Configure Duo Multi Factor Authentication para que funcione con UCS Manager

Contenido

Introducción

Este documento describe la configuración y las prácticas recomendadas para implementar Cisco Duo Multi-Factor Authentication (MFA) con UCS Manager.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- UCS Manager
- Cisco Duo

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cisco UCS Manager utiliza la autenticación de dos factores para los inicios de sesión de usuarios remotos. El inicio de sesión de autenticación de dos factores requiere un nombre de usuario, un token y una combinación de contraseña en el campo de contraseña.

Se admite la autenticación de dos factores cuando se utiliza el servicio de usuario de acceso telefónico de autenticación remota (RADIUS) o los grupos de proveedores del sistema de control de acceso del controlador de acceso de terminal +(TACACS+) con dominios de autenticación designados con autenticación de dos factores para esos dominios. La autenticación de dos factores no admite el monitor de rendimiento entre redes (IPM) y no se admite cuando el rango de autenticación está establecido en el protocolo ligero de acceso a directorios (LDAP), local o ninguno.

Con la implementación de Duo, la autenticación multifactor se realiza a través del proxy de autenticación dúo, que es un servicio de software en las instalaciones que recibe solicitudes de autenticación de sus dispositivos y aplicaciones locales a través de RADIUS o LDAP, opcionalmente realiza la autenticación primaria contra su directorio LDAP o servidor de autenticación RADIUS, y luego se pone en contacto con Duo para realizar la autenticación secundaria. Una vez que el usuario aprueba la solicitud de dos factores, que se recibe como notificación de inserción de Duo Mobile, o como llamada telefónica, etc, el proxy Duo devuelve la aprobación de acceso al dispositivo o aplicación que solicitó autenticación.

Configurar

Esta configuración cubre los requisitos para una implementación Duo exitosa con UCS Manager a través de LDAP y Radius.

> **Nota:** Para la configuración básica de Duo Authentication Proxy, consulte las pautas de Duo Proxy: Documento de Proxy Duo

Integración de LDAP

UCS Manager

Navegue hasta **UCS Manager > Admin Section > User Management > LDAP** y habilite **LDAP Providers SSL**, esto significa que se requiere cifrado para las comunicaciones con la base de datos LDAP. LDAP utiliza STARTTLS. Esto permite la comunicación cifrada por el puerto de uso 389. Cisco UCS negocia una sesión de seguridad de la capa de transporte (TLS) en el puerto 636 para SSL, pero la conexión inicial comienza sin cifrar en el puerto 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 funciona en un puerto LDAP estándar, por lo que a diferencia de LDAPS, las integraciones STARTTLS utilizan el campo **port=** field not **ssl_port=** en el Proxy de Autenticación Duo.

En el Proxy de autenticación 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
```

Integración de Radius

UCS Manager

Navegue hasta **UCS Manager > Admin > User Management > Radius** y haga clic en **Proveedores Radius:**

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

Proxy de autenticación 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
```

Prácticas recomendadas para instalar y configurar el proxy de autenticación Duo

Implemente el Proxy de Autenticación en una red interna con firewall que:

- Permite la comunicación saliente del Proxy de autenticación a la Internet general en TCP/443. Si se requieren más restricciones, consulte la lista de intervalos IP de Duo a la lista permitida.
- El Duo Authentication Proxy también se puede configurar para alcanzar el servicio de Duo a través de un proxy web previamente configurado que admita el protocolo CONNECT.

- Se puede conectar a los IDP adecuados, normalmente a través de TCP/636, TCP/389 o UDP/1812

- Permite la comunicación con el proxy en los puertos RADIUS, LDAP o LDAPS apropiados. Estas reglas permiten a los dispositivos/aplicaciones autenticar a los usuarios con los proxies.

- Si existe algún dispositivo de inspección SSL en el entorno, inhabilite/permita la inspección SSL de lista para las IP de proxy de autenticación.

- Configure cada **sección [radius_server_METHOD(X)]** y **[ldap_server_auto(X)]** para escuchar en un puerto único.
  Obtenga más información sobre cómo utilizar el proxy de autenticación Duo para suministrar energía a varias aplicaciones en el sitio Duo [Duo Proxy para varias aplicaciones.]

- Utilice secretos RADIUS y contraseñas únicos para cada dispositivo.

- Utilice contraseñas protegidas/cifradas en el archivo de configuración de proxy.

- Aunque el Proxy de autenticación puede coexistir en servidores multipropósito con otros servicios, se recomienda utilizar un servidor dedicado.

- Asegúrese de que el Proxy de autenticación apunte a un servidor NTP confiable para garantizar una fecha y hora precisas.

- Antes de la actualización del Proxy de autenticación, realice siempre una copia de seguridad del archivo de configuración.
- Para los servidores del Proxy de autenticación basado en Windows, configure el Servicio del Proxy de autenticación de seguridad Duo para incluir algunas opciones de recuperación en caso de fallos de alimentación o de red:

  Paso 1. Dentro de **Services** en su servidor, haga clic con el botón derecho en el servicio **Duo Security Authentication Proxy** y, a continuación, haga clic en **Preferences.**
  Paso 2. Haga clic en **Recuperación** y, a continuación, configure las opciones para reiniciar el servicio después de las fallas.

- Para los servidores del Proxy de autenticación basado en Linux, haga clic en **yes** en el mensaje visible en la instalación que pregunta si desea crear un script de inicialización. A continuación, cuando inicie el Proxy de autenticación, utilice un comando como **sudo service duoauthproxy start**, para que el comando para el script de inicialización pueda variar en función del sistema en el que se encuentre.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente no hay información de troubleshooting específica disponible para esta configuración.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems