配置Duo Multi Factor Authentication以與UCS Manager配合使用

目錄

簡介

本文檔介紹使用UCS Manager實施Cisco Duo多重身份驗證(MFA)的配置和最佳實踐。

必要條件

需求

思科建議您瞭解以下主題：

- UCS管理器
- Cisco Duo

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

Cisco UCS Manager對遠端使用者登入使用雙因素身份驗證。雙因素身份驗證登入需要在密碼欄位中提供使用者名稱、令牌和密碼組合。

在使用遠端身份驗證撥入使用者服務(RADIUS)或終端訪問控制器訪問控制系統+(TACACS+)提供程式組時，支援雙因素身份驗證，這些提供程式組具有指定身份驗證域，這些域具有雙因素身份驗證。雙重身份驗證不支援網際網路效能監視器(IPM)，並且在身份驗證領域設定為輕量級目錄訪問協定時不受支援
(LDAP)、本地或無。

在Duo實施中，多因素身份驗證通過Duo身份驗證代理執行，該代理是一種本地軟體服務，通過RADIUS或LDAP從本地裝置和應用程式接收身份驗證請求，可以選擇對LDAP目錄或RADIUS身份驗證伺服器執行主要身份驗證，然後聯絡Duo以執行輔助身份驗證。使用者批准二元請求後，Duo Mobile會以推送通知或電話呼叫等方式接收該請求，Duo Proxy將向請求身份驗證的裝置或應用程式返回訪問批准。

設定

此配置可滿足通過LDAP和Radius成功實施UCS Manager的Duo的要求。

> **附註**：有關基本Duo身份驗證Proxy配置，請檢視Duo Proxy指南：Duo Proxy文檔

LDAP整合

UCS管理器

導航到**UCS Manager > Admin Section > User Management > LDAP** 並啟用**LDAP Providers SSL**，這意味著與LDAP資料庫的通訊需要加密。LDAP使用STARTTLS。這允許使用埠389進行加密通訊。Cisco UCS在埠636上為SSL協商傳輸層安全(TLS)會話，但在埠389上初始連線開始時未加密。

```
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
```

> **附註**：STARTTLS在標準LDAP埠上運行，因此，與LDAPS不同，STARTTLS整合使用Duo Authentication Proxy上的**port=** field not **ssl_port=** 欄位。

在Duo Authentication Proxy上

```
[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整合

UCS管理器

導航到**UCS Manager > Admin > User Management > Radius**，然後點選**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
```

安裝和配置Duo Authentication Proxy的最佳實踐

在具有防火牆的內部網路中部署身份驗證代理，該內部網路可以：

- 允許從TCP/443上的身份驗證代理到常規Internet的出站通訊。如果需要進一步的限制，請參閱Duo的List of IP ranges to Allowed List。
- 也可以將Duo身份驗證代理配置為通過支援CONNECT協定的先前配置的Web代理訪問Duo的服務。
- 可以連線到適當的IDP，通常通過TCP/636、TCP/389或UDP/1812
- 允許與適當RADIUS、LDAP或LDAPS埠上的代理進行通訊。這些規則允許裝置/應用程式根據代理驗證使用者。
- 如果環境中存在任何SSL檢查裝置，請對身份驗證代理IP禁用/允許清單SSL檢查。
- 配置每個**[radius_server_METHOD(X)]**和**[ldap_server_auto(X)]**部分以偵聽唯一埠。
  詳細瞭解如何使用Duo Authentication Proxy為Duo站點上的多個應用程式提供電源。
- 對每個裝置使用唯一的RADIUS機密和密碼。
- 在代理配置檔案中使用受保護/加密的密碼。

- 雖然驗證代理可以與其他服務共存於多用途伺服器上，但建議使用專用伺服器。

- 確保身份驗證代理指向可靠的NTP伺服器，以確保準確的日期和時間。

- 升級驗證代理之前，請一律製作組態檔的備份副本。
- 對於基於Windows的身份驗證代理伺服器，配置Duo Security Authentication Proxy服務，使其在電源或網路故障時包含一些恢複選項：

  步驟1.在伺服器的**服務**中，按一下右鍵**Duo Security Authentication Proxy**服務，然後按一下**首選項。**
  步驟2.按一下**Recovery**，然後配置選項以在發生故障後重新啟動服務。

- 對於基於Linux的身份驗證代理伺服器，按一下**yes**可顯示安裝中詢問是否要建立init指令碼的提示。然後，當您啟動身份驗證代理時，使用諸如**sudo service duoauthproxy start**之類的命令，該命令用於init指令碼的命令可能會因您使用的系統而異。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- [技術支援與文件 - Cisco Systems]