Windows Server Hardening para Cisco Unified Attendant Console Advanced Server

Contenido

Overview

Este documento describe varios cambios de configuración que se pueden realizar en un servidor Cisco Unified Attendant Console Advanced (CUACA) para hacerlo más seguro. El proceso de hacer que el sistema Windows sea más seguro se conoce como Windows Hardening. La información que se muestra a continuación se puede utilizar como guía para reforzar los servidores avanzados de Cisco Unified Attendant Console.

Firewall y políticas de grupo

Una vez agregado el servidor de Windows al dominio, las políticas de grupo se podrían enviar a Windows. Las políticas de firewall y las políticas de grupo que se envían al servidor CUACA no deben bloquear ni interrumpir el trabajo de los siguientes servicios y puertos:

- Instrumental de administración de Windows (WMI)
- Coordinador de transacciones distribuidas (MDDTC): solo se requiere si se utiliza la replicación/resistencia de SQL
- Bus de mensaje (MBUS): abrir los puertos de entrada y de salida 61616 y 61618 (solo se requiere si se utiliza la replicación/resistencia de SQL)
- exe - *Por ejemplo: C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn\sqlservr.exe*
- Números de puerto (utilizados por CUAC):

Números de puerto	Tipo de puerto
80	TCP
389	TCP
443	TCP
636	TCP
1433 y 1434	TCP
1859	TCP
1862	TCP
1863	TCP
1864	TCP
2748	TCP
5060	UDP
5061 y 5062	TCP
11859	TCP

61616	TCP
61618	TCP
49152 a 65535	TCP
1025 a 5000	TCP

número de puerto	Uso
389	El servidor LDAP no utiliza SSL y no está configurado como el Catálogo Global.
636	El servidor LDAP utiliza SSL y no está configurado como el Catálogo Global.
3268	El servidor LDAP no utiliza SSL y está configurado como el Catálogo Global.
3269	El servidor LDAP utiliza SSL y está configurado como el Catálogo Global.

Consulte las últimas Guías de administración e instalación antes de la implementación para validar la lista de exclusiones.

Software antivirus

Instale un software antivirus en el servidor de Windows para mantenerlo a salvo del malware, virus, etc. Sin embargo, las aplicaciones antivirus ralentizan la funcionalidad del servidor CUACA, ya que necesita acceso continuo a algunas carpetas mientras el antivirus las analiza. Por lo tanto, se recomienda agregar los siguientes archivos y carpetas como exclusiones en el software antivirus:

Carpeta predeterminada	Contiene
\\DBData	Bases de datos de configuración del sistema
\\Programa Files\Cisco\	Archivos de seguimiento de aplicaciones y software
\\Apache	Carpeta MQ activa
\\Temp\Cisco\Trace	Archivos de seguimiento de Cisco TSP
\\%ALLUSERSPROFILE%\Cisco\CUACA	perfil de Cisco

Estas son las ubicaciones predeterminadas que utiliza el instalador CUACA. En caso de que el administrador cambie la ubicación de estas carpetas o utilice otras, las exclusiones de antivirus deben cambiarse en consecuencia.

Consulte las últimas Guías de administración e instalación antes de la implementación para validar la lista de exclusiones.

Inhabilitación de Ruteo de Origen de IP

El ruteo de IP Source se utiliza raramente en la actualidad; sin embargo, los hackers pueden utilizarlo para eludir el firewall y, por lo tanto, Cisco aconseja desactivarlo.

A continuación se indican los pasos para inhabilitar el IP Source Routing:

- Abrir Regedit
- Establezca o cree estos valores:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\

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

  Nombre del valor: DisableIPSourceRouting
  Tipo de valor: REG_DWORD
  Valor: 2

- Cierre Regedit.

Actualizaciones de Windows

Cisco recomienda mantener parcheado el servidor de Windows con las últimas actualizaciones de Microsoft Windows y SQL Server y los Service Packs. Las actualizaciones automáticas y las comprobaciones automáticas de las actualizaciones deben desactivarse.

Las actualizaciones automáticas de Java no se admiten porque a veces fallan y esto puede dar lugar a sistemas inutilizables. Se admiten actualizaciones menores.

Todas las comprobaciones de las actualizaciones y la instalación de las actualizaciones deben ejecutarse fuera de la producción. Después de la instalación, reinicie el sistema operativo del servidor.

Otros requisitos de refuerzo según la política de la empresa

Sin embargo, Cisco aconseja reforzar Windows Server según los requisitos/políticas, el administrador debe asegurarse de que todos los requisitos CUACA se cumplen después de endurecer. Para obtener información detallada sobre los requisitos de CUACA, consulte la guía de diseño de CUACA y la guía de instalación de CUAC.