适用于虚拟设备和AD连接器部署的安全Cisco Umbrella

目录

简介

本文档介绍有关思科Umbrella虚拟设备(VA)和Active Directory(AD)连接器部署的最佳实践和建议，以降低因使用这些组件而引发的任何内部攻击的风险。

VA运行Ubuntu Linux 20.04的强化版本。仅向客户提供用于配置和故障排除的限制访问权限。客户不能在VA上部署其他软件或脚本。

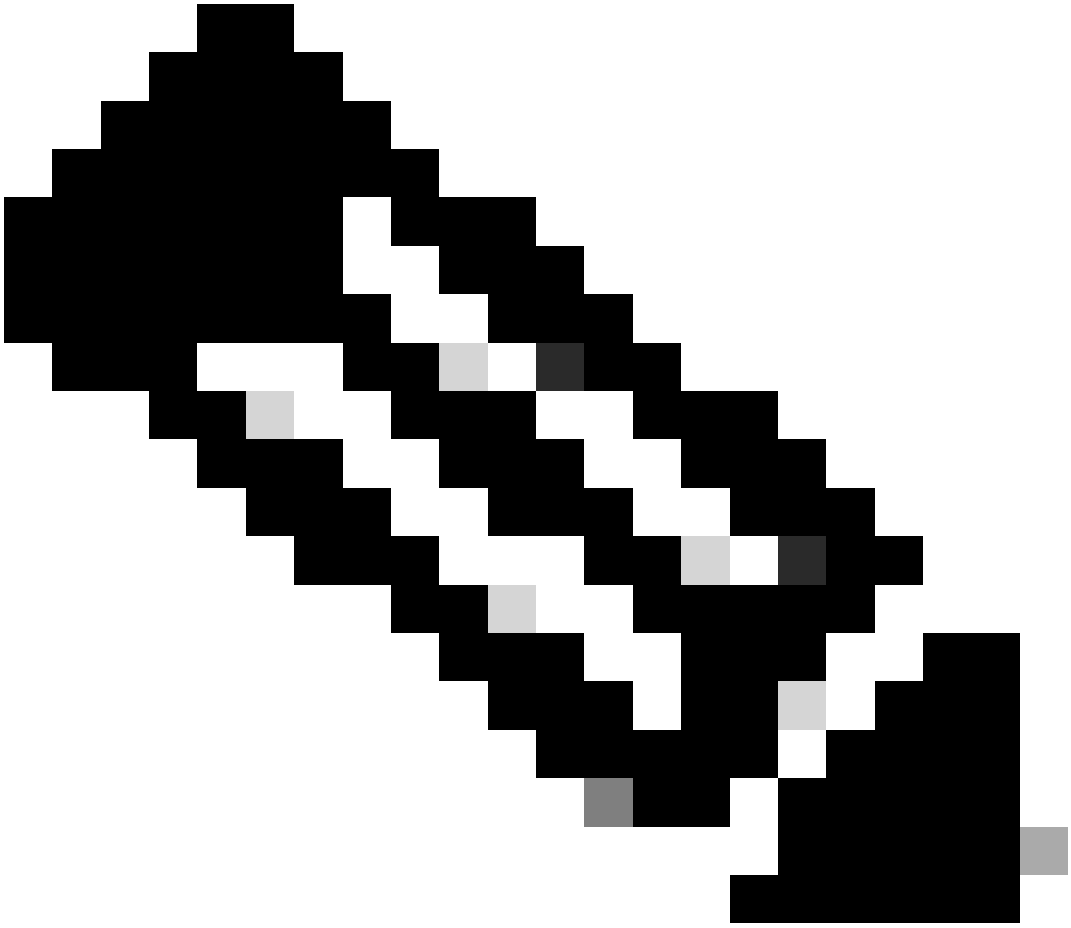
思科Umbrella虚拟设备

管理.tar文件：

- Cisco Umbrella虚拟设备(VA)软件从Umbrella控制面板下载为.tar文件，其中包含实际VA映像和该映像的签名。
- Cisco建议验证签名以验证VA映像的完整性。

配置端口：

- 默认情况下，在部署时，仅端口53和443对入站流量开放。
- 如果您在Azure、KVM、Nutanix、AWS或GCP上运行VA，则默认情况下还会启用端口22，以允许SSH连接配置VA。
- 对于在VMware和Hyper-V上运行的VA，只有在VA上运行启用SSH的命令时，才会打开端口22。
- VA通过特定端口/协议对Umbrella文档中提到的目标进行出站查询。
- Cisco Umbrella建议在防火墙上设置规则以阻止从您的VA到所有其他目的地的任何流量。



注意：与VA之间的所有HTTPS通信仅通过TLS 1.2进行。不使用较旧的协议。

管理密码：

- 首次登录VA时需要更改密码。
- Cisco建议在此初始密码更改后定期在VA上轮换密码。

缓解DNS攻击：

- 要降低在VA上运行的DNS服务受到内部拒绝服务攻击的风险，您可以在VA上为DNS配置每个IP的速率限制。
- 默认情况下未启用此功能，必须使用Umbrella文档中记录的说明进行显式配置。

通过SNMP监控VA:

- 如果您通过SNMP监控您的VA，Cisco Umbrella建议使用具有身份验证和加密功能的SNMPv3。
- 相关说明见Umbrella文档。

- 一旦启用SNMP监控，VA上的端口161将针对入站流量打开。
- 您可以通过SNMP监控VA上的各种属性，例如CPU、负载和内存。

使用Cisco AD与VA的集成：

- 如果将VA与Cisco Umbrella Active Directory集成配合使用，则最佳实践是调整（或调整）VA上的用户缓存持续时间，以匹配您的DHCP租用时间。
- 请参阅虚拟设备中的说明：调整用户机箱设置文档。这样可以最大程度地降低用户属性不正确的风险。

配置审核日志记录：

- VA维护在VA上执行的所有配置更改的审核日志。
- 根据Umbrella文档中的说明，您可以将此审核日志远程记录到系统日志服务器。

配置VA:

- 每个Umbrella站点至少必须配置两个VA，并且这两个VA的IP地址可以作为DNS服务器分发到终端。
- 为了获得更多冗余，您可以在VA上配置任播编址。这允许多个VA共享一个任播地址。
- 因此，您可以有效地部署多个VA，同时仍仅向每个终端分配两个DNS服务器IP。如果任何VA发生故障，任播会确保DNS查询路由到共享同一任播IP的其他VA。
- 详细了解在VA上配置任播的步骤。

配置Cisco Umbrella Active Directory连接器

创建自定义帐户名称：

- Cisco Umbrella AD连接器的最佳实践之一是使用自定义帐户名称而不是默认的OpenDNS_Connector。
- 可以在连接器部署之前创建此帐户并授予所需的权限。
- 需要在连接器安装过程中指定帐户名称。

使用AD连接器配置LDAPS:

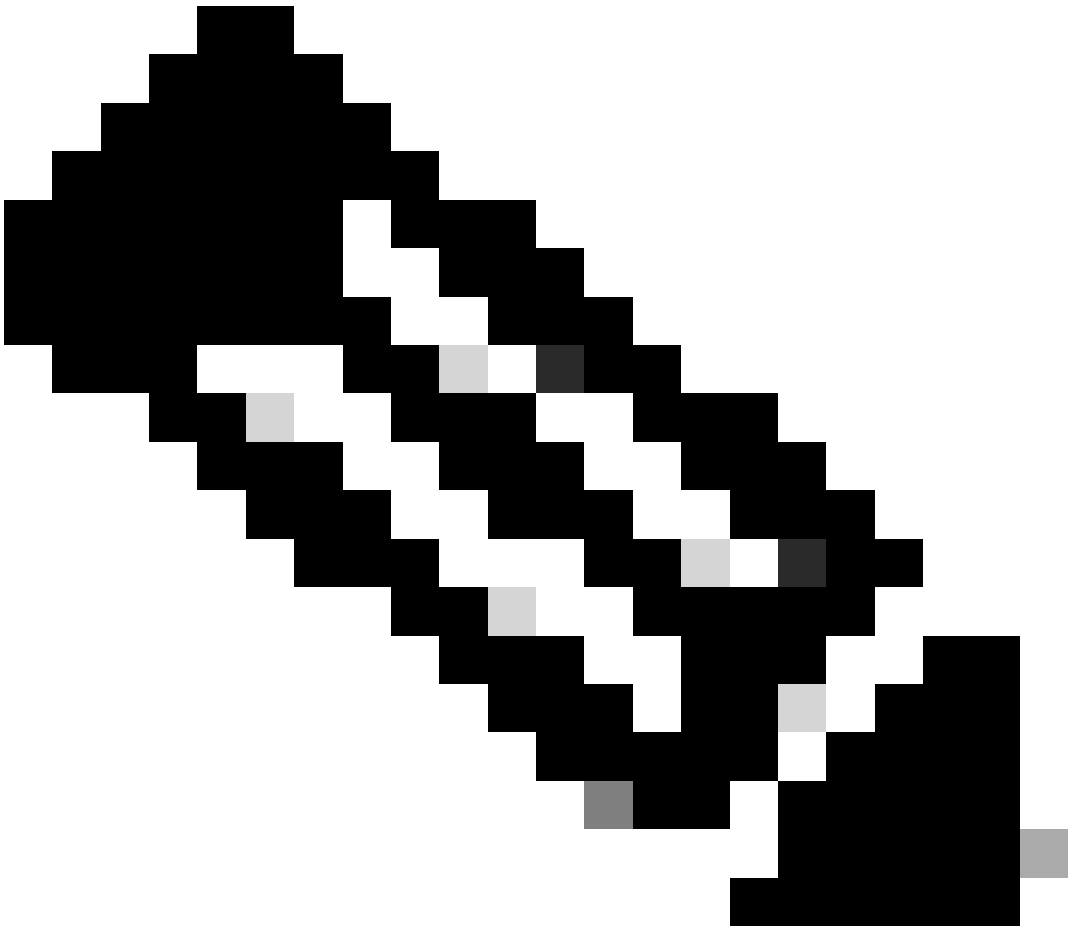
- Umbrella AD连接器尝试通过LDAPS（通过安全信道传输的数据）检索用户组信息，但未能成功，它以该顺序通过Kerberos切换到LDAP（数据包级别加密）或通过NTLM切换到LDAP（仅身份验证，无加密）。
- Cisco Umbrella建议在域控制器上设置LDAPS，以便连接器可以通过加密通道检索此信息。

管理.ldif文件：

- 默认情况下，连接器将从域控制器中检索到的用户和组的详细信息存储在.ldif本地文件中。
- 由于此信息可能是存储在纯文本中的敏感信息，因此您可以限制对运行连接器的服务器的访问。
- 或者，在安装时，可以选择不在本地存储.ldif文件。

配置端口：

- 由于连接器是Windows服务，因此它不会启用/禁用主机上的任何端口。Cisco Umbrella建议在专用Windows服务器上运行Cisco Umbrella AD连接器服务。
- 与VA类似，连接器通过特定端口/协议向Umbrella文档中提到的目标进行出站查询。Cisco Umbrella建议在防火墙上设置规则，以阻止从连接器到所有其他目的地的任何流量。



注意：与连接器的所有HTTPS通信仅通过TLS 1.2进行。不使用较旧的协议。

管理连接器密码：

- Cisco建议定期旋转连接器密码。
- 这可以通过在Active Directory中更改连接器帐户密码，然后使用连接器文件夹中的“PasswordManager”工具更新密码来实现。

接收用户IP映射：

- 默认情况下，连接器会通信专用IP。
- AD通过明文向VA发送用户映射。

- 您可以选择根据此知识库文章中记录的说明，配置VA和连接器以通过加密通道进行通信。

证书管理：

- 证书管理和撤销不属于VA的范围，您负责确保VA和连接器上存在相关的最新证书/证书链。
- 为此通信设置加密信道会影响VA和连接器的性能。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。