

REQUISITOS DEL CLENTE DE CHANGE AUDITOR (COMPONENTE OPCIONAL)

Los agentes de workstation de Change Auditor se pueden implementar con el fin de capturar actividades de autenticación y eventos de inicio de sesión para workstations monitoreadas cuando se aplique la licencia de Change Auditor for Logon Activity Workstation, y la información del almacenamiento de los servicios en la nube (Box, DropBox y OneDrive) cuando se aplique la licencia de Change Auditor for Cloud Storage.

NOTA: La instalación recomendada para las workstations del dominio es desde la pestaña Implementación del cliente Windows® de Change Auditor. Sin embargo, para las workstations que no son del dominio, debe instalar manualmente el agente de workstation de Change Auditor. Consulte la Guía de instalación de Change Auditor para conocer las recomendaciones y las instrucciones sobre la implementación manual de agentes de workstation.

Procesador

Intel® Core™ i5 de doble núcleo, superior o equivalente

Memoria

Mínima: 2 GB de RAM; recomendada: 4 GB de RAM o superior

Sistema operativo

Plataformas de instalación compatibles hasta las siguientes versiones:

- Windows 7 (Pro, Enterprise y Ultimate)
- Windows 8 y 8.1 (Pro y Enterprise)

NOTA: Se debe habilitar Microsoft® Data Access Components (MDAC). MDAC es parte del sistema operativo y está habilitado de forma predeterminada.

NOTA: Los agentes de workstation no son compatibles con Windows 8.1 para el monitoreo de almacenamiento en la nube.

Software y configuración del cliente

- Versiones x86 o x64 de Microsoft .NET Framework 4.0 (o superior)
- Versiones x86 o x64 de Microsoft XML Parser (MSXML) 6.0
- Versiones x86 o x64 de Microsoft SQLXML 4.0
- El agente debe tener conectividad LDAP y GC con todas las controladoras de dominio en el dominio local y el dominio raíz del bosque.

El servicio del agente de workstation de Change Auditor depende de los siguientes servicios de Windows para su funcionamiento:

- Cliente DNS
- Llamada a procedimiento remoto (RPC)
- Registro de eventos de Windows

NOTA: Garantice las comunicaciones mediante RPC entre los coordinadores y los agentes.

NOTA: Para la administración de registros de workstations (tales como Obtener registros o Ver registro del agente), se debe habilitar lo siguiente en la workstation:

- El Instrumental de administración de Windows (WMI) debe estar habilitado en el conjunto de reglas del firewall (por lo general, el dominio) en la workstation.
- La detección de redes y el uso compartido de archivos deben estar habilitados.
- El servicio de registro remoto debe estar configurado en “Iniciar automáticamente”. De forma predeterminada, este servicio está detenido y configurado en “Manual” para Windows 7 y Windows 8/8.1.

Con el fin de capturar los eventos de actividad de autenticación, primero debe habilitar (habilitar Éxito y Falla) la política de auditoría de los “eventos de inicio de sesión de auditoría” para todos los servidores y todas las workstations.

Auditoría de actividades de autenticación

- Dominio: Política grupal: para capturar los eventos de la actividad de autenticación, primero debe activar (es decir, configurar en Correcto, Falla) la política de auditoría de “eventos de inicio de sesión de auditoría” para todos los servidores o todas las workstations:

Política de dominio predeterminada\Configuración de computadora\Configuración de Windows\Configuración de seguridad\
Políticas locales\Política de auditoría\Eventos de inicio de sesión de auditoría

- Grupo de trabajo: Política grupal local:

- Política de computadora local\Configuración de computadora\Configuración de Windows\Configuración de seguridad\
Políticas locales\Política de auditoría\Eventos de inicio de sesión de auditoría

Consulte la Guía del usuario de Change Auditor for Logon Activity para obtener más información sobre su uso y la Guía de referencia de eventos de Change Auditor for Cloud Storage para obtener más información sobre su uso.