ISE(Identity Service Engine) 및 AD(Active Directory) 이해

목차

소개

이 문서에서는 ISE(Identity Service Engine)와 AD(Active Directory)가 통신하는 방법, 사용되는 프로토콜, AD 필터 및 흐름에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음에 대한 기본 지식을 권장합니다.

- ISE 2.x 및 Active Directory 통합 .
- ISE의 외부 ID 인증

사용되는 구성 요소

- ISE 2.x .
- Windows Server(Active Directory) .

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.

AD 프로토콜

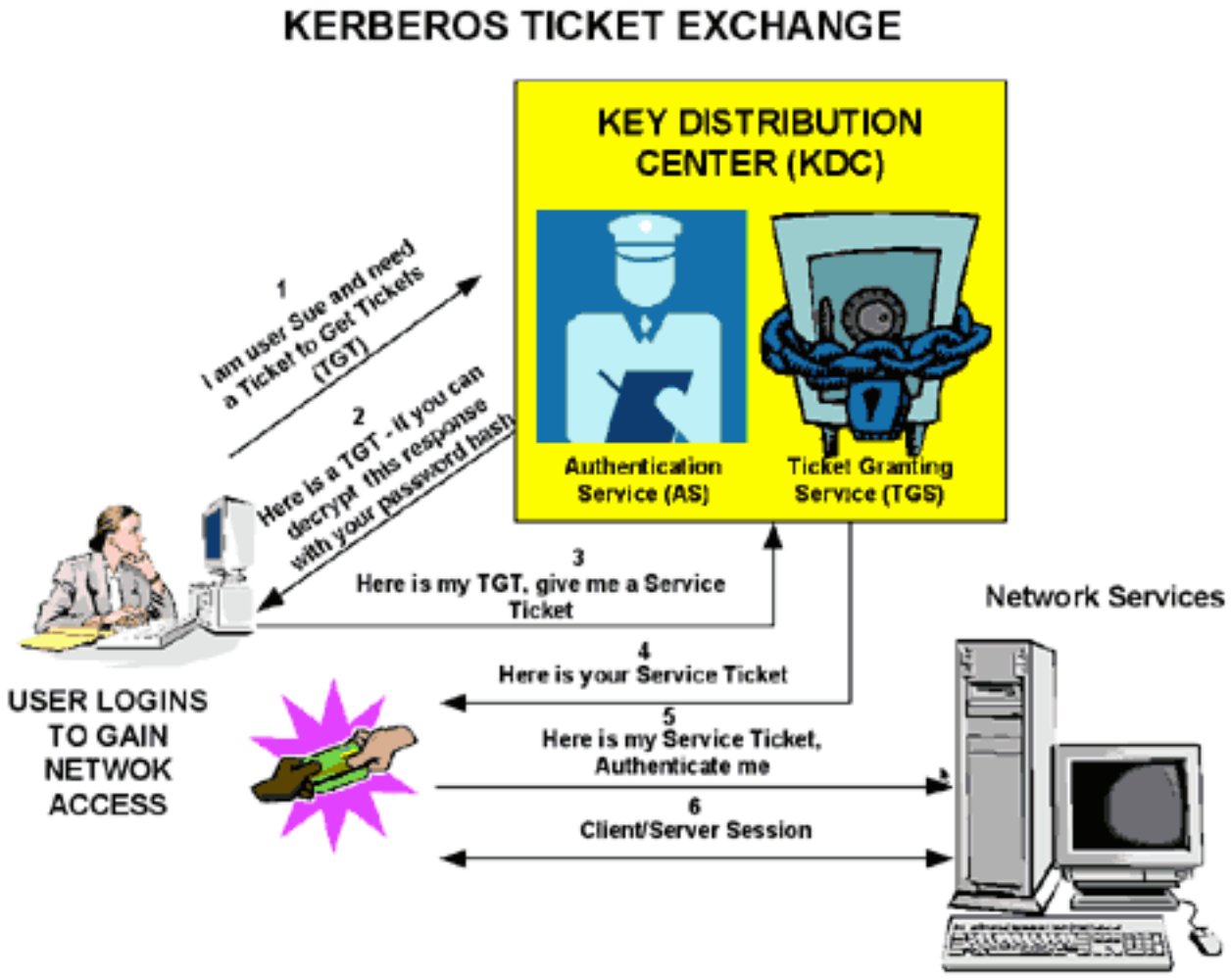
Kerberos 프로토콜

Kerberos의 3개 헤드는 KDC(Key Distribution Center), 클라이언트 사용자 및 액세스할 서버로 구성됩니다.

KDC는 DC(Domain Controller)의 일부로 설치되며 두 가지 서비스 기능을 수행합니다. AS(Authentication Service) 및 TGS(Ticket-Granting Service).

클라이언트가 서버 리소스에 처음 액세스할 때 다음 세 가지 교환이 포함됩니다.

1. AS Exchange입니다.
2. TGS 교환
3. 클라이언트/서버(CS) Exchange.



- 도메인 컨트롤러 = KDC(AS + TGS).
- 비밀번호를 사용하여 AS(SSO 포털)에 인증합니다.
- TGT(Ticket Granting Ticket)(세션 쿠키)를 가져옵니다.
- 서비스(SRV01)에 로그인을 요청합니다.
- SRV01이 사용자를 KDC로 리디렉션합니다.
- KDC에 TGT 표시 - (이미 인증됨)
- KDC에서는 SRV01에 대한 TGS를 제공합니다.

- SRV01로 리디렉션합니다.
- SRV01에 대한 서비스 티켓을 표시합니다.
- SRV01은 서비스 티켓을 확인/신뢰합니다.
- 서비스티켓에 제 모든 정보가 있습니다
- SRV01에서 로그인합니다.

네트워크에 처음 로그온할 때 사용자는 액세스 협상을 수행하고 도메인 내 KDC의 AS 부분에서 확인할 수 있도록 로그인 이름과 비밀번호를 제공해야 합니다.

KDC는 Active Directory 사용자 계정 정보에 액세스할 수 있습니다. 인증되면 사용자에게 로컬 도메인에 유효한 TGT(Ticket Granting Ticket)가 부여됩니다.

TGT의 기본 수명은 10시간이며 사용자가 비밀번호를 다시 입력할 필요 없이 사용자 로그온 세션 내내 갱신됩니다.

TGT는 로컬 시스템의 휘발성 메모리 공간에 캐시되며 네트워크 전체에서 서비스에 대한 세션을 요청하는 데 사용됩니다.

사용자는 서버 서비스에 대한 액세스가 필요할 때 KDC의 TGS 부분에 TGT를 제공합니다.

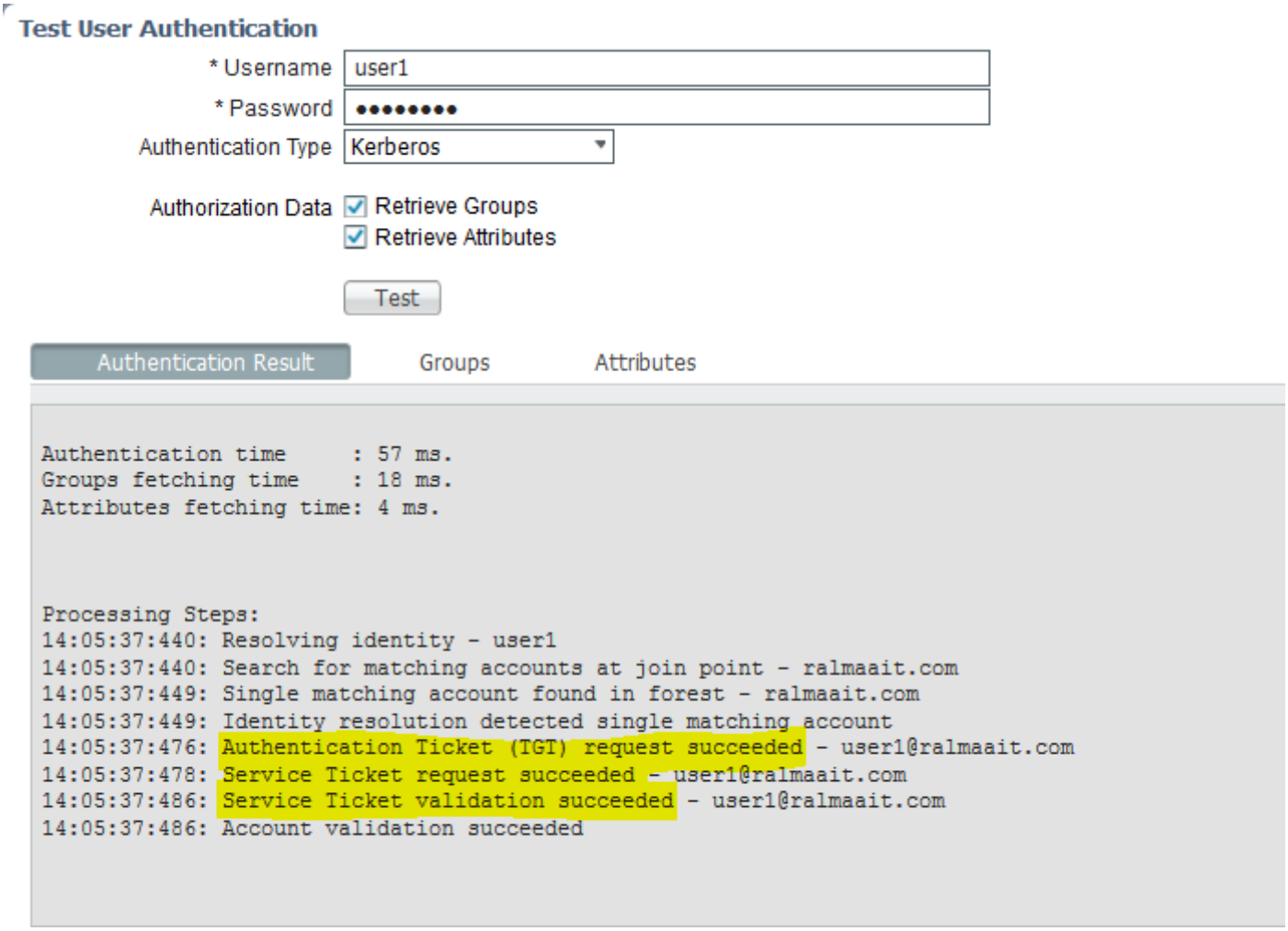
KDC의 TGS는 사용자 TGT를 인증하고 클라이언트와 원격 서버 모두에 대한 티켓 및 세션 키를 생성합니다. 그런 다음 이 정보(서비스 티켓)는 클라이언트 컴퓨터에서 로컬로 캐시됩니다.

TGS는 클라이언트 TGT를 받고 자체 키로 읽습니다. TGS가 클라이언트 요청을 승인하면 클라이언트와 대상 서버 모두에 대해 서비스 티켓이 생성됩니다.

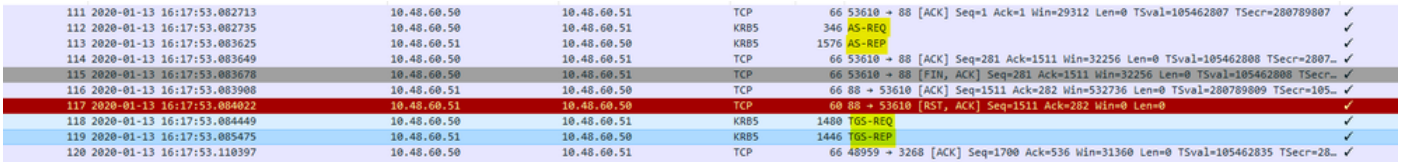
클라이언트는 이전에 AS 회신에서 검색된 TGS 세션 키를 사용하여 해당 부분을 읽습니다.

클라이언트는 다음 클라이언트/서버 교환에서 TGS 응답의 서버 부분을 대상 서버에 표시합니다.

예:



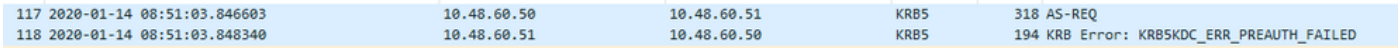
인증된 사용자에 대한 ISE의 패킷 캡처:



AS-REQ에는 사용자 이름이 포함됩니다. 비밀번호가 정확하면 AS 서비스는 사용자 비밀번호로 암호화된 TGT를 제공합니다. 그런 다음 TGT가 TGT 서비스에 제공되어 세션 티켓을 가져옵니다.

세션 티켓을 받으면 인증에 성공합니다.

클라이언트가 제공한 암호가 잘못된 예입니다.



비밀번호가 잘못된 경우 AS 요청이 실패하고 TGT가 수신되지 않습니다.

```
Processing Steps:
13:19:55:837:   Resolving Identity - User1
13:19:55:837:   Search For Matching Accounts At Join Point - Ralmaait.com
13:19:55:843:   Single Matching Account Found In Forest - Ralmaait.com
13:19:55:843:   Identity Resolution Detected Single Matching Account
13:19:55:856:   Authentication Ticket (TGT) Request Failed - User1@ralmaait.com,ERROR_PASSWORD_MISMATCH
```

비밀번호가 잘못된 경우 ad_agent.log 파일에 로그온합니다.

2020-01-14 13:36:05,442 디버그 ,140574072981248,krb5: RALMAAIT.COM,LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325에 요청(276바이트)을 보냈습니다.

2020-01-14 13:36:05,444 디버그 ,140574072981248,krb5: KDC에서 오류 수신: -1765328360/사전 인증 실패,LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05,444 디버그 ,140574072981248,krb5: 사전 인증 다시 입력 유형: 16, 14, 19, 2,LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05,444 WARNING,140574072981248,[LwKrb5GetTgtImpl ../../lwadvapi/threaded/krbtgt.c:329] KRB5 오류 코드: -1765328360(메시지: 사전 인증 실패),LwTranslateKrb5Error(),lwadvapi/threaded/lwkrb5.c:892

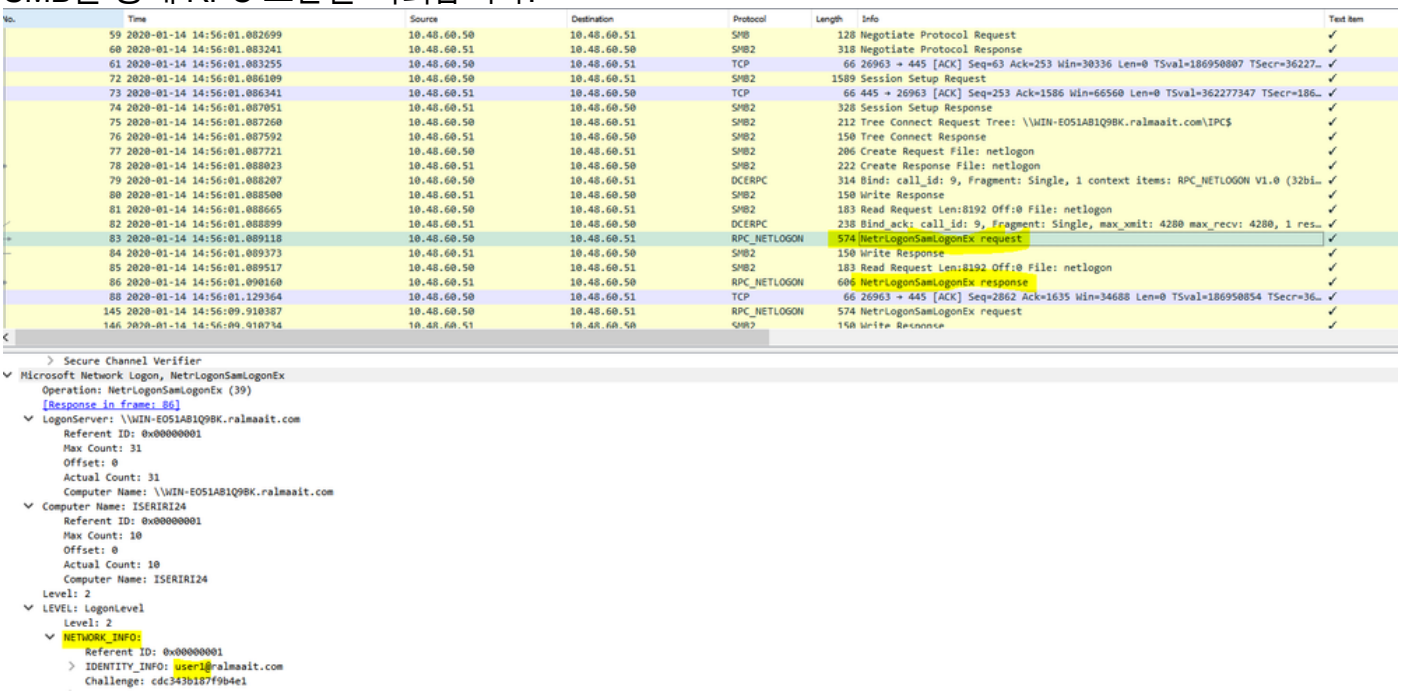
2020-01-14 13:36:05,444 DEBUG ,140574072981248,[LwKrb5InitializeUserLoginCredentials()] 오류 코드: 40022(기호: LW_ERROR_PASSWORD_MISMATCH),LwKrb5InitializeUserLoginCredentials(),lwadvapi/threaded/lwkrb5.c:1453

MS-RPC 프로토콜

ISE는 MS-RPC over SMB를 사용하며, SMB는 인증을 제공하며, 지정된 RPC 서비스가 있는 위치를 찾기 위해 별도의 세션이 필요하지 않습니다. 클라이언트와 서버 간의 통신에 "명명된 파이프"라는 메커니즘을 사용합니다.

- SMB 세션 연결을 생성합니다.
- RPC 메시지를 SMB/CIFS.TCP 포트 445를 통해 전송으로 전송
- SMB 세션은 특정 RPC 서비스가 실행되고 사용자 인증을 처리하는 포트를 식별합니다.
- 프로세스 간 통신을 위해 숨겨진 공유 IPC$에 연결합니다.
- 원하는 RPC 리소스/기능에 대해 적절한 명명된 파이프를 엽니다.

SMB를 통해 RPC 교환을 처리합니다.



이 **negotiate protocol request/response** 라인은 SMB의 사투리를 협상합니다. 이 **session setup**

request/response 인증을 수행합니다.

트리 연결 요청 및 응답이 요청된 리소스에 연결합니다. 특별 공유 IPC$에 연결되었습니다.

이 프로세스 간 통신 공유는 호스트 간의 통신 수단을 제공하며 MSRPC 기능을 위한 전송으로도 사용됩니다.

패킷 77은 **Create Request File** 파일 이름은 연결된 서비스(이 예에서는 netlogon 서비스)의 이름입니다.

패킷 83 및 86에서 NetlogonSamLogonEX 요청은 Network_INFO 필드의 AD에 ISE의 클라이언트 인증을 위한 사용자 이름을 보내는 것입니다.

NetlogonSamLogonEX 응답 패킷이 결과에 응답합니다.

NetlogonSamLogonEX 응답에 대한 일부 플래그 값:
0xc000006a는 STATUS_WRONG_PASSWORD입니다.
0x00000000은 STATUS_SUCCESS입니다.
0x00000103은 STATUS_PENDING입니다.

ISE와 AD(Active Directory) 통합

ISE는 LDAP, KRB 및 MSRBC를 사용하여 가입/탈퇴 및 인증 프로세스 동안 AD와 통신합니다.

다음 섹션에서는 AD에서 특정 DC에 연결하고 해당 DC에 대한 사용자 인증에 사용되는 프로토콜, 검색 형식 및 메커니즘을 제공합니다.

어떤 이유로든 DC가 오프라인 상태가 될 경우 ISE는 사용 가능한 다음 DC로 장애 조치하며 인증 프로세스는 영향을 받지 않습니다.

GC(글로벌 카탈로그 서버)는 포리스트에 있는 모든 Active Directory 개체의 복사본을 저장하는 도메인 컨트롤러입니다.

도메인의 디렉터리에 있는 모든 개체의 전체 복사본과 다른 모든 포리스트 도메인의 모든 개체의 부분 복사본을 저장합니다.

따라서 Global Catalog(글로벌 카탈로그)를 사용하면 사용자와 애플리케이션이 GC에 포함된 특성을 검색하여 현재 포리스트의 모든 도메인에서 객체를 찾을 수 있습니다.

글로벌 카탈로그는 각 도메인의 각 포리스트 객체에 대한 기본(불완전한) 특성 집합(Partial Attribute Set, PAT)을 포함합니다.

GC는 포리스트의 모든 도메인 디렉토리 파티션에서 데이터를 수신합니다. 표준 AD 복제 서비스와 함께 복사됩니다.

ISE를 AD에 가입

Active Directory 및 ISE 통합의 사전 요구 사항

1. ISE에서 수퍼 관리자 또는 시스템 관리자 권한이 있는지 확인합니다.
2. NTP(Network Time Protocol) 서버 설정을 사용하여 Cisco 서버와 Active Directory 간의 시간을 동기화합니다. ISE와 AD 간의 최대 허용 시간 차이는 5분입니다
3. ISE에 구성된 DNS는 추가 사이트 정보가 있거나 없는 DC, GC 및 KDC에 대한 SRV 쿼리에 응답할 수 있어야 합니다.
4. 모든 DNS 서버가 가능한 모든 Active Directory DNS 도메인에 대한 정방향 및 역방향 DNS 쿼리에 응답할 수 있는지 확인합니다.
5. AD에는 Cisco가 작동하고 액세스할 수 있는 하나 이상의 글로벌 카탈로그 서버가 Cisco에 가입한 도메인에 있어야 합니다.

AD 도메인 가입

ISE는 도메인 검색을 적용하여 3단계로 조인 도메인에 대한 정보를 가져옵니다.

1. 조인된 도메인 쿼리 - 포리스트에서 도메인을 검색하고 외부에서 조인된 도메인으로 트러스트된 도메인을 검색합니다.
2. 포리스트의 루트 도메인 쿼리 — 포리스트와의 트러스트를 설정합니다.
3. 신뢰할 수 있는 포리스트의 루트 도메인 쿼리 - 신뢰할 수 있는 포리스트에서 도메인을 검색합니다.

또한 Cisco ISE는 DNS 도메인 이름(UPN 접미사), 대체 UPN 접미사 및 NTLM 도메인 이름을 검색합니다.

ISE는 DC 검색을 적용하여 사용 가능한 DC 및 GC에 대한 모든 정보를 가져옵니다.

1. 가입 프로세스는 도메인 자체에 존재하는 AD에 대한 슈퍼 관리자의 입력 자격 증명으로 시작합니다. 다른 도메인 또는 하위 도메인에 있는 경우 사용자 이름은 UPN 표기법(username@domain)으로 기록해야 합니다.
2. ISE는 모든 DC, GC 및 KDC 레코드에 대한 DNS 쿼리를 보냅니다. DNS 회신에 답변에 이러한 응답 중 하나가 없으면 DNS 관련 오류로 인해 통합이 실패합니다.
3. ISE는 CLDAP ping을 사용하여 SRV 레코드의 우선 순위에 해당하는 DC에 보낸 CLDAP 요청을 통해 모든 DC 및 GC를 검색합니다. 첫 번째 DC 응답이 사용되고 ISE가 해당 DC에 연결됩니다.

DC 우선순위를 계산하는 데 사용되는 한 가지 요소는 DC가 CLDAP ping에 응답하는 데 걸리는 시간입니다. 더 빠른 응답이 더 높은 우선순위를 수신합니다.

> **참고:** CLDAP는 ISE에서 DC와의 연결을 설정하고 유지하는 데 사용하는 메커니즘입니다. 첫 번째 DC 응답까지의 응답 시간을 측정합니다. DC에서 응답이 없으면 실패합니다. 응답 시간이 2.5초보다 클 경우 경고 사이트의 모든 DC를 ping하는 CLDAP(사이트가 없는 경우 도메인의 모든 DC) CLDAP 응답에는 DC 사이트 및 클라이언트 사이트(ISE 시스템이 할당된 사이트)가 포함됩니다.

4. 그런 다음 ISE는 'join user' 자격 증명이 포함된 TGT를 수신합니다.
5. MSRPC를 사용하여 ISE 컴퓨터 계정 이름을 생성합니다(SAM 및 SPN).
6. ISE 컴퓨터 계정이 이미 있는 경우 SPN으로 AD를 검색합니다. ISE 시스템이 없으면 ISE는 새 시스템을 생성합니다.
7. 머신 계정을 열고 ISE 머신 계정 암호를 설정하고 ISE 머신 계정에 액세스할 수 있는지 확인합

니다.
8. ISE 컴퓨터 계정 특성(SPN, dnsHostname 등)을 설정합니다.
9. KRB5를 통해 ISE 머신 자격 증명으로 TGT를 가져오고 모든 신뢰할 수 있는 도메인을 검색합니다.
10. 조인이 완료되면 ISE 노드는 AD 그룹 및 연결된 SID를 업데이트하고 SID 업데이트 프로세스를 자동으로 시작합니다. AD 측에서 이 프로세스를 완료할 수 있는지 확인합니다.

AD 도메인 나가기

ISE가 종료되면 AD는 다음을 고려해야 합니다.

1. 전체 AD 관리자 사용자를 사용하여 탈퇴 프로세스를 수행합니다. 이렇게 하면 ISE 시스템 계정이 Active Directory 데이터베이스에서 제거되었는지 확인합니다.
2. AD에 자격 증명이 없으면 ISE 계정이 AD에서 제거되지 않으며 수동으로 삭제해야 합니다.
3. CLI에서 ISE 컨피그레이션을 재설정하거나 백업 또는 업그레이드 후 컨피그레이션을 복원할 경우 종료 작업을 수행하고 Active Directory 도메인에서 ISE 노드의 연결을 끊습니다. (조인된 경우) 그러나 ISE 노드 계정은 Active Directory 도메인에서 제거되지 않습니다.
4. 또한 Active Directory 도메인에서 노드 계정을 제거하기 때문에 Active Directory 자격 증명을 사용하여 관리 포털에서 나가기 작업을 수행하는 것이 좋습니다. ISE 호스트 이름을 변경할 때도 이 방법이 권장됩니다.

DC 장애 조치

ISE에 연결된 DC가 오프라인 상태가 되거나 어떤 이유로든 연결할 수 없는 경우 DC 장애 조치가 ISE에서 자동으로 트리거됩니다. DC 장애 조치는 다음 조건에 의해 트리거될 수 있습니다.

1. AD 커넥터가 일부 CLDAP, LDAP, RPC 또는 Kerberos 통신 시도 중에 현재 선택한 DC를 사용할 수 없게 되었음을 감지했습니다. 이러한 경우 AD 커넥터는 DC 선택을 시작하고 새로 선택된 DC로 장애 조치됩니다.
2. DC가 작동 중이며 CLDAP ping에 응답하지만 AD 커넥터가 어떤 이유로 인해 DC와 통신할 수 없습니다(예: RPC 포트가 차단됨, DC가 '중단된 복제' 상태, DC가 제대로 해제되지 않음)

이러한 경우 AD 커넥터는 차단된 목록("불량" DC가 차단된 목록에 있음)으로 DC 선택을 시작하고 선택된 DC와의 통신을 시도합니다. 차단 목록에서 선택한 DC가 캐시되지 않았습니다.

AD 커넥터는 적절한 시간 내에 장애 조치를 완료해야 합니다(또는 불가능할 경우 실패). 따라서 AD 커넥터는 장애 조치 중에 제한된 수의 DC를 시도합니다.

ISE가 잘못된 DC를 사용하지 못하도록 복구할 수 없는 네트워크 또는 서버 오류가 있는 경우 ISE는 AD 도메인 컨트롤러를 차단합니다. DC가 CLDAP ping에 응답하지 않으면 차단 목록에 추가되지 않습니다. ISE는 응답하지 않는 DC의 우선순위만 낮춥니다.

LDAP를 통한 ISE-AD 통신

ISE는 이러한 검색 형식 중 하나를 사용하여 AD에서 시스템 또는 사용자를 검색합니다. 검색이 시스템에 대한 것이면 ISE는 시스템 이름 끝에 "$"를 추가합니다. AD에서 사용자를 식별하는 데 사용되는 ID 유형 목록입니다.

- SAM 이름: 사용자 이름 또는 도메인 마크업이 없는 시스템 이름. AD의 사용자 로그온 이름입니다. **예: sajeda 또는 sajeda$**

- CN: 는 AD의 사용자 표시 이름입니다. SAM과 동일해서는 안 됩니다. **예: 사제다 아메드**
- UPN(사용자 계정 이름): SAM 이름과 도메인 이름의 조합입니다(SAM_NAME@domian). **예: sajeda@cisco.com 또는 sajeda$@cisco.com**
- 대체 UPN: 는 도메인 이름 이외의 AD에 구성된 추가/대체 UPN 접미사입니다. 이 컨피그레이션은 AD에 전역적으로 추가되며(사용자별로 구성되지 않음) 실제 도메인 이름 접미사가 아니어도 됩니다.

각 AD에는 여러 UPN 접미사(@alt1.com,@alt2.com,..., 등)를 사용할 수 있습니다. **예: 기본 UPN(sajeda@cisco.com), 대체 UPN :sajeda@domain1 , sajeda@domain2**

- NetBIOS 접두사 이름: 시스템 이름의 도메인 이름\사용자 이름입니다. **예: CISCO\sajeda 또는 CISCO\machine$**
- 정규화되지 않은 시스템의 호스트/접두사: 머신 이름이 호스트/머신 이름뿐인 경우 머신 인증에 사용됩니다. **예: 호스트/시스템**
- 정규화된 시스템이 포함된 호스트/접두사: 시스템 FQDN을 사용하는 경우 시스템 인증에 사용됩니다. 일반적으로 인증서 인증의 경우 시스템의 호스트/FQDN입니다. **예: host/machine.cisco.com**
- SPN 이름: 클라이언트가 서비스의 인스턴스를 고유하게 식별하는 데 사용되는 이름입니다(예: HTTP, LDAP, SSH).

AD 흐름에 대한 사용자 인증:

1. ID를 확인하고 ID 유형(SAM, UPN, SPN)을 확인합니다. ISE가 ID를 사용자 이름으로만 수신하는 경우 AD에서 연결된 SAM 계정을 검색합니다. ISE가 ID를 username@domain으로 수신하는 경우 AD에서 일치하는 UPN 또는 메일을 검색합니다. 두 시나리오 모두에서 ISE는 시스템 또는 사용자 이름에 대해 추가 필터를 사용합니다.
2. 도메인 또는 포리스트 검색(ID 유형에 따라 다름)
3. 모든 연결된 어카운트에 대한 정보 유지(JP, DN, UPN, Domain)
4. 연결된 계정이 없으면 AD가 사용자에 대한 회신을 알 수 없습니다.
5. 연결된 각 계정에 대해 MS-RPC(또는 Kerberos) 인증 수행
6. 단일 계정만 입력 ID 및 비밀번호와 일치하는 경우 인증에 성공합니다
7. 여러 계정이 수신 ID와 일치하는 경우 ISE는 비밀번호를 사용하여 모호성을 해결하므로 연결된 비밀번호의 계정이 인증되고 다른 계정은 잘못된 비밀번호 카운터를 1씩 늘립니다.
8. 수신 ID 및 암호와 일치하는 계정이 없으면 AD가 잘못된 암호로 회신합니다.

ISE 검색 필터

필터는 AD와 통신할 엔터티를 식별하는 데 사용됩니다. ISE는 항상 사용자 및 시스템 그룹에서 해당 엔터티를 검색합니다.

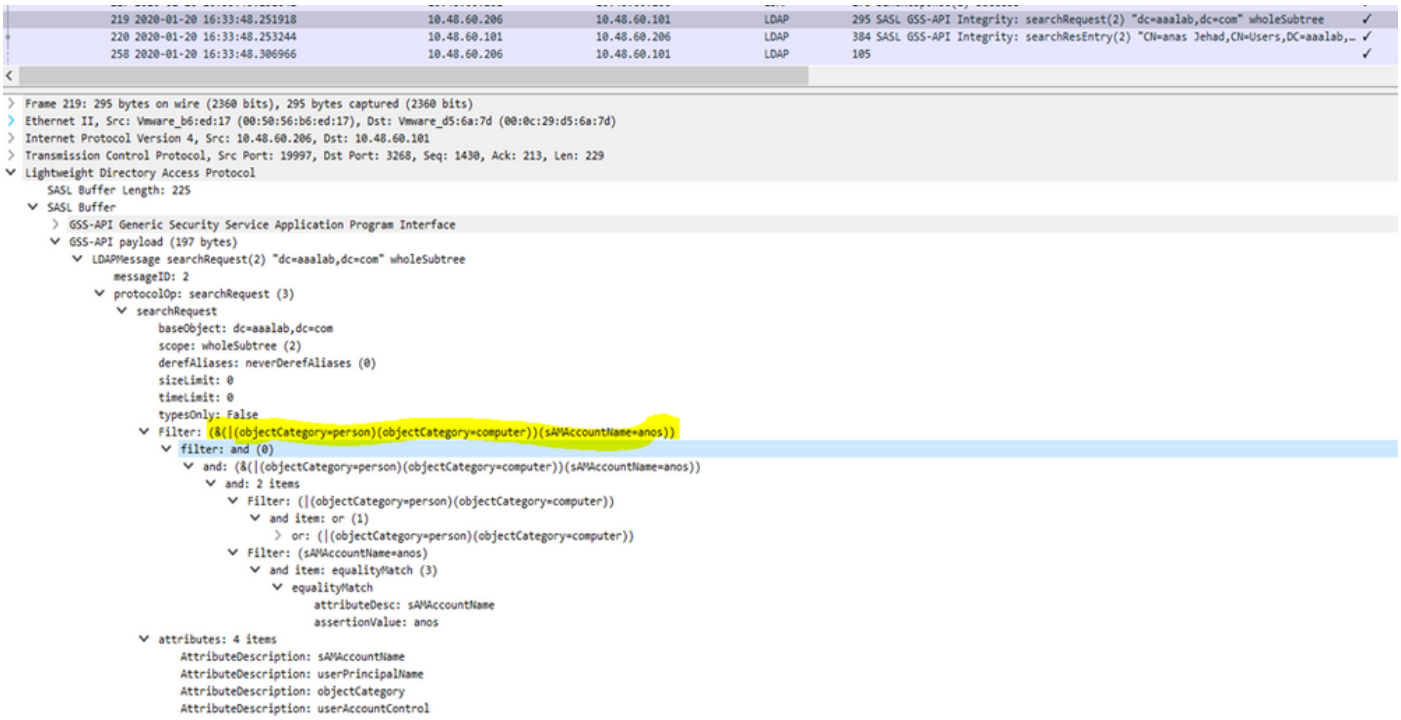
검색 필터의 예:

1. **SAM 검색:** ISE가 도메인 마크업 없이 사용자 이름으로만 ID를 수신하는 경우 ISE는 이 사용자 이름을 SAM으로 취급하고 AD에서 해당 ID를 SAM 이름으로 사용하는 모든 시스템 사용자 또는 시스템을 검색합니다.

SAM 이름이 고유하지 않은 경우 ISE는 비밀번호를 사용하여 사용자를 구분하고 ISE는 EAP-TLS와 같은 비밀번호가 없는 프로토콜을 사용하도록 구성됩니다.

올바른 사용자를 찾을 수 있는 다른 기준이 없으므로 ISE는 "모호한 ID" 오류와 함께 인증에 실패합니다.

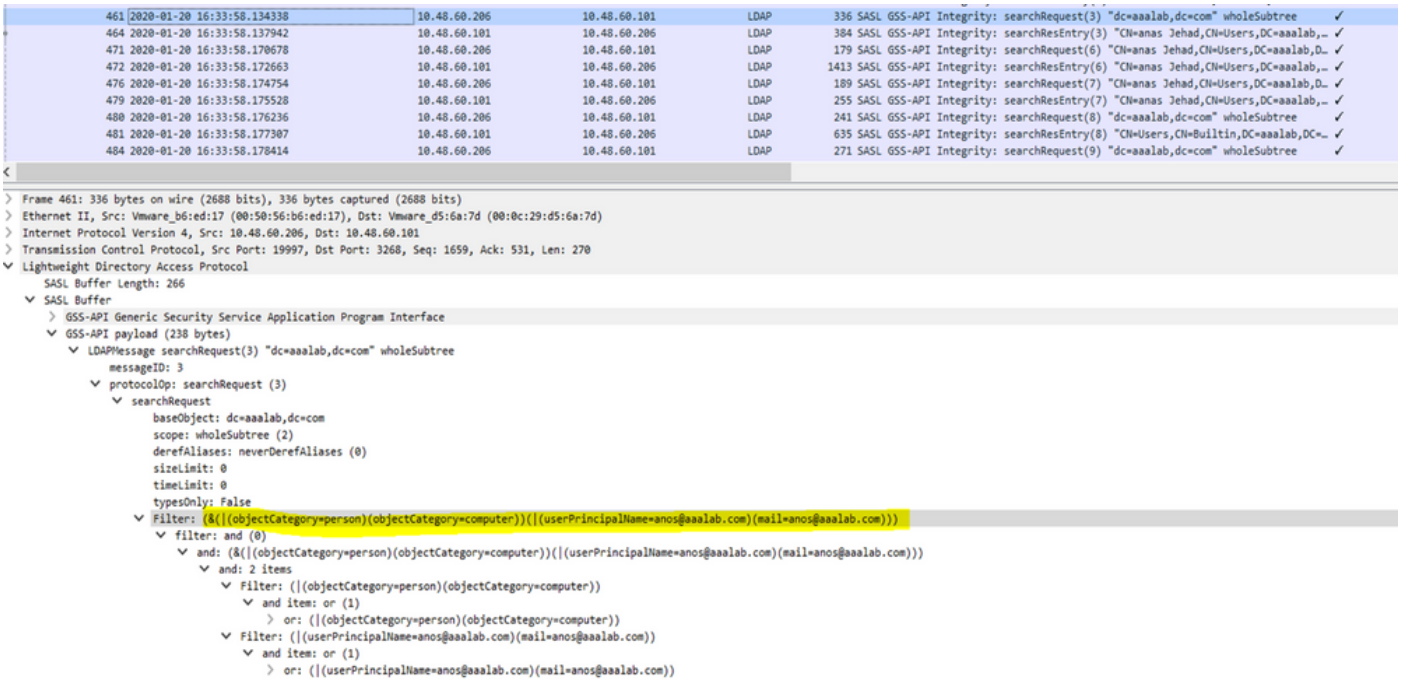
그러나 사용자 인증서가 Active Directory에 있는 경우 Cisco ISE는 이진 비교를 사용하여 ID를 확인합니다.



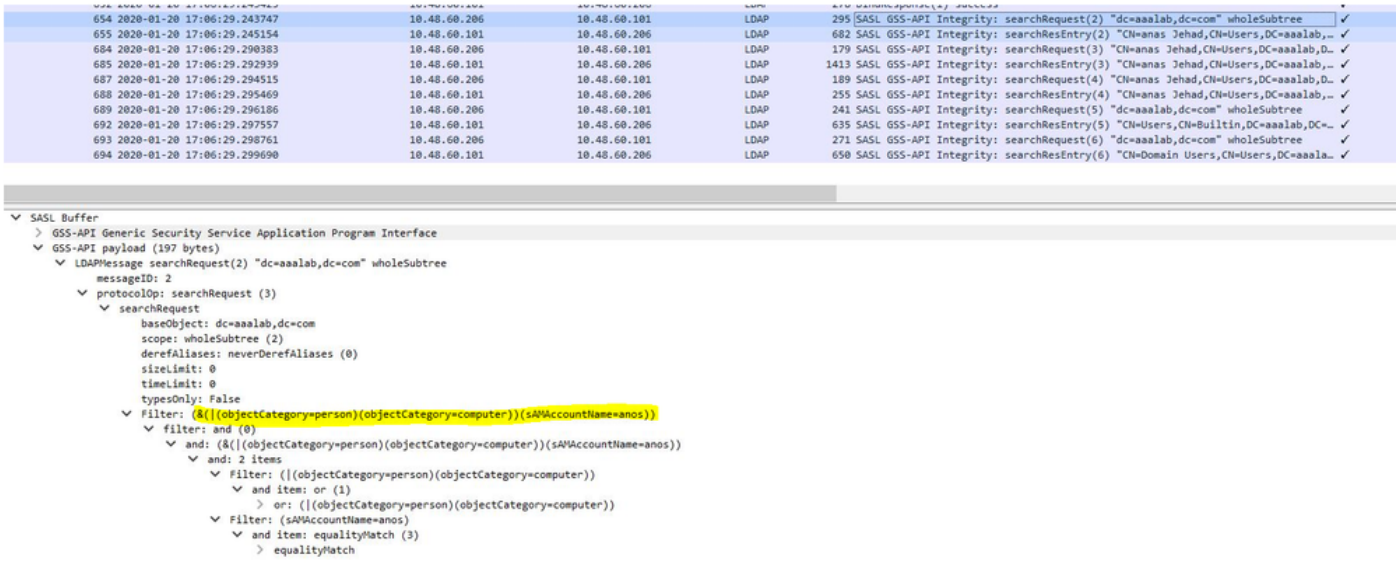
2. **UPN 또는 메일 검색:** ISE에서 ID를 username@domain으로 수신하는 경우 ISE는 각 포리스트 글로벌 카탈로그에서 해당 UPN ID 또는 메일 ID "identity=matched UPN or email"과 일치하는 항목을 검색합니다.

고유한 일치 항목이 있는 경우 Cisco ISE는 AAA 플로우를 진행합니다.

동일한 UPN과 비밀번호 또는 동일한 UPN과 메일을 사용하는 가입 포인트가 여러 개 있는 경우 Cisco ISE는 "모호한 ID" 오류와 함께 인증에 실패합니다.



3. **NetBIOS 검색:** ISE가 NetBIOS 도메인 접두사(예: CISCO\sajedah)를 가진 ID를 수신하면 ISE는 포리스트에서 NetBIOS 도메인을 검색합니다. 그런 다음 제공된 SAM 이름(이 예에서는 sajeda)을 찾습니다

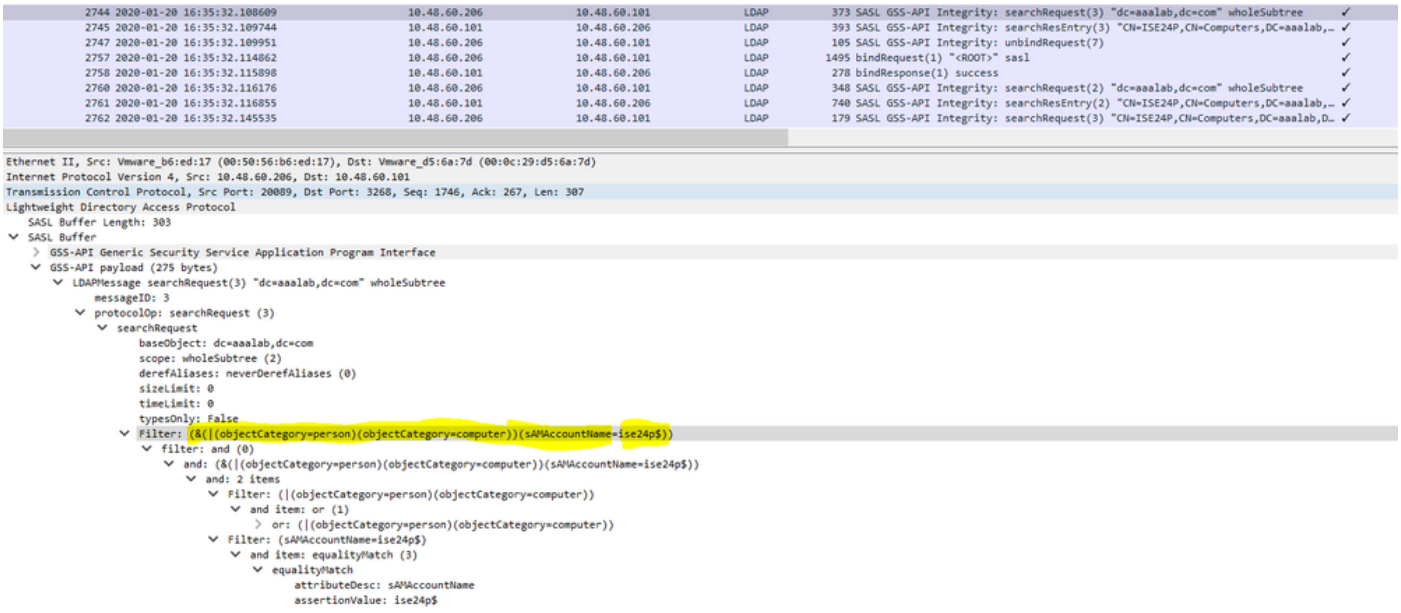


4. **장비 기반 검색:** ISE가 호스트/접두사 ID와 함께 머신 인증을 수신하면 ISE는 포리스트에서 일치하는 servicePrincipalName 특성을 검색합니다.

ID에 정규화된 도메인 접미사(예: host/machine.domain.com)가 지정된 경우 Cisco ISE는 해당 도메인이 존재하는 포리스트를 검색합니다.

ID가 호스트/머신 형식인 경우 Cisco ISE는 모든 포리스트에서 서비스 사용자 이름을 검색합니다.

일치하는 항목이 두 개 이상인 경우 Cisco ISE는 "모호한 ID" 오류와 함께 인증에 실패합니다.



참고: ISE ad-agent.log 파일에 동일한 필터가 표시됨

참고: ISE 2.2 패치 4 및 이전 및 2.3 패치 1 및 이전 사용자는 SAM, CN 또는 둘 다 특성을 가지고 있습니다. Cisco ISE, 릴리스 2.2 패치 5 이상 및 2.3 패치 2 이상에서는 sAMAccountName 특성만 기본 특성으로 사용합니다.

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.