt LDAP die Art, wie die Daten in einem Verzeichnisdienst für Benutzer dargestellt werden sollen, definiert Anforderungen für die Komponenten, die zum Erstellen von Dateneinträgen in einem Verzeichnisdienst verwendet werden, und beschreibt, wie verschiedene primitive Elemente zum Erstellen von Einträgen verwendet werden. Attribute:

Die Daten selbst in einem LDAP-System werden hauptsächlich in Elementen gespeichert, die als Attribute bezeichnet werden. Attribute sind im Wesentlichen Schlüssel-Wert-Paare.

Einträge:

Attribute allein sind nicht sehr nützlich. Um Sinn zu haben, müssen sie mit etwas assoziiert werden. Innerhalb von LDAP verwenden Sie Attribute innerhalb eines Eintrags. Ein Eintrag ist im Grunde eine Sammlung von Attributen unter einem Namen, die verwendet werden, um etwas zu beschreiben.

Sie können zum Beispiel einen Eintrag für einen Benutzer in Ihrem System oder für jeden Artikel in einem Inventar haben. Dies entspricht in etwa einer Zeile in einem relationalen Datenbanksystem oder einer einzelnen Seite in einem Adressbuch (die Attribute hier würden die verschiedenen Felder in jedem dieser Modelle darstellen). Während ein Attribut eine Qualität oder ein Merkmal einer Sache definiert, beschreibt ein Eintrag das Element selbst, indem er diese Attribute einfach unter einem Namen sammelt.

Alle Einträge werden einem LDAP-System als Verzweigungen in Bäumen hinzugefügt, die als Dateninformationsbäume oder DITs bezeichnet werden.

Ein DIT stellt eine Organisationsstruktur dar, die einem Dateisystem ähnelt, in dem jeder Eintrag (außer dem Eintrag auf oberster Ebene) genau einen übergeordneten Eintrag und möglicherweise eine beliebige Anzahl untergeordneter Einträge enthält. Da Einträge in einem LDAP-Baum so ziemlich alles repräsentieren können, werden einige Einträge hauptsächlich für organisatorische Zwecke verwendet, ähnlich wie Verzeichnisse innerhalb eines Dateisystems.

Beispiele:

```
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

Auflösung

Der Benutzer hatte einen userBaseFilter wie den folgenden:

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

Die Benutzer, die diese langsame Leistung beobachteten, gehörten möglicherweise nicht zu allen im ursprünglichen userBaseFilter aufgeführten Abteilungen. Entfernen Sie eine oder zwei Abteilungen, sodass die Suchvorgänge bei jeder Authentifizierung weniger umfangreich wären, da der LDAP-Server nur die Einträge einer Abteilung überprüfen müsste.

Verwandte Links

Splunk-Antworten:

Warum schlägt die LDAP-Authentifizierung mit Fehlern bei der Größenbeschränkung fehl, wenn Splunk 6.2 unter Windows 2008 R2 verwendet wird?

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.