Configuratie van duo Multi Factor Verificatie om met UCS Manager te werken

Inhoud

Inleiding

Dit document beschrijft de configuratie en de beste werkwijzen om Cisco Duo Multi-Factor Verificatie (MFA) met UCS Manager te implementeren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- UCS Manager
- Cisco Duo

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Cisco UCS Manager maakt gebruik van bidirectionele verificatie voor externe gebruikershandleidingen. Voor de inlognaam van de twee-factor authenticatie is een gebruikersnaam, een token en een wachtwoordcombinatie nodig in het veld Wachtwoord.

Verificatie met twee factoren wordt ondersteund wanneer u groepen van leveranciers met TACACS+ (Terminal Access Control System) of met twee-factor verificatie voor deze domeinen gebruik maakt van een inbel-gebruikersservice (RADIUS) of een terminale toegangscontrolelijst voor TACACS+). Tweeledige verificatie ondersteunt Internetwork Performance Monitor (IPM) niet en wordt niet ondersteund wanneer het verificatiegebied is ingesteld op Lichtgewicht Directory Access Protocol
(LDAP), lokaal of geen.

Met de Duo-implementatie wordt de Multifactor-verificatie uitgevoerd via de Duo-verificatieproxy, een softwaredienst die op het bedrijf een verificatieaanvraag van uw lokale apparaten en toepassingen via RADIUS of LDAP ontvangt, die optioneel een primaire verificatie uitvoert aan de hand van uw LDAP-directory of RADIUS-verificatieserver en vervolgens contact opneemt met Duo om secundaire verificatie uit te voeren. Zodra de gebruiker het twee-factor-verzoek goedkeurt, dat ontvangen wordt als een drukknop van Duo Mobile, of als een telefoongesprek, enz., geeft de Duo-proxy de toegangsgoedkeuring terug aan het apparaat of de applicatie die om verificatie heeft verzocht.

Configureren

Deze configuratie betreft de vereisten voor een succesvolle implementatie van de Duo met UCS Manager via LDAP en Radius.

> **Opmerking:** Controleer voor de configuratie van de Duo-verificatieproxy de Duo Proxy-richtlijnen: Duo Proxy-document

LDAP-integratie

UCS Manager

Navigeren naar **UCS Manager > Admin Section > User Management > LDAP** en **LDAP Providers SSL** inschakelen, dit betekent dat encryptie vereist is voor communicatie met de LDAP-database. LDAP gebruikt STARTTLS. Dit staat gecodeerde communicatie door de gebruikpoort 389 toe. Cisco UCS bespreekt een (TLS) sessie van de Vervoerlaag Beveiliging op poort 636 voor SSL, maar de eerste verbinding begint niet versleuteld op poort 389.

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

Opmerking: STARTTLS werkt op een standaard LDAP poort, dus in tegenstelling tot LDAPS gebruiken STARTTLS-integraties het veld **port= ssl_port=** veld op de Duo Verificatieproxy.

Op de Duo-verificatieproxy

```
[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
```

Straalintegratie

UCS Manager

Navigatie naar **UCS Manager > Admin > User Management > Radius** en klik op **Radius Providers:**

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

Duo-verificatieproxy

```
[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
```

Beste praktijken om de dubbele verificatieproxy te installeren en configureren

Hiermee implementeert u de verificatieproxy in een firewallnetwerk dat:

- Hiermee kan uitgaande communicatie van de verificatieproxy naar het algemene internet op TCP/443 worden gegenereerd. Als verdere beperkingen vereist zijn, raadpleegt u de lijst van IP-bereik van Duo in de toegestane lijst.
- De proxy voor Duo-verificatie kan ook worden geconfigureerd om de service van Duo te bereiken via een eerder geconfigureerd webproxy die het CONNECT-protocol ondersteunt.
- Kan verbinding maken met de juiste IDP's, doorgaans via TCP/636, TCP/389 of UDP/1812

- Maakt communicatie naar de proxy mogelijk via de juiste RADIUS-, LDAP- of LDAPS-poorten. Deze regels maken het mogelijk apparaten/toepassingen te certificeren tegen de handlangers.

- Als er SSL-inspectietoestellen in de omgeving aanwezig zijn, schakelt u een SSL-inspectie van de Lijst voor Auth Proxy-IP's in.

- Configureer elke **[straal_server_METHOD(X)]** en **[ldap_server_auto(X)]** secties om op een unieke poort te luisteren.
  Lees meer over hoe u de Duo-verificatieproxy kunt gebruiken om meerdere toepassingen op de Duo-site Duo Proxy voor meerdere toepassingen aan te zetten.

- Gebruik unieke RADIUS-geheimen en wachtwoorden voor elk apparaat.

- Gebruik beschermde/gecodeerde wachtwoorden in het configuratiebestand.

- Hoewel de Verificatieproxy kan bestaan op multifunctionele servers met andere services, wordt aanbevolen een speciale server(s) te gebruiken.

- Verzeker de Verificatieproxy punten naar een betrouwbare NTP-server om een nauwkeurige datum en tijd te garanderen.

- Maak altijd een reservekopie van het configuratiebestand voor de upgrade van de verificatieproxy.
- Voor Windows-gebaseerde verificatieproxy-servers moet u de Duo Security Verificatieproxy-service configureren om een aantal herstelopties op te nemen in geval van stroom of netwerkfouten:

  Stap 1. Klik binnen **de services** op uw server met de rechtermuisknop op de **Duo Security Verificatieproxy** en klik vervolgens op **Voorkeuren.**
  Stap 2. Klik op **Herstel** en vervolgens op de opties om de service na een defect te hervatten.

- Voor Linux-gebaseerde Verificatieproxy-servers klikt u op **ja** voor de melding die zichtbaar is op de installatie die vraagt of u een ingebouwde script wilt maken. Wanneer u de Verificatieproxy start, gebruik dan een opdracht zoals **sudo-service bij** aanloop, dat de opdracht voor het initscript kan verschillen op basis van het gebruikte systeem.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke informatie over probleemoplossing beschikbaar voor deze configuratie.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems