SWA에서 Kerberos 인증 문제 해결

목차

소개

이 문서에서는 Kerberos 인증의 기본 사항 및 SWA(Secure Web Appliance)에서 Kerberos 인증 문제를 해결하는 단계에 대해 설명합니다.

용어

SWA	Secure Web Appliance
CLI	명령줄 인터페이스
광고	액티브 디렉토리
DC	도메인 컨트롤러
SPN	서비스 사용자 이름

KDC	Kerberos 키 배포 센터
TGT	인증 티켓 (Ticket Granting Ticket)
태그	티켓 부여 서비스
하	고가용성
VRRP	가상 라우터 이중화 프로토콜
잉어	CN(Common Address Redundancy Protocol)
SPN	서비스 사용자 이름
LDAP	LDS(Lightweight Directory Access Protocol)

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

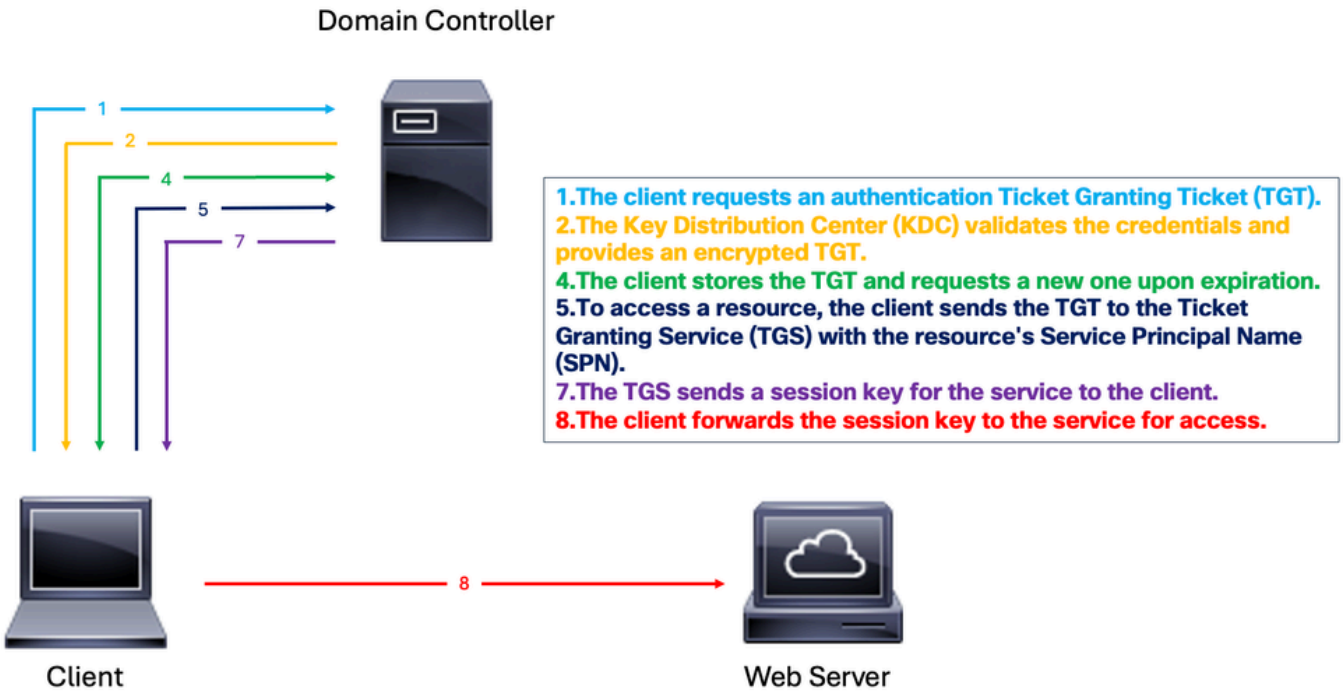
- Active Directory 및 Kerberos 인증
- SWA 인증 및 영역

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

Kerberos 네트워크 흐름



이미지: 샘플 Kerberos 흐름

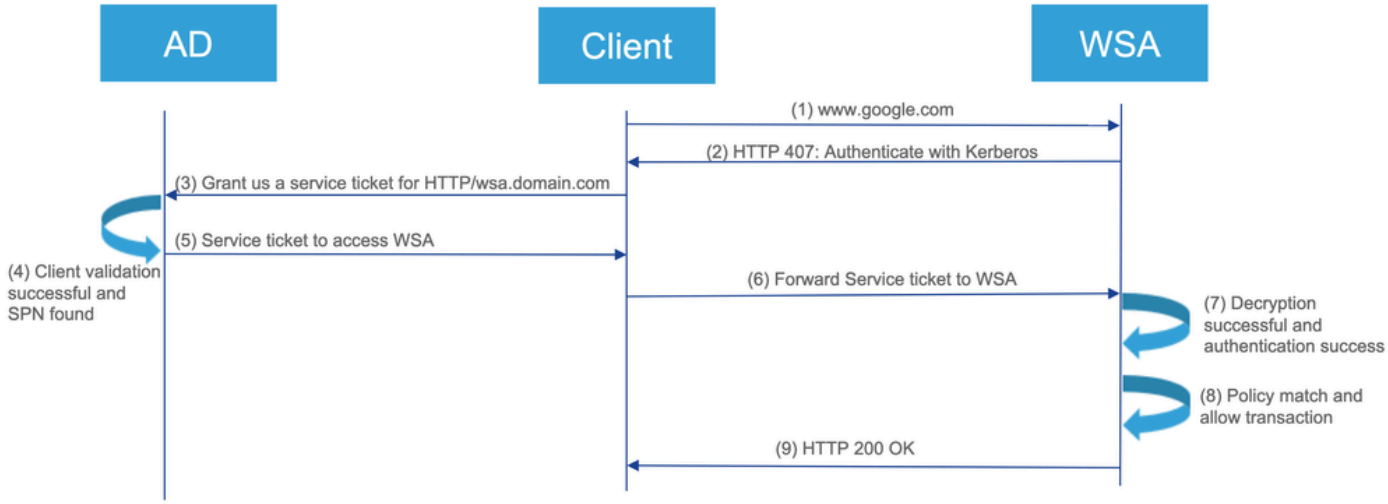
Kerberized 환경에서 인증을 위한 기본 단계는 다음과 같습니다.

1. 클라이언트가 KDC(Key Distribution Center)에서 TGT(Ticket Granting Ticket)를 요청합니다.
2. KDC는 클라이언트 시스템 사용자 자격 증명을 확인하고 암호화된 TGT 및 세션 키를 다시 전송합니다.
3. TGT는 TGS(Ticket Granting Service) 비밀 키로 암호화됩니다.
4. 클라이언트는 TGT를 저장하고 만료되면 자동으로 새 TGT를 요청합니다.

서비스 또는 리소스에 액세스하는 경우
1. 클라이언트가 원하는 리소스의 SPN(서비스 사용자 이름)과 함께 TGT를 TGS에 보냅니다.
2. KDC는 TGT를 확인하고 사용자 클라이언트 시스템 액세스 권한을 확인합니다.

3. TGS가 클라이언트에 서비스별 세션 키를 보냅니다.
4. 클라이언트가 액세스를 증명하기 위해 서비스에 세션 키를 제공하고, 서비스는 액세스를 허용합니다.

SWA의 Kerberos 인증 흐름



1. 클라이언트는 SWA를 통해 www.google.com에 대한 액세스를 요청합니다.
2. SWA는 인증을 요청하면서 "HTTP 407" 상태로 응답합니다.
3. 클라이언트는 도메인 가입 중에 받는 TGT를 사용하여 AD 서버에서 HTTP/SWA.domain.com 서비스에 대한 서비스 티켓을 요청합니다.
4. AD 서버는 클라이언트를 검증하고 서비스 티켓을 발급하며, 성공하고 SWA의 SPN(Service Principal Name)을 찾은 경우 다음 단계로 진행합니다.
5. 클라이언트가 SWA에 이 티켓을 보냅니다.
6. SWA는 티켓을 해독하고 인증을 확인합니다.
7. 인증에 성공하면 SWA는 정책을 확인합니다.
8. 트랜잭션이 허용되는 경우 SWA는 클라이언트에 "HTTP 200/OK" 응답을 보냅니다.

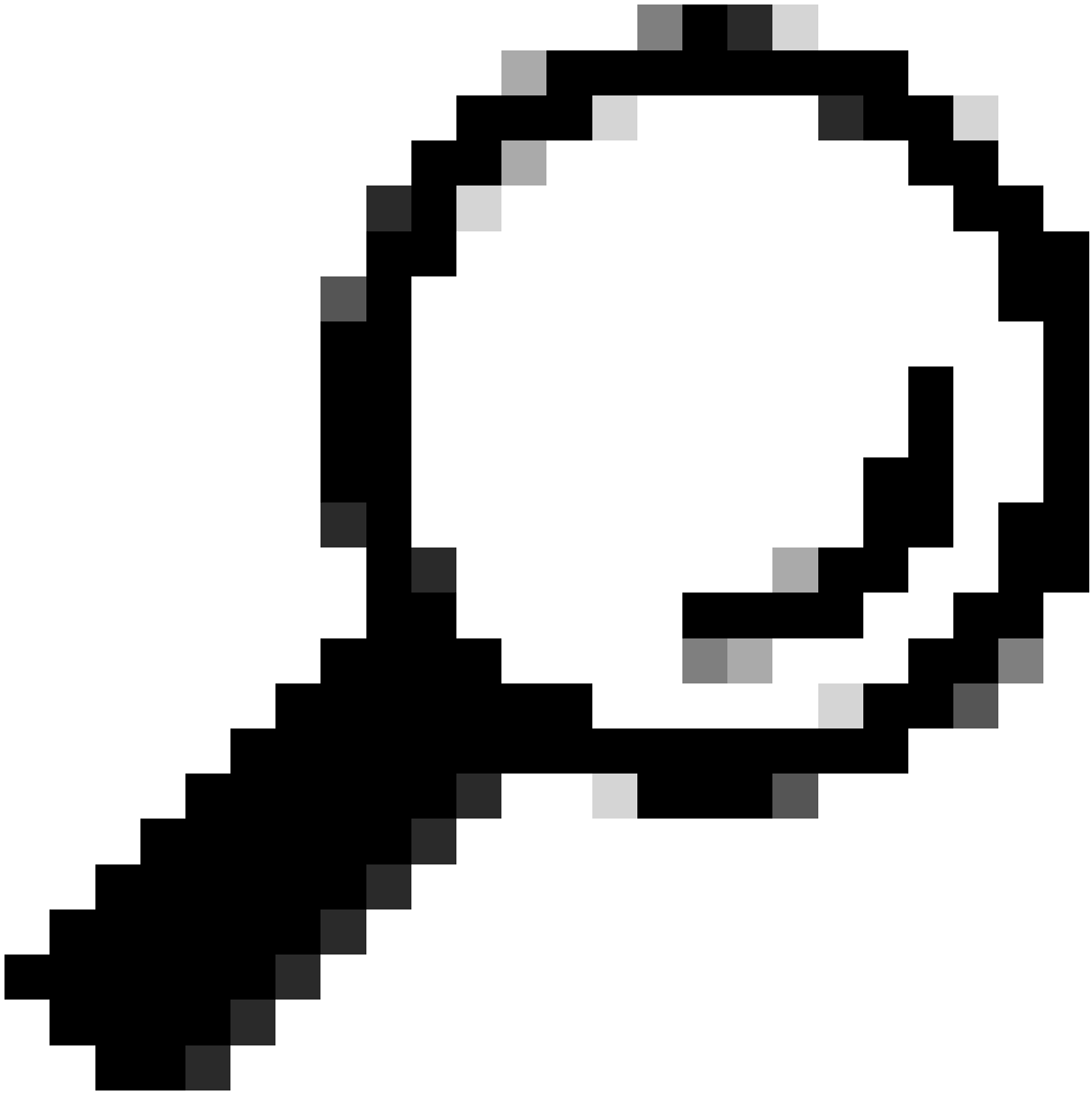
SPN의 목적은 무엇입니까?

SPN(서비스 사용자 이름)은 Kerberos 인증에서 서비스 인스턴스를 고유하게 식별합니다. 서비스 인스턴스를 서비스 계정에 연결하므로 고객은 계정 이름 없이 서비스에 대한 인증을 요청할 수 있습니다. AD 또는 Open LDAP와 같은 KDC(Key Distribution Center) 구현의 각 계정에는 SPN이 있습니다. SPN은 서비스를 엄격하게 식별하지만, 서비스가 클라이언트 역할을 하는 시나리오에서 클라이언트 이름(UPN)을 참조하는 데 잘못 사용되는 경우가 있습니다.

Kerberos에서 SPN(서비스 사용자 이름)은 네트워크 내에서 서비스 인스턴스를 고유하게 식별합니다. 클라이언트가 특정 서비스에 대한 인증을 요청할 수 있습니다. SPN은 서비스 인스턴스를 해당 계정에 연결하여 Kerberos가 해당 서비스에 대한 액세스 요청을 올바르게 인증하고 권한을 부여할 수 있도록 합니다.

Active Directory 서버 컨피그레이션

1. 새 사용자 계정을 만들거나 사용할 기존 사용자 계정을 선택합니다.
2. 선택한 사용자 계정에 사용할 SPN을 등록합니다.
3. 중복 SPN이 등록되어 있지 않은지 확인하십시오.



팁: 로드 밸런서 또는 트래픽 관리자/트래픽 셰이퍼 뒤에서 SWA를 사용하는 Kerberos는 어떻게 다릅니까? HA 가상 호스트 이름에 대한 SPN을 사용자 계정과 연결하는 대신 HTTP 트래픽 리디렉션 디바이스에 대한 SPN을 연결합니다(예: AD에 사용자 계정이 있는 LoadBalancer(Traffic Manager).

Kerberos 구현에 대한 모범 사례를 찾을 수 있습니다.

- 보안 웹 어플라이언스 모범 사례
- SWA 연결을 위한 방화벽 포트 구성

문제 해결

SPN 명령으로 Kerberos 문제 해결

다음은 Kerberos 환경에서 SPN(서비스 사용자 이름)을 관리하기 위한 유용한 setspn 명령 목록입니다. 이러한 명령은 일반적으로 Windows 환경에서 관리 권한을 가진 명령줄 인터페이스에서 실행됩니다.

특정 계정의 SPN 나열:	setspn -L <사용자/컴퓨터 계정 이름> 지정된 계정에 대해 등록된 모든 SPN을 나열합니다.
계정에 SPN 추가:	setspn -A <SPN> <사용자/컴퓨터 계정 이름> 지정된 SPN을 지정된 계정에 추가합니다.
계정에서 SPN 삭제:	setspn -D <SPN> <사용자/컴퓨터 계정 이름> 지정된 SPN을 지정된 계정에서 제거합니다.
SPN이 이미 등록되어 있는지 확인:	setspn -Q <SPN> 지정한 SPN이 도메인에 이미 등록되어 있는지 확인합니다.
도메인의 모든 SPN 나열	setspn -L <사용자/컴퓨터 계정> 도메인에 있는 모든 SPN을 나열합니다.
컴퓨터 계정에 대한 SPN 설정:	setspn -S <SPN> <사용자/컴퓨터 계정 이름> SPN을 컴퓨터 계정에 추가하여 중복 항목이 없도록 합니다.
특정 계정의 SPN 재설정:	setspn -R <사용자/컴퓨터 계정 이름> 지정한 계정의 SPN을 다시 설정하여 중복된 SPN 문제를 해결합니다.

SPN 명령 및 출력의 예

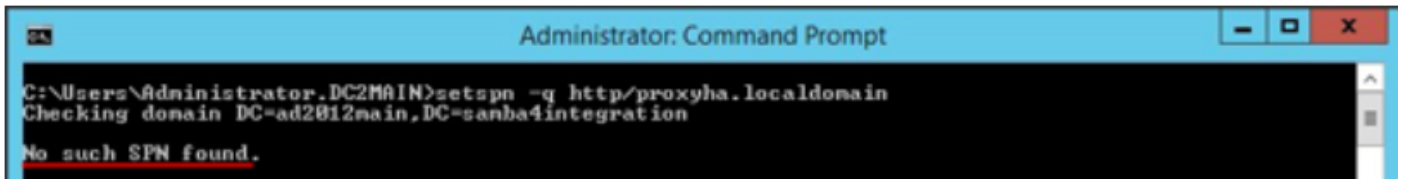
제공된 예는 사용 방법을 보여줍니다.

- 사용자/컴퓨터 계정: vrpserviceuser
- SPN: http/WsaHostname.com 또는 http/proxyha.localdomain

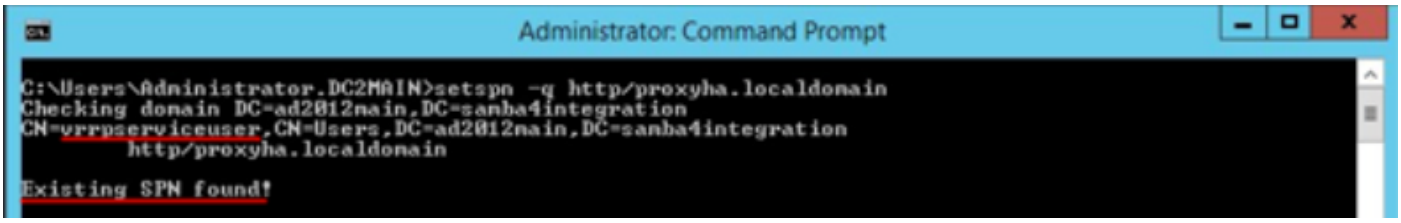
SPN이 사용자 계정과 이미 연결되어 있는지 확인:
setspn -q <SPN>

setspn -q http/proxyha.localdomain

시나리오 1: SPN을 찾을 수 없음



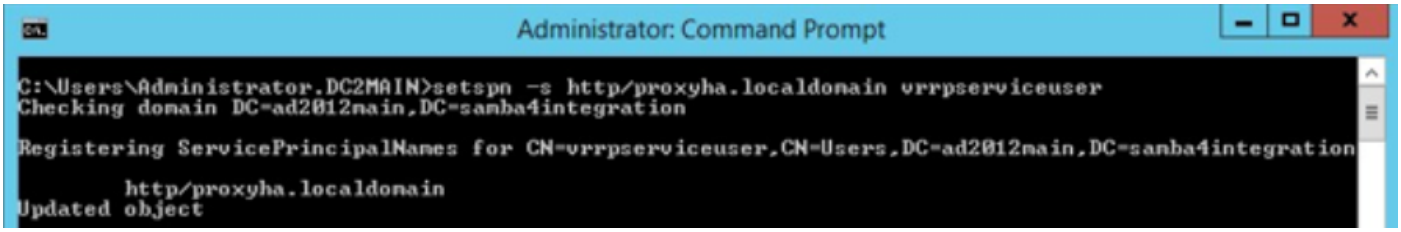
시나리오 2: SPN 찾음



- SPN을 올바른 사용자/컴퓨터 계정과 연결:

구문: setspn -s <SPN> <사용자/컴퓨터 계정>

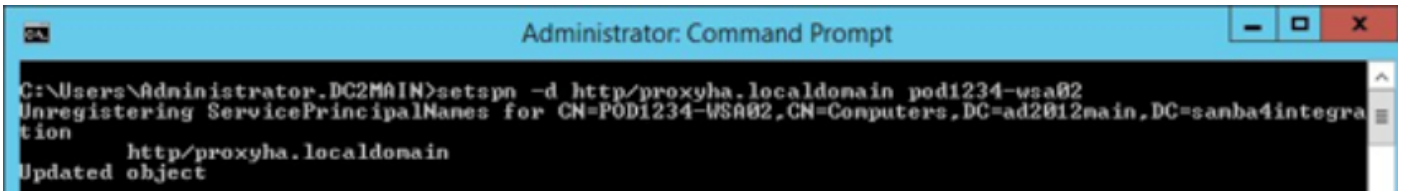
예를 들면 다음과 같습니다. setspn -s http/proxyha.localdomain vrpserviceuser



- 사용자 또는 컴퓨터 계정과 이미 연결되어 있는 SPN을 삭제/제거합니다.

구문: setspn -d <SPN> <사용자/컴퓨터 계정>

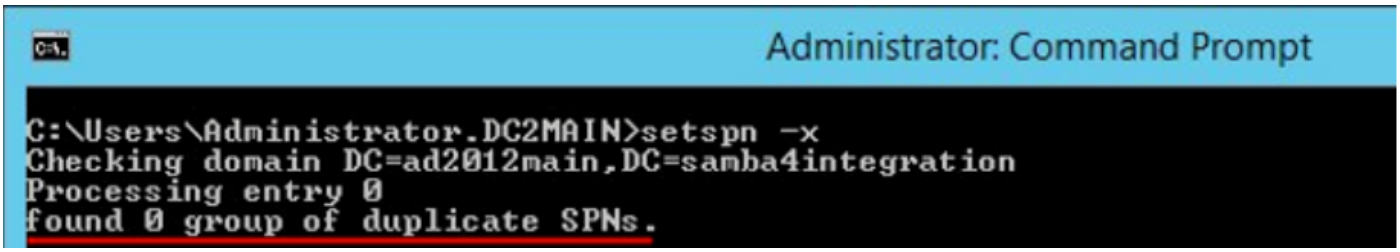
예를 들면 다음과 같습니다. setspn -d http/proxyha.localdomain pod1234-wsa0

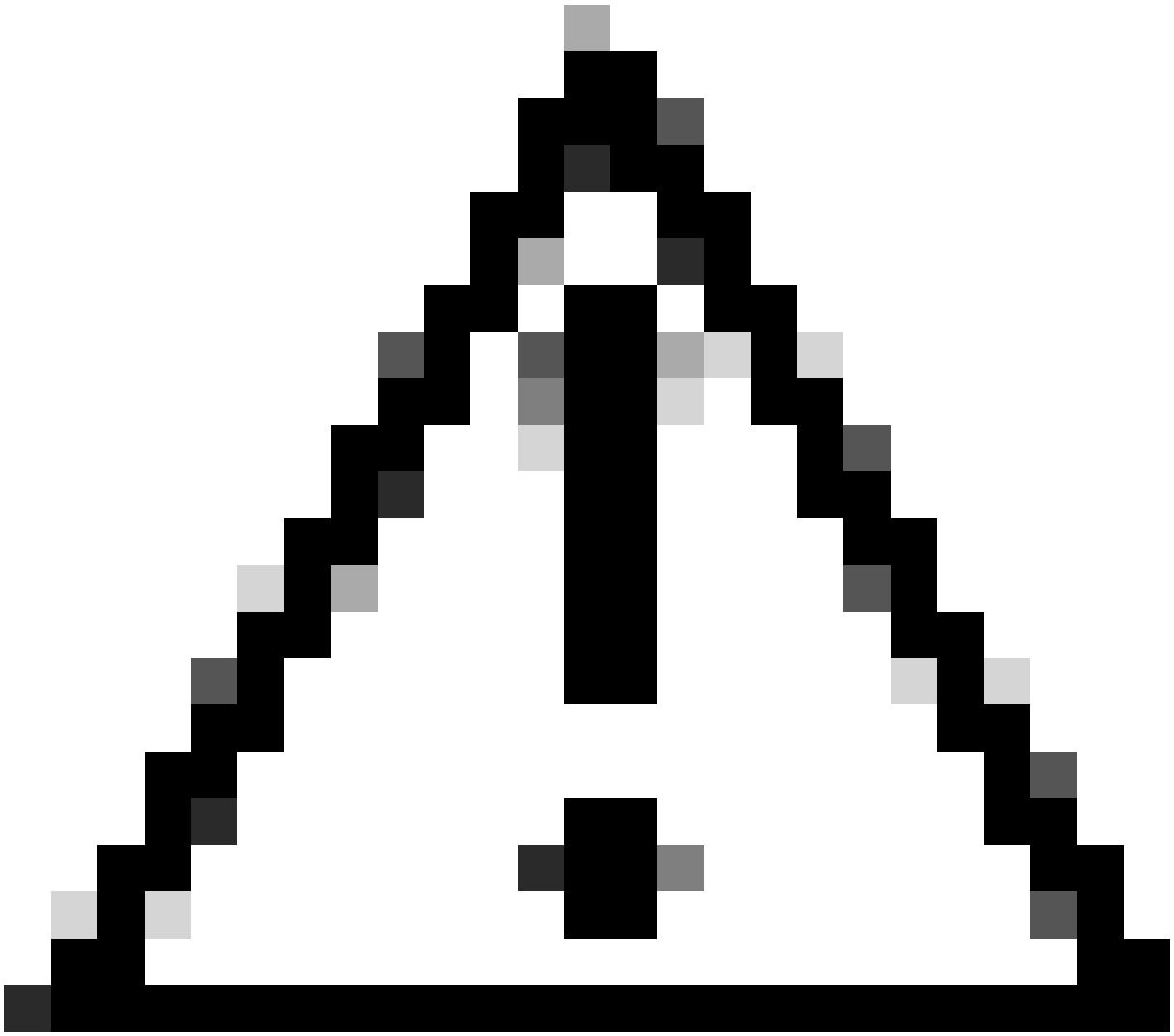


나중에 오류가 발생할 수 있으므로 HA 가상 호스트 이름에 대해 중복된 SPN이 없는지 확인합니다.

- 사용할 명령: setspn -x

따라서 Kerberos 서비스 티켓이 클라이언트에 제공되지 않으며 Kerberos 인증이 실패합니다.



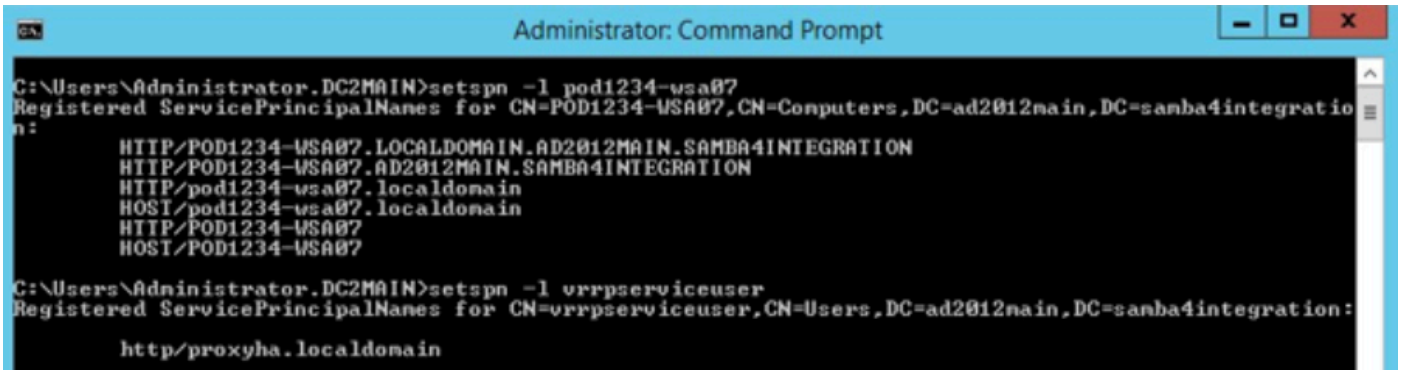


주의: 중복 항목이 있는 경우 setspn -d 명령을 사용하여 중복 항목을 제거하십시오.

- 계정과 연결된 모든 SPN 나열:

구문: setspn -l <사용자/컴퓨터 계정>

예를 들면 다음과 같습니다. setspn -l vrpserviceuser



SWA에서 Kerberos 트러블슈팅

Kerberos 인증 문제를 해결할 때 Cisco Support에서 받아야 하는 정보:

- 현재 컨피그레이션 세부사항.
- 인증 로그(디버그 또는 추적 모드).
- (적절한 필터를 사용하여) 수행된 패킷 캡처:

  (a) 클라이언트 디바이스

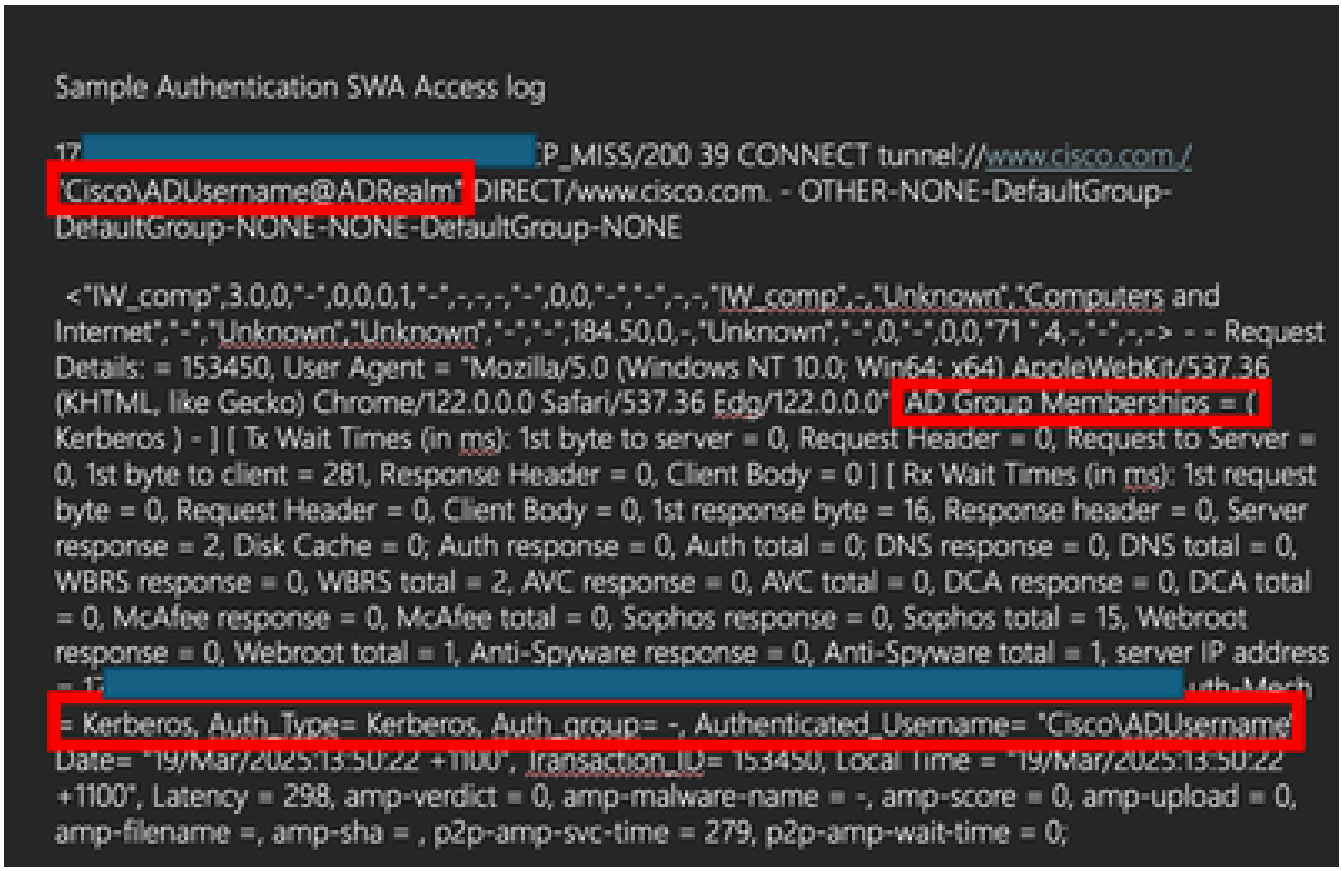
  나. 특공대

- %m개의 사용자 지정 형식 지정자가 활성화된 로그에 액세스합니다. 특정 트랜잭션에 사용된 인증 메커니즘을 표시해야 합니다.
- 자세한 인증 정보를 보려면 작동/비작동 프록시의 액세스 로그에 이러한 사용자 지정 필드를 추가하여 자세한 정보를 얻거나 액세스 로그의 매개변수 추가 하이퍼링크를 참조하십시오.
- SWA GUI에서 System administration(시스템 관리) > Log subscription(로그 서브스크립션) > Access logs(액세스 로그) > Custom fields(맞춤형 필드) > Add this string for authentication issues(인증 문제에 대해 이 문자열 추가)로 이동합니다.

```
server IP address = %k, Client IP address= %a, Auth-Mech = %m, Auth_Type= %m, Auth_group= %g, Authentic
```

```
a;
```

- 사용자 인증 세부 정보를 위한 SWA 액세스 로그
- Cisco SWA는 인증된 사용자 이름을 Domain\username@authentication_realm 형식으로 기록합니다.



- GUI에서 테스트 인증 영역 설정을 실행합니다. Network(네트워크) > Authentication(인증)으로 이동한 다음 Test Current Settings(현재 설정 테스트) 섹션에서 Realm(영역) 이름을 클릭합니다. 테스트 시작을 클릭합니다.

Kerberos 데이터베이스에서 서버를 찾을 수 없습니다.

한 가지 일반적인 오류 사례는 "Kerberos 데이터베이스에서 서버를 찾을 수 없음"으로 인해 웹 요청이 실패한 경우입니다.

```
curl -vx proxyha.local:3128 --proxy-negotiate -u: http://www.cisco.com/
* About to connect() to proxy proxyha.localdomain port 3128 (#0)
* Connected to proxyha.local (10.8.96.30) port 3128 (#0)
< HTTP/1.1 407 Proxy Authentication Required
< Via: 1.1 pod1234-wsa02.local:80 (Cisco-SWA/10.1.2-003)
< Content-Type: text/html
gss_init_sec_context() failed: : Server not found in Kerberos database
< Proxy-Authenticate: Negotiate
< Connection: close
* HTTP/1.1 proxy connection set close!
```

이 경우 오류는 프록시 주소 값 proxyha.local에 해당하는 서비스 사용자 이름이 Active Directory 서버에 등록되지 않았음을 나타냅니다. 이 문제를 해결하려면 SPN http/proxyha.local이 AD DC에 등록되어 있고 적절한 서비스 계정에 추가되었는지 확인해야 합니다.

추가 정보 및 참조

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.