Sicherer Cisco Umbrella für virtuelle Appliance- und AD Connector-Bereitstellungen

Inhalt

Einleitung

In diesem Dokument werden Best Practices und Empfehlungen für die Bereitstellung von Cisco Umbrella Virtual Appliance (VA) und Active Directory (AD) Connector beschrieben, um das Risiko interner Angriffe durch die Verwendung dieser Komponenten zu minimieren.

Die VA verwendet eine robuste Version von Ubuntu Linux 20.04. Kunden erhalten nur zu Konfigurations- und Fehlerbehebungszwecken eingeschränkten Zugriff. Kunden können in der VA keine zusätzliche Software oder Skripte bereitstellen.

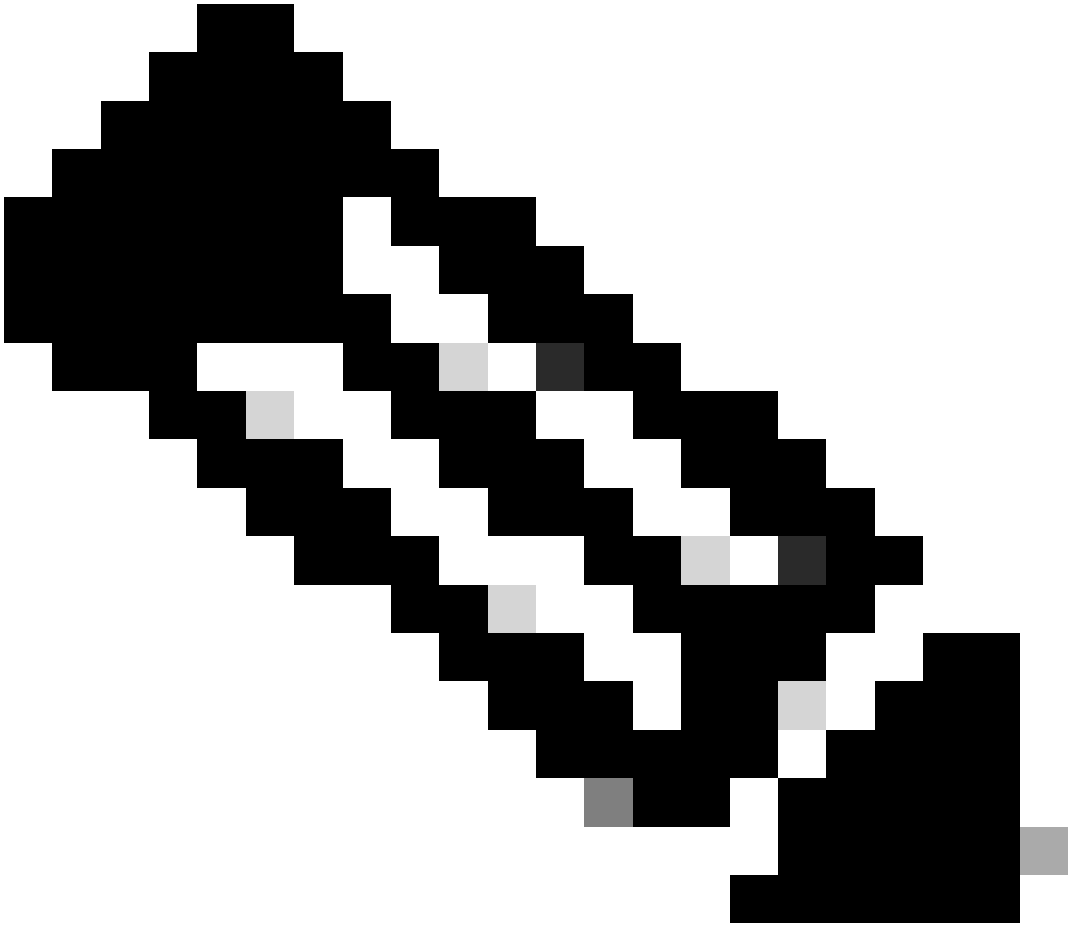
Virtuelle Cisco Umbrella Appliance

Verwalten der TAR-Datei:

- Die Cisco Umbrella Virtual Appliance (VA)-Software lädt vom Umbrella Dashboard als .tar-Datei herunter, die das eigentliche VA-Image und eine Signatur für dieses Image enthält.
- Cisco empfiehlt, die Signatur zu validieren, um die Integrität des VA-Images zu überprüfen.

Konfigurieren von Ports:

- Standardmäßig sind bei der Bereitstellung nur die Ports 53 und 443 für eingehenden Datenverkehr geöffnet.
- Wenn Sie die VA auf Azure, KVM, Nutanix, AWS oder GCP ausführen, ist Port 22 ebenfalls standardmäßig aktiviert, um SSH-Verbindungen für die Konfiguration der VA zuzulassen.
- Bei VAs, die auf VMware und Hyper-V ausgeführt werden, wird Port 22 nur geöffnet, wenn der Befehl zum Aktivieren von SSH auf der VA ausgeführt wird.
- Die VA sendet ausgehende Abfragen über bestimmte Ports/Protokolle an die in der Umbrella-Dokumentation genannten Ziele.
- Cisco Umbrella empfiehlt, Regeln auf Ihrer Firewall einzurichten, um jeglichen Verkehr von Ihren VAs zu allen anderen Zielen zu blockieren.



Anmerkung: Die gesamte HTTPS-Kommunikation von und zu der VA erfolgt nur über TLS 1.2. Ältere Protokolle werden nicht verwendet.

Passwörter verwalten:

- Für die erstmalige Anmeldung bei der VA ist eine Kennwortänderung erforderlich.
- Cisco empfiehlt, das Kennwort nach der ersten Kennwortänderung regelmäßig in der VA zu ändern.

Abwehr von DNS-Angriffen:

- Um das Risiko eines internen Denial-of-Service-Angriffs auf den in der VA ausgeführten DNS-Service zu verringern, können Sie Durchsatzbegrenzungen pro IP für den DNS in der VA konfigurieren.
- Diese Funktion ist nicht standardmäßig aktiviert und muss explizit mithilfe der Anweisungen in der Umbrella-Dokumentation konfiguriert werden.

Überwachen von VAs über SNMP:

- Wenn Sie Ihre VAs über SNMP überwachen, empfiehlt Cisco Umbrella die Verwendung von SNMPv3 mit Authentifizierung und Verschlüsselung.
- Anleitungen hierzu finden Sie in der Umbrella-Dokumentation.
- Sobald Sie die SNMP-Überwachung aktivieren, wird Port 161 der VA für eingehenden Datenverkehr geöffnet.
- Sie können verschiedene Attribute wie CPU, Last und Speicher in der VA über SNMP überwachen.

Verwendung der Cisco AD-Integration mit VAs:

- Wenn Sie die VAs mit der Cisco Umbrella Active Directory-Integration verwenden, empfiehlt es sich, die Dauer des Benutzer-Caches in der VA an die DHCP-Leasedauer anzupassen (oder anzupassen).
- Weitere Informationen finden Sie in den Anweisungen zur virtuellen Appliance: Anpassung der Dokumentation zu den Einstellungen für die Benutzercaseheft. Dadurch wird das Risiko falscher Benutzerzuschreibungen minimiert.

Konfigurieren der Überwachungsprotokollierung:

- Die VA verwaltet ein Prüfprotokoll aller Konfigurationsänderungen, die an der VA durchgeführt wurden.
- Sie können die Remote-Protokollierung dieses Prüfprotokolls an einen Syslog-Server gemäß den Anweisungen in der Umbrella-Dokumentation konfigurieren.

Konfigurieren von VAs:

- Pro Umbrella-Standort müssen mindestens zwei VAs konfiguriert werden, und die IP-Adresse dieser beiden VAs kann als DNS-Server an Endpunkte verteilt werden.
- Für zusätzliche Redundanz kann die Anycast-Adressierung in der VA konfiguriert werden. Auf diese Weise können mehrere VAs eine einzelne Anycast-Adresse gemeinsam nutzen.
- Auf diese Weise können Sie mehrere VAs bereitstellen und gleichzeitig nur zwei DNS-Server-IPs an jeden Endpunkt verteilen. Wenn eine VA ausfällt, stellt Anycast sicher, dass die DNS-Abfragen an die andere VA mit derselben Anycast-IP weitergeleitet werden.
- Lesen Sie mehr über die Schritte zum Konfigurieren von Anycast auf der VA.

Konfigurieren des Cisco Umbrella Active Directory Connectors

Erstellen eines benutzerdefinierten Kontonamens:

- Eine der Best Practices für Cisco Umbrella AD Connector besteht darin, anstelle des standardmäßigen OpenDNS_Connector-Kontos einen benutzerdefinierten Kontonamen zu verwenden.
- Dieses Konto kann vor der Connectorbereitstellung erstellt werden und erhält die erforderlichen Berechtigungen.
- Der Kontoname muss im Rahmen der Connector-Installation angegeben werden.

Konfigurieren von LDAPS mit dem AD-Connector:

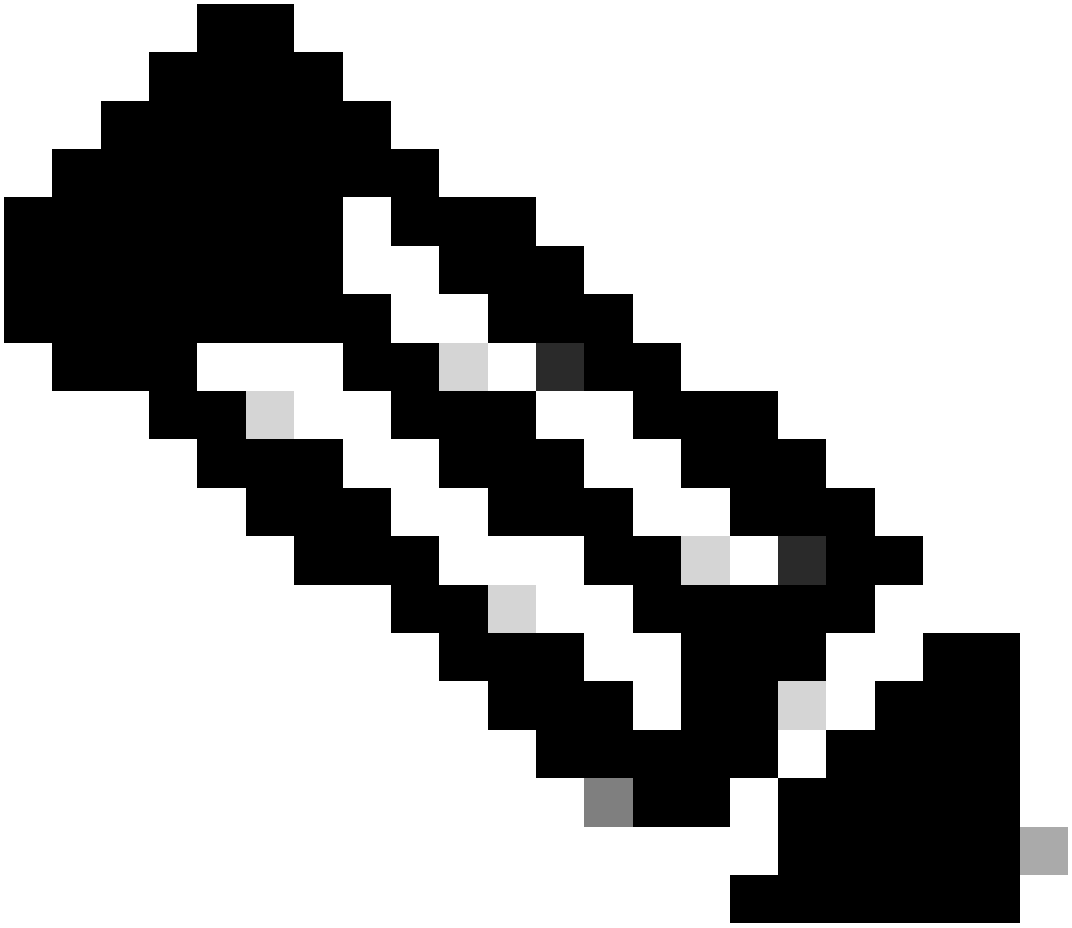
- Der Umbrella AD Connector versucht, Benutzergruppeninformationen über LDAPS (Daten, die über einen sicheren Kanal übertragen werden) abzurufen, andernfalls wechselt er über Kerberos (Verschlüsselung auf Paketebene) oder LDAP über NTLM (nur Authentifizierung, keine Verschlüsselung) in dieser Reihenfolge zu LDAP.
- Cisco Umbrella empfiehlt die Einrichtung von LDAPS auf Ihren Domänencontrollern, damit der Connector diese Informationen über einen verschlüsselten Kanal abrufen kann.

Verwaltung der .ldif-Datei:

- Der Connector speichert standardmäßig die Details der von den Domänencontrollern abgerufenen Benutzer und Gruppen in einer .ldif-Datei lokal.
- Da es sich hierbei um vertrauliche Informationen handeln kann, die im Nur-Text-Format gespeichert werden, können Sie den Zugriff auf den Server beschränken, der den Connector ausführt.
- Alternativ können Sie bei der Installation festlegen, dass die .ldif-Dateien nicht lokal gespeichert werden.

Konfigurieren von Ports:

- Da es sich bei dem Connector um einen Windows-Dienst handelt, werden keine Ports auf dem Host-Rechner aktiviert bzw. deaktiviert. Cisco Umbrella empfiehlt, den Cisco Umbrella AD Connector-Dienst auf einem dedizierten Windows-Server auszuführen.
- Ähnlich wie bei der VA führt der Connector ausgehende Abfragen über bestimmte Ports/Protokolle an die in der Umbrella-Dokumentation genannten Ziele durch. Cisco Umbrella empfiehlt, Regeln auf Ihrer Firewall einzurichten, um jeglichen Datenverkehr von Ihren Connectors zu allen anderen Zielen zu blockieren.



Anmerkung: Die gesamte HTTPS-Kommunikation zum/vom Connector erfolgt nur über TLS 1.2. Ältere Protokolle werden nicht verwendet.

Verwalten des Connector-Passworts:

- Cisco empfiehlt, das Connector-Kennwort regelmäßig zu ändern.
- Dies kann durch Ändern des Connector-Kontokennworts in Active Directory und anschließendes Aktualisieren des Kennworts mithilfe des Tools "PasswordManager" im Connector-Ordner erfolgen.

Empfangen von Benutzer-IP-Zuordnungen:

- Standardmäßig kommuniziert der Connector private IP.
- AD sendet Benutzerzuordnungen über Klartext an die VA.
- Sie können die VA und den Connector für die Kommunikation über einen verschlüsselten Kanal konfigurieren, wie in diesem Knowledge Base-Artikel beschrieben.

Zertifikatsverwaltung:

- Die Zertifikatverwaltung und der Widerruf liegen außerhalb des Gültigkeitsbereichs der VA, und Sie müssen sicherstellen, dass die neueste Zertifikat-/Zertifikatskette auf der VA und dem Connector vorhanden ist, sofern relevant.
- Die Einrichtung eines verschlüsselten Kanals für diese Kommunikation beeinträchtigt die Leistung der VA und des Anschlusses.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.