Configure a autenticação multifator dupla para funcionar com o UCS Manager

Contents

Introduction

Este documento descreve a configuração e as práticas recomendadas para implementar a autenticação multifator (MFA) do Cisco Duo com o UCS Manager.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- UCS Manager
- Cisco Duo

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Cisco UCS Manager usa autenticação de dois fatores para logins de usuário remoto. O login de autenticação de dois fatores exige uma combinação de nome de usuário, token e senha no campo de senha.

A autenticação de dois fatores é suportada quando você usa grupos de provedores RADIUS (Remote Authentication Dial-In User Service) ou TACACS+ (Terminal Access Controller Access Control System + TACACS+) com domínios de autenticação designados com autenticação de dois fatores para esses domínios. A autenticação de dois fatores não suporta o IPM (Internetwork Performance Monitor) e não é suportada quando o domínio de autenticação está definido como Lightweight Diretory Access Protocol
(LDAP), local ou nenhum.

Com a implementação Duo, a Autenticação Multifator é executada através do Proxy de Autenticação Duo, que é um serviço de software local que recebe solicitações de autenticação de seus dispositivos e aplicativos locais via RADIUS ou LDAP, opcionalmente executa a autenticação primária em seu diretório LDAP ou servidor de autenticação RADIUS e, em seguida, entra em contato com Duo para executar a autenticação secundária. Quando o usuário aprova a solicitação de dois fatores, que é recebida como uma notificação push do Duo Mobile, como uma chamada telefônica, etc., o proxy Duo retorna a aprovação de acesso ao dispositivo ou aplicativo que solicitou a autenticação.

Configurar

Essa configuração abrange os requisitos para uma implementação Duo bem-sucedida com o UCS Manager por LDAP e Radius.

> **Note**: Para obter a configuração básica do Proxy de Autenticação Duo, consulte as diretrizes do Proxy Duo: Documento Proxy Duo

Integração LDAP

UCS Manager

Navegue para **UCS Manager > Admin Section > User Management > LDAP** e ative **LDAP Providers SSL**, significa que a criptografia é necessária para comunicações com o banco de dados LDAP. O LDAP usa STARTTLS. Isso permite a comunicação criptografada pela porta de uso 389. O Cisco UCS negocia uma sessão de TLS (Transport Layer Security) na porta 636 para SSL, mas a conexão inicial começa sem criptografia na porta 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 opera em uma porta LDAP padrão, portanto, diferentemente do LDAPS, as integrações STARTTLS usam o campo **port=** não **ssl_port=** no Proxy de Autenticação Duo.

No Proxy de Autenticação 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
```

Integração de RADIUS

UCS Manager

Navegue até **UCS Manager > Admin > User Management > Radius** e clique em **Radius Providers:**

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

Proxy de Autenticação 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
```

Práticas recomendadas para instalar e configurar o proxy de autenticação dupla

Implante o proxy de autenticação em uma rede interna com firewall que:

- Permite a comunicação de saída do Proxy de Autenticação para a Internet geral no TCP/443. Se forem necessárias mais restrições, consulte a Lista de intervalos de IP de Duo para a Lista Permitida.
- O Proxy de Autenticação Duo também pode ser configurado para acessar o serviço de Duo por meio de um proxy da Web previamente configurado que suporte o protocolo CONNECT.

- Pode se conectar aos IDPs apropriados, geralmente sobre TCP/636, TCP/389 ou UDP/1812
- Permite a comunicação com o proxy nas portas RADIUS, LDAP ou LDAPS apropriadas. Essas regras permitem que os dispositivos/aplicativos autentiquem usuários contra os proxies.
- Se houver algum dispositivo de inspeção SSL no ambiente, desative/permita a inspeção SSL da lista para IPs de proxy de autenticação.
- Configure cada seção **[radius_server_MethOD(X)]** e **[ldap_server_auto(X)]** para ouvir em uma porta exclusiva.
  Leia mais sobre como usar o Proxy de Autenticação Duo para alimentar vários aplicativos no Proxy Duo do site Duo para Vários Aplicativos.
- Use segredos e senhas RADIUS exclusivos para cada dispositivo.
- Use senhas protegidas/criptografadas no arquivo de configuração de proxy.
- Embora o Proxy de Autenticação possa coexistir em servidores multiuso com outros serviços, é recomendável usar um ou mais servidores dedicados.
- Certifique-se de que o Proxy de Autenticação aponte para um servidor NTP confiável para garantir uma data e hora precisas.
- Antes da atualização do Proxy de Autenticação, faça sempre uma cópia de backup do arquivo de configuração.
- Para servidores Proxy de Autenticação baseados no Windows, configure o Serviço Proxy de Autenticação de Segurança Duo para incluir algumas opções de recuperação em caso de falha de energia ou de rede:

  Etapa 1. Em **Serviços** em seu servidor, clique com o botão direito do mouse no serviço **Proxy de Autenticação de Segurança Duo** e clique em **Preferências.**
  Etapa 2. Clique em **Recuperação** e configure as opções para reiniciar o serviço após falhas.
- Para servidores Proxy de Autenticação baseados em Linux, clique em **sim** para o prompt visível na instalação que pergunta se você deseja criar um script de inicialização. Em seguida, quando você iniciar o Proxy de Autenticação, use um comando como **sudo service duoauthproxy start**, que o comando para o script de inicialização pode ser diferente com base em qual sistema você está.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não há informações específicas de solução de problemas disponíveis para esta

configuração.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems