Konfigurieren der Duo Multi-Factor-Authentifizierung für die Arbeit mit UCS Manager

Inhalt

Einführung

Dieses Dokument beschreibt die Konfiguration und Best Practices für die Implementierung von Cisco Duo Multi-Factor Authentication (MFA) mit UCS Manager.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- UCS Manager
- Cisco Duo

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Cisco UCS Manager verwendet eine Zwei-Faktor-Authentifizierung für Remote-Benutzeranmeldungen. Für die Anmeldung bei der Zwei-Faktor-Authentifizierung sind ein Benutzername, ein Token und eine Kennwortkombination im Kennwortfeld erforderlich.

Die Zwei-Faktor-Authentifizierung wird unterstützt, wenn Sie die Anbietergruppen Remote Authentication Dial-In User Service (RADIUS) oder Terminal Access Controller Access Control System +(TACACS+) mit festgelegten Authentifizierungsdomänen mit Zwei-Faktor-Authentifizierung für diese Domänen verwenden. Die Zwei-Faktor-Authentifizierung unterstützt Internetwork Performance Monitor (IPM) nicht und wird nicht unterstützt, wenn der Authentifizierungsbereich auf Lightweight Directory Access Protocol festgelegt ist. (LDAP), lokal oder gar nicht.

Bei der Duo-Implementierung wird die Multi-Factor-Authentifizierung über den Duo Authentication Proxy durchgeführt. Hierbei handelt es sich um einen Software-Service vor Ort, der Authentifizierungsanforderungen von lokalen Geräten und Anwendungen über RADIUS oder LDAP empfängt, optional eine primäre Authentifizierung für das LDAP-Verzeichnis oder den RADIUS-Authentifizierungsserver durchführt und anschließend Kontakte Duo für die Durchführung einer sekundären Authentifizierung auswählt. Sobald der Benutzer die Zwei-Faktor-Anforderung genehmigt, die als Push-Benachrichtigung von Duo Mobile oder als Telefonanruf usw. empfangen wird, gibt der Duo-Proxy die Zugriffsgenehmigung für das Gerät oder die Anwendung zurück, die eine Authentifizierung angefordert hat.

Konfiguration

Diese Konfiguration deckt die Anforderungen für eine erfolgreiche Duo-Implementierung mit UCS Manager über LDAP und Radius ab.

> **Hinweis:** Eine grundlegende Duo Authentication Proxy-Konfiguration finden Sie in den Duo Proxy-Richtlinien: Duo Proxy-Dokument

LDAP-Integration

UCS Manager

Navigieren Sie zu **UCS Manager > Admin Section > User Management > LDAP,** und aktivieren Sie **LDAP Providers SSL**. Dies bedeutet, dass für die Kommunikation mit der LDAP-Datenbank eine Verschlüsselung erforderlich ist. LDAP verwendet STARTTLS. Dies ermöglicht die verschlüsselte Kommunikation über den Nutzungsport 389. Das Cisco UCS handelt eine Transport Layer Security (TLS)-Sitzung an Port 636 für SSL aus, die erste Verbindung beginnt jedoch unverschlüsselt an 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

> **Hinweis:** STARTTLS wird auf einem Standard-LDAP-Port ausgeführt. Anders als LDAPS verwenden STARTTLS-Integrationen das **port=-**Feld und nicht das **ssl_port=-**Feld im Duo Authentication Proxy.

Im Duo Authentication Proxy

```
[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-Integration

UCS Manager

Navigieren Sie zu **UCS Manager > Admin > User Management > Radius**, und klicken Sie auf **Radius Providers:**

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

Duo-Authentifizierungsproxy

```
[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
```

Best Practices für die Installation und Konfiguration von Duo Authentication Proxy

Bereitstellen des Authentifizierungsproxys in einem internen Firewall-Netzwerk, das:

- Ermöglicht die ausgehende Kommunikation vom Authentifizierungsproxy zum allgemeinen Internet über TCP/443. Falls weitere Einschränkungen erforderlich sind, lesen Sie bitte die Liste der IP-Bereiche von Duo auf die Liste der zulässigen IP-Bereiche.

- Der Duo Authentication Proxy kann auch so konfiguriert werden, dass er den Dienst von Duo über einen zuvor konfigurierten Webproxy erreicht, der das CONNECT-Protokoll unterstützt.

- Verbindung zu den entsprechenden IDPs möglich, in der Regel über TCP/636, TCP/389 oder UDP/1812

- Ermöglicht die Kommunikation mit dem Proxy über die entsprechenden RADIUS-, LDAP- oder LDAPS-Ports. Diese Regeln ermöglichen Appliances/Anwendungen die Authentifizierung von Benutzern gegenüber den Proxys.

- Wenn in der Umgebung SSL Inspection-Appliances vorhanden sind, deaktivieren/Zulassen von SSL-Listenprüfung für Auth Proxy-IPs.

- Konfigurieren Sie alle **[radius_server_METHOD(X)]** und **[ldap_server_auto(X)]** Abschnitte, um auf einem eindeutigen Port zuzugreifen.
  Lesen Sie mehr darüber, wie Sie mit dem Duo Authentication Proxy mehrere Anwendungen auf dem Duo Site Duo Proxy für mehrere Anwendungen betreiben können.

- Verwenden Sie eindeutige RADIUS-Geheimnisse und Kennwörter für jede Appliance.

- Verwenden Sie in der Proxy-Konfigurationsdatei geschützte/verschlüsselte Kennwörter.

- Der Authentifizierungsproxy kann zwar gleichzeitig auf Mehrzweck-Servern mit anderen Diensten vorhanden sein, es wird jedoch empfohlen, einen oder mehrere dedizierte Server zu verwenden.

- Stellen Sie sicher, dass der Authentifizierungsproxy auf einen zuverlässigen NTP-Server verweist, um sicherzustellen, dass Datum und Uhrzeit korrekt sind.

- Erstellen Sie vor dem Upgrade des Authentifizierungsproxys immer eine Sicherungskopie der Konfigurationsdatei.
- Konfigurieren Sie für Windows-basierte Authentifizierungs-Proxy-Server den Duo Security Authentication Proxy Service so, dass er bei Stromversorgungs- oder Netzwerkausfällen einige Wiederherstellungsoptionen enthält:

  Schritt 1: Klicken Sie im Bereich **Dienste** auf Ihrem Server mit der rechten Maustaste auf den **Duo Security Authentication Proxy**-Dienst, und klicken Sie dann auf **Voreinstellungen.**
  Schritt 2: Klicken Sie auf **Wiederherstellung**, und konfigurieren Sie dann Optionen, um den Dienst nach Fehlern neu zu starten.

- Klicken Sie bei Linux-basierten Authentifizierungsproxyservern auf **Ja**, um die Eingabeaufforderung anzuzeigen, die bei der Installation angezeigt wird und fragt, ob Sie ein Init-Skript erstellen möchten. Wenn Sie dann den Authentifizierungsproxy starten, verwenden Sie einen Befehl, z. B. **sudo service duoauthproxy start**, der angibt, dass der Befehl für das Init-Skript je nach System, auf dem Sie sich befinden, abweichen kann.

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme