ManageEngine
ADAudit Plus

Vista de águila

Cuente con un monitoreo exhaustivo y una mejor visión de los cambios en su entorno Windows Server

ACTIVE DIRECTORY | WORKSTATIONS | FILE SERVERS | MEMBER SERVERS

ManageEngine

DID : +1 408 916 9890
Website : www.adauditplus.com
Support : support@adauditplus.com

Informes

Acceda a los más de 150 informes de auditoría prediseñados gracias a la generación periódica de informes de auditoría, directo en su buzón de entrada. Más de 50 atributos de búsqueda I Programación de informes por email | Filtrar informes en horas laborales / no laborales / todas las horas I Basado en web.

Active Directory

Los administradores pueden hacer seguimiento de todos los eventos de dominio tales como inicio / cierre de sesión, auditoría de usuarios, grupos, computadoras, GPOs, cambios de OU gracias a los más de 150 informes prediseñados y alertas por email. Exportación de informes | Almacenamiento de datos de auditoría | Asignación de roles de operador (vista de informes únicamente) para conformidad ante regulaciones | Mucho, mucho más.

Servidor de archivos

Realice de manera segura el seguimiento de servidores de archivos / FailOver Cluster ante cambios de documentos en archivos (creación / modificación / eliminación de archivos) y auditoría-acceso a carpetas, shares y permisos.

Integridad de archivos

Monitoree intentos de cambios / cambios no autorizados de configuraciones, archivos (log, auditoría, texto, exe, web, configuración, BD) y atributos de archivo (dll, exe y otros archivos de sistema). Garantice la conformidad con los requerimientos de seguridad de Windows Servers y PCI, SOX, HIPAA & FISMA.

Almacenamiento removible

Monitoree cambios en cada dispositivo de almacenamiento removible gracias a los informes sobre todos los cambios en archivos o carpetas, archivos leídos / modificados / copiados y pegados. Esta funcionalidad solamente es soportada con Windows Server 2012 & Windows 8.

Bases de datos

Audite su entorno Windows Server con una variedad de formatos de base de datos: SQL Server, PostgreSQL y MySQL.

Admin

El administrador puede realizar la auditoría y monitoreo gracias a los más de 150 informes prediseñados y alertas instantáneas vía email para obtener un panorama claro de los cambios en el entorno Windows Server.

Conformidad

Obtenga un 'conjunto de informes gráficos detallados' para SOX, HIPAA, GLBA, PCI y FISMA para cumplir fácilmente todos los requisitos de conformidad.

Alertas

Alertas instantáneas en pantalla y envío de alertas a su buzón de entrada. Las alertas de umbrales basadas en usuarios, tiempo y volumen permiten identificar el problema de manera precisa. Notificación por email I Web I Análisis detallado de eventos.

Workstations

Monitoree cada inicio / cierre de sesión y conozca las acciones de usuario diarias mediante informes detallados de cada evento de inicio de sesión fallido / exitoso en las workstations en la red.

Member Server

Monitoree cada cambio en Windows Member Server con diversos informes detallados: informe de resumen, seguimiento de procesos, cambios en políticas, eventos del sistema, administración de objetos y tareas programadas.

NetApp

Audite, monitoree e informe centralizadamente con alertas instantáneas ante cambios en NetApp Filer CIFS Shares. Vea informes sobre archivos creados / modificados / eliminados, cambios en permisos, intentos fallidos de lectura / escritura.

Impresoras

Realice un seguimiento de todos los archivos impresos en la red Windows, con informes exhaustivos sobre el uso de las impresoras, tareas de impresión recientes, informes según usuario / impresora para mayor seguridad y conformidad con SOX, HIPAA.

Otros objetos AD

Realice un seguimiento de otros objetos de AD significativos: contenedores, contactos, esquemas, configuraciones, sitios, DNS y cambios de permisos.

Facilidad de uso

Operado centralizadamente, basado en web, brinda informes detallados pero simples incluso para personal no técnico con alertas que ayudan a responder las cuatro preguntas vitales: 'quién' realizó 'cuál' acción, 'cuando' y desde 'dónde'. Además permite exportar los resultados para análisis en formatos xls, html, pdf y csv.

Almacenamiento de datos

Para controlar el crecimiento de la base de datos, los datos de logs de eventos procesados que son más antiguos que los requeridos para los informes de auditoría inmediatos, pueden eliminarse de la base de datos de ADAudit Plus y pueden almacenarse, ahorrando espacio. Descomprímalos fácilmente para obtener el historial de informes, conformidad y análisis forense.

Auditoría de servidores de archivos Windows

Realice de forma segura el seguimiento de servidores de archivos, NetApp Filers y FailOver Clusters ante accesos, cambios de los documentos en su estructura de archivos y carpetas, shares y permisos. Acceda a informes exclusivos de auditoría de archivos con más de 50 atributos de búsqueda y filtros según informes de usuarios / servidor de archivos / personalizado / para contar con información muy detallada.

- Análisis forense detallado de todos los cambios / intentos no exitosos de creación, eliminación y modificación de archivos y estructura de carpetas.
- Seguimiento de permisos y propietarios de archivos y carpetas.
- Auditoría de Windows FailOver Clusters para un entorno de red seguro, libre de inactividad y en conformidad.
- Monitoreo de creación, modificación, eliminación y cambios de permisos en archivos / carpetas de NetApp Filers CIFS.
- Almacenamiento de datos de eventos por seguridad y análisis forense.

Auditoría de Windows Server

Los Member Servers son los caballos de batalla (de archivos, impresiones, webs, aplicaciones y comunicaciones) de cualquier entorno Microsoft Server. Monitoree cada cambio en Windows Member Server con varios informes detallados: informe de resumen, seguimiento de procesos, cambios de políticas, eventos de sistema, administración de objetos y tareas planificadas.

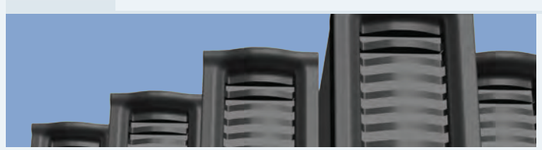
- Monitoreo de Member Servers gracias a su informe de resumen de eventos, seguimiento de tareas programadas y eventos de sistema, seguimiento de todos los procesos y cambios en políticas.
- Monitoreo de integridad de archivos (FIM) del sistema, configuración, modificaciones de archivos y de atributos de archivo.
- Identificación en tiempo real de todos los archivos impresos en la red Windows.
- Listas de detalles de archivos con hora y fecha, nombre de usuario, páginas, copias, nombre de impresora y detalles del servidor.

Auditoría de Active Directory

Por razones de seguridad, es crucial monitorear los cambios en los recursos críticos. ADAudit Plus lista la información completa para hacer seguimiento de la información de los usuarios en cuanto a inicio / cierre de sesión, GPO, GPO avanzado, grupos, computadoras, OUs, configuraciones, DNS, permisos, cambios de esquemas, con más de 150 informes específicos de eventos detallados y alertas instantáneas por email, y además exporta los resultados en formatos xls, html, pdf y csv para ayudar a la interpretación y análisis forense de computadoras.

- Seguimiento de todos los cambios en Windows AD, sistemas, permisos, configuraciones y modificaciones de archivos por el administrador, usuarios, Helpdesk, RR.HH, etc.
- Completo dashboard con todos los datos críticos de auditoría para los dominios configurados.
- Más de 150 informes pre-configurados y establecimiento de alertas ante cambios en carpetas / archivos monitoreados.
- Cumplimiento de PCI, SOX, GLBA, FISMA, HIPAA.... Conformidad con informes de auditoría en formatos XLS, CSV, PDF y HTML.
- Almacenamiento de datos de eventos de AD por seguridad y análisis forense.

Auditoría de workstations



Permite a los administradores ver la hora exacta del inicio / cierre de sesión en una workstation junto con la duración de la sesión. Estos datos críticos son increíblemente fáciles de ver en caso de un ingreso no autorizado o monitoreo regular. Las acciones de workstation de usuario monitoreadas, auditadas e informadas gráficamente son 'duración de la sesión', 'fallos en el inicio de sesión', 'historial de inicio de sesión', 'actividad de Terminal Services', y 'duración de sesión de usuarios en las computadoras'.

- Seguimiento del inicio / cierre de sesión de los usuarios en las workstations.
- Ver informes pre-configurados; automatización de informes periódicos.
- Establecer alertas por email para cuentas críticas, acceso no autorizado.
- Inicios de sesión para auditores de TI como usuarios de sólo lectura para el acceso a los informes.