El Servidor Windows que endurecía para Cisco unificó el Advanced Server de la Consola de Attendant

Contenido

Información general

Este documento describe varios cambios de configuración que se puedan realizar en un servidor avanzado Consola de Attendant unificado Cisco (CUACA) para hacerlo más seguro. El proceso de hacer el Sistema Windows asegura más se conoce como endurecimiento de Windows. La información enumerada abajo se puede utilizar como guía para endurecer sus servidores avanzados Consola de Attendant unificados Cisco.

Directivas del Firewall y del grupo

Una vez que han agregado al Servidor Windows al dominio, las directivas del grupo se podrían avanzar a Windows. Las políticas del firewall y las directivas del grupo avanzadas al servidor CUACA no deben bloquear o interrumpir el funcionamiento de los servicios siguientes y de los puertos:

- Windows Management Instrumentation (WMI)
- Coordinador de transacciones distribuidas (MDDTC) – requerido solamente si usa la réplica de SQL/la resistencia
- El bus del mensaje (MBUS) – abra entrante y los puertos de egreso 61616 y 61618 (requerido solamente si usan la réplica de SQL/la resistencia)
- exe – *Por ejemplo: C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn\sqlservr.exe*
- Números del puerto (usados 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	Utilice

puerto	
389	El servidor LDAP no utiliza el SSL y no se configura como el catálogo global.
636	El servidor LDAP utiliza el SSL y no se configura como el catálogo global.
3268	El servidor LDAP no utiliza el SSL y se configura como el catálogo global.
3269	El servidor LDAP utiliza el SSL y se configura como el catálogo global.

Refiera a la últimas administración y guías de instalación antes de la implementación para validar la lista de exclusiones.

Software del contra virus

Instale un software del contra virus en el Servidor Windows para mantenerlo seguro del malware, de los virus etc. Sin embargo, la aplicación del antivirus retrasa la funcionalidad de servidor CUACA mientras que necesita el acceso continuo a pocas carpetas mientras que el contra virus las analiza. Por lo tanto se aconseja agregar los archivos siguientes y las carpetas como exclusiones en el Software anti virus:

Carpeta predeterminada	Contiene
\ \ DBData	Bases de datos de la configuración del sistema
\ \ archivos de programa \ Cisco \	Archivos de traza del software y de la aplicación
\ \ Apache	Carpeta activa MQ
\ \ temporeros \ Cisco \ traza	Archivos de traza de Cisco TSP
\ \ el %ALLUSERSPROFILE% \ Cisco \ CUACA	Perfil de Cisco

Éstas son ubicaciones predeterminadas usadas por el instalador CUACA. En caso de que el administrador cambie la ubicación de estas carpetas o utilice algunas otras carpetas, las exclusiones en la necesidad del contra virus de ser cambiado por consiguiente.

Refiera a la últimas administración y guías de instalación antes de la implementación para validar la lista de exclusiones.

Inhabilitación de Ruteo de Origen de IP

El rutear del IP de origen es raramente hoy en día usados sin embargo hackers puede utilizarla para desviar el Firewall y por lo tanto, los Ciscos recomienda para inhabilitarlo.

Los siguientes son los pasos para inhabilitar rutear del IP de origen:

- Abra Regedit
- El conjunto o crea estos valores:
  HKEY_LOCAL_MACHINE \ sistema \ CurrentControlSet \ servicios \ Tcpip \ parámetros \

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 aconseja para mantener al Servidor Windows parcheado con últimos Microsoft Windows y actualizaciones y Service Packs del SQL Server. Las actualizaciones automáticas y las comprobaciones para autos las actualizaciones deben ser inhabilitadas.

Los automóviles Update Button de las Javas no se soportan mientras que fallan a veces y éste puede dar lugar al sistema inutilizable. Se soportan las actualizaciones de menor importancia.

Todas las comprobaciones para las actualizaciones y la instalación de las actualizaciones se deben ejecutar fuera de la producción. La instalación de siguiente recomienza el servidor OS.

Otros requisitos de endurecimiento según la directiva de compañía

Los Ciscos recomienda para endurecer el Servidor Windows según el requisito/la directiva sin embargo, administrador necesitan aseegurarse que todos los requisitos CUACA estén cumplidos después de endurecer. Para el conocimiento detallado en los requisitos CUACA, refiera a la guía de diseño CUACA y CUAC instalan la guía.