UCS Manager와 작동하도록 Duo Multi Factor Authentication 구성

목차

소개

이 문서에서는 UCS Manager를 사용하여 Cisco Duo MFA(Multi-Factor Authentication)를 구현하는 컨피그레이션 및 모범 사례에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- UCS 관리자
- Cisco Duo

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.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

Cisco UCS Manager는 원격 사용자 로그인에 2단계 인증을 사용합니다.2단계 인증 로그인은 비밀번호 필드에 사용자 이름, 토큰 및 비밀번호 조합이 필요합니다.

2단계 인증은 RADIUS(Remote Authentication Dial-In User Service) 또는 Terminal Access Controller Access Control System +(TACACS+) 공급자 그룹을 사용할 때 지원되며 해당 도메인에 대해 2단계 인증을 가진 지정된 인증 도메인이 있는 공급자 그룹이 지원됩니다.2단계 인증은 IPM(Internetwork Performance Monitor)을 지원하지 않으며 인증 영역이 LDS(Lightweight Directory Access Protocol)로 설정된 경우 지원되지 않습니다.
(LDAP), 로컬 또는 없음

Duo 구현을 통해 Multi-Factor Authentication은 RADIUS 또는 LDAP를 통해 로컬 디바이스 및 애플리케이션에서 인증 요청을 수신하는 온프레미스 소프트웨어 서비스인 Duo 인증 프록시를 통해 수행되며, 선택적으로 LDAP 디렉토리 또는 RADIUS 인증 서버에 대해 기본 인증을 수행한 다음 Duo에 연결하여 보조 인증을 수행합니다.사용자가 Duo Mobile에서 푸시 알림으로 수신되거나 전화 통화 등으로 수신되는 2단계 요청을 승인하면 Duo 프록시는 인증을 요청한 디바이스 또는 애플리케이션에 액세스 승인을 반환합니다.

구성

이 컨피그레이션에서는 LDAP 및 Radius를 통해 UCS Manager를 통한 성공적인 Duo 구현에 대한 요구 사항을 다룹니다.

> **참고:**기본 Duo 인증 프록시 컨피그레이션은 Duo Proxy 지침: Duo Proxy Document를 확인하십시오.

LDAP 통합

UCS 관리자

UCS **Manager(UCS 관리자) > Admin Section(관리 섹션) > User Management(사용자 관리) > LDAP**로 이동하고 **LDAP Providers SSL(LDAP 제공자 SSL)**을 활성화하면 LDAP 데이터베이스와의 통신에 암호화가 필요합니다.LDAP는 STARTTLS를 사용합니다.이를 통해 사용 포트 389에 의한 암호화된 통신이 가능합니다. Cisco UCS는 SSL을 위해 포트 636에서 TLS(Transport Layer Security) 세션을 협상하지만 초기 연결은 포트 389에서 암호화되지 않습니다.

Bind DN: Full DN path, it must be the same DN that is entered in the Duo Authentication Proxy for exempt_ou_1= below
Base DN: Specify DN path
Port: 389 or whatever your preference is for STARTTLS traffic.
Timeout: 60 seconds
Vendor: MS AD

> **참고:**STARTTLS는 표준 LDAP 포트에서 작동하므로 LDAPS와 달리 STARTTLS 통합에서는 **Duo 인증 프록시에서 ssl_port=** 필드가 아닌 **port=** 필드를 사용합니다.

Duo 인증 프록시

```
[ldap_server_auto]
ikey=
skey_protected= ==
api_host=api.XXXXXX.duosecurity.com
client=ad_client1
failmode=secure
port=389 or the port of your LDAP or STARTTLS traffic.
ssl_port=636 or the port of your LDAPS traffic.
allow_unlimited_binds=true
exempt_primary_bind=false
ssl_key_path=YOURPRIVATE.key
ssl_cert_path=YOURCERT.pem
exempt_primary_bind=false
exempt_ou_1=full DN path
```

RADIUS 통합

UCS 관리자

UCS Manager(UCS 관리자) > Admin(관리) > User Management(사용자 관리) > Radius(RADIUS)로 이동하고 Radius Providers(RADIUS 제공자)를 클릭합니다.

Key and Authorization Port: Must match the Radius/ Authentication Proxy configuration.
Timeout: 60 seconds
Retries: 3

Duo 인증 프록시

```
[radius_server_auto]
ikey=DIXXXXXXXXXXXXXXXXX
skey=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
api_host=api-XXXXXXXX.duosecurity.com
radius_ip_1=5.6.7.8
radius_secret_1=radiussecret1
client=ad_client
port=18121
failmode=safe
```

Duo 인증 프록시를 설치 및 구성하는 모범 사례

방화벽 내부 네트워크에 다음과 같은 인증 프록시를 구축합니다.

- TCP/443에서 인증 프록시에서 일반 인터넷으로 아웃바운드 통신을 허용합니다. 추가 제한이 필요한 경우 Duo의 허용 목록에 대한 IP 범위 목록을 참조하십시오.
- CONNECT 프로토콜을 지원하는 이전에 구성된 웹 프록시를 통해 Duo의 서비스에 연결하도록 Duo 인증 프록시를 구성할 수도 있습니다.
- 일반적으로 TCP/636, TCP/389 또는 UDP/1812를 통해 적절한 IDP에 연결할 수 있습니다.
- 적절한 RADIUS, LDAP 또는 LDAPS 포트에서 프록시에 대한 통신을 허용합니다.이러한 규칙을 사용하면 어플라이언스/애플리케이션에서 프록시에 대해 사용자를 인증할 수 있습니다.

- 환경에 SSL 검사 어플라이언스가 있는 경우 인증 프록시 IP에 대한 List SSL 검사를 비활성화/허용합니다.

- 고유한 포트에서 수신 대기할 각 **[radius_server_METHOD(X)]** 및 **[ldap_server_auto(X)]** 섹션을 구성합니다.
  Duo Authentication Proxy를 사용하여 여러 응용 프로그램의 전원을 켜는 방법을 여러 응용 프로그램용 Duo 사이트 Duo Proxy에 자세히 알아보십시오.

- 모든 어플라이언스에 고유한 RADIUS 암호 및 비밀번호를 사용합니다.

- 프록시 컨피그레이션 파일에서 보호/암호화된 비밀번호를 사용합니다.

- 인증 프록시는 다른 서비스와 함께 다목적 서버에 공존할 수 있지만 전용 서버를 사용하는 것이 좋습니다.

- 인증 프록시가 신뢰할 수 있는 NTP 서버를 가리키도록 하여 정확한 날짜와 시간을 보장합니다.

- 인증 프록시를 업그레이드하기 전에 항상 구성 파일의 백업 복사본을 만듭니다.
- Windows 기반 인증 프록시 서버의 경우 전원 또는 네트워크 장애 시 일부 복구 옵션을 포함하도록 Duo 보안 인증 프록시 서비스를 구성합니다.

  1단계. 서버의 **서비스**에서 **Duo 보안 인증 프록시** 서비스를 마우스 오른쪽 단추로 클릭한 다음 기본 설정을 **클릭합니다.**
  2단계. **Recovery(복구)**를 클릭한 다음 실패 후 서비스를 다시 시작하는 옵션을 구성합니다.

- Linux 기반 인증 프록시 서버의 경우 초기화 스크립트를 생성할지 묻는 메시지가 표시되면 **예**를 클릭합니다.그런 다음 인증 프록시를 시작할 때 sudo **service duoauthproxy start**와 같은 명령을 사용하여 init 스크립트에 대한 명령이 현재 시스템에 따라 다를 수 있습니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 구성에 대해 사용 가능한 특정 문제 해결 정보가 없습니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems