適用於虛擬裝置和AD聯結器部署的安全Cisco Umbrella

目錄

簡介

本文檔介紹有關Cisco Umbrella虛擬設備(VA)和Active Directory(AD)聯結器部署的最佳實踐和建議，以減輕因使用這些元件而引發的任何內部攻擊的風險。

VA運行的是強化版Ubuntu Linux 20.04。客戶僅能有限地訪問配置和故障排除。客戶不能在VA上部署其他軟體或指令碼。

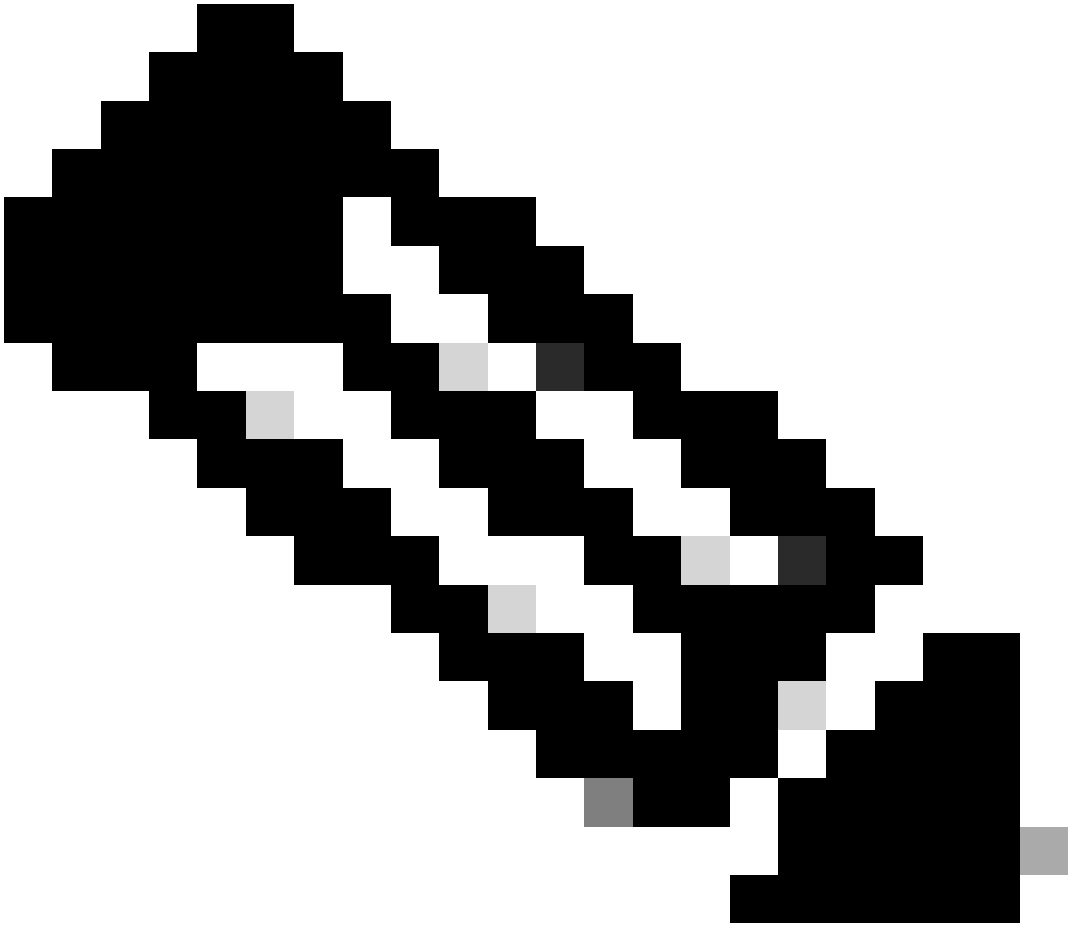
思科雨傘虛擬裝置

管理.tar檔案：

- Cisco Umbrella Virtual Appliance(VA)軟體從Umbrella Dashboard下載為.tar檔案，其中包含實際的VA映像和該映像的簽名。
- 思科建議驗證簽名以驗證VA映像的完整性。

配置埠：

- 預設情況下，在部署時，只有埠53和443對入站流量開放。
- 如果您在Azure、KVM、Nutanix、AWS或GCP上運行VA，則預設情況下還啟用port 22，以允許配置VA的SSH連線。
- 對於在VMware和Hyper-V上運行的VA，僅當在VA上運行啟用SSH的命令時，才會開啟埠22。
- VA通過特定埠/協定向Umbrella文檔中提到的目標發出出站查詢。
- Cisco Umbrella建議在防火牆上設定規則，以阻止從您的VA到所有其他目的地的任何流量。



附註：與VA之間的所有HTTPS通訊僅通過TLS 1.2進行。不使用較早的協定。

管理密碼：

- 首次登入VA時需要更改密碼。
- 思科建議在此初始密碼更改後定期在VA上旋轉密碼。

減輕DNS攻擊：

- 要降低在VA上運行的DNS服務發生內部拒絕服務攻擊的風險，您可以為VA上的DNS配置每個IP速率限制。
- 預設情況下，此功能未啟用，必須使用Umbrella文檔中記錄的說明進行明確配置。

使用SNMP監控VA:

- 如果您正在通過SNMP監控VA，Cisco Umbrella建議使用具有驗證和加密功能的SNMPv3。
- 相關說明見Umbrella文檔。
- 啟用SNMP監控後，VA上的埠161將針對入站流量開啟。

- 您可以通過SNMP監控VA上的各種屬性，例如CPU、負載和記憶體。

使用Cisco AD與VA的整合：

- 如果將VA與Cisco Umbrella Active Directory整合配合使用，則最佳實踐是調整（或調整）VA上的使用者快取持續時間，以與您的DHCP租用時間相匹配。
- 請參閱虛擬裝置中的說明：調整使用者機箱設定文檔。這樣可最大程度降低錯誤使用者屬性的風險。

配置審計日誌記錄：

- VA維護在VA上執行的所有配置更改的稽核日誌。
- 根據Umbrella文檔中的說明，您可以配置此稽核日誌到系統日誌伺服器的遠端日誌記錄。

配置VA:

- 每個Umbrella站點至少必須配置兩個VA，並且這兩個VA的IP地址可以作為DNS伺服器分發到終端。
- 為了獲得更多冗餘，您可以在VA上配置任播定址。這允許多個VA共用一個任播地址。
- 因此，您可以有效地部署多個VA，同時仍然只向每個端點分發兩個DNS伺服器IP。如果任何VA失敗，任播可確保將DNS查詢路由到共用相同任播IP的另一個VA。
- 瞭解更多有關在VA上配置任播的步驟。

配置Cisco Umbrella Active Directory聯結器

建立自定義帳戶名稱：

- Cisco Umbrella AD Connector的最佳實踐之一是使用自定義帳戶名稱而不是預設的OpenDNS_Connector。
- 可以在聯結器部署之前建立此帳戶並授予所需的許可權。
- 需要在聯結器安裝過程中指定帳戶名。

使用AD聯結器配置LDAPS:

- Umbrella AD聯結器嘗試通過LDAPS（通過安全通道傳輸的資料）檢索使用者組資訊，但未能成功，它以該順序通過Kerberos切換到LDAP（資料包級別加密）或通過NTLM切換到LDAP（僅身份驗證，無加密）。
- Cisco Umbrella建議在域控制器上設定LDAPS，以便聯結器能夠通過加密通道檢索此資訊。

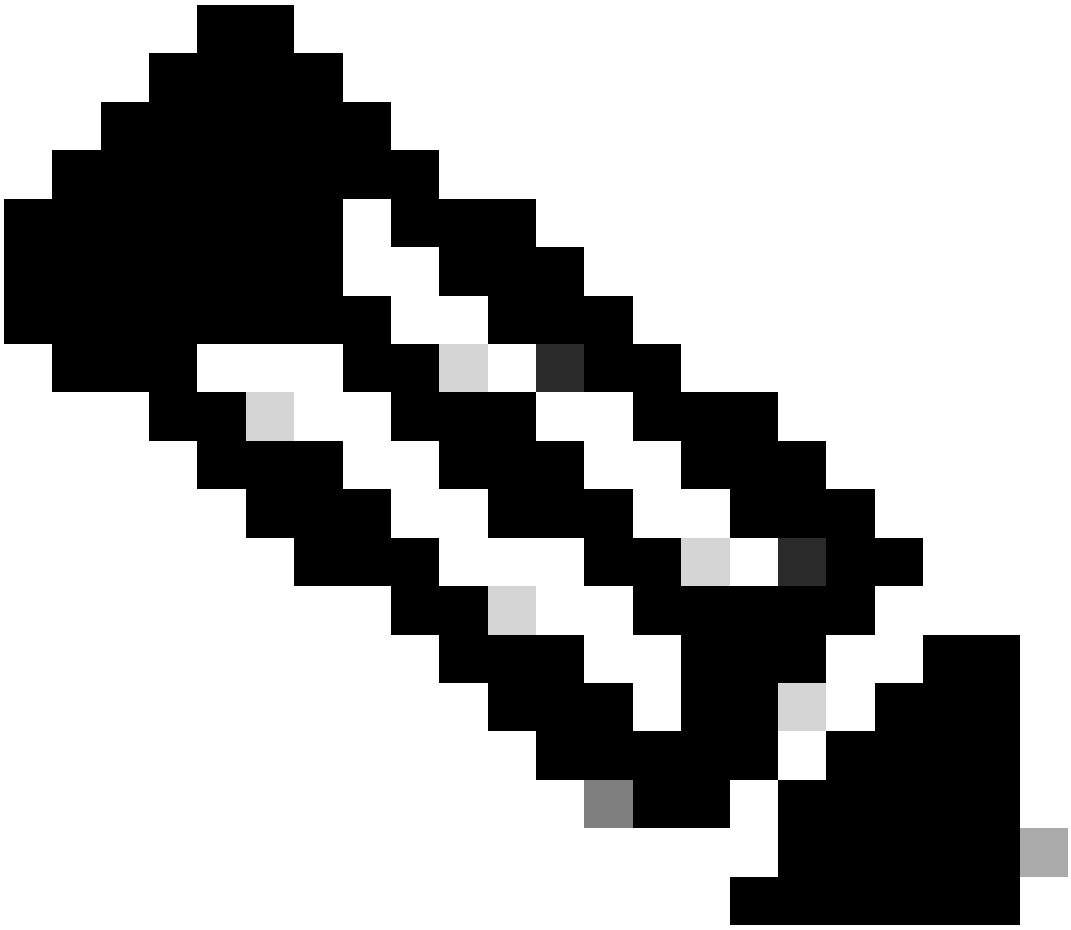
管理.ldif檔案：

- 預設情況下，聯結器將從域控制器中檢索到的使用者和組的詳細資訊儲存在.ldif本地檔案中。
- 由於該資訊可能是儲存在純文字檔案中的敏感資訊，因此您可以限制對運行聯結器的伺服器的訪問。
- 或者，在安裝時，可以選擇不在本地儲存.ldif檔案。

配置埠：

- 由於聯結器是Windows服務，因此它不會啟用/禁用主機上的任何埠。Cisco Umbrella建議在

專用的Windows伺服器上運行Cisco Umbrella AD聯結器服務。
- 與VA類似，聯結器會通過特定埠/協定向Umbrella文檔中提到的目標發出出站查詢。Cisco Umbrella建議在防火牆上設定規則，以阻止從聯結器到所有其他目的地的任何流量。



附註：與聯結器的所有HTTPS通訊僅通過TLS 1.2進行。不使用較早的協定。

管理聯結器密碼：

- 思科建議定期旋轉聯結器密碼。
- 要完成此操作，請在Active Directory中更改聯結器帳戶密碼，然後使用聯結器資料夾中的「PasswordManager」工具更新密碼。

接收使用者 — IP對映：

- 預設情況下，聯結器會傳送私有IP。
- AD通過明文向VA傳送使用者對映。
- 您可以選擇根據此知識庫文章中記錄的說明配置VA和聯結器以通過加密通道進行通訊。

證書管理：

- 證書管理和吊銷超出了VA的範圍，並且您負責確保VA和聯結器上存在相關的最新證書/證書鏈。
- 為此通訊設定加密通道會影響VA和聯結器的效能。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。