AD 동기화를 위한 Umbrella 암호화 이해

목차

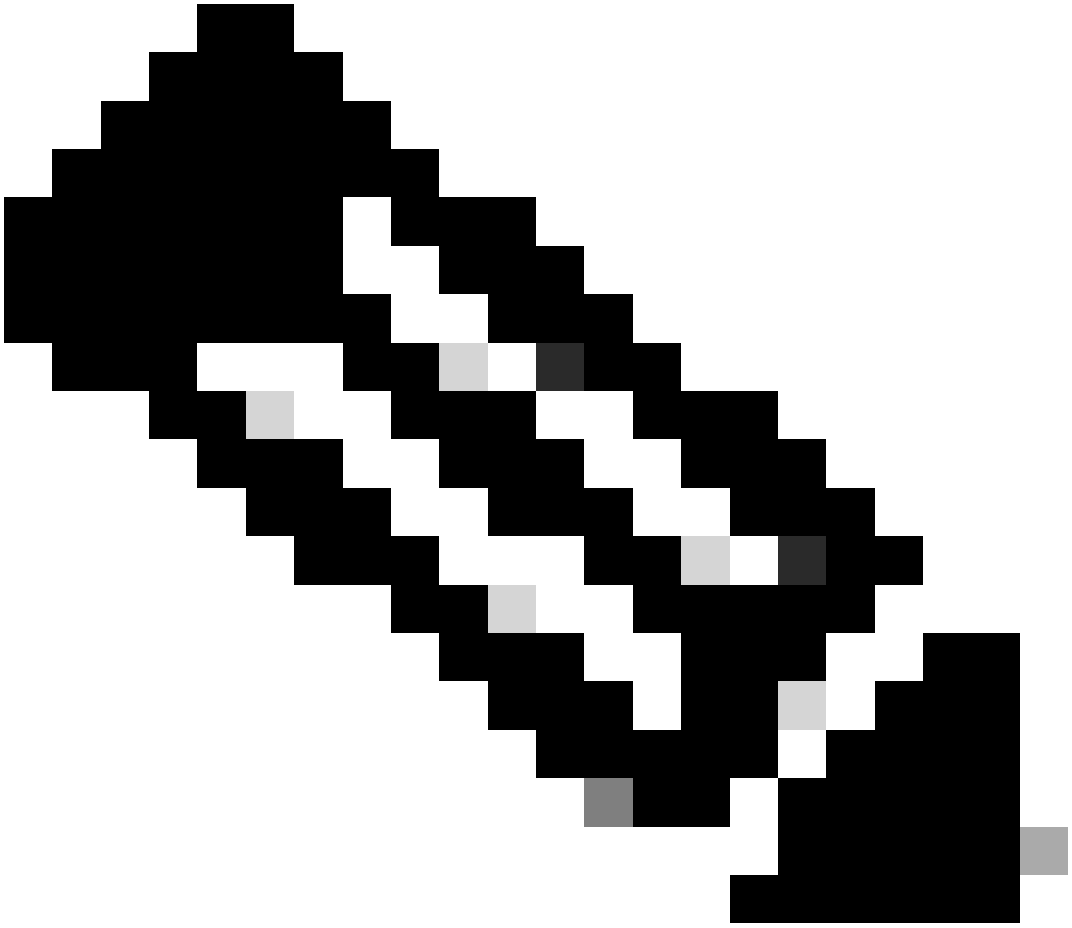
소개

이 문서에서는 AD 동기화를 위한 Umbrella 암호화에 대해 설명합니다(예: 데이터 전송 암호화 방법).

배경 정보

Umbrella AD Connector 소프트웨어는 LDAP를 사용하여 AD 도메인 컨트롤러에서 사용자, 컴퓨터 및 그룹 정보의 세부 정보를 검색합니다. 각 개체에는 필요한 특성만 저장됩니다. 여기에는 sAMAccountName, dn, userPrincipalName, memberOf, objectGUID, primaryGroupId(사용자 및 컴퓨터용) 및 primaryGroupToken(그룹용)이 포함됩니다.

그런 다음 이 데이터는 Umbrella에 업로드되어 정책 컨피그레이션 및 보고에 사용됩니다. 이 데이터는 사용자별 또는 컴퓨터별 필터링에도 필요합니다.



참고: objectGUID가 해시된 형식으로 전송됩니다.

동기화 중인 항목을 정확하게 알아보려면 다음 항목에 포함된 .ldif 파일을 확인할 수 있습니다.

```
C:\Program Files\OpenDNS\OpenDNS Connector\ADSync\*.ldif
```

이 문서에서는 이 데이터 전송이 어떻게 암호화되는지 설명합니다.

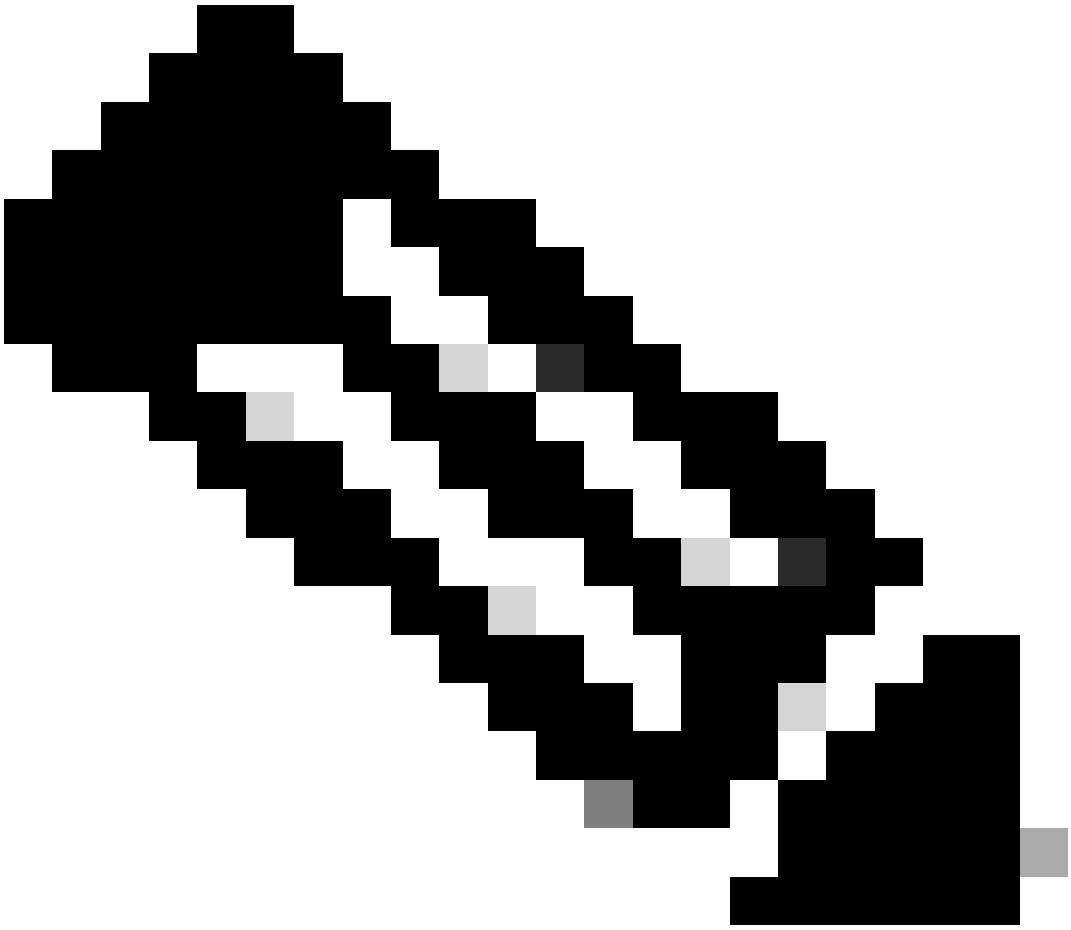
AD 데이터 업로드를 위한 암호화

Umbrella AD Connector는 보안 HTTPS 연결을 사용하여 AD 정보를 Umbrella에 업로드합니다. Connector <> Umbrella 클라우드 간 업로드는 항상 암호화됩니다.

AD 데이터 검색을 위한 암호화

v1.1.22부터 Connector는 이제 Domain Controller <> Connector 간의 암호화로 사용자 세부 정보를 검색하려고 시도합니다. 두 가지 방법이 시도됩니다.

- LDAPS. 데이터는 보안 터널을 통해 전송됩니다.
- Kerberos 인증을 사용하는 LDAP. 패킷 레벨 암호화를 제공합니다.



참고: LDAPS는 커넥터 소프트웨어가 ADsync에 사용된 도메인 컨트롤러와 동일한 서버에서 실행되는 경우 사용되지 않습니다.

어떤 이유로든 이 시도가 실패하면 이 메커니즘으로 돌아갑니다.

- NTLM 인증을 사용하는 LDAP. 이렇게 하면 보안 인증이 제공되지만 DC > Connector 간의 데이터 전송은 암호화 없이 발생합니다.

암호화가 가능하도록 하려면 다음을 수행하는 것이 좋습니다.

- 도메인 컨트롤러에서 LDAPS를 활성화합니다. 이는 Umbrella의 지원 범위를 벗어나지만 Microsoft 설명서로 활성화할 수 있습니다.
- 도메인 컨트롤러의 호스트 이름이 'Deployments(구축) > Sites and AD(사이트 및 AD)'에서 올바르게 구성되어 있는지 확인합니다. 두 암호화 방법 모두에 올바른 호스트 이름이 필요합니다. 호스트 이름이 잘못된 경우 컨피그레이션 스크립트를 사용하여 도메인 컨트롤러를 다시 등록하거나 Umbrella 지원에 문의하십시오.

암호화를 확인하는 중입니다. 여기서 로그 파일을 확인할 수 있습니다.

```
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\<VERSION>\OpenDNSAuditClient.log
```

AD 동기화 중에 다음과 같은 로그 항목이 표시됩니다.

LDAPS 연결 성공:
<SERVER> 통신에 SSL을 사용하여 DN을 가져옵니다.

Kerberos 인증 성공:
<SERVER> 통신에 Kerberos를 사용하여 DN을 가져옵니다.

NTLM 페일백 메커니즘 사용 중:
DC 호스트 <SERVER>에 대한 Kerberos가 실패했습니다. 호스트 이름이 올바르지 않을 수 있습니다. NTLM 쿼리로 돌아갑니다.

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.