Tivoli software

IBM Tivoli Access Manager for Operating Systems

Destaque

- Defenda-se contra uma das principais ameaças de segurança que as empresas enfrentam: comportamento inadequado de usuários internos e funcionários.
- Ajude a obter segurança de autorização minuciosa para sistemas UNIX e Linux, tanto para administradores como para usuários.
- Agilize o gerenciamento de sistemas UNIX® e Linux® heterogêneos com administração integrada e delegada.
- Use recursos extensíveis e configuráveis de auditoria para documentar a conformidade com regulamentos governamentais, políticas corporativas e outras ordens de segurança.
- Aproveite modelos de política de segurança descritos nas melhores práticas para ajudar a minimizar o esforço e o tempo de implementação.
- Aproveite a segurança e a auditoria de categoria de mainframe em um produto leve e fácil de usar.

Atenda aos desafios atuais de segurança

Funcionários – não hackers ou vírus – são a maior ameaça à segurança de TI. Usuários internos respondem pela maioria dos casos de ciber-roubo e dano maldoso a sistemas corporativos. Eles sabem onde ficam os dados mais importantes e os momentos em que estão mais vulneráveis.

Administradores UNIX e Linux bem-intencionados podem acidentalmente deixar vulneráveis seus sistemas e aplicativos críticos para os negócios. Esses administradores costumam criar rotas de acesso por "porta dos fundos" que os hackers exploram com frequência.

Apenas as defesas de limite seguro não fornecem proteção adequada para seus sistemas de negócios críticos. Os ataques vêm de muitas formas, muitas vezes explorando as fraquezas de aplicativos e outros protocolos de alto nível. Um objetivo comum desses ataques é obter direitos irrestritos de "superusuário" sobre os sistemas-alvo.

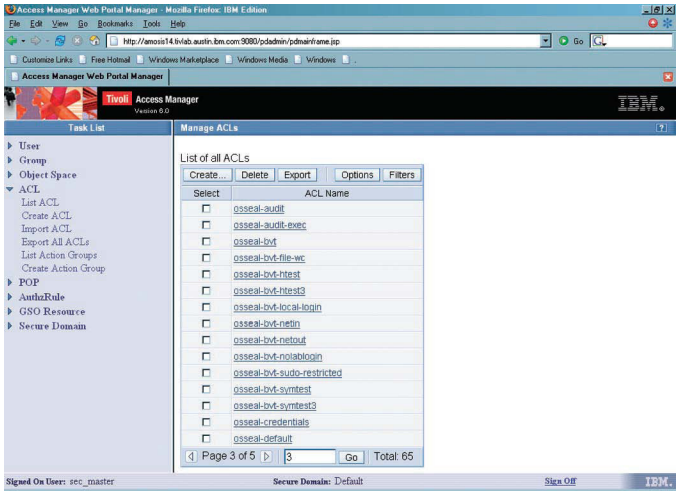
Para defender seus sistemas e aplicativos críticos para os negócios contra essas ameaças internas e externas, sua empresa precisa de uma solução de segurança minuciosa guiada por políticas. Proteger sua infraestrutura de servidores com o IBM Tivoli Access Manager for Operating Systems é um passo vital para facilitar a conformidade com políticas de segurança corporativa e requisitos regulamentares. Ele pode fornecer autorização minuciosa – a recurso do sistema de arquivos, serviços de rede remota e local, serviços de login, mudanças de identidade de usuário e de grupo, e muito mais. Por mais importante que seja proteger seus sistemas, é igualmente importante auditar a conformidade com a política de segurança. A auditoria não só é exigida por regulamentos federais e boas práticas corporativas, mas ajuda a identificar brechas na política de segurança. Por exemplo, usando o Tivoli Access Manager for Operating Systems, os auditores podem determinar se os administradores estão usando seus privilégios de forma adequada. Se houver atividade imprópria, o Tivoli Access Manager for Operating Systems permite que a política de segurança seja restrita adicionalmente.

Trate da segurança de forma consistente em toda a empresa.
O software IBM Tivoli inclui um portfólio abrangente de soluções de gerenciamento de identidade e segurança. Um componente integrante desse conjunto corporativo é o Tivoli Access Manager for Operating Systems, que fornece controle de acesso minucioso baseado na identidade do usuário, bem como serviços de auditoria para os ambientes dos sistemas operacionais UNIX e Linux.

Componentes compartilhados no portfólio de gerenciamento de segurança Tivoli fornecem interfaces consistentes com o usuário e modelos de segurança que uma organização pode usar para ajudar a garantir a segurança de vários recursos dentro da empresa. A administração de uma política consistente facilita para os administradores de segurança definir políticas exatas e mais abrangentes baseadas em identidade e reduz os erros que criam brechas na segurança que os hackers e malware podem atacar.

O software de gerenciamento de segurança Tivoli também aproveita o inovador IBM Tivoli Common Auditing and Reporting Service para ajudar a simplificar a conformidade com requisitos de políticas corporativas e regulamentares. Essa plataforma comum inclui:

- *Coleta de dados de auditoria centralizada.*
- *Gerenciamento de log de auditoria.*
- *Recursos de geração de relatório.*



O Tivoli Access Manager for Operating Systems fornece uma interface de usuário administrativo intuitiva para ajudá-lo a definir uma política de segurança exata e consistente.

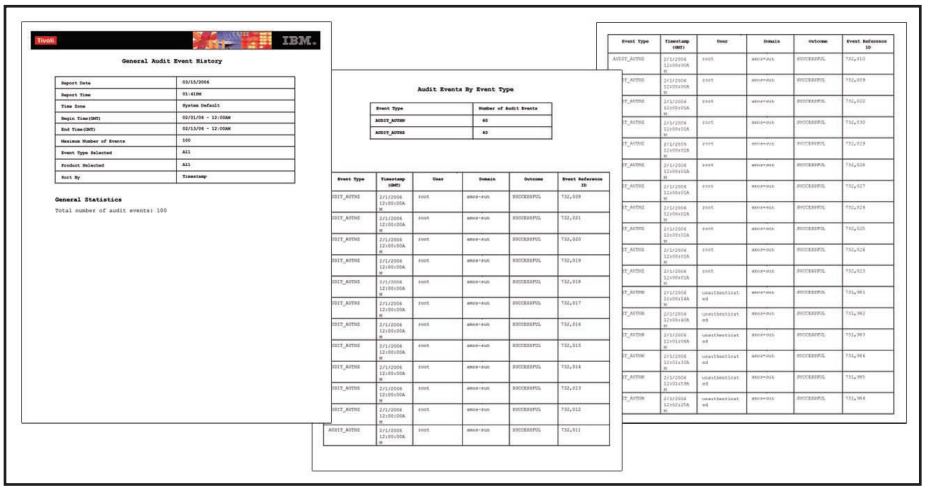
Ajude a simplificar a administração de segurança usando ferramentas flexíveis.
O Tivoli Access Manager for Operating Systems inclui Web Portal Manager, uma ferramenta de gerenciamento acessível via Web, baseada em GUI. Essa ferramenta permite que você gerencie a política de segurança em um formato apontar e clicar. As interfaces da linha de comandos, acomodação de scripts e APIs para C e Java™ fornecem aos especialistas em UNIX e Linux ferramentas que eles podem usar para agilizar e automatizar várias tarefas de gerenciamento.

Além disso, o Web Portal Manager dá aos gerentes de segurança a flexibilidade para delegar autoridade limitada em questões de rotina ou emergência para os administradores locais de subdomínio ou unidades de negócios – sem sacrificar o controle. No caso de interrupção de rede, por exemplo, pode-se delegar o controle para administradores locais de subdomínio sem lhes dar acesso excessivo ou acesso a outros subdomínios.

O Tivoli Access Manager for Operating Systems também ajuda a simplificar a administração permitindo que você agrupe os sistemas UNIX e Linux que compartilham necessidades de segurança específicas. É possível então gerenciar esse conjunto de recursos como grupo em vez de gerenciar cada sistema individualmente.

Além disso, o recurso de gerenciamento de política multidimensional do Tivoli Access Manager for Operating Systems permite que os administradores definam a política de acesso com base em vários atributos diferentes de um recurso. O resultado é que os administradores podem se esforçar significativamente menos ao lidar com recursos similares e não precisam mais sincronizar manualmente as políticas entre esses recursos.

Estabeleça rapidamente uma política de segurança com base em boas práticas
Quando a empresa estiver pronta para desenvolver rapidamente uma segurança eficaz, você pode usar o Fast Track Policy Modules do Tivoli Access Manager for Operating Systems para facilitar a customização. Essas políticas de segurança pré-escritas com base em boas práticas vêm em versões específicas para cada aplicativo para facilitar a adaptação da política de segurança a missões específicas. Melhor ainda, você pode usar o Web Portal Manager para customizar os modelos de política baseados em boas práticas a fim de que se ajustem às suas necessidades exclusivas.



O Tivoli Access Manager for Operating Systems permite que os auditores customizem e gerem relatórios facilmente entre domínios e até mesmo sobre usuários root privilegiados.

Por exemplo, você pode procurar melhorar a segurança Web ou defender os aplicativos de gerenciamento de relação com o cliente, os aplicativos de planejamento de recursos corporativos, outros aplicativos e bancos de dados. Os Fast Track Policy Modules o ajudam a combinar sua política de segurança com suas metas de negócios.

Faça auditoria de eventos relacionados à segurança de forma flexível.
Para facilitar a conformidade com seus requisitos de auditoria, o Tivoli Access Manager for Operating Systems fornece ferramentas poderosas e flexíveis de auditoria. É possível usar o software para manter a segurança constante sobre logs de auditoria referentes a usuários, programas, arquivos, portas, recursos e sistemas. Os administradores podem usar relatórios centralizados sobre eventos de segurança para repassar como e quando certos usuários acessaram os recursos.

A coleta segura e gerenciamento de dados de auditoria é também crítica para facilitar a conformidade com a política de segurança corporativa e com requisitos regulamentares. Assim, o Tivoli Access Manager for Operating Systems se integra com o Tivoli Common Auditing and Reporting Service. Quando são coletados dados para o log de auditoria de uma variedade de fontes, é mais fácil gerenciar e gerar relatórios sobre dados de auditoria.

Inclua o gerenciamento de identidade nas contas de superusuários.
As contas não monitoradas de superusuários (ou “root”) são famosas por abrirem a porta para uso impróprio. O uso compartilhado de contas root por várias pessoas aumenta a vulnerabilidade e os problemas de prestação de contas inerentes aos sistemas UNIX e Linux. O Tivoli Access Manager for Operating Systems responde a essa ameaça oferecendo controles baseados no usuário para contas de superusuários UNIX e Linux, ajudando a evitar o uso impróprio, acidental ou deliberado, desses aplicativos e dados.

O software controla e faz um log das atividades de cada usuário que usa essas contas root. Visto que nem mesmo um superusuário pode modificar os logs de auditoria do software para remover vestígios de suas ações, sua organização pode, de forma confiável, registrar e monitorar as atividades dos usuários privilegiados no seu ambiente.

Diferentemente de ofertas da concorrência, o Tivoli Access Manager for Operating Systems fornece esses controles sem acrescentar o fardo administrativo de alterar seus processos de negócios.

Os administradores podem continuar a executar suas tarefas sem alterar seus procedimentos operacionais. A proteção se aplica quer os usuários acessem os recursos do sistema diretamente pelo sistema operacional, quer por meio de um shell de comando ou aplicativo. O design multiencadeado do Tivoli Access Manager for Operating Systems acrescenta essa segurança rigorosa sem impedir os aplicativos nem causar impacto no trabalho do usuário.

Para clientes que precisam de completa percepção das mudanças de certos programas críticos, o Tivoli Access Manager for Operating Systems permite definí-los como parte de uma Trusted Computing Base (TCB). Arquivos que fazem parte da TCB são monitorados quanto a mudanças na sua assinatura. Se o Tivoli Access Manager for Operating Systems detecta que a integridade de um programa definido na TCB está comprometida, ele registra esse programa como "não confiável" e não permite que ele seja executado até que um administrador recoloque-o explicitamente na lista de programas confiáveis.

Sobre o software Tivoli da IBM

O software Tivoli da IBM ajuda as organizações a gerenciar efetiva e eficazmente recursos, tarefas e processos de tecnologia da informação (TI) para atender requisitos empresariais em constante mudança e entregar um gerenciamento dos serviços de TI flexível e ágil, enquanto ajuda a reduzir custos. O portfólio da Tivoli compreende software de segurança, conformidade, armazenamento, desempenho, disponibilidade, configuração, operações e gerenciamento do ciclo de vida de TI, e conta com o apoio dos serviços, suporte e pesquisa de classe mundial da IBM.

Para mais informações

Para aprender mais sobre as soluções de gerenciamento de segurança Tivoli e as soluções integradas da IBM, entre em contato com o representante de vendas IBM ou com o Parceiro de Negócios IBM, ou acesse:

ibm.com/tivoli/solutions/security

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo – Brasil

O site da IBM pode ser encontrado em:
ibm.com

Produzido nos Estados Unidos da América
04-06

G325-6788-03-PT