DATASHEET

ManageEngine
ADAudit Plus

Un auditor del cambio impulsado por UBA

Proteja su empresa de amenazas internas y ciberataques auditando su Active Directory, servidores de archivos, servidores Windows y estaciones de trabajo con ManageEngine ADAudit Plus.

Auditoría de cambios de Active Directory y Azure AD

- **Audite los cambios de AD:**
  Realice un seguimiento de los cambios en unidades organizativas (OU), usuarios, grupos, equipos, grupos administrativos y otros objetos de AD.

- **Rastree el historial de cambios de los objetos:**
  Reciba informes detallados de auditoría de cambios con información sobre los valores antiguos y nuevos de los atributos modificados.

- **Supervisión de DNS y cambios de esquema:**
  Obtenga visibilidad de la adición, modificación y eliminación de nodos y zonas DNS; supervise los cambios en el esquema y la configuración de AD; y mucho más.

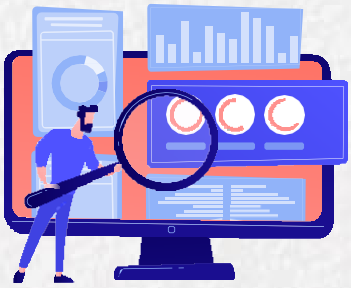
- **Seguimiento de los cambios de permisos de AD:**
  Ver todos los cambios en los permisos de AD, como los realizados en los permisos a nivel de dominio, OUs, esquema, configuración y DNS.

- **Auditoría de la gestión de cuentas de usuario:**
  Seguimiento de la creación, eliminación y modificación de usuarios, restablecimiento de contraseñas y otras acciones de gestión de cuentas.

- **Supervisión de entornos AD híbridos :**
  Obtenga una vista unificada de todas las actividades que tienen lugar en sus entornos locales y Azure AD con alertas para eventos críticos.

Módulos de licencia : Controladores de dominio, Azure AD Tenants

Plataformas compatibles : Windows Server 2003 y superiores



Supervisión de cambios en los archivos

- **Supervisar los accesos a archivos y carpetas:**
  Realice un seguimiento en tiempo real de los intentos de acceso a los archivos (creación, lectura, eliminación, modificación, copia, pegado y traslado).

- **Cambios en los permisos de auditoría:**
  Rastree los cambios de permisos NTFS y comparta junto a detalles como sus valores antiguos y nuevos.

- **Supervisar la integridad de los archivos:**
  Reciba informes detallados sobre todos los cambios realizados en archivos críticos del sistema y de programas, y active alertas cuando se detecte actividad sospechosa.

- **Informe sobre los cambios en los archivos compartidos:**
  Realice un seguimiento de todos los accesos y cambios realizados en los archivos y carpetas compartidos de su dominio con detalles sobre quién accedió a qué, cuándo y desde dónde.

- **Agilizar las auditorías de conformidad:**
  Reciba informes listos para usar con HIPAA, GDPR, FISMA, PCI DSS, SOX, GLBA, ISO 27001, etc.

- **Auditoría en múltiples plataformas:**
  Visualice los cambios en servidores de archivos Windows, clusters de conmutación por error, archivadores NetApp, Synology NAS, Hitachi NAS, EMC VNX, VNXe, Isilon, Celerra y Unity desde una sola consola.

Módulos de licencia :
Windows File Servers, NAS Servers

Plataformas compatibles:
Windows Server 2003 y superiores - Dell VNX, VNXe, Celerra, Unity, and Isilon - Synology DSM 5.0 y superiores - NetApp ONTAP 7.2 y superiores para archivadores - NetApp ONTAP 8.2.1 y superior para clusters - Hitachi NAS 13.2 y superiores - Huawei OceanStor V5 series y OceanStor 9000 V5 sistemas de almacenamiento.

Auditoría de cambios de las configuraciones en las políticas de grupos

- **Auditoría de objetos de política de grupo:** Controle la creación, eliminación y modificación de objetos de directiva de grupo (GPO), etc.

- **Seguimiento de los cambios de configuración de GPO:** Realice un seguimiento de los cambios realizados en la configuración de GPO y vea quién ha cambiado qué configuración, cuándo, desde dónde y los valores de la configuración antes y después del cambio.

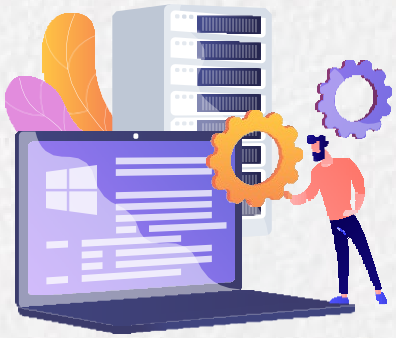
- **Rastrear el historial de cambios de GPO:** Vea el historial de cambios de uno o varios GPO en un dominio para detectar actividades injustificadas.

- **Configurar alertas para cambios críticos:** Active alertas instantáneas por correo electrónico y SMS para cambios críticos, como cambios en la configuración de los ordenadores y en la política de bloqueo de contraseñas y cuentas.

- **Programar informes de modificación de GPO:** Envíe informes programados sobre cambios importantes en GPO o en la configuración de GPO a los destinatarios especificados.

Módulos de licencia: Controladores de dominio

Plataformas compatibles: Windows Server 2003 y superior



Auditoría e informes de servidores Windows

- **Auditar servidores Windows:**
  Supervise los cambios en la pertenencia a grupos administrativos locales, usuarios locales, derechos de usuario, políticas locales, etc.

- **Seguimiento de tareas y procesos programados:**
  Informe sobre la creación, eliminación y modificación de tareas y procesos programados.

- **Monitoreo del uso de USB e impresora:**
  Realice un seguimiento del uso de USB y de las transferencias de archivos a dispositivos de almacenamiento extraíbles. Registra también qué archivo se imprimió, cuándo, por quién, el número de páginas y copias impresas, y mucho más.

- **Auditoría de procesos PowerShell:**
  Supervise los procesos PowerShell que se ejecutan en sus servidores Windows, junto con los comandos que se ejecutan en ellos.

- **Supervisar ADFS, LAPS y ADLDS:**
  Realice un seguimiento de los intentos de autenticación de ADFS, los usuarios que han visto las contraseñas de administrador local, los cambios realizados en la fecha o la hora de caducidad de una contraseña, etc.

Módulos de licencia: Miembros del servidor

Plataformascompatibles : Windows Server 2003 y superiores

Auditoría de inicio y cierre de sesión

- **Auditoría de entradas y salidas:**
  Realice un seguimiento de la actividad de inicio y cierre de sesión y de la duración del inicio de sesión en sus controladores de dominio (DC), servidores Windows y estaciones de trabajo.

- **Seguimiento del historial de inicio de sesión de los usuarios:**
  Registre la actividad de inicio de sesión de cada usuario, identifique a los usuarios que han iniciado sesión en ese momento, enumere los usuarios que han iniciado sesión en varios equipos y mucho más.

- **Auditoría de inicios de sesión RADIUS:**
  Obtenga visibilidad de los inicios de sesión en sus servidores RADIUS con informes sobre inicios de sesión RADIUS, fallos de inicio de sesión e historial de inicio de sesión RADIUS (NPS).

- **Analizar los fallos de inicio de sesión:**
  Realice un seguimiento de todos los intentos fallidos de inicio de sesión con detalles sobre quién intentó iniciar sesión, en qué máquina intentó hacerlo, cuándo y el motivo del fallo.

- **Responder a actividades de inicio de sesión malintencionadas:**
  Aproveche el aprendizaje automático para detectar y responder rápidamente a volúmenes inusuales de fallos de inicio de sesión, tiempos de inicio de sesión inusuales, etc.

Módulos de licencia:
Controladores de dominio, miembros del servidor, estaciones de trabajo.

Plataformas compatibles:
Windows Server 2003 y superiores - Windows XP y superiores

Análisis del bloqueo de cuentas

- **Recibir notificaciones de bloqueo de cuenta:**
  Detecte los bloqueos de cuentas de usuarios AD en tiempo real con alertas por correo electrónico y SMS, y reduzca la duración del bloqueo de cuentas.

- **Encontrar la fuente de bloqueo de la cuenta:**
  Analice los inicios de sesión en teléfonos móviles, las sesiones RDP, los servicios, las tareas programadas y mucho más en busca de credenciales obsoletas, e identifique el origen de los bloqueos de cuentas.

- **Comprobar el estado de bloqueo de la cuenta:**
  Obtenga informes sobre el estado de cada cuenta bloqueada, la hora en que se produjo el bloqueo y mucho más.

- **Examinar el bloqueo de cuentas con UBA:**
  Identifique a los usuarios negligentes y a los intrusos malintencionados detectando actividades de bloqueo anómalas con el análisis del comportamiento de los usuarios (UBA).

- **Mejorar la eficiencia del servicio de asistencia:**
  Visualice reportes con toda la información que necesita el personal del servicio de asistencia para resolver más rápidamente los problemas de bloqueo de cuentas y minimizar el tiempo de inactividad del servicio.

- **Analizar la causa raíz:**
  Mantenga una pista de auditoría clara de los restablecimientos de contraseña, los cambios de contraseña y las fuentes de bloqueo de cuentas para agilizar el análisis forense.

Módulos de licencia:
Controladores de dominio, miembros del servidor, estaciones de trabajo.

Plataformas compatibles:
Windows Server 2003 y superior - Windows XP y superior

Control de la actividad de los empleados

- **Medir la productividad de los empleados:**
  Conozca cómo pasan los empleados sus horas de trabajo con las horas de arranque y apagado del ordenador, los detalles del historial de inicio de sesión, la actividad de los archivos y mucho más.

- **Seguimiento de la asistencia de los empleados:**
  Mantenga hojas de asistencia precisas para sus empleados con sus horas de entrada y salida, y analice la duración de su conexión.

- **Calcular las horas de trabajo reales:**
  Encuentre la lista de usuarios conectados en ese momento y calcule sus horas de trabajo reales con detalles sobre cuándo estuvieron activos y cuándo inactivos.

- **Controlar a los trabajadores a distancia:**
  Realice un seguimiento de los inicios de sesión de la pasarela de escritorio remoto y RADIUS, y sepa quién ha intentado iniciar sesión de forma remota, cuándo, si lo ha conseguido y cuánto ha durado la sesión.

- **Supervisar la actividad informática de los empleados:**
  Encuentra las últimas horas de arranque y apagado de un ordenador, junto con detalles sobre quién lo inició, el tipo de apagado y mucho más.

- **Identificar las actividades de inicio de sesión peligrosas:**
  Detecte y analice los repetidos intentos fallidos de iniciar sesión en estaciones de trabajo, máquinas remotas y servidores críticos con alertas instantáneas por correo electrónico y SMS.

Módulos de licencia :
Estaciones de trabajo

Plataformas compatibles:
Windows XP y superiores

Monitoreo de usuarios con privilegios

- **Auditoría de la actividad del administrador:**
  Realice un seguimiento de las acciones administrativas de los usuarios en el esquema de AD, la configuración, los usuarios, los grupos, las OU, los GPO, etc.

- **Revisar la actividad de los usuarios con privilegios:**
  Cumpla las distintas normativas de TI manteniendo un registro de auditoría de las actividades realizadas por los usuarios con privilegios en su dominio.

- **Detectar la escalada de privilegios:**
  Identifique la escalada de privilegios con informes que documenten el primer uso de privilegios por parte de los usuarios, y verifique si los privilegios de un usuario son necesarios para su función.

- **Detectar anomalías de comportamiento:**
  Identificar las acciones que se desvían de los patrones de acceso normales para encontrar a los atacantes que utilizan credenciales robadas o compartidas de cuentas privilegiadas.

- **Recibir alertas sobre actividades sospechosas:**
  Detecte y responda rápidamente a los eventos de alto riesgo, como el borrado de registros de auditoría o el acceso a datos críticos fuera del horario laboral, con alertas instantáneas.

Módulos de licencia:
Controladores de dominio, miembros del servidor

Plataformas compatibles:
Windows Server 2003 y superior

Detección de malware y amenazas internas

- **Caza de amenazas potenciada por UBA:**
  Detecte rápidamente fallos repetidos en el inicio de sesión, anomalías en la actividad de los usuarios, escalada de privilegios, filtración de datos y mucho más con UBA.

- **Detectar intrusiones de ransomware:**
  Detecte indicadores reveladores de intrusiones de ransomware, como picos inusuales en los eventos de cambio de nombre, eliminación o cambio de permisos de archivos.

- **Responda las amenazas al instante:**
  Ejecute automáticamente secuencias de comandos para cerrar máquinas, sesiones de usuarios finales o llevar a cabo otras respuestas a medida para mitigar las amenazas.

- **Identificar anomalías en la actividad de los archivos:**
  Active alertas para actividades sospechosas, como la eliminación de archivos críticos, aumentos repentinos en el acceso a archivos o actividades de archivos en momentos inusuales.

- **Detectar el movimiento lateral:**
  Detecte indicadores de movimiento lateral como actividad de escritorio remoto fuera de lo común o la ejecución de nuevos procesos.

Módulos de licencia :
Controladores de dominio, miembres del servidor, servidores de archivos Windows, servidores NAS, estaciones de trabajo.

Plataformas compatibles :
Windows Server 2003 y superiores - Dell VNX, VNXe, Celerra, Unity, e Isilon - Synology DSM 5.0 y superior - NetApp ONTAP 7.2 y superiores para archivadores - NetApp ONTAP 8.2.1 y superiores para clusters - Hitachi NAS 13.2 y superiores - Huawei OceanStor V5 series y OceanStor 9000 V5 sistemas de almacenamiento - Windows X y superiores

Informes de cumplimiento

- **Aproveche más de 250 informes:**
  Realice auditorías de cumplimiento fácilmente con informes detallados sobre los cambios en AD, servidores de archivos, servidores Windows y estaciones de trabajo.

- **Reciba informes de auditoría listos para usar:**
  Programe informes periódicos listos para HIPAA, PCI DSS, GDPR, ISO 27001, GLBA, FISMA y SOX,y personalice informes para otras normativas.

- **Realizar un análisis de las causas profundas:**
  En caso de infracción, analice el incidente a fondo, identifique el origen de las filtraciones o intrusiones con datos forenses precisos y comparta sus conclusiones con informes personalizados.

- **Supervisar la integridad de los archivos:**
  Rastrea todos los accesos a archivos del sistema operativo, bases de datos y software; registros e informes de auditoría archivados y otros archivos críticos.

- **Configurar alertas instantáneas:**
  Detecte rápidamente los incidentes de seguridad mediante alertas por correo electrónico y SMS específicas de archivos, usuarios, periodos de tiempo o eventos. Reduzca los falsos positivos con UBA.

- **Mitigue los daños con respuestas automatizadas:**
  Ahorre tiempo crucial con respuestas automatizadas, como la ejecución de secuencias de comandos personalizadas para desactivar cuentas o apagar dispositivos.

Módulos de licencia:
Controladores de dominio, miembres del servidor, servidores de archivos Windows, servidores NAS, estaciones de trabajo.

Plataformas Compatibles:
Windows Server 2003 y superiores - Dell VNX, VNXe, Celerra, Unity, e Isilon - Synology DSM 5.0 y superiores - NetApp ONTAP 7.2 y superiores para archivadores - NetApp ONTAP8.2.1 y superiores para clusters - Hitachi NAS Version 13.2 y superiores - Huawei OceanStor V5 series y OceanStor 9000 V5 sistemas de almacenamiento - Windows XP y superiores

Requisitos del sistema

Para conocer todos los requisitos del sistema, consulte la Guía de inicio rápido.

Navegadores compatibles:
Internet Explorer 8 y superiores, Mozilla Firefox 3.6 y superiores, Google Chrome, Microsoft Edge

Procesador: 2.4GHz

RAM: 8GB

Espacio de disco: 50GB

Plataformas compatibles

Auditoría de DC y servidores miembros	Auditoría de archivos	Otros componentes
Versiones de Windows Server 2003/2003 R2 2008/2008 R2 2012/2012 R2 2016/2016 R2 2019	**Auditoría del servidor de archivos de Windows:** Windows File Server 2003 y superiores **Auditoría de EMC:** VNX, VNXe, Celerra, Unity, Isilon **Auditoría de Synolog:** DSM 5.0 y superior **Auditoría de archivadores NetApp:** Data ONTAP 7.2 y superior **Auditoría de clusters de NetApp:** Data ONTAP 8.2.1 y superior **Auditoría Hitachi NAS:** Hitachi NAS 13.2 y superior **Auditoría de Huawei OceanStor:** OceanStor V5 series y 9000 V5	**Auditoría ADFS:** ADFS 2.0 y superior **Auditoría de estaciones de trabajo:** Windows XP y superior **Auditoría de PowerShell:** PowerShell 4.0 o 5.0

ManageEngine ADAudit Plus

Un auditor de cambios basado en UBA que mantiene su AD, servidores Windows, servidores de archivos y estaciones de trabajo seguros y conformes.

Descargar ahora

Contáctenos

Website:
www.manageengine.com/latam/active-directory-audit/

Demo personalizada:
https://www.manageengine.com/latam/active-directory-audit/solicitud-demo-gratis.html

Cotización:
https://www.manageengine.com/latam/active-directory-audit/obtener-cotizacion.html