보안 클라이언트 VPN을 위해 ASA에서 LDAP 특성 매핑 구성

목차

- 소개
  - 요구 사항
    - Cisco ASA 요구 사항
    - 네트워크 요구 사항
    - 클라이언트 요구 사항
  - 사용되는 구성 요소
- 컨피그레이션 단계
  - 1단계. 그룹 정책 정의
  - 2단계. LDAP 특성 맵 구성
  - 3단계. LDAP AAA 서버 구성
  - 4단계. 터널 그룹 정의
- 다음을 확인합니다.
  - VPN 세션 할당 확인
- 문제 해결
  - LDAP 디버깅 활성화
  - VPN 연결 시작
  - 디버그 출력 검토
  - 확인 후 디버깅 사용 안 함
  - 일반적인 문제

소개

이 문서에서는 Active Directory 그룹을 기반으로 VPN 그룹 정책을 할당하도록 Cisco ASA에서 LDAP 특성 매핑을 구성하는 방법에 대해 설명합니다.

요구 사항

Cisco ASA 요구 사항

- 지원되는 소프트웨어 버전을 실행하는 Cisco ASA.
- ASA 디바이스에 대한 관리 액세스.

네트워크 요구 사항

- ASA에 액세스할 수 있는 AD(Active Directory) 도메인.
- AD 서버에 구성된 LDAP over SSL(LDAPS)(기본 포트 636).

클라이언트 요구 사항

- 클라이언트 장치에 설치된 보안 클라이언트.

사용되는 구성 요소

이 문서의 정보는 특정 소프트웨어 및 하드웨어 버전으로 제한되지 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.

컨피그레이션 단계

1단계. 그룹 정책 정의

그룹 정책은 VPN 사용자의 권한 및 제한을 결정합니다. 조직의 액세스 요구 사항에 맞는 필요한 그룹 정책을 생성합니다.

인증된 사용자에 대한 그룹 정책 생성

```
group-policy VPN_User_Policy internal
group-policy VPN_User_Policy attributes
  vpn-simultaneous-logins 3
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value SPLIT_TUNNEL_ACL
```

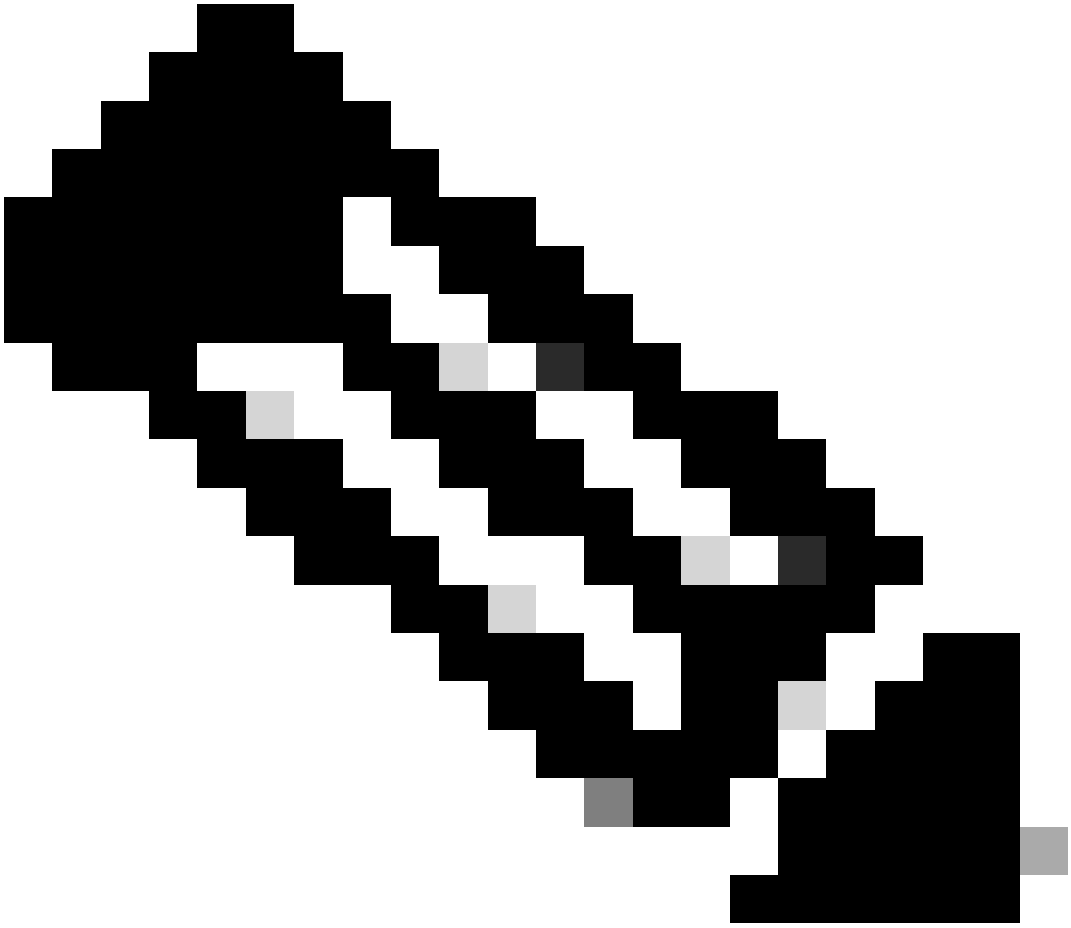
액세스를 거부할 기본 그룹 정책을 생성합니다.

```
group-policy No_Access_Policy internal
group-policy No_Access_Policy attributes
  vpn-simultaneous-logins 0
```

2단계. LDAP 특성 맵 구성

특성 맵은 LDAP 특성을 ASA 특성으로 변환하므로 ASA는 LDAP 그룹 멤버십을 기반으로 올바른 그룹 정책에 사용자를 할당할 수 있습니다.

```
ldap attribute-map VPN_Access_Map
  map-name  memberOf Group-Policy
  map-value memberOf "CN=VPN_Users,OU=Groups,DC=example,DC=com" VPN_User_Policy
```



참고: LDAP 그룹의 DN(Distinguished Name)은 항상 큰따옴표("")로 묶어야 합니다. 이렇게 하면 ASA에서 DN의 공백과 특수 문자를 올바르게 해석합니다.

3단계. LDAP AAA 서버 구성

인증 및 그룹 매핑을 위해 AD 서버와 통신하도록 ASA를 설정합니다.

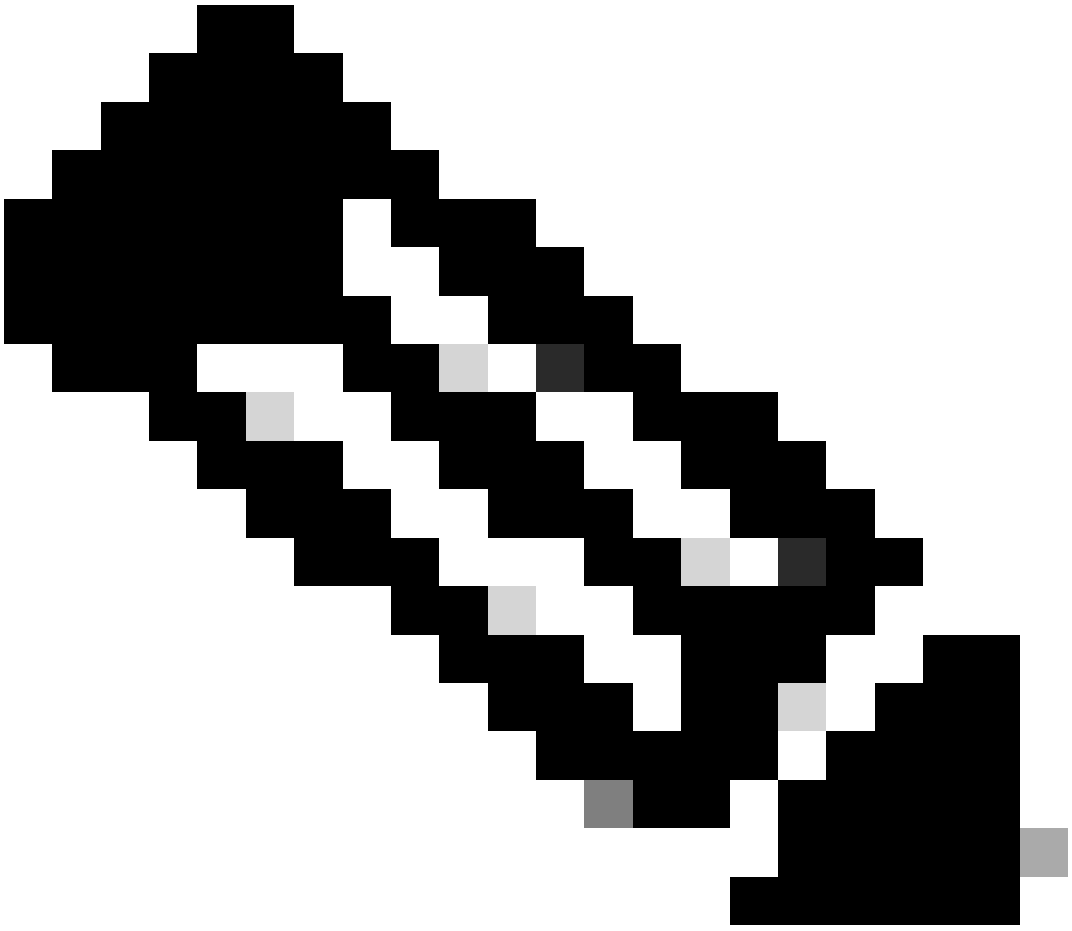
```
aaa-server AD_LDAP_Server protocol ldap
aaa-server AD_LDAP_Server (inside) host 192.168.1.10
  ldap-base-dn dc=example,dc=com
  ldap-scope subtree
  ldap-naming-attribute sAMAccountName
  ldap-login-password ********
  ldap-login-dn CN=ldap_bind_user,OU=Service Accounts,DC=example,DC=com
  ldap-over-ssl enable
  ldap-attribute-map VPN_Access_Map
```

4단계. 터널 그룹 정의

터널 그룹은 VPN 매개변수를 정의하고 LDAP 서버에 인증을 연결합니다.

```
tunnel-group VPN_Tunnel type remote-access
tunnel-group VPN_Tunnel general-attributes
  address-pool VPN_Pool
  authentication-server-group AD_LDAP_Server
  default-group-policy No_Access_Policy

tunnel-group VPN_Tunnel webvpn-attributes
  group-alias VPN_Tunnel enable
```



참고: default-group-policy는 No_Access_Policy로 설정되어 LDAP 특성 맵 기준과 일치하지 않는 사용자에 대한 액세스를 거부합니다.

다음을 확인합니다.

설치를 완료한 후 사용자가 올바르게 인증되고 적절한 그룹 정책이 할당되었는지 확인합니다.

VPN 세션 할당 확인

```
show vpn-sessiondb anyconnect filter name
```

<username>을(를) 실제 테스트 계정으로 교체합니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결합니다.

LDAP 디버깅 활성화

사용자가 필요한 그룹 정책을 받지 못하는 경우 디버깅을 활성화하여 문제를 식별합니다.

```
debug ldap 255
debug aaa common 255
debug aaa shim 255
```

VPN 연결 시작

테스트 사용자가 Cisco Secure Client를 사용하여 연결을 시도하도록 합니다.

디버그 출력 검토

Cisco ASA 로그를 확인하여 사용자가 AD(Active Directory) 그룹 멤버십을 기반으로 올바른 그룹 정책에 매핑되었는지 확인합니다.

확인 후 디버깅 사용 안 함

```
undebug all
```

일반적인 문제

LDAP 특성 매핑은 대/소문자를 구분합니다. map-value 문의 AD 그룹 이름이 대/소문자를 포함하여 정확하게 일치하는지 확인합니다.

사용자가 지정된 AD 그룹의 직접 구성원인지 확인합니다. 중첩된 그룹 멤버 자격이 항상 인식되지 않으므로 권한 부여 문제가 발생합니다.

맵 값 기준과 일치하지 않는 사용자는 default-group-policy(이 경우 No_Access_Policy)를 수신하므로 액세스가 차단됩니다.

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.