DATENBLATT

ManageEngine
ADAudit Plus

Eine UBA-unterstützte Change-Auditing-Lösung

Schützen Sie Ihr Unternehmen vor Insider-Threats und Cyberattacken, indem Sie alle Änderungen in Ihrem Active Directory (AD), auf Dateiservern, Windows-Servern und Workstations mit ManageEngine ADAudit Plus überwachen und auditieren.

Change-Auditing für Active Directory und Entra ID

- **AD-Änderungen überwachen:**
  Verfolgen Sie Änderungen an Organisationseinheiten (OUs), Benutzern, Gruppen, Computern, Verwaltungsgruppen und anderen AD-Objekten.

- **Änderungshistorie von Objekten nachvollziehen:**
  Erhalten Sie detaillierte Change-Audit-Reports mit Informationen über die alten und neuen Werte der geänderten Attribute.

- **Monitoring von DNS- and Schema-Änderungen:**
  Verschaffen Sie sich einen Überblick über neu hinzugefügte, geänderte oder gelöschte DNS-Nodes und -Zonen. Überwachen Sie Änderungen an AD-Schema-Daten und -Konfigurationen und vieles mehr.

- **Änderungen an AD-Berechtigungen verfolgen:**
  Lassen Sie sich alle Änderungen an AD-Berechtigungen anzeigen, z. B. an Domänen-, OU-, Schema-, Konfigurations- und DNS-Berechtigungen.

- **Audit der Benutzerkontenverwaltung:**
  Verfolgen Sie die Erstellung, Löschung und Änderung von Benutzerkonten, Passwort-Zurücksetzungen und andere Account-Management-Aktionen.

- **Monitoring von hybriden AD-Umgebungen:**
  Erhalten Sie einen umfassenden Überblick über alle Aktivitäten in Ihrer lokalen und Entra-ID- Umgebung mit Warnmeldungen für kritische Ereignisse.

Lizenz-Module:
Domain-Controller, Entra-ID-Tenants

Unterstützte Plattformen:
- Windows Server 2003 und höher

Monitoring von Dateiänderungen

- **Überwachung von Datei- und Ordnerzugriffen:**
  Verfolgen Sie erfolgreiche und fehlgeschlagene Dateizugriffsversuche in Echtzeit – einschließlich Aktionen wie „Erstellen“, „Lesen“, „Löschen“, „Ändern“, „Kopieren“, „Einfügen“ sowie „Verschieben“.

- **Audit von Berechtigungsänderungen:**
  Verfolgen Sie Änderungen an NTFS- und Freigabeberechtigungen inklusive Details wie die alten und neuen Werte.

- **Dateiintegritäts-Monitoring:**
  Erhalten Sie detaillierte Berichte über alle Änderungen an kritischen System- und Programmdateien und lassen Sie sich mittels Warnmeldungen alarmieren, wenn verdächtige Aktivitäten erkannt werden.

- **Bericht über Änderungen an Dateifreigaben:**
  Verfolgen Sie jeden Zugriff und jede Änderung an freigegebenen Dateien und Ordnern in Ihrer Domäne mit Details darüber, wer wann und von wo aus auf was zugegriffen hat.

- **Compliance-Audits:**
  Nutzen Sie die vorkonfigurierten und sofort einsatzbereiten Berichte, um die Compliance mit DSGVO, ISO 27001, SOX, PCI DSS, HIPAA, FISMA, GLBA etc. nachzuweisen.

- **Plattform-übergreifendes Auditing:**
  Überwachen Sie Änderungen auf Windows-Dateiservern, Failover-Clustern, NetApp-Filern, Synology NAS, Hitachi NAS, EMC VNX, VNXe, Isilon, Celerra und Unity in einer zentralen Benutzeroberfläche.

Lizenz-Module:
Windows-Dateiserver, NAS-Server

Unterstützte Plattformen:
• Windows Server 2003 und höher • Dell VNX, VNXe, Celerra, Unity und Isilon • Synology DSM 5.0 und höher • NetApp ONTAP 7.2 und höher (für Filer) • NetApp ONTAP 8.2.1 und höher (für Cluster) • Hitachi NAS 13.2 und höher • Huawei OceanStor V5 Serie und OceanStor 9000 V5 Speichersysteme

Change-Auditing für Gruppenrichtlinien

- **Audit von Gruppenrichtlinienobjekten:**
  Überwachen Sie Aktionen wie das Erstellen, Löschen oder Ändern von Gruppenrichtlinien-objekten (Group Policy Objects (GPO)).

- **Monitoring von Änderungen an den GPO-Einstellungen:**
  Verfolgen Sie Änderungen an den GPO-Einstellungen und sehen Sie, wer welche Einstellung wann und von wo aus geändert hat, sowie die Werte der Einstellung vor und nach der Änderung.

- **Monitoring der GPO-Änderungshistorie:**
  Sehen Sie sich die Änderungshistorie eines oder mehrerer GPOs in einer Domäne an, um unerwünschte Aktivitäten zu erkennen.

- **Konfiguration von Benachrichtigungen für kritische Änderungen:**
  Lassen Sie sich sofort per E-Mail- oder SMS-Benachrichtigung über kritische Änderungen z. B. an den Computer-konfigurationen, Passwort- oder Kontosperr-Richtlinien informieren.

- **Regelmäßige GPO-Änderungsberichte:**
  Planen Sie Berichte zu wichtigen GPO- oder GPO-Einstellungsänderungen, die regelmäßig an bestimmte Empfänger versendet werden.

Lizenz-Module:
Domänen-Controller

Unterstützte Plattformen:
- Windows Server 2003 und höher

Windows-Server-Auditing und -Reports

- **Auditing der Windows-Server:**
  Überwachen Sie Änderungen an lokalen administrativen Gruppenmitgliedschaften, lokalen Benutzern, Benutzerrechten, lokalen Richtlinien und mehr.

- **Geplante Aufgaben und Prozesse überwachen:**
  Erstellen Sie Berichte über die Erstellung, Löschung und Änderung geplanter Aufgaben und Prozesse.

- **Monitoring von USB- und Druckernutzung:**
  Überwachen Sie die USB-Nutzung sowie Dateitransfers auf Wechseldatenträger. Erfassen Sie außerdem, welche Datei wann, von wem und wie oft gedruckt wurde, inklusive Anzahl der Seiten und Kopien.

- **Audit der PowerShell-Prozesse:**
  Überwachen Sie PowerShell-Prozesse, die auf Ihren Windows-Servern ausgeführt werden, zusammen mit den dabei ausgeführten Befehlen.

- **ADFS-, LAPS- und ADLDS-Monitoring:**
  Überwachen Sie ADFS-Authentifizierungsversuche, Benutzer, die sich lokale Administrator-Passwörter angesehen haben, Änderungen an der Gültigkeitsdauer oder dem Ablaufdatum eines Passworts und vieles mehr .

Lizenz-Module:
Member-Server

Unterstützte Plattformen:
- Windows Server 2003 und höher

Auditing der An- und Abmeldungen

- **Audit der Log-ons und Log-offs:**
  Überwachen Sie die An- und Abmeldeaktivitäten sowie die Anmeldedauer auf Ihren Domain-Controllern (DCs), Windows-Servern und Workstations.

- **Historie der Benutzeranmeldungen protokollieren:**
  Protokollieren Sie die Anmeldeaktivitäten aller Benutzer, identifizieren Sie Benutzer, die gerade angemeldet sind oder an mehreren Computern angemeldet sind, und vieles mehr.

- **Audit der RADIUS-Anmeldungen:**
  Verschaffen Sie sich einen Überblick über Anmeldungen auf Ihren RADIUS-Servern mit Berichten zu RADIUS-Anmeldungen, Anmeldefehlern und zur RADIUS-(NPS)-Anmeldehistorie.

- **Analyse von Anmeldefehlern:**
  Erfassen Sie alle fehlgeschlagenen Anmeldeversuche mit Details darüber, wer wann versucht hat, sich auf einem bestimmten Computer anzumelden, und aus welchem Grund die Anmeldung fehlgeschlagen ist.

- **Reaktion auf böswillige Anmeldeaktivitäten:**
  Erkennen Sie durch maschinelles Lernen ungewöhnlich viele Anmeldefehler, ungewöhnliche Anmeldezeiten etc. und reagieren Sie umgehend darauf.

Lizenz-Module:
Domain-Controller, Member-Server, Workstations

Unterstützte Plattformen:
• Windows Server 2003 und höher • Windows XP und höher

Analyse von Account-Sperrungen

- **Benachrichtigungen zu Kontosperrungen erhalten:**
  Erkennen Sie Sperrungen von AD-Benutzerkonten in Echtzeit mit E-Mail- und SMS-Benachrichtigungen und reduzieren Sie die Dauer der Kontosperrungen.

- **Ursache für Kontosperrungen ermitteln:**
  Analysieren Sie Anmeldungen über Mobiltelefone, RDP-Sitzungen, Dienste, geplante Aufgaben usw., um veraltete Anmeldedaten zu finden und die Ursache für die Kontosperrung zu ermitteln.

- **Status von Kontosperrungen überprüfen:**
  Sie können Berichte über den Status jedes gesperrten Kontos, das Datum der Sperrung und vieles mehr abrufen.

- **Kontosperrungen mit UBA untersuchen:**
  Identifizieren Sie fahrlässige Benutzer und böswillige Insider, indem Sie mit Hilfe von User Behavior Analytics (UBA) ungewöhnliche Account-Lockout-Aktivitäten erkennen.

- **Effizienz des Helpdesks verbessern:**
  Erstellen Sie Berichte mit allen Informationen, die das Helpdesk-Personal benötigt, um Probleme rund um gesperrte Konten schneller zu lösen und die Serviceausfallzeiten zu minimieren.

- **Analyse der Root Cause:**
  Führen Sie einen lückenlosen Audit-Trail für Passwortänderungen und -zurücksetzungen sowie zu den Quellen für Kontosperrungen, um die forensische Analyse zu optimieren.

Lizenz-Module:
Domain-Controller, Member-Server, Workstations

Unterstützte Plattformen:
• Windows Server 2003 und höher • Windows XP und höher

Monitoring von Benutzeraktivitäten

- **Produktivitätsmessung:**
  Start- und Shutdown-Zeiten von Computern, Anmeldehistorie, Dateiaktivitäten und mehr helfen, Produktivitätstrends zu verstehen.

- **Anwesenheitszeiten dokumentieren:**
  Erfassen Sie die Ein- und Ausstempelzeiten Ihrer Anwender und deren Anmeldedauer.

- **Berechnung aktiver Zeiten:**
  Ermitteln Sie die derzeit angemeldeten Benutzer und erhalten Sie Informationen zu aktiven Zeiten.

- **Monitoring von Remote-Anmeldungen:**
  Dokumentieren Sie Anmeldungen über Remote-Desktop-Gateways sowie RADIUS-Anmeldungen inklusive Details zu Anmeldezeitpunkt, -erfolg und Sitzungsdauer.

- **Monitoring von Computer-Aktivitäten:**
  Lassen Sie sich bei Bedarf die letzten Start- und Shutdown-Zeiten eines Computers anzeigen, inklusive Details darüber, wer diese initiiert hat, die Art des Shutdowns und mehr.

- **Identifikation riskanter Anmeldeaktivitäten:**
  Erkennen und analysieren Sie mehrfach fehlgeschlagene Anmeldeversuche an Workstations, Remote-Computern und kritischen Servern mit sofortigen E-Mail- und SMS-Benachrichtigungen.

Lizenz-Module:
Workstations

Unterstützte Plattformen:
- Windows XP und höher

Privileged User Monitoring

- **Auditing von Administrator-Aktivitäten:**
  Dokumentieren Sie Benutzerverwaltungsaktionen, wie Änderungen an AD-Schemadaten, Konfigurationen, Benutzern, Gruppen, OUs, GPOs und mehr.

- **Aktivitäten privilegierter Benutzer überprüfen:**
  Erfüllen Sie verschiedene IT-Vorschriften, indem Sie einen Audit-Trail aller Aktivitäten privilegierter Benutzer in Ihrer Domäne erstellen.

- **Berechtigungserweiterungen erkennen:**
  Identifizieren Sie die Ausweitung von Berechtigungen mit Berichten, die die erstmalige Nutzung von Privilegien durch Benutzer dokumentieren und überprüfen Sie, ob die Berechtigungen für die Rolle und Aufgaben eines Benutzers erforderlich sind.

- **Anomalien im Benutzerverhalten erkennen:**
  Erkennen Sie verdächtige Aktivitäten, die vom normalen Zugriffsmuster abweichen, um Angreifer aufzuspüren, die gestohlene oder weitergegebene Anmeldedaten privilegierter Konten verwenden.

- **Warnungen für verdächtige Aktivitäten einrichten:**
  Erkennen Sie schnell kritische Ereignisse wie das Löschen von Audit-Protokollen oder den Zugriff auf sensible Daten außerhalb der Geschäftszeiten und reagieren Sie mit Hilfe von Warnmeldungen sofort darauf.

Lizenz-Module:
Domain-Controller, Member-Server

Unterstützte Plattformen:
- Windows Server 2003 und höher

Erkennung von Malware und Insider-Bedrohungen

- **UBA-gestützte Bedrohungserkennung:**
  Erkennen Sie mit UBA schnell sich wiederholende Anmeldefehler, Anomalien in der Benutzeraktivität, die Ausweitung von Privilegien, die Exfiltration von Daten etc.

- **Ransomware-Angriffe erkennen:**
  Erkennen Sie verräterische Anzeichen für Ransomware-Angriffe, z. B. ungewöhnlich viele Dateiumbenennungen, Löschungen oder Berechtigungsänderungen.

- **Sofortige Reaktion auf Bedrohungen:**
  Minimieren Sie Bedrohungen durch die automatische Ausführung von Skripten zum Herunterfahren von Endpoints, Beenden von Benutzersitzungen oder Ausführen anderer benutzerdefinierter Reaktionen.

- **Identifizieren von Anomalien in Dateiaktivitäten:**
  Lassen Sie Alarme für verdächtige Aktivitäten auslösen. Dazu gehören das Löschen kritischer Dateien, ein plötzlicher Anstieg von Dateizugriffen oder Dateiaktivitäten zu ungewöhnlichen Zeiten.

- **Laterale Bewegungen erkennen:**
  Erkennen Sie Indikatoren für laterale Bewegungen wie ungewöhnliche Remote-Desktop-Aktivitäten oder die Ausführung neuer Prozesse.

Lizenz-Module:
Domain-Controller, Member-Server, Windows-Dateiserver, NAS-Server, Workstations

Unterstützte Plattformen:
• Windows Server 2003 und höher • Dell VNX, VNXe, Celerra, Unity und Isilon • Synology DSM 5.0 und höher • NetApp ONTAP 7.2 und höher (für Filer) • NetApp ONTAP 8.2.1 und höher (für Cluster) • Hitachi NAS 13.2 und höher • Huawei OceanStor V5 Serie und OceanStor 9000 V5 Speichersysteme • Windows XP und höher

Compliance-Berichte

- **Mehr als 250 Berichte:**
  Detaillierte Berichte über Änderungen an AD, Dateiservern, Windows-Servern und Workstations erleichtern Compliance-Audits.

- **Sofort einsatzbereite Audit-Berichte:**
  Planen Sie regelmäßige, vorgefertigte Berichte für DSGVO, ISO 27001, PCI DSS, FISMA, SOX, GLBA oder HIPAA und passen Sie Berichte für andere Vorschriften an.

- **Root-Cause-Analysen durchführen:**
  Analysieren Sie Datenlecks gründlich, ermitteln Sie die Quelle von Lecks oder Eindringlingen mit präzisen forensischen Daten und teilen Sie Ihre Erkenntnisse mit individuellen Berichten.

- **Monitoring der Dateiintegrität:**
  Verfolgen Sie jeden Zugriff auf Betriebssystem-, Datenbank- und Software-Dateien, archivierte Audit-Protokolle und -Berichte sowie auf andere kritische Dateien.

- **Konfiguration sofortiger Benachrichtigungen:**
  Erkennen Sie Sicherheitsvorfälle schnell mithilfe von E-Mail- und SMS-Benachrichtigungen, die auf Dateien, Benutzer, Zeiträume oder Ereignisse zugeschnitten sind. Reduzieren Sie Fehlalarme mit UBA.

- **Schadensbegrenzung durch automatische Reaktionen:**
  Gewinnen Sie wertvolle Zeit durch automatisierte Reaktionen wie die Ausführung individueller Skripte, um Konten zu deaktivieren oder Geräte auszuschalten.

Lizenz-Module:
Domain-Controller, Member-Server, Windows-Dateiserver, NAS-Server, Workstations

Unterstützte Plattformen:
• Windows Server 2003 und höher • Dell VNX, VNXe, Celerra, Unity und Isilon • Synology DSM 5.0 und höher • NetApp ONTAP 7.2 und höher (für Filer) • NetApp ONTAP 8.2.1 und höher (für Cluster) • Hitachi NAS Version 13.2 und höher • Huawei OceanStor V5 Serie und OceanStor 9000 V5 Speichersysteme • Windows XP und höher

System-anforderungen

Die vollständigen Systemanforderungen finden Sie im englischen Quick Start Guide.

Unterstützte Browser:
Internet Explorer 8 und höher, Mozilla Firefox 3.6 und höher, Google Chrome, Microsoft Edge
Prozessor: 2.4GHz
RAM: 8GB
Festplattenspeicher: 50GB

Unterstützte Plattformen

Weitere Informationen zu den unterstützten Plattformen finden Sie im englischen Quick Start Guide.

Verfügbare Editionen

FREE EDITION	STANDARD EDITION	PROFESSIONAL EDITION
Unbegrenzt gültig » Datenaudit und -erfassung von 25 Workstations » Erstellung von Berichten aus den während der Evaluationsphase gesammelten Protokolldaten Jetzt testen	Alle Funktionen der Free Edition + » Berichte und Alarme zu Ereignisprotokolldaten von diesen lizenzierten Komponenten: • Domain-Controller • Azure AD-Tenants • Windows-Server • Workstations • Windows-Dateiserver • NAS-Geräte Jetzt testen	Alle Funktionen der Standard-Edition + » Analyse von Account-Sperrungen » Change-Auditing für AD-Berechtigungen » Change-Auditing für GPO-Einstellungen » Change-Auditing für DNS- und AD-Schema-Daten » Alte und neue Werte bei Änderungen der AD-Objektattribute » Unterstützung von MS SQL-Datenbanken » Und vieles mehr Jetzt testen

ManageEngine ADAudit Plus

Eine UBA-unterstützte Change-Auditing-Lösung, die Sicherheit und Compliance für Ihr AD, Ihre Windows-Server, Dateiserver und Workstations gewährleistet.

Download

Kostenlose, 30 Tage gültige Testversion

Kontakt

Website:
www.manageengine.de/adauditplus

Ihr ManageEngine-Partner:
MicroNova AG | Unterfeldring 6 |
D-85256 Vierkirchen

E-Mail:
sales-ManageEngine@micronova.de

Support:
www.manageengine.de/support