BeyondTrust

SOLUTION BRIEF

15 Casos de Uso de Gerenciamento de Privilégios em Servidores Unix e Linux

Este White Paper foi elaborado para que os gestores de TI e de segurança saibam como as soluções de gerenciamento de privilégios nos endpoints para ambientes Unix & Linux, e Active Directory Bridge podem ajudá-los a aprimorar os controles de segurança de acessos privilegiados e eliminar o sudo, centralizando os processos de gestão, auditoria e de elaboração de relatórios.

Índice

Sumário Executivo 2

15 Casos de Uso de Gerenciamento de Privilégios em Servidores 3

1. Eliminando a Necessidade de Fazer Login Como Root 3
2. Obtendo Conformidade para Contas Root 3
3. Quando o Sudo Não é Mais o Suficiente.....3
4. Controlando Permissões e Acessos aos Sistemas de Arquivos.....4
5. Controlando Acessos e Auditando Ações de Script 4
6. Controlando os Acessos Até o Nível do Sistema 4
7. Consolidando Logs de Eventos, Relatórios e Análises.....5
8. Forense - O Tempo é Essencial 5
9. Gravação de Sessão (O que é Digitado é Visto) 6
10. Obtendo o Gerenciamento de Senhas e a Restrição de Privilégios 6
11. Integrando o Gerenciamento de Senhas Privilegiadas à Execução de Comandos.....6
12. Gerenciamento Centralizado de Controles de Políticas Sudo 6
13. Armazenamento Centralizado de Dados de Auditoria Sudo 7
14. Consolidando Contas e Diretórios 7
15. Estendendo as Políticas De Grupo Para Sistemas Não Windows 8

A plataforma de Gerenciamento de Acessos Privilegiados BeyondTrust ...8

Próximos passos.....8

Sumário Executivo

O conceito de restrição de privilégios determina que os usuários devem ter o mínimo de privilégios de acesso necessário para realizar uma tarefa. No entanto, muitas funções básicas do sistema operacional, gerenciamento, aplicações e software (por exemplo, utilitários de configuração) requerem mais do que privilégios básicos. Consequentemente, os usuários necessitam de privilégios elevados na forma de usuários e senhas de administrador, ou root. Para minimizar os riscos de privilégios excessivos, as empresas devem eliminar a necessidade de uso de credenciais root e de admin – e se possível nem revelá-las aos usuários finais –porém sem impactar a produtividade.

A solução de gerenciamento de privilégios nos endpoints da BeyondTrust (Endpoint Privilege Management) permite que as equipes de TI gerenciem quem pode acessar servidores Unix, Linux e Windows, e o que esses usuários fazem com esses acessos. Com isso, as empresas melhoram a segurança dos servidores, simplificam implantações de gerenciamento de acessos privilegiados e garantem a produtividade.

O Endpoint Privilege Management inclui recursos para:

- Descobrir, gerenciar e monitorar automaticamente os acessos a senhas root, admin e outras senhas privilegiadas, além de chaves SSH;
- Elevar comandos e delegar privilégios com controles refinados, fornecendo gestão robusta sobre o que os usuários Windows, Unix e Linux podem fazer depois de realizar login em um sistema;
- Habilitar o SSO (Single Sign on) e a política simplificada, consolidando contas de várias plataformas em um único conjunto de políticas de controle de acesso;
- Fornecer visibilidade de risco para aplicações direcionadas à elevação de privilégios;
- Analisar, registrar e gerar relatórios sobre o comportamento de senhas, usuários e contas privilegiadas.

Este white paper explica casos de uso comuns para gerenciamento de privilégios em servidores Unix/Linux, incluindo os recursos disponíveis no Privilege Management for Unix & Linux e no Active Directory Bridge (AD Bridge), que fazem parte da solução de gerenciamento de privilégios em endpoints da BeyondTrust. Esses casos de uso são progressivos, sendo os mais diretos listados primeiro, seguidos pelos de maior complexidade.

15 casos de uso de Gerenciamento de Privilégios em Servidores

1. Eliminando a Necessidade de Fazer Login Como Root

Muitos usuários de sistemas e aplicações Unix/Linux usam a frase "Eu preciso de root", indicando que eles só podem executar suas funções diárias de trabalho se logados utilizando o os recursos de usuário mais poderoso do sistema, "root". Root é frequentemente chamado de usuário "Deus", pois praticamente não há nada que o usuário root não possa fazer.

O uso de uma conta root implica na impossibilidade de auditar as ações de um indivíduo (especialmente permitindo o compartilhamento de contas), além de inibir o uso de uma senha forte e mutável, em função de várias pessoas usarem a conta e usufruirem de seus privilégios. O uso da conta root e de práticas como o compartilhamento de contas aumentam drasticamente o risco de ameaças internas através de comportamentos maliciosos e acidentais, além das ameaças externas.

A solução Privilege Management for Unix & Linux implementa um modelo de delegação de privilégios mínimos que pode eliminar ou restringir muito o uso da conta root - sem prejudicar o trabalho dos usuários. Com a ferramenta, os usuários podem executar qualquer comando com elevação de privilégios, de acordo com a política estabelecida. A “não necessidade” de se logar como root permite que a conta do usuário root tenha controles de segurança muito mais rígidos ou seja movida para um sistema de gerenciamento de senhas como o BeyondTrust Password Safe.

2. Obtendo Conformidade Para a Contas Root

Os administradores de sistemas podem, ocasionalmente, precisar usar a conta root em virtude de alterações feitas no nível do sistema, ou simplesmente em função da natureza *ad-hoc* dos comandos que eles precisam executar.

No entanto, o time de compliance precisa monitorar TODAS as atividades e garantir a “responsabilidade” pelas ações. Para permitir que os administradores acessem uma conta privilegiada, as equipes de compliance precisam das ferramentas e processos corretos para poder identificar quem está usando a conta root, quando e quais alterações são feitas por esse usuário. Além disso, é imperativo que os arquivos de log sejam imunes a qualquer tipo de violação.

O Privilege Management for Unix & Linux permite que as contas padrão subam ao nível root com o registro completo da sessão, fornecendo uma trilha de auditoria centralizada e de forma transparente para cada administrador de sistema.

3. Quando o Sudo não é maiso suficiente

O sudo existe há muito tempo, mas à medida que o número de sistemas e usuários cresce, gerenciá-lo tornou-se uma tarefa extremamente demorada. Além das limitações de controle disponíveis no sudo, os sistemas agora parecem estar expostos a um número crescente de ameaças internas e externas à segurança.

O Privilege Management for Unix & Linux fornece uma linguagem de política muito mais flexível, permitindo que políticas granulares sejam criadas no nível de comando e de sistema. A solução da BeyondTrust aumenta a segurança de várias maneiras, como por exemplo,

retirando informações de políticas e dados de login das estações de trabalho ou do servidor dos usuários, ou utilizando tecnologias de criptografia para dados em trânsito e em repouso.

4. Controlando Permissões e Acessos aos Sistemas de Arquivos

Os sistemas de arquivos autorizam a configuração de permissões individuais de arquivos e pastas, como leitura, gravação, execução, etc. No entanto, as permissões de arquivos e pastas são de natureza estática e precisam ser definidas em cada host. Também existem riscos ao permitir que contas altamente privilegiadas (como root) acessem um servidor ou estação de trabalho, pois uma conta com esse tipo de privilégio pode facilmente manipular permissões e configurações de propriedade usando comandos como "chmod" e "chown". Oferecer acesso ilimitado a arquivos e dados de uma conta pode representar um risco significativo.

Nossa solução Privilege Management for Unix & Linux resolve esse dilema, permitindo que a configuração de tempo de execução seja controlada centralmente, protegendo assim as contas privilegiadas. As políticas de controle e auditoria avançados (Advanced Control and Audit – ACA) do Privilege Management for Unix & Linux podem ser aplicadas dinamicamente, admitindo a imposição de regras de permissão do sistema de arquivos durante determinados períodos, ou consentindo o acesso apenas se determinadas condições forem atendidas (como a autenticação de dois fatores ou fornecendo um número válido no sistema de ticketing).

Com esse recurso, é possível conceder aos usuários acesso no nível 'root', mas, ao mesmo tempo, impedir que o usuário root possa acessar qualquer arquivo de usuário armazenado em '/ home', ou permitir a execução de scripts, mas não a visualização ou edição dos mesmos.

5. Controlando Acessos e Auditando Ações de Script

Os administradores Unix e Linux dependem muito do uso de scripts para executar tarefas diárias de administração do sistema. Muitos desses scripts precisam ser executados como usuário privilegiado, como 'root', ou chamar funções que, por sua vez, exigem altos níveis de privilégio. Usar uma solução que restringe privilégios é essencial para os usuários que precisam de direitos elevados. Tradicionalmente, a melhor maneira de auditar as atividades desses usuários era habilitar alguma forma de gravação de sessão, ou seja, gravar stdin e stdout, ou registrar tudo o que o usuário digita e vê na tela. O problema dessa abordagem é que, ao registrar essas ações, não há maneira de checar quais delas foram executadas no script, quais dados podem ter sido afetados ou como o sistema pode ter sido manipulado.

Ao usar o Privilege Management for Unix & Linux e seu recurso de auditoria e controle avançados (Advanced Control and Audit – ACA), os scripts não apenas podem ser controlados com mais rigor (por exemplo, eles podem ser executados e visualizados, mas não modificados - mesmo pelo root), mas os gestores de TI também podem logar e registrar todas as chamadas feitas no nível do sistema, independentemente de sua origem, durante a sessão.

Esse recurso permite que ações, como a execução de um script, sejam detalhadamente registradas (lidas, gravadas, executadas, etc.). Além disso, a solução Privilege Management for Unix & Linux também controla ações individuais no script, e permite ou bloqueia seletivamente essas ações sem interromper o processamento do script.

6. Controlando os Acessos até o Nível do Sistema

As ferramentas tradicionais de restrição de privilégios, como o sudo, são focadas em controlar o que o usuário digita na linha de comando, e não o que o sistema realmente tenta processar. As regras definidas nessas ferramentas conecentram-se no que o usuário está digitando e não no que o sistema realmente fará. Na maioria dos sistemas operacionais, no entanto, essas duas ações podem ser muito diferentes. Por exemplo, no Windows, é simples criar um atalho para um item, como "notepad.exe" e nomeá-lo como "Meu Editor de Texto Favorito.lnk". Se uma

empresa tiver uma política que impeça alguém de clicar em um ícone chamado notepad.exe, o que acontecerá quando alguém tentar acessar esse atalho?

A mesma situação ocorre no mundo Unix/Linux: como se trata de um sistema operacional de linha de comando, as políticas de segurança se concentram fortemente no que o usuário digita no prompt de comando. O problema é que os atalhos (conhecidos como links simbólicos e links físicos) também podem ser usados para chamar binários (executáveis) e scripts, ou arquivos de referência. Além disso, os binários (executáveis) também podem ser renomeados para burlar as políticas de segurança. Imagine se alguém copiasse o binário 'shutdown' e renomeasse como 'ping'. O shutdown pode ser bloqueado pelo sudo, mas o ping não. Um administrador malicioso poderia executar o 'sudo ping' e o sistema seria desligado sem que ninguém conseguisse descobrir o que aconteceu.

As regras de política ACA (Advanced Control and Audit) do Privilege Management for Unix & Linux possibilitam que controles de uma linha sejam colocados em arquivos e pastas, permitindo “mirar” arquivos e pastas com uma determinada nomenclatura, inclusive subpastas. Esses controles consentem que permissões granulares sejam definidas em relação ao destino. Mas, o mais importante é que o ACA opera no nível do sistema e não no nível da linha de comando. Independente de como o comando 'shutdown' é chamado, seja diretamente '/ usr / sbin / shutdown', um link para '/ usr / sbin / shutdown' ou uma cópia renomeada do comando shutdown, o ACA é inteligente o suficiente para bloquear a execução do comando emitido.

7. Consolidando Logs de Eventos, Relatórios e Análises

Pela natureza da linha de comando, os sistemas Unix e Linux não são os mais amigáveis quando se trata de emissão de relatórios. No entanto, essa função é essencial - especialmente ao realizar investigações forenses em logs ou detectar anomalias.

A BeyondTrust resolve esse problema com a integração entre o Privilege Management for Unix & Linux e sua plataforma BeyondInsight. O Privilege Management for Unix & Linux envia dados de log de eventos para o dashboard do BeyondInsight: informações detalhadas sobre quem, o que, onde e quando. Esses dados podem ser apresentados em relatórios de fácil leitura e entendimento, e com ferramentas de business intelligence, podem ser usados para a geração de relatórios personalizados. Os dados também podem ser correlacionados com outros utilizando o Auditor do BeyondInsight para detecção e geração de relatórios de anormalidades.

Essa integração torna os relatórios sobre eventos Unix e Linux mais simples, rápidos e fáceis de ler, para que os gestores possam ter uma visão mais clara dos riscos com acessos privilegiados.

8. Forense - O Tempo é Essencial

O registro de todas as atividades dos usuários Unix/Linux pode se tornar uma tarefa exaustiva. Em geral, as equipes de TI perdem muito tempo para emitir relatórios no caso de uma investigação forense.

Com o Privilege Management for Unix & Linux, os logs de eventos podem ser nomeados dinamicamente, são armazenados centralmente, e o acesso é controlado pelo console do BeyondInsight. A solução usa o SOLR para indexar todas as sessões gravadas, com todas as informações acessíveis via linha de comando ou API REST.

9. Gravação de Sessão (O que é Digitado é Visto)

A restrição de privilégios é a condição ideal para a maioria das equipes de segurança, mas às vezes só é preciso ativar um shell privilegiado, como o root. Por isso, uma auditoria rigorosa é fundamental. Para os honestos, um shell root geralmente não apresenta problemas, desde que a atividade do administrador seja registrada de maneira inviolável. Esse nível de supervisão ajuda a garantir que os administradores não abusem de seus privilégios, além de auxiliar a equipe de TI a atender aos requisitos de conformidade em relação aos acessos privilegiados.

Uma simples linha na política do Privilege Management for Unix & Linux ativa a gravação de sessão completa, que é nomeada dinamicamente e indexada automaticamente usando o SOLR. Esse recurso permite que o time de TI visualize a sessão de várias maneiras diferentes: interativa, por vídeo, visualização da transcrição da sessão, exibição do histórico de comandos ou por um índice pesquisável. Esse recurso fornece flexibilidade para ativar e pesquisar rapidamente a atividade de uso, ajudando você a gerenciar melhor os riscos.

10. Obtendo o Gerenciamento de Senhas e a Restrição de Privilégios

Para que uma solução de armazenamento de senhas opere, é necessário um segundo nível de conta (conta funcional) para que o cofre de senhas possa realizar alterações, caso a senha da conta gerenciada fique fora de sincronia ou seja desconhecida pelo cofre. Isso também é verdade para qualquer aplicação que precise de privilégios mais altos, como ferramentas de verificação, administração remota automatizada, etc. Essas contas representam um risco em virtude do nível de privilégio necessário para o "gestor das senhas de usuários".

Ao instalar o Privilege Management for Unix & Linux com o Password Safe (e adicionar uma política simples), qualquer conta de usuário - mesmo com privilégios extremamente limitados - pode receber os privilégios necessários para o Password Safe funcionar. Isso garante maior segurança e compliance (já que não há necessidade de se ter contas privilegiadas para que as contas funcionais operem), enquanto reduz a superfície de ataque do host especificado.

11. Integrando o Gerenciamento de Senhas Privilegiadas à Execução de Comandos

Às vezes, os administradores precisam executar uma ação em um host de destino que exije o uso de uma conta/senha, que pode não residir no próprio host. Executando um comando via Privilege Management for Unix & Linux, por exemplo, pbrun sqlplus, a ferramenta pode recuperar credenciais de uma solução de armazenamento de senhas para uso na execução do comando solicitado. Essa integração garante que as equipes de TI não apenas controlem suas credenciais privilegiadas, mas também habilitem um controle de comando granular nos sistemas de destino depois que as credenciais forem recuperadas.

12. Gerenciamento Centralizado de Controles de Política Sudo

Mesmo para os usuários já acostumados com uma solução de restrição de privilégios, quase sempre haverá algumas máquinas que ainda têm acesso ao sudo. Com tantas iterações diferentes do arquivo de políticas sudoers usadas pelas várias equipes na empresa, a necessidade de controlar e rastrear as alterações feitas nos sudoers rapidamente se torna uma tarefa incontrolável. Quase todos os usuários sudo enfrentam o desafio de gerenciar adequadamente os sudoers criados em cada host Unix ou Linux.

As ferramentas de sincronização manual e as soluções de LDAP/banco de dados podem, a princípio, parecer atraentes, mas os controles de confiabilidade, complexidade e segurança acabam reduzindo drasticamente a eficácia dessas configurações, geralmente causando mais problemas do que soluções. Não existe uma maneira eficaz de desfazer alterações em um ou mais arquivos sudoers ou voltar para um determinado ponto/versão de um arquivo de políticas sudoers.

O Privilege Management for Unix & Linux fornece uma maneira de centralizar rapidamente um ou mais arquivos sudoers, permitindo o gerenciamento de alterações e o controle de versão. As alterações de política podem ser validadas antes que as alterações no arquivo sejam feitas, ou comparadas com as diferenças destacadas entre duas versões de sudoers. A funcionalidade de retroceder/avançar permite alternar rapidamente entre duas versões salvas dos sudoers que estão sendo gerenciadas pelo PMUL. Os hosts de conexão podem ser agrupados opcionalmente ou executados em um híbrido de hosts individuais. Isso permite acesso simples e controlado a arquivos sudoers específicos localizados em um ou mais servidores centralizados, com base na associação ao grupo do host solicitante.

13. Armazenamento Centralizado de Dados de Auditoria Sudo

Usar o sudo significa inserir dados de log de diferentes locais em diferentes sistemas. Dependendo da versão do Unix ou Linux, os dados de eventos acabam em diferentes arquivos syslog e também são misturados com outros dados de eventos do sistema. Uma melhor maneira de mover e armazenar com segurança os dados de log e de sessão do sudo é claramente necessária.

O Privilege Management for Unix & Linux fornece uma conexão segura a um servidor centralizado que armazena dados de eventos e sessões (criptografados se desejado), à medida que são gravados, eliminando a capacidade de enviar aos usuários a violação dos logs e permitindo uma revisão e análise forense muito mais rápidas, quando necessário.

14. Consolidar Contas e Diretórios

Quando usuários e administradores exigem acesso a um sistema, uma conta de usuário precisa ser criada em cada host, a fim de fornecer acesso ao sistema para aquele usuário. Os privilégios dessas contas geralmente são inflados e a limpeza delas geralmente não é feita quando um colaborador muda de função ou sai da empresa. Por isso, as organizações precisam reduzir o número de contas criadas, controlar em qual servidor essas contas podem efetuar logon e exercer controle sobre quais privilégios os usuários possuem após a autenticação.

O BeyondTrust Active Directory Bridge (AD Bridge) e o Privilege Management for Unix & Linux têm o recurso de consolidação de contas, além de direitos de acesso a sistemas consolidados, após o login. O Active Directory permite controlar quais servidores esse usuário acessa, e uma política centralizada irá controlar e auditar rigorosamente as atividades desse usuário durante cada sessão autenticada.

Outro benefício é que o AD Bridge permite que os usuários façam login nos sistemas Unix, Linux ou Mac usando seus nomes de usuário e senhas do Active Directory (AD), sem exigir infraestrutura adicional ou sincronização de senhas.

Com essas soluções integradas, é possível facilitar a migração a partir de vários mecanismos, de autenticação, identidades e diretórios, para uma única infraestrutura baseada no Active Directory para todos os sistemas e usuários. Isso centraliza o controle e acelera o acesso do usuário.

15. Estendendo as Políticas de Grupo para Sistemas não Windows

Algumas equipes de TI optam por gerenciar centralmente seus sistemas Windows, Unix e Linux, a fim de obter benefícios de segurança, conformidade e eficiência. Entretanto, precisam se esforçar para garantir que as políticas de configuração sejam aplicadas de maneira consistente em toda a empresa.

O AD Bridge e o Privilege Management for Unix & Linux permitem uma configuração consistente em toda a empresa, estendendo as ferramentas nativas de gerenciamento de políticas de grupo para incluir configurações específicas de políticas de grupo para Unix, Linux

e Mac. Esse recurso oferece suporte à conformidade com SOX, PCI, HIPAA, entre outros, substituindo o NIS com uma infraestrutura do Active Directory.

A plataforma de Gerenciamento de Acessos Privilegiados BeyondTrust

O Privilege Management for Unix e Linux e o Active Directory Bridge (AD Bridge) fazem parte das soluções da BeyondTrust para o Gerenciamento de Privilégios nos Endpoints. A plataforma é uma solução integrada para fornecer controle e visibilidade sobre todas as contas e usuários privilegiados.

Próximos Passos

Este documento apresentou casos de uso comuns para a delegação de privilégios com base em políticas e elevação de comandos para servidores Unix e Linux. Para mais informações sobre como a BeyondTrust pode ajudar sua empresa, visite beyondtrust.com/endpoint-privilege-management.