ManageEngine ADAudit Plus

نظارت هوشمند از نمای بالا

پایش و حسابرسی فایل‌سرورهای ویندوزی (WINDOWS FILE SERVER AUDITING)

امنیت داده‌های خود را با ردیابی دقیق و یکپارچه دسترسی‌ها و تغییرات در محیط‌های ویندوزی تضمین کنید. این راهکار به شما امکان می‌دهد تا تمام ابعاد امنیتی پلتفرم‌های ذخیره‌سازی نظیر فایل‌سرورها، تجهیزات NETAPP FILERS و کلاسترهای FAILOVER را به طور کامل تحت کنترل داشته باشید.

قابلیت‌های کلیدی و مانیتورینگ پیشرفته:

- **ردیابی همه‌جانبه دسترسی‌ها و تغییرات:** پایش دقیق تمام تغییرات اعمال‌شده روی اسناد، ساختار فایل‌ها و پوشه‌ها، اشتراک‌گذاری‌ها (Shares) و مجوزهای دسترسی (Permissions).
- **گزارش‌دهی تخصصی و فیلترینگ هوشمند:** دسترسی به گزارش‌های اختصاصی پایش فایل با بیش از ۵۰ ویژگی جستجو و امکان فیلتر کردن بر اساس کاربر، فایل‌سرور، گزارش‌های سفارشی یا اشتراک‌گذاری‌ها جهت دستیابی به اطلاعات دقیق و شفاف.
- **تحلیل جرم‌شناسی و کالبدشکافی دقیق خطاها (Detailed Forensics):** ثبت و تحلیل جزئیات تمامی تغییرات و تلاش‌های ناموفق برای ایجاد، حذف یا تغییر فایل‌ها و ساختار پوشه‌ها.
- **کنترل دارنده و مجوزهای دسترسی:** نظارت پیوسته بر سطوح دسترسی (Permissions) فایل‌ها و پوشه‌ها و شناسایی دقیق مالکان (Owners) داده‌ها.
- **حسابرس کلاسترهای ویندوزی (FailOver Clusters):** پایش مداوم کلاسترهای FailOver ویندوز به منظور تضمین امنیت، انطباق با استانداردهای حفاظتی (Compliance) و جلوگیری از قطعی شبکه.
- **پایش تجهیزات لایه‌بندی داده NetApp (NetApp Filers):** مانیتورینگ دقیق فرآیندهای ایجاد، تغییر، حذف و اصلاح مجوزهای دسترسی در فایل‌ها و پوشه‌های تحت پروتکل CIFS.

پایش و حسابرسی سرورهای ویندوز (WINDOWS SERVER AUDITING)

سرورهای عضو (MEMBER SERVERS) اعم از سرورهای فایل، پرینت، وب، اپلیکیشن و ارتباطات، ستون فقرات و موتورهای محرک هر زیرساخت ویندوزی به شمار می‌روند. این راهکار با ارائه گزارش‌های دقیق، امنیت و پایداری این سرورهای حیاتی را تضمین می‌کند.

نظارت همه‌جانبه بر تغییرات سرور (MEMBER SERVER MONITORING): با استفاده از ابزارهای نظارتی پیشرفته، تمامی رویدادها و تغییرات ساختاری سرورها را ردیابی کرده و به گزارش‌های جامع زیر دسترسی داشته باشید:

- **گزارش خلاصه رویدادها:** دریافت نمایه کلی از وضعیت و حوادث سرور.
- **ردیابی فرآیندها (Process Tracking):** پایش تمام فعالیت‌ها و فرآیندهای در حال اجرا بر روی سیستم.
- **تغییرات سیاست‌های امنیتی (Policy Changes):** نظارت بر هرگونه تغییر در پولیسی‌ها و سطوح دسترسی.
- **رویدادهای سیستمی و وظایف زمان‌بندی‌شده:** ردیابی مداوم رویدادهای سیستم (System Events) و تسک‌های زمان‌بندی‌شده (Scheduled Tasks).

نظارت همه‌جانبه بر تغییرات سرور (MEMBER SERVER MONITORING): با استفاده از ابزارهای نظارتی پیشرفته، تمامی رویدادها و تغییرات ساختاری سرورها را ردیابی کرده و به گزارش‌های جامع زیر دسترسی داشته باشید:

قابلیت‌های ویژه و استراتژیک:

- **نظارت بر یکپارچگی فایل‌ها (FIM - File Integrity Monitoring):** پایش پیوسته و هوشمند هرگونه تغییر، دستکاری یا اصلاح در فایل‌های اصلی سیستم، تنظیمات پیکربندی (Configuration)، ساختار فایل‌ها و ویژگی‌های آن‌ها (File Attributes).
- **حسابرس و مانیتورینگ آنی فرآیند پرینت (Print Auditing):** شناسایی و ردیابی لحظه‌ای (Real-time) تمامی فایل‌های پرینت‌شده در بستر شبکه ویندوز. این ویژگی گزارش دقیقی از جزئیات زیر را در اختیار شما قرار می‌دهد:

1-نام کاربری، تاریخ و ساعت دقیق پرینت | 2-تعداد صفحات، تعداد کپی‌ها و حجم فایل. | 3- نام چاپگر و مشخصات سرور مربوطه.

پایش و حسابرسی جامع اکتیو دایرکتوری (ACTIVE DIRECTORY AUDITING)

به دلایل امنیتی، مانیتورینگ تغییرات در منابع حیاتی شبکه امری ضروری است. ADAUDIT PLUS تمامی اطلاعات لازم را برای ردیابی رویدادهای ورود/خروج کاربران، تغییرات GPO، ADVANCED GPO، گروه‌ها، کامپیوترها، OU، تنظیمات، DNS، مجوزها و اسکیما (SCHEMA) فراهم می‌کند. این نرم‌افزار با ارائه بیش از ۱۵۰ گزارش دقیق و رویدادمحور و همچنین هشدارهای ایمیلی آنی، امکان خروجی گرفتن از نتایج در فرمت‌های PDF، HTML، XLS و CSV را جهت تحلیل و جرم‌شناسی رایانه‌ای (COMPUTER FORENSICS) میسر می‌سازد.

ویژگی‌های کلیدی:

ردیابی همه‌جانبه کاربران و ادمین‌ها: ثبت و پایش ریزترین تغییرات در سطوح دسترسی، تنظیمات و فایل‌ها توسط ادمین‌ها، کاربران عادی، تیم پشتیبانی (Helpdesk)، منابع انسانی (HR) و غیره.

داشبورد مدیریتی واحد (Single Dashboard): نمایش متمرکز و یکپارچه تمامی داده‌های حیاتی حسابرسی و مانیتورینگ برای تمامی دامین‌های پیکربندی‌شده در یک پنل واحد.

بیش از ۱۵۰ گزارش پیش‌فرض و هشدارهای آنی: دسترسی به بیش از ۱۵۰ قالب گزارش تخصصی (رویدادمحور) به همراه امکان فعال‌سازی هشدارهای ایمیلی لحظه‌ای (Instant Alerts) به محض تغییر در پوشه‌ها یا فایل‌های تحت نظارت.

انطباق با استانداردها: برآورده کردن الزامات و استانداردهای سخت‌گیرانه بین‌المللی نظیر HIPAA، FISMA، GLBA، SOX، PCI و غیره از طریق گزارش‌های حسابرسی با فرمت‌های PDF، CSV، XLS و HTML.

آرشیو داده‌ها: بایگانی و آرشیو کردن اطلاعات رویدادهای اکتیو دایرکتوری (AD Event Archiving) جهت استفاده در سناریوهای بلندمدت امنیتی و جرم‌شناسی رایانه‌ای.

پایش و حسابرسی ایستگاه‌های کاری (WORKSTATIONS AUDITING)

مدیران شبکه می‌توانند زمان دقیق ورود و خروج کاربران (LOGON & LOGOFF) را به همراه مدت‌زمان حضور آن‌ها (LOGON DURATION) مشاهده کنند. دسترسی به این داده‌های حیاتی، نظارت منظم و بررسی سریع در صورت بروز دسترسی‌های غیرمجاز را بسیار آسان می‌کند. تمامی اقدامات کاربران در ایستگاه‌های کاری پایش، حسابرسی و در قالب گزارش‌های گرافیکی شامل «مدت‌زمان اتصال»، «ورودهای ناموفق»، «تاریخچه ورودها»، «فعالیت‌های ترمینال سرویس (تراکنش‌های ریموت)» و «مدت‌زمان اتصال کاربران در کامپیوترهای مختلف» ارائه می‌شود.

ویژگی‌های کلیدی:

- **ردیابی ورود و خروج:** پایش دقیق زمان ورود و خروج کاربران به ایستگاه‌های کاری (Workstations).
- **گزارش‌های پیش‌فرض و خودکار:** دسترسی به گزارش‌های از پیش تنظیم‌شده و امکان خودکارسازی فرآیند گزارش‌گیری دوره‌ای از طریق زمان‌بندی (Scheduled Reports).
- **هشدارهای ایمیلی هوشمند:** قابلیت تنظیم هشدارهای ایمیلی برای حساب‌های کاربری حساس و تلاش‌های مربوط به دسترسی‌های غیرمجاز.
- **دسترسی اختصاصی ممیزی:** امکان تعریف دسترسی‌های ویژه برای حسابرسان (IT Auditors) با قابلیت «فقط مشاهده» (View-only) گزارش‌ها.

ManageEngine
ADAudit Plus

REPORTS

مشاهده بیش از ۱۵۰ گزارش پیش‌فرض ممیزی به همراه قابلیت صدور و ارسال خودکار و دوره‌ای گزارش‌ها مستقیم به ایمیل شما. دارای بیش از ۵۰ ویژگی جستجو زمان‌بندی ارسال ایمیلی گزارش‌ها | امکان فیلتر کردن گزارش‌ها بر اساس ساعات کاری / غیرکاری / تمام ساعات | مبتنی بر مرورگر (تحت وب).

ACTIVE DIRECTORY

امکان ردیابی تمامی رویدادهای دامین مانند ورود/خروج کاربران و حسابرسی تغییرات مربوط به کاربران، گروه‌ها، کامپیوترها، GPO و OU توسط مدیران شبکه، به همراه بیش از ۱۵۰ گزارش آماده و هشدارهای ایمیلی. قابلیت خروجی گرفتن از گزارش‌ها | آرشیو داده‌های ممیزی | امکان تخصیص نقش اپراتور (فقط مشاهده گزارش‌ها) جهت تطبیق با استانداردهای حفاظتی | و بسیاری قابلیت‌های دیگر.

FILE SERVER

ردیابی امن فایل‌سرورها و کلاسترهای FAILOVER جهت مانیتورینگ تغییرات اسناد و فایل‌ها (ایجاد، تغییر و حذف فایل) به همراه حسابرسی دسترسی به پوشه‌ها، اشتراک‌گذاری‌ها و مجوزها

FILE INTEGRITY

پایش تمامی تغییرات ناموفق یا غیرمجاز در تنظیمات، فایل‌ها (مانند فایل‌های لاگ، ممیزی، متنی، اجرایی، وب، پیکربندی و پایگاه داده) و ویژگی‌های فایل (نظیر فایلهای dll، exe و سایر فایل‌های سیستمی). تضمین امنیت سرورهای ویندوز و برآورده کردن الزامات و استانداردهای حفاظتی نظیر PCI، SOX، HIPAA و FISMA.

REMOVABLE STORAGE

پایش تمامی تغییرات در انواع تجهیزات ذخیره‌سازی قابل حمل، به همراه ارائه گزارش از تمام تغییرات فایل‌ها و پوشه‌ها شامل خواندن، تغییر دادن، و کپی و پیست کردن فایل‌ها. نکته: این قابلیت تنها در ویندوز سرور 2012 و ویندوز 8 (و نسخه‌های بعد از آن) پشتیبانی می‌شود.

DATABASES

قابلیت حسابرسی و مانیتورینگ زیرساخت سرورهای ویندوز با امکان انتخاب و پشتیبانی از انواع پایگاه‌های داده: MYSQL و SQL SERVER، POSTGRESQL.

ADMIN

امکان مانیتورینگ و حسابرسی زیرساخت توسط مدیر شبکه با استفاده از بیش از ۱۵۰ گزارش پیش‌فرض و هشدارهای ایمیلی آنی، جهت ایجاد اشراف و دیدی شفاف نسبت به تمامی تغییرات در محیط سرورهای ویندوز.

COMPLIANCE

دسترسی به مجموعه‌ای اختصاصی از گزارش‌های گرافیکی و دقیق برای استانداردهای PCI، GLBA، HIPAA، SOX و FISMA جهت برآورده کردن آسان تمامی الزامات و

DATA ARCHIVING

جهت کنترل رشد حجم پایگاه داده، می‌توان داده‌های پردازش‌شده‌ی رویدادها (EVENT LOGS) را که قدیمی‌تر از بازه زمانی مورد نیاز برای گزارش‌های ممیزی فوری هستند، از دیتابیس ADAUDIT PLUS پاکسازی و آرشیو کرد تا در فضای ذخیره‌سازی صرفه‌جویی شود. همچنین امکان خارج کردن آسان این داده‌ها از حالت فشرده (UNZIP) جهت گزارش‌گیری از سوابق، احراز انطباق با استانداردها و تحلیل‌های جرم‌شناسی دیجیتال (FORENSIC ANALYSIS) وجود دارد.

ALERTS

ارسال آنی هشدارهای درون‌برنامه‌ای (روی صفحه) و ارسال همزمان اعلان‌ها به ایمیل شما! قابلیت تعریف آستانه مجاز (THRESHOLD) بر اساس کاربر، زمان و حجم رویدادها جهت شناسایی دقیق و مینیاتوری مشکلات. اعلان‌های ایمیلی | تحت وب | تحلیل عمیق رویدادها

WORKSTATIONS

پایش تمامی فرآیندهای ورود و خروج کاربران و اشراف بر فعالیت‌های روزانه آن‌ها، به همراه گزارش‌های دقیق از تمامی رویدادهای موفق یا ناموفق ورود (LOGON) در سطح ایستگاه‌های کاری شبکه

MEMBER SERVER

پایش تمامی فرآیندهای ورود و خروج کاربران و اشراف بر فعالیت‌های روزانه آن‌ها، به همراه گزارش‌های دقیق از تمامی رویدادهای موفق یا ناموفق ورود (LOGON) در سطح ایستگاه‌های کاری شبکه

NETAPP

حسابرسی، مانیتورینگ و گزارش‌دهی متمرکز به همراه هشدارهای آنی برای تمامی تغییرات در اشتراک‌گذاری‌های CIFS در تجهیزات NETAPP FILER. مشاهده گزارش‌های مربوط به ایجاد، تغییر و حذف فایل‌ها، تغییرات مجوزها، و تلاش‌های ناموفق برای خواندن یا نوشتن فایل‌ها

PRINTERS

ردیابی تمام فایل‌های چاپ‌شده در شبکه ویندوز، به همراه گزارش‌های جامع از میزان مصرف پرینتر، دستورات چاپ اخیر (Print Jobs)، و گزارش‌های مجزا بر اساس کاربر یا پرینتر جهت ارتقای امنیت و تضمین انطباق با استانداردهای SOX و HIPAA

OTHER AD OBJECTS

ردیابی و پایش سایر اشیاء حیاتی اکتیو دایرکتوری شامل: کانتینرها (CONTAINERS)، مخاطبین (CONTACTS)، اسکیما (SCHEMA)، تنظیمات (CONFIGURATION)، سایت‌ها (SITES)، سرویس DNS و تمامی تغییرات مربوط به مجوزها

سهولت در استفاده

مدیریت متمرکز، تحت وب و ارائه گزارش‌های دقیق اما ساده حتی برای پرسنل غیرفنی به همراه سیستم هشداردهی، جهت پاسخ به چهار سوال حیاتی : " چه کسی" ، "چه کاری" را در "چه زمانی" و از "کجا" انجام داده است! همچنین امکان خروجی گرفتن از نتایج در قالب‌های PDF، HTML، XLS و CSV جهت تحلیل و بررسی بیشتر.