FICHA TÉCNICA

ManageEngine
ADAudit Plus

Um auditor de mudanças orientado por UBA

Proteja sua empresa contra ameaças internas e ataques cibernéticos auditando seu Active Directory (AD), servidores de arquivos, Windows servers e estações de trabalho com o ADAudit Plus da ManageEngine.

Auditoria de mudanças do Active Directory e Azure AD

- **Audite mudanças do AD:**
  Rastreie as alterações em unidades organizacionais (UOs), usuários, grupos, computadores, grupos administrativos e outros objetos do AD.

- **Rastreie o histórico de mudanças de objetos:**
  Receba relatórios detalhados de auditoria de mudanças com informações sobre os valores antigos e novos dos atributos alterados.

- **Monitore mudanças de DNS e schema:**
  Obtenha visibilidade sobre a adição, modificação e exclusão de nós e zonas de DNS, monitore mudanças de schemas e configuração do AD, e muito mais.

- **Rastreie as mudanças de permissões do AD:**
  Veja todas as alterações nas permissões do AD, como aquelas realizadas em permissões no nível de domínio, unidades organizacionais, schema configuração e DNS.

- **Gerenciamento de contas de usuários de auditoria:**
  Rastreie a criação, exclusão e modificação de usuários, redefinições de senhas, e outras ações de gerenciamento de contas.

- **Monitore ambientes híbridos do AD:**
  Obtenha uma visão unificada de todas as atividades que ocorrem nos ambientes locais e do Azure AD com alertas para eventos críticos.

Módulos de licença:
Controladores de domínio, locatários do Azure AD

Plataformas suportadas:
Windows Server 2003 e superior

Monitoramento de mudanças de arquivos

- **Monitore os acessos a arquivos e pastas:**
  Rastreie tentativas de acesso a arquivos bem-sucedidas e fracassadas, incluindo a criação, leitura, exclusão, modificação, copiar e colar, e movimentação — em tempo real.

- **Mudanças de permissões de auditoria:**
  Rastreie o NTFS e compartilhe mudanças de permissões, juntamente com detalhes como valores antigos e novos.

- **Monitore a integridade dos arquivos:**
  Receba relatórios detalhados sobre todas as mudanças realizadas em arquivos críticos do sistema e de programas e acione alertas quando atividades suspeitas forem detectadas.

- **Relatório sobre mudanças no compartilhamento de arquivos:**
  Rastreie todos os acessos e mudanças realizados em arquivos e pastas compartilhados no seu domínio com detalhes sobre quem acessou o quê, quando e de onde.

- **Simplifique as auditorias de conformidade:**
  Receba relatórios out-of-the-box sobre HIPAA, GDPR, FISMA, PCI DSS, SOX, GLBA, ISO 27001, e muito mais.

- **Auditoria em diversas plataformas:**
  Veja as alterações em servidores de arquivos do Windows, clusters de failover, arquivadores NetApp, Synology NAS, Hitachi NAS, EMC VNX, VNXe, Isilon, Celerra e Unity em um único console.

Módulos de licença:
Servidores de arquivos Windows, servidores NAS

Plataformas suportadas:
• Windows Server 2003 e superior • Dell VNX, VNXe, Celerra, Unity e Isilon • Synology DSM 5.0 e superior • NetApp ONTAP 7.2 e superior para arquivadores • NetApp ONTAP 8.2.1 e superior para clusters • Hitachi NAS 13.2 e superior • Sistemas de armazenamento série Huawei OceanStor V5 e OceanStor 9000 V5

Auditoria de mudanças de configurações de Políticas do Grupo

- **Audite objetos de políticas do grupo:**
  Acompanhe a criação, exclusão, modificação do Objeto de Políticas do Grupo (GPO), e muito mais.

- **Rastreie as mudanças nas configurações do GPO:**
  Rastreie as mudanças realizadas nas configurações do GPO e veja quem alterou qual configuração, quando, de onde e os valores da configuração antes e depois da alteração.

- **Rastreie o histórico de mudanças do GPO:**
  Veja o histórico de mudanças de um ou vários GPOs em um domínio para detectar atividades não justificadas.

- **Configuração de alertas para mudanças críticas:**
  Acione alertas instantâneos por e-mail e SMS para mudanças críticas, como alterações na configuração do computador e na política de bloqueio de senhas e contas.

- **Agende relatórios de mudanças do GPO:**
  Envie relatórios agendados sobre alterações importantes do GPO ou suas configurações para destinatários específicos.

Módulos de licença:
Controladores de Domínio

Plataformas suportadas:
Windows Server 2003 e superior

Auditoria e relatórios do Windows Server

- **Windows servers de auditoria:**
  Monitore mudanças nas associações de grupos administrativos locais, usuários locais, direitos de usuários, políticas locais, e muito mais.

- **Rastreie tarefas e processos agendados:**
  Relatório sobre a criação, exclusão e modificação de tarefas e processos agendados.

- **Monitore o uso de USB e impressoras:**
  Rastreie o uso de USB e transferências de arquivos para dispositivos de armazenamento removíveis. Rastreie também qual arquivo foi impresso, quando, por quem, o número de páginas e cópias impressas, e muito mais.

- **Auditoria de processos do PowerShell:**
  Monitore os processos do PowerShell executados nos seus Windows servers, juntamente com os comandos executados neles.

- **Monitore o ADFS, LAPS e ADLDS:**
  Rastreie tentativas de autenticação de ADFS, usuários que viram senhas de administradores locais, alterações feitas na hora ou data de expiração de uma senha, e muito mais.

Módulos de licença:
Servidores membro

Plataformas suportadas:
Windows Server 2003 e superior

Auditoria de login e logoff

- **Logons e logoffs de auditoria:**
  Rastreie a atividade de login e logoff e a duração do login nos seus controladores de domínio (DCs), Windows servers e estações de trabalho.

- **Analise falhas de login:**
  Rastreie todas as tentativas de login malsucedidas com detalhes sobre quem tentou efetuar o login, em qual máquina, quando e o motivo da falha.

- **Rastreie o histórico de logins do usuário:**
  Registre a atividade de login de cada usuário, identifique os usuários que estão conectados no momento, liste os usuários conectados em várias máquinas, e muito mais.

- **Responda à atividade de login maliciosa:**
  Aproveite o machine learning para detectar e responder rapidamente a volumes incomuns de falhas de login, tempos de login não usuais, e muito mais.

- **Auditoria de logins do RADIUS:**
  Obtenha visibilidade dos logins nos seus servidores RADIUS com relatórios sobre logins do RADIUS, falhas de login e histórico de login do RADIUS (NPS).

Módulos de licença:
Controladores de domínio, Member Servers, estações de trabalho

Plataformas suportadas:
• Windows Server 2003 e superior • Windows XP e superior

Análise de bloqueios de conta

- **Receba notificações de bloqueio de contas:**
  Detecte bloqueios de contas de usuários do AD em tempo real com alertas por e-mail e SMS e reduza a duração desses bloqueios.

- **Encontre a origem do bloqueio de contas:**
  Analise logins de telefones celulares, sessões de RDP, serviços, tarefas agendadas e muito mais em busca de credenciais obsoletas e identificação da origem dos bloqueios de contas.

- **Verifique o status de bloqueio de contas:**
  Obtenha relatórios sobre o status de cada conta bloqueada, o horário em que o bloqueio ocorreu, e muito mais.

- **Examine os bloqueios de contas com o UBA:**
  Identifique usuários negligentes e pessoas mal-intencionadas detectando atividades anormais de bloqueio com análise de comportamento do usuário (UBA).

- **Melhore a eficiência do help desk:**
  Veja relatórios com todas as informações exigidas pela equipe de help desk para resolver problemas de bloqueio de contas com mais rapidez e minimizar o tempo de inatividade do serviço.

- **Analise a causa raiz:**
  Mantenha uma trilha de auditoria clara de redefinições de senhas, alterações de senhas e fontes de bloqueio de contas para agilizar a análise forense.

Módulos de licença:
Controladores de domínio, Member Servers, estações de trabalho

Plataformas suportadas:
• Windows Server 2003 e superior • Windows XP e superior

Monitoramento de atividade dos funcionários

- **Mensure a produtividade dos funcionários:**
  Saiba como os funcionários gastam suas horas de trabalho com horários de inicialização e desligamento de computadores, detalhes do histórico de login, atividade de arquivos e muito mais.
- **Rastreie frequência dos funcionários:**
  Mantenha folhas de ponto precisas para seus funcionários com seus horários de entrada e saída e analise a duração do login.
- **Calcule as horas de trabalho reais:**
  Encontre a lista de usuários conectados no momento e calcule suas horas de trabalho reais, com detalhes sobre quando eles estavam ativos e ociosos.
- **Monitore trabalhadores remotos:**
  Rastreie logins de gateway de desktop remoto e RADIUS e saiba quem tentou efetuar o login remotamente, quando, se ele foi bem-sucedido e quanto tempo durou a sessão.
- **Monitore a atividade dos computadores dos funcionários:**
  Encontre horários recentes de inicialização e desligamento de um computador, juntamente com detalhes sobre quem o iniciou, o tipo de desligamento, e muito mais.
- **Identifique atividades de login arriscadas:**
  Identifique e analise repetidas tentativas fracassadas de efetuar o login em estações de trabalho, máquinas remotas e servidores críticos com alertas instantâneos por e-mail e SMS.

Módulos de licença:
Estações de trabalho

Plataformas suportadas:
Windows XP e superior

Monitoramento de usuários privilegiados

- **Atividade do administrador de auditoria:**
  Rastreie ações administrativas de usuários em schema, configurações, usuários, grupos, UOs, GPOs do AD, e muito mais.

- **Revise a atividade de usuários privilegiados:**
  Cumpra diversas regulamentações de TI mantendo uma trilha de auditoria das atividades realizadas por usuários privilegiados no seu domínio.

- **Detecte a escalação de privilégios:**
  Identifique o escalonamento de privilégios com relatórios que documentam o uso de privilégios pelos funcionários pela primeira e verifique se os privilégios de um usuário são necessários para sua função.

- **Detecte anomalias comportamentais:**
  Identifique ações que fogem dos padrões normais de acesso para encontrar invasores que usam credenciais roubadas ou compartilhadas de contas privilegiadas.

- **Receba alertas sobre atividades suspeitas:**
  Identifique e responda rapidamente a eventos de alto risco, como a limpeza de registros de auditoria ou o acesso a dados críticos fora do horário comercial, com alertas instantâneos.

Módulos de licença:
Controladores de domínio, Member Servers

Plataformas suportadas:
Windows Server 2003 e superior

Detecção de malware e ameaças internas

- **Caça a ameaças com tecnologia de UBA:**
  Identifique rapidamente falhas repetidas de login, anomalias na atividade dos usuários, escalações de privilégios, exfiltração de dados, e muito mais, com o UBA.

- **Detecte invasões de ransomware:**
  Identifique indicadores que revelam invasões de ransomware, como picos incomuns em eventos de renomeação, exclusão ou alteração de permissão de arquivos.

- **Responda às ameaças instantaneamente:**
  Execute scripts automaticamente para desligar máquinas, finalizar sessões de usuários ou realizar outras respostas personalizadas para mitigar ameaças.

- **Identifique anomalias de atividade de arquivos:**
  Acione alertas para atividades suspeitas, como exclusão de arquivos críticos, picos repentinos no acesso a arquivos ou atividades de arquivos em momentos incomuns.

- **Detecte o movimento lateral:**
  Identifique indicadores de movimento lateral, como atividades incomuns no desktop remoto ou execução de novos processos.

Módulos de licença:
Controladores de domínio, Member Servers, servidores de arquivos Windows, servidores NAS, estações de trabalho

Plataformas suportadas:
• Windows Server 2003 e superior • Dell VNX, VNXe, Celerra, Unity e Isilon • Synology DSM 5.0 e superior • NetApp ONTAP 7.2 e superior para arquivadores • NetApp ONTAP 8.2.1 e superior para clusters • Hitachi NAS 13.2 e superior • Sistemas de armazenamento série Huawei OceanStor V5 e OceanStor 9000 V5 • Windows XP e superior

Relatórios de conformidade

- **Utilize mais de 250 relatórios:**
  Realize auditorias de conformidade facilmente com relatórios detalhados sobre mudanças no AD, servidores de arquivos, Windows servers e estações de trabalho.

- **Receba relatórios de auditoria out-of-the-box:**
  Agende relatórios periódicos e prontos para HIPAA, PCI DSS, GDPR, ISO 27001, GLBA, FISMA e SOX e personalize relatórios para outras regulamentações.

- **Realize uma análise de causa raiz:**
  No caso de uma violação, analise o incidente minuciosamente, identifique a origem dos vazamentos ou invasões com dados forenses precisos e compartilhe suas descobertas com relatórios personalizados

- **Monitore a integridade dos arquivos:**
  Rastreie todos os acessos ao sistema operacional, banco de dados e arquivos de software; logs e relatórios de auditoria arquivados; e outros arquivos críticos.

- **Configure alertas instantâneos:**
  Detecte incidentes de segurança rapidamente usando alertas por e-mail e SMS específicos para arquivos, usuários, períodos ou eventos. Reduza os falsos positivos com UBA.

- **Mitigue os danos com respostas automatizadas:**
  Economize um tempo crucial com respostas automatizadas, como a execução de scripts personalizados para desabilitar contas ou desligar dispositivos.

Módulos de licença:
Controladores de domínio, Member Servers, servidores de arquivos Windows, servidores NAS, estações de trabalho

Plataformas suportadas:
• Windows Server 2003 e superior • Dell VNX, VNXe, Celerra, Unity e Isilon • Synology DSM 5.0 e superior • NetApp ONTAP 7.2 e superior para arquivadores • NetApp ONTAP 8.2.1 e superior para clusters • Hitachi NAS versão 13.2 e superior • Sistemas de armazenamento série Huawei OceanStor V5 e OceanStor 9000 V5 • Windows XP e superior

Requisitos do sistema

Para os requisitos completos do sistema, consulte o Guia de Início Rápido.

Navegadores suportados:
Internet Explorer 8 e superior, Mozilla Firefox 3.6 e superior, Google Chrome, Microsoft Edge
Processador: 2,4 GHz
RAM: 8 GB
Espaço em disco: 50 GB

Plataformas suportadas

Auditoria de DC e member server	Auditoria de arquivos	Outros componentes
Versões do Windows Server: 2003/2003 R2 2008/2008 R2 2012/2012 R2 2016/2016 R2 2019	**Auditoria de servidores de arquivos Windows:** Servidor de arquivos do Windows 2003 e superior **Auditoria de EMC:** VNX, VNXe, Celerra, Unity, Isilon **Auditoria do Synology:** DSM 5.0 e superior **Auditoria de arquivadores NetApp:** Dados do ONTAP 7.2 e superior **Auditoria de cluster de NetApp:** Dados do ONTAP 8.2.1 e superior **Auditoria de NAS Hitachi:** Hitachi NAS 13.2 e superior **Auditoria do Huawei OceanStor:** Série OceanStor V5 e 9000 V5	**Auditoria de ADFS** ADFS 2.0 e superior **Auditoria de estações de trabalho:** Windows XP e superior **Auditoria de PowerShell:** PowerShell 4.0 ou 5.0

ManageEngine ADAudit Plus

Um auditor de mudanças orientado por UBA que mantém seu AD, Windows servers, servidores de arquivos e estações de trabalho seguros e anuentes.

Baixe agora

Teste grátis de 30 dias

Detalhes de contato

Site:
www.adauditplus.com.br

Demonstração personalizada:
https://www.manageengine.com/br/active-directory-audit/demo-form.html

Faça uma cotação:
https://www.manageengine.com/br/active-directory-audit/get-quote.html

Suporte técnico por e-mail:
tech-br@manageengine.com

Consultas de vendas:
latam-sales@manageengine.com