Windows Server-Härtung für Cisco Unified Attendant Console Advanced Server

Inhalt

Übersicht

In diesem Dokument werden verschiedene Konfigurationsänderungen beschrieben, die auf einem Cisco Unified Attendant Console Advanced (CUACA)-Server vorgenommen werden können, um die Sicherheit zu erhöhen. Der Prozess, Windows sicherer zu machen, wird als Windows-Sicherung bezeichnet. Die unten aufgeführten Informationen können als Anleitung zur Härtung Ihrer Cisco Unified Attendant Console Advanced-Server verwendet werden.

Firewall- und Gruppenrichtlinien

Nachdem der Windows-Server der Domäne hinzugefügt wurde, können Gruppenrichtlinien an Windows gesendet werden. Firewall-Richtlinien und Gruppenrichtlinien, die auf den CUACA-Server übertragen werden, dürfen das Arbeiten der folgenden Services und Ports nicht blockieren oder unterbrechen:

- Windows-Verwaltungsinstrumentation (WMI)
- Distributed Transaction Coordinator (MDDTC) - nur erforderlich, wenn SQL-Replikation/-Ausfallsicherheit verwendet wird
- Message Bus (MBUS) - offene Eingangs- und Ausgangs-Ports 61616 und 61618 (nur erforderlich, wenn SQL-Replikation/-Ausfallsicherheit verwendet wird)
- exe - *Beispiel: C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn\sqlservr.exe*
- Portnummern (von CUAC verwendet):

Portnummern	Port-Typ
80	TCP
389	TCP
443	TCP
636	TCP
1433 und 1434	TCP
1859	TCP
1862	TCP
1863	TCP
1864	TCP
2748	TCP
5060	UDP
5061 und 5062	TCP
11859	TCP
61616	TCP
61618	TCP
49152 bis 65535	TCP
1.025 bis 5.000	TCP

Port-Nummer	Verwenden
389	LDAP-Server verwendet nicht SSL und ist nicht als globaler Katalog konfiguriert.

636	LDAP-Server verwendet SSL und ist nicht als globaler Katalog konfiguriert.
3268	LDAP-Server verwendet nicht SSL und wird als globaler Katalog konfiguriert.
3269	LDAP-Server verwendet SSL und wird als globaler Katalog konfiguriert.

Lesen Sie die neuesten Administrations- und Installationsanleitungen vor der Implementierung, um die Ausschlussliste zu validieren.

Antivirensoftware

Installieren Sie eine Antivirus-Software auf dem Windows-Server, um sie vor Malware, Viren usw. zu schützen. Allerdings verlangsamt eine Antivirus-Anwendung die CUACA-Serverfunktionalität, da sie kontinuierlichen Zugriff auf wenige Ordner benötigt, während sie vom Antivirus überprüft wird. Daher wird empfohlen, folgende Dateien und Ordner als Ausschluss der Antivirus-Software hinzuzufügen:

Standardordner	Enthält
\\DBData	Systemkonfigurationsdatenbanken
Files\Cisco\	Ablaufverfolgungsdateien für Software und Anwendungen
\\Apache	Aktiver MQ-Ordner
\\Temp\Cisco\Trace	Cisco TSP-Ablaufverfolgungsdateien
\\%ALLUSERSPROFILE%\Cisco\CUACA	Cisco Profil

Dies sind die Standardspeicherorte, die vom CUACA-Installationsprogramm verwendet werden. Falls der Administrator den Speicherort dieser Ordner ändert oder andere Ordner verwendet, müssen die Ausschlüsse für den Virenschutz entsprechend geändert werden.

Lesen Sie die neuesten Administrations- und Installationsanleitungen vor der Implementierung, um die Ausschlussliste zu validieren.

IP Source Routing deaktivieren

IP Source Routing wird heutzutage selten verwendet, kann jedoch von Hackern verwendet werden, um die Firewall zu umgehen. Cisco empfiehlt daher, diese zu deaktivieren.

Im Folgenden werden die Schritte zum Deaktivieren des IP-Source-Routings beschrieben:

- Regedit öffnen
- Legen Sie folgende Werte fest oder erstellen Sie diese:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\

  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip6\Parameters\

  Wertname: DisableIPSourceRouting

Werttyp: REG_DWORD
Wert: 2

- Schließen Sie Regedit.

Windows-Updates

Cisco empfiehlt, Windows-Server-Patches mit den neuesten Microsoft Windows- und SQL Server-Updates und Service Packs beizubehalten. Automatische Updates und automatische Prüfungen auf Updates sollten deaktiviert werden.

Automatische Java-Updates werden nicht unterstützt, da sie manchmal fehlschlagen und dies zu unbrauchbarem System führen kann. Geringfügige Updates werden unterstützt.

Alle Überprüfungen auf Updates und die Installation von Updates sollten außerhalb der Produktion durchgeführt werden. Nach der Installation starten Sie das Serverbetriebssystem neu.

Weitere Härtungsanforderungen gemäß Unternehmensrichtlinie

Cisco empfiehlt jedoch, Windows Server entsprechend den Anforderungen/Richtlinien zu härten. Der Administrator muss jedoch sicherstellen, dass alle CUACA-Anforderungen nach der Härtung erfüllt werden. Detaillierte Informationen zu den CUACA-Anforderungen finden Sie im CUACA Designleitfaden und im CUAC Installationsleitfaden.