Configurazione di Duo Multi Factor Authentication per l'utilizzo di UCS Manager

Sommario

Introduzione

In questo documento vengono descritte la configurazione e le best practice per implementare Cisco Duo Multi-Factor Authentication (MFA) con UCS Manager.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- UCS Manager
- Cisco Duo

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Cisco UCS Manager utilizza l'autenticazione a due fattori per gli accessi degli utenti remoti. L'accesso con autenticazione a due fattori richiede una combinazione di nome utente, token e password nel campo della password.

L'autenticazione a due fattori è supportata quando si utilizzano i gruppi di provider RADIUS (Remote Authentication Dial-In User Service) o TACACS+ (Terminal Access Controller Access Control System) con domini di autenticazione designati con autenticazione a due fattori per tali domini. L'autenticazione a due fattori non supporta IPM (Internetwork Performance Monitor) e non è supportata quando il realm di autenticazione è impostato su Lightweight Directory Access Protocol
(LDAP), locale o nessuna.

Con l'implementazione Duo, Multi-Factor Authentication viene eseguito tramite Duo Authentication Proxy, un servizio software locale che riceve richieste di autenticazione dai dispositivi e dalle applicazioni locali tramite RADIUS o LDAP, esegue facoltativamente l'autenticazione primaria sulla directory LDAP o sul server di autenticazione RADIUS e quindi contatta Duo per eseguire l'autenticazione secondaria. Una volta che l'utente approva la richiesta a due fattori, che viene ricevuta come notifica push da Duo Mobile, o come chiamata telefonica, ecc, il proxy Duo restituisce l'approvazione di accesso al dispositivo o all'applicazione che ha richiesto l'autenticazione.

Configurazione

Questa configurazione soddisfa i requisiti per la corretta implementazione di Duo con UCS Manager tramite LDAP e Radius.

> **Nota:** Per la configurazione di base del proxy di autenticazione Duo, consultare le linee guida Duo Proxy: Duo Proxy Document

Integrazione LDAP

UCS Manager

Selezionare **UCS Manager > Admin Section > User Management > LDAP** e abilitare **LDAP Providers SSL**. Ciò significa che la crittografia è necessaria per le comunicazioni con il database LDAP. LDAP utilizza STARTTLS. Ciò consente la comunicazione crittografata tramite la porta utente 389. Cisco UCS negozia una sessione TLS (Transport Layer Security) sulla porta 636 per SSL, ma la connessione iniziale viene avviata senza crittografia sulla porta 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

Nota: STARTTLS funziona su una porta LDAP standard, quindi a differenza di LDAPS, le integrazioni STARTTLS utilizzano il campo **port=** e non **ssl_port=** sul proxy di autenticazione Duo.

Sul proxy di autenticazione Duo

```
[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
```

Integrazione Radius

UCS Manager

Selezionare **UCS Manager > Admin > User Management > Radius** e fare clic su **Radius Providers:**

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

Duo Authentication Proxy

```
[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
```

Procedure ottimali per l'installazione e la configurazione del proxy di autenticazione Duo

Distribuire il proxy di autenticazione in una rete interna firewall che:

- Consente le comunicazioni in uscita dal proxy di autenticazione verso Internet su TCP/443. Se sono necessarie ulteriori restrizioni, vedere Duo's List of IP ranges to Allowed List.
- Il proxy di autenticazione Duo può anche essere configurato per raggiungere il servizio di Duo tramite un proxy Web precedentemente configurato che supporta il protocollo CONNECT.

- Possibilità di connessione agli IDP appropriati, in genere su TCP/636, TCP/389 o UDP/1812
- Consente la comunicazione con il proxy sulle porte RADIUS, LDAP o LDAPS appropriate. Queste regole consentono ad appliance/applicazioni di autenticare gli utenti in base ai proxy.
- Se nell'ambiente sono presenti appliance di ispezione SSL, disabilitare/consentire l'ispezione SSL dell'elenco per gli IP proxy di autenticazione.
- Configurare ciascuna sezione **[radius_server_METHOD(X)]** e **[ldap_server_auto(X)]** per l'ascolto su una porta univoca.
  Ulteriori informazioni su come utilizzare il proxy di autenticazione Duo per alimentare più applicazioni sul sito Duo Duo Proxy per più applicazioni.
- Per ogni accessorio utilizzare password e segreti RADIUS univoci.
- Utilizzare password protette/crittografate nel file di configurazione del proxy.
- Sebbene il proxy di autenticazione possa coesistere su server multifunzione con altri servizi, è consigliabile utilizzare server dedicati.
- Accertarsi che il proxy di autenticazione punti a un server NTP affidabile per garantire l'accuratezza di data e ora.
- Prima dell'aggiornamento del proxy di autenticazione, creare sempre una copia di backup del file di configurazione.
- Per i server proxy di autenticazione basati su Windows, configurare il servizio Duo Security Authentication Proxy in modo che includa alcune opzioni di ripristino in caso di interruzione dell'alimentazione o di errori di rete:

  Passaggio 1. All'interno di **Servizi** sul server, fare clic con il pulsante destro del mouse sul servizio **Duo Security Authentication Proxy** e quindi scegliere **Preferenze.**

  Passaggio 2. Fare clic su **Ripristino**, quindi configurare le opzioni per riavviare il servizio dopo gli errori.
- Per i server proxy di autenticazione basati su Linux, fare clic su **sì** al prompt visualizzato nell'installazione in cui viene richiesto se si desidera creare uno script di inizializzazione. Quindi, quando si avvia il proxy di autenticazione, utilizzare un comando quale **sudo service duoauthproxy start**, in modo che il comando per lo script init possa differire in base al sistema in cui ci si trova.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche per la risoluzione dei problemi per questa configurazione.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems