

LDAP 인증 속도가 느림

적용 가능성

Splunk Enterprise

설명

사용자는 LDAP를 인증 방법으로 사용할 때 성능이 매우 느렸습니다.

조사

LDAP:

LDAP(Lightweight Directory Access Protocol)는 계층적 디렉토리 구조에서 데이터를 저장하고 검색하는 데 사용되는 개방형 프로토콜입니다. 일반적으로 조직, 해당 자산 및 사용자에 대한 정보를 저장하는 데 사용되는 LDAP는 모든 유형의 엔티티 및 특성을 정의하는 유연한 솔루션입니다.

디렉토리 서비스:

디렉토리 서비스는 키 값 형식 형식으로 데이터를 저장, 구성 및 표시하는 데 사용됩니다. 일반적으로 디렉토리는 쓰기 작업을 통한 조회, 검색 및 읽기 작업에 최적화되므로 자주 참조되지만 자주 변경되지 않는 데이터에 대해 매우 잘 작동합니다.

LDAP(Lightweight Directory Access Protocol)는 디렉토리 서비스에 액세스할 수 있는 방법을 정의하는 통신 프로토콜입니다. 보다 광범위하게 말하면, LDAP는 디렉토리 서비스 내의 데이터가 사용자에게 표시되는 방식을 형성하고, 디렉토리 서비스 내에서 데이터 엔트리를 생성하는 데 사용되는 구성 요소에 대한 요구 사항을 정의하고, 엔트리를 작성하는 데 다른 기본 요소가 사용되는 방식을 간략하게 설명합니다. 특성:

LDAP 시스템의 데이터 자체는 주로 특성이라는 요소에 저장됩니다. 속성은 기본적으로 키-값 쌍입니다.

항목:

속성 자체는 그다지 유용하지 않습니다. 의미를 가지려면, 그들은 어떤 것과 연관되어야 한다.

LDAP 내에서 항목 내의 특성을 사용합니다. 항목은 기본적으로 어떤 것을 설명하는 데 사용되는 이름 아래의 속성 모음입니다.

예를 들어 시스템의 사용자 또는 인벤토리의 각 항목에 대한 항목을 가질 수 있습니다. 이는 관계형 데이터베이스 시스템의 행 또는 주소록 내의 단일 페이지와 대략적으로 유사합니다(여기서 속성은 각 모델의 다양한 필드를 나타냄). 속성이 어떤 것의 품질이나 특성을 정의하는 반면, 항목은 단순히

이름 아래에 이러한 속성을 수집하여 항목 자체를 설명합니다.

항목은 모두 데이터 정보 트리 또는 DIT라는 트리의 분기로 LDAP 시스템에 추가됩니다.

DIT는 파일 시스템과 유사한 조직 구조를 나타냅니다. 각 항목(최상위 항목 제외)에는 정확히 하나의 상위 항목이 있으며 그 아래에 하위 항목이 몇 개 있을 수 있습니다. LDAP 트리의 항목은 거의 모든 항목을 나타낼 수 있으므로 일부 항목은 파일 시스템 내의 디렉토리와 마찬가지로 주로 조직적 목적으로 사용됩니다.

예를 들면 다음과 같습니다.

```
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` 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.

해결

사용자에게 다음과 같은 `userBasefilter`가 있습니다.

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

이 느린 성능을 관찰하던 사용자가 원래 userBaseFilter에 나열된 모든 부서에 속하지 않았을 수 있습니다. LDAP 서버는 한 부서의 항목만 검사하면 되기 때문에 인증이 발생할 때마다 검색 범위가 줄어들도록 한 부서 또는 두 부서를 제거합니다.

관련 링크

Splunk 답변:

Windows 2008 R2에서 Splunk 6.2를 사용하는 동안 "size limit exceeded" 오류로 인해 LDAP 인증이 실패한 이유는 무엇입니까?

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.