Configurer l'authentification multifacteur Duo pour fonctionner avec UCS Manager

Contenu

Introduction

Ce document décrit la configuration et les meilleures pratiques pour mettre en oeuvre Cisco Duo Multi-Factor Authentication (MFA) avec UCS Manager.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- UCS Manager
- Cisco Duo

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Cisco UCS Manager utilise une authentification à deux facteurs pour les connexions utilisateur distantes. La connexion d'authentification à deux facteurs nécessite un nom d'utilisateur, un jeton et une combinaison de mot de passe dans le champ de mot de passe.

L'authentification à deux facteurs est prise en charge lorsque vous utilisez les groupes de fournisseurs RADIUS (Remote Authentication Dial-In User Service) ou TACACS+ (Terminal Access Controller Access Control System) avec des domaines d'authentification désignés avec authentification à deux facteurs pour ces domaines. L'authentification à deux facteurs ne prend pas en charge l'IPM (Internetwork Performance Monitor) et n'est pas prise en charge lorsque le domaine d'authentification est défini sur Lightweight Directory Access Protocol (LDAP), local ou aucun.

Avec la mise en oeuvre de Duo, l'authentification multifacteur est effectuée via le proxy d'authentification Duo, qui est un service logiciel local qui reçoit des demandes d'authentification de vos périphériques et applications locaux via RADIUS ou LDAP, effectue éventuellement une authentification primaire sur votre répertoire LDAP ou votre serveur d'authentification RADIUS, puis contacte Duo pour effectuer une authentification secondaire. Une fois que l'utilisateur a approuvé la demande à deux facteurs, qui est reçue en tant que notification push de Duo Mobile, ou en tant qu'appel téléphonique, etc., le proxy Duo retourne l'approbation d'accès au périphérique ou à l'application qui a demandé l'authentification.

Configuration

Cette configuration couvre les exigences d'une mise en oeuvre Duo réussie avec UCS Manager via LDAP et Radius.

> **Note**: Pour la configuration de base du proxy d'authentification Duo, consultez les directives du proxy Duo : Document du proxy Duo

Intégration LDAP

UCS Manager

Accédez à **UCS Manager > Admin Section > User Management > LDAP** et activez **LDAP Providers SSL**, ce qui signifie que le chiffrement est requis pour les communications avec la base de données LDAP. LDAP utilise STARTTLS. Cela permet la communication cryptée par le port d'utilisation 389. Cisco UCS négocie une session TLS (Transport Layer Security) sur le port 636 pour SSL, mais la connexion initiale démarre non chiffrée sur le port 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

Note: STARTTLS fonctionne sur un port LDAP standard, donc contrairement à LDAPS, les intégrations STARTTLS utilisent le champ **port=** non **ssl_port=** sur le proxy d'authentification Duo.

Sur le proxy d'authentification 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
```

Intégration Radius

UCS Manager

Accédez à **UCS Manager > Admin > User Management > Radius** et cliquez sur **Radius Providers :**

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

Proxy d'authentification Duo

```
[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
```

Méthodes Recommandées pour installer et configurer le proxy d'authentification Duo

Déployer le proxy d'authentification dans un réseau interne pare-feu qui :

- Permet la communication sortante du proxy d'authentification vers Internet général sur TCP/443. Si d'autres restrictions sont nécessaires, veuillez consulter la liste des plages d'adresses IP à la liste autorisée de Duo.
- Le proxy d'authentification Duo peut également être configuré pour atteindre le service Duo via un proxy Web précédemment configuré qui prend en charge le protocole CONNECT.

- Peut se connecter aux personnes déplacées appropriées, généralement via TCP/636, TCP/389 ou UDP/1812

- Permet la communication au proxy sur les ports RADIUS, LDAP ou LDAPS appropriés. Ces règles permettent aux appliances/applications d'authentifier les utilisateurs par rapport aux serveurs proxy.

- Si des appliances d'inspection SSL existent dans l'environnement, désactivez/autorisez l'inspection SSL de liste pour les adresses IP du proxy d'authentification.

- Configurez chaque section **[radius_server_Method(X)]** et **[ldap_server_auto(X)]** pour écouter sur un port unique.
  Pour en savoir plus sur l'utilisation du proxy d'authentification Duo pour alimenter plusieurs applications sur le site Duo [Duo Proxy for Multiple Applications.]

- Utilisez des mots de passe et des secrets RADIUS uniques pour chaque appliance.

- Utilisez des mots de passe protégés/chiffrés dans le fichier de configuration du proxy.

- Bien que le proxy d'authentification puisse coexister sur des serveurs polyvalents avec d'autres services, il est recommandé d'utiliser un ou plusieurs serveurs dédiés.

- Assurez-vous que le proxy d'authentification pointe vers un serveur NTP fiable pour garantir une date et une heure précises.

- Avant la mise à niveau du proxy d'authentification, effectuez toujours une copie de sauvegarde du fichier de configuration.
- Pour les serveurs proxy d'authentification Windows, configurez le service proxy d'authentification de sécurité Duo pour inclure certaines options de récupération en cas de panne d'alimentation ou de réseau :

  Étape 1. Dans **Services** sur votre serveur, cliquez avec le bouton droit sur le service **Duo Security Authentication Proxy**, puis cliquez sur **Préférences.**
  Étape 2. Cliquez sur **Récupération**, puis configurez les options pour redémarrer le service après les échecs.

- Pour les serveurs proxy d'authentification basés sur Linux, cliquez sur **yes** à l'invite visible sur l'installation qui vous demande si vous voulez créer un script d'initialisation. Ensuite, lorsque vous démarrez le proxy d'authentification, utilisez une commande telle que **sudo service duoauthproxy start**, selon laquelle la commande du script init peut différer selon le système sur lequel vous vous trouvez.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Aucune information de dépannage spécifique n'est actuellement disponible pour cette configuration.

Informations connexes

- Support et documentation techniques - Cisco Systems