Windows Server Hardening for Cisco Unified Attendant Console Advanced Server

Contents

Overview

This document describes several configuration changes that can be made on a Cisco Unified Attendant Console Advanced (CUACA) server in order to make it more secure. The process of making Windows system more secure is known as Windows Hardening. The information listed below can be used as a guide to harden your Cisco Unified Attendant Console Advanced server(s).

Firewall and Group Policies

Once the Windows server has been added to the domain, group policies could be pushed to Windows. Firewall policies and group policies pushed to CUACA server should not block or interrupt working of following services and ports:

- Windows Management Instrumentation (WMI)
- Distributed Transaction Coordinator (MDDTC) – only required if using SQL replication/resilience
- Message Bus (MBUS) – open inbound and outbound ports 61616 and 61618 (only required if using SQL replication/resilience)
- exe – *For example: C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn\sqlservr.exe*
- Port Numbers (Used by CUAC):

Port Numbers	Port Type
80	TCP
389	TCP
443	TCP
636	TCP
1433 and 1434	TCP
1859	TCP
1862	TCP
1863	TCP
1864	TCP
2748	TCP
5060	UDP
5061 and 5062	TCP
11859	TCP
61616	TCP
61618	TCP
49152 to 65535	TCP
1025 to 5000	TCP

Port Number	Use
389	LDAP server does not use SSL and is not configured as the Global Catalog.
636	LDAP server uses SSL and is not configured as

	the Global Catalog.
3268	LDAP server does not use SSL and is configured as the Global Catalog.
3269	LDAP server uses SSL and is configured as the Global Catalog.

Refer to the latest Administration and Installation Guides prior to implementation to validate list of exclusions.

Anti-virus software

Install an anti-virus software on the Windows server to keep it safe from malware, viruses etc. However, antivirus application slows down CUACA server functionality as it needs continuous access to few folders while anti-virus scans them. Hence it is advised to add following files and folders as exclusions on antivirus software:

Default Folder	Contains
\\DBData	System configuration databases
\\Program Files\Cisco	Software and application trace files
\\Apache	Active MQ folder
\\Temp\Cisco\Trace	Cisco TSP trace files
\\%ALLUSERSPROFILE%\Cisco\CUACA	Cisco profile

These are default locations used by CUACA installer. In case administrator changes the location of these folders or use some other folders, exclusions on anti-virus need to be changed accordingly.

Refer to the latest Administration and Installation Guides prior to implementation to validate list of exclusions.

Disable IP Source Routing

IP Source routing is rarely used nowadays however hackers can use it to bypass firewall and hence, Cisco advices to disable it.

Following are the steps to disable IP Source routing:

- Open Regedit
- Set or create these values:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\

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

  Value Name: DisableIPSourceRouting
  Value Type: REG_DWORD
  Value: 2

- Close Regedit.

Windows Updates

Cisco advises to keep Windows server patched with latest Microsoft Windows and SQL Server updates and Service Packs. Automatic updates and auto checks for updates should be disabled.

Java auto-updates are not supported as they fail sometimes and this may result in unusable system. Minor updates are supported.

All checks for updates and installation of updates should be executed outside of production. Following installation restart the server OS.

Other Hardening Requirements as per Company's policy

Cisco advices to harden Windows Server as per requirement/policy however, administrator needs to make sure that all CUACA requirements are met after hardening. For detailed knowledge on CUACA requirements, refer to CUACA Design guide and CUAC Install guide.