Proteger o Cisco Umbrella para implantações de dispositivos virtuais e conectores AD

Contents

Introdução

Este documento descreve as práticas recomendadas e as recomendações sobre as implantações do Cisco Umbrella Virtual Appliance (VA) e do Ative Diretory (AD) Connector para reduzir o risco de ataques internos que surgem com o uso desses componentes.

O VA executa uma versão reforçada do Ubuntu Linux 20.04. Os clientes recebem acesso restrito apenas para fins de configuração e solução de problemas. Nenhum software ou script adicional pode ser implantado no VA pelos clientes.

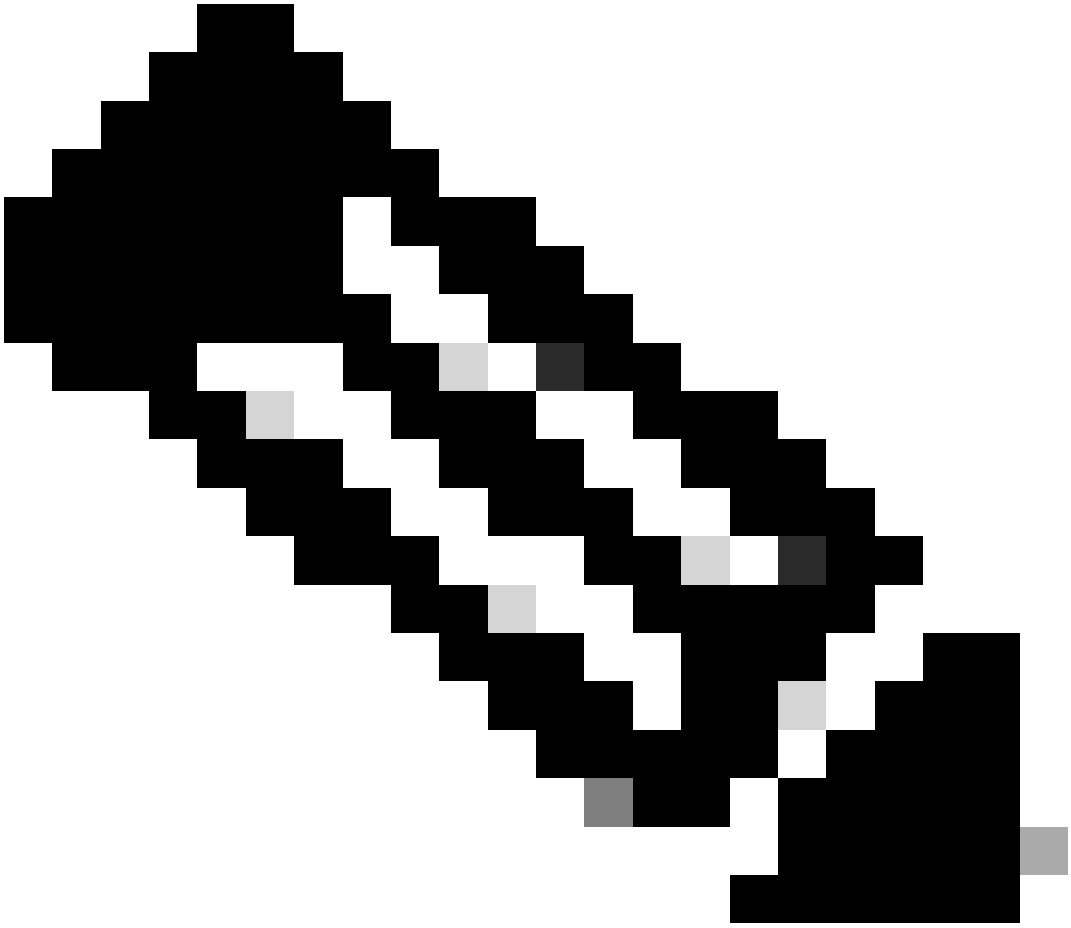
Dispositivo virtual Cisco Umbrella

Gerenciando o arquivo .tar:

- O software Cisco Umbrella Virtual Appliance (VA) é baixado do Umbrella Dashboard como um arquivo .tar que contém a imagem VA real e uma assinatura para essa imagem.
- A Cisco recomenda validar a assinatura para verificar a integridade da imagem VA.

Configurando portas:

- Por padrão, na implantação, somente as portas 53 e 443 são abertas para o tráfego de entrada.
- Se você estiver executando o VA no Azure, KVM, Nutanix, AWS ou GCP, a porta 22 também será habilitada por padrão para permitir conexões SSH para configurar o VA.
- Para VAs em execução no VMware e Hyper-V, a porta 22 é aberta apenas se o comando para habilitar o SSH for executado no VA.
- O VA faz consultas externas sobre portas/protocolos específicos para os destinos mencionados na documentação do Umbrella.
- O Cisco Umbrella recomenda a configuração de regras no seu firewall para bloquear qualquer tráfego dos seus VAs para todos os outros destinos.



Note: Toda comunicação HTTPS de/para VA acontece somente sobre TLS 1.2. Protocolos mais antigos não são usados.

Gerenciando senhas:

- O login inicial no VA requer uma alteração de senha.
- A Cisco recomenda a rotação periódica da senha no VA após essa alteração inicial de senha.

Atenuação de ataques de DNS:

- Para reduzir o risco de um ataque interno de negação de serviço no serviço DNS em execução no VA, você pode configurar limites de taxa por IP para o DNS no VA.
- Isso não é habilitado por padrão e deve ser explicitamente configurado usando as instruções documentadas na documentação do Umbrella.

Monitorando VAs sobre SNMP:

- Se você estiver monitorando seus VAs por SNMP, o Cisco Umbrella recomenda o uso de SNMPv3 com autenticação e criptografia.
- As instruções para o mesmo estão na documentação do Umbrella.
- Quando você habilita o monitoramento SNMP, a porta 161 no VA é aberta para tráfego de entrada.
- Você pode monitorar vários atributos como a CPU, a carga e a memória no VA sobre SNMP.

Usando a integração do Cisco AD com VAs:

- Se você estiver usando os VAs com a integração do Ative Diretory do Cisco Umbrella, é recomendável ajustar (ou ajustar) a duração do cache do usuário no VA para corresponder ao tempo de aluguel do DHCP.
- Consulte as instruções no Virtual Appliance: Ajustando a documentação de Definições de Caixa do Usuário. Isso minimiza o risco de atribuições de usuário incorretas.

Configurando o log de auditoria:

- O VA mantém um log de auditoria de todas as alterações de configuração executadas no VA.
- Você pode configurar o registro remoto desse registro de auditoria em um servidor syslog de acordo com as instruções na documentação do Umbrella.

Configurando VAs:

- Pelo menos dois VAs devem ser configurados por site Umbrella, e o endereço IP desses dois VAs pode ser distribuído como servidores DNS para endpoints.
- Para redundância adicional, você pode configurar o endereçamento Anycast no VA. Isso permite que vários VAs compartilhem um único endereço Anycast.
- Assim, você pode implantar vários VAs enquanto distribui apenas dois IPs de servidor DNS para cada endpoint. Se qualquer VA falhar, o Anycast garantirá que as consultas de DNS sejam roteadas para o outro VA que compartilhe o mesmo IP do Anycast.
- Leia mais sobre as etapas para configurar o Anycast no VA.

Configurando o Cisco Umbrella Ative Diretory Connector

Criando um nome de conta personalizado:

- Uma das práticas recomendadas para o Cisco Umbrella AD Connector é usar um nome de conta personalizado em vez do OpenDNS_Connector padrão.
- Esta conta pode ser criada antes da implantação do conector e receber as permissões necessárias.
- O nome da conta precisa ser especificado como parte da instalação do conector.

Configurando LDAPS com o Conector AD:

- O Umbrella AD Connector tenta recuperar informações de grupos de usuários por meio de LDAPS (dados transmitidos por um canal seguro), com falha em que ele alterna para LDAP

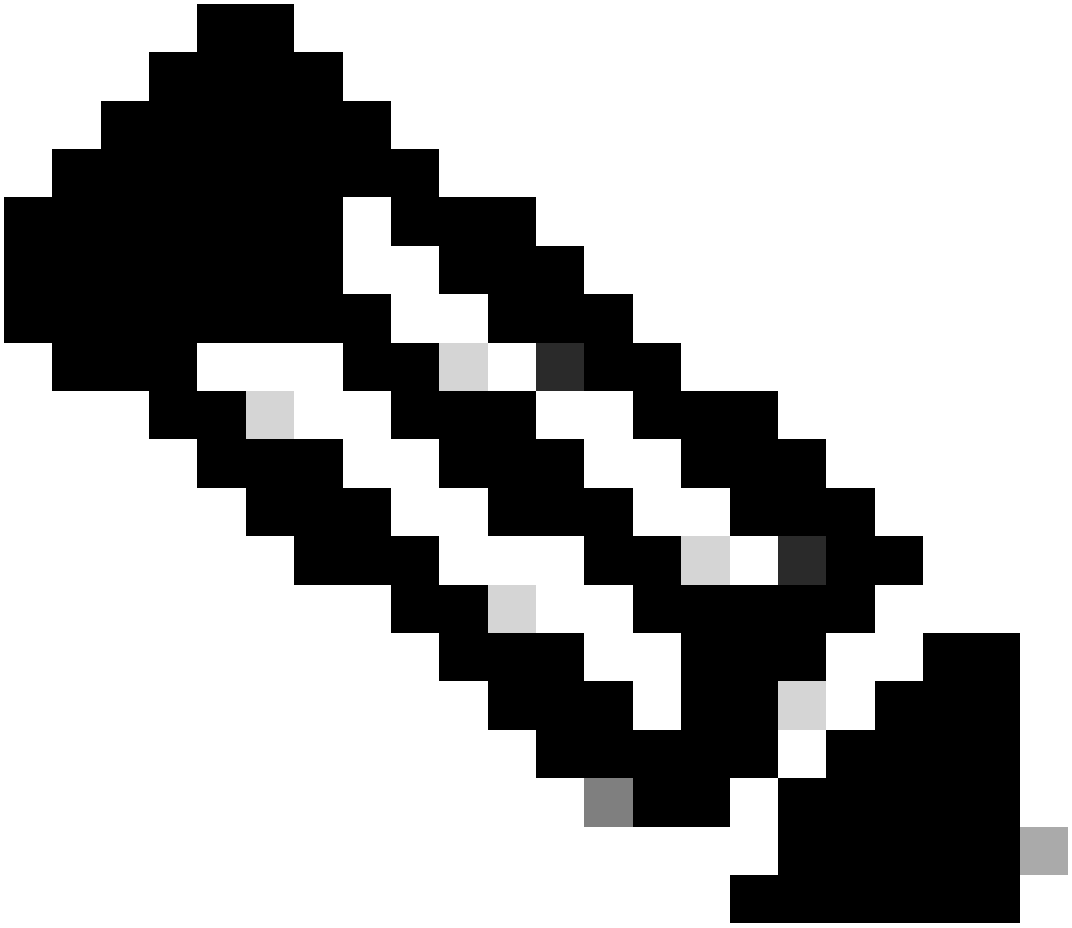
por Kerberos (criptografia em nível de pacote) ou LDAP por NTLM (somente autenticação, sem criptografia) nessa ordem.
- O Cisco Umbrella recomenda a configuração de LDAPS nos controladores de domínio para que o conector possa recuperar essas informações em um canal criptografado.

Gerenciando o arquivo .ldif:

- O conector, por padrão, armazena os detalhes dos usuários e grupos recuperados dos controladores de domínio em um arquivo .ldif localmente.
- Como podem ser informações confidenciais armazenadas em texto sem formatação, você pode restringir o acesso ao servidor que executa o conector.
- Como alternativa, no momento da instalação, você pode optar por não armazenar os arquivos .ldif localmente.

Configurando portas:

- Como o conector é um serviço do Windows, ele não habilita/desabilita nenhuma porta na máquina host. O Cisco Umbrella recomenda a execução do serviço Cisco Umbrella AD Connector em um servidor Windows dedicado.
- Semelhante ao VA, o conector faz consultas externas sobre portas/protocolos específicos para os destinos mencionados na documentação do Umbrella. O Cisco Umbrella recomenda configurar regras no seu firewall para bloquear qualquer tráfego dos seus conectores para todos os outros destinos.



Note: Toda a comunicação HTTPS de/para o conector acontece somente sobre TLS 1.2. Protocolos mais antigos não são usados.

Gerenciando a senha do conector:

- A Cisco recomenda girar a senha do conector periodicamente.
- Isso pode ser feito alterando a senha da conta do conector no Ative Diretory e, em seguida, atualizando a senha usando a ferramenta "PasswordManager" na pasta do conector.

Recebendo mapeamentos de IP de usuário:

- Por padrão, o conector comunica o IP privado.
- O AD envia mapeamentos de usuário para o VA em texto simples.
- Você pode optar por configurar o VA e o conector para se comunicar em um canal criptografado, de acordo com as instruções documentadas neste artigo da Base de conhecimento.

Gerenciamento de certificados:

- O gerenciamento e a revogação de certificados estão fora do escopo do VA, e você é responsável por garantir que a cadeia de certificado/certificado mais recente esteja presente no VA e no conector, conforme relevante.
- A configuração de um canal criptografado para essa comunicação afeta o desempenho do VA e do conector.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.