配置双核多因素身份验证以与UCS Manager配合使用

目录

简介
先决条件
要求
使用的组件
背景信息
配置
LDAP集成
UCS 管理器
Duo认证代理
Radius集成
UCS 管理器
双核身份验证代理
安装和配置双核身份验证代理的最佳实践
验证
故障排除
相关信息

简介

本文档介绍使用UCS Manager实施思科双核多因素身份验证(MFA)的配置和最佳实践。

先决条件

要求

Cisco 建议您了解以下主题：

- UCS 管理器
- 思科双核

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

Cisco UCS Manager对远程用户登录使用双因素身份验证。双因素身份验证登录要求在密码字段中输入用户名、令牌和密码组合。

当您使用远程身份验证拨入用户服务(RADIUS)或终端访问控制器访问控制系统+(TACACS+)提供程序组（具有针对这些域的双因素身份验证的指定身份验证域）时，支持双因素身份验证。双因素身份验证不支持网际网络性能监控器(IPM)，当身份验证领域设置为轻量级目录访问协议时不支持(LDAP)、本地或无。

在Duo实施中，多重身份验证通过Duo身份验证代理执行，该本地软件服务通过RADIUS或LDAP接收来自本地设备和应用的身份验证请求，或者针对LDAP目录或RADIUS身份验证服务器执行主身份验证，然后联系Duo以执行辅助身份验证。一旦用户批准双因素请求，Duo代理将返回访问批准给请求身份验证的设备或应用。

配置

此配置涵盖通过LDAP和Radius使用UCS Manager成功实施Duo的要求。

> **注意**：有关基本双核身份验证代理配置，请检查双核代理指南：双核代理文档

LDAP集成

UCS 管理器

导航至**UCS Manager > Admin Section > User Management > LDAP**并启**用LDAP提供程序SSL**，这意味着与LDAP数据库的通信需要加密。LDAP使用STARTTLS。这允许使用端口389进行加密通信。Cisco UCS在端口636上为SSL协商传输层安全(TLS)会话，但初始连接在端口389上开始未加密。

```
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
```

> **注意**：STARTTLS在标准LDAP端口上运行，因此与LDAPS不同，STARTTLS集成使用Duo身份验证代理**上的**port= **field not ssl_port=** 字段。

Duo认证代理

```
[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集成

UCS 管理器

导航至**UCS Manager > Admin > User Management > Radius**，然后单击**Radius Providers:**

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

双核身份验证代理

```
[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
```

安装和配置双核身份验证代理的最佳实践

在防火墙内部网络中部署身份验证代理，该网络具有以下特点：

- 允许从身份验证代理到TCP/443上常规Internet的出站通信。如果需要进一步限制，请参阅Duo的IP范围列表到允许的列表。
- Duo身份验证代理也可以配置为通过支持CONNECT协议的先前配置的Web代理访问Duo的服务。
- 可以连接到适当的IDP，通常通过TCP/636、TCP/389或UDP/1812
- 允许与相应RADIUS、LDAP或LDAPS端口上的代理通信。这些规则允许设备/应用根据代理对用户进行身份验证。
- 如果环境中存在任何SSL检测设备，请禁用/允许对身份验证代理IP的SSL检测。
- 配置每个**[radius_server_METHOD(X)]**和**[ldap_server_auto(X)]**节以侦听唯一端口。
  详细了解如何使用双核身份验证代理为多应用双核站点双核代理上的多个应用程序供电。
- 为每台设备使用唯一的RADIUS密钥和密码。
- 在代理配置文件中使用受保护/加密的密码。
- 虽然身份验证代理可以与其他服务共存于多用途服务器上，但建议使用专用服务器。

- 确保身份验证代理指向可靠的NTP服务器，以确保日期和时间准确。

- 在升级身份验证代理之前，请始终创建配置文件的备份副本。
- 对于基于Windows的身份验证代理服务器，请配置Duo安全身份验证代理服务以在电源或网络故障时包括一些恢复选项：

  步骤1.在您的服**务器**上的“服务”中，右键单击**Duo Security Authentication Proxy Service**，然后单击“首选**项”。**
  步骤2.单击**Recovery**，然后配置选项以在发生故障后重新启动服务。

- 对于基于Linux的身份验证代理服务器，请单击**yes**，看到安装时显示的提示，提示是否要创建初始脚本。然后，在启动身份验证代理时，使用诸如**sudo service douathproxy start**之类的命令，该命令对于init脚本的命令可能会因您所在的系统而异。

验证

当前没有可用于此配置的验证过程。

故障排除

当前没有可用于此配置的特定故障排除信息。

相关信息

- 技术支持和文档 - Cisco Systems