WHITEPAPER

PAM, JUMP SERVER E BASTION HOST: CONTROLE DE ACESSOS PRIVILEGIADOS EM AMBIENTES OT

Entenda PAM, jump server, bastion host, cofre de credenciais, rotação, sessões, fornecedores, MFA e controle de acessos privilegiados em OT.

A3A® Engenharia de Sistemas

SUMÁRIO

PAM, jump server e bastion host são controles usados para reduzir o risco de acessos administrativos a servidores, estações de engenharia, firewalls, switches, RTUs, aplicações e outros ativos críticos. PAM gerencia identidades e credenciais privilegiadas; jump server centraliza o caminho de acesso; bastion host é um sistema endurecido exposto a uma zona de maior risco para intermediar conexões.

Em ambientes OT, esses controles são especialmente relevantes para manutenção remota, fornecedores, equipes de automação e administradores. O acesso precisa ser individual, temporário, aprovado, registrado e limitado aos ativos necessários. Credenciais compartilhadas e VPNs com alcance amplo reduzem rastreabilidade e aumentam o impacto de comprometimento.

Uma arquitetura madura combina VPN ou ZTNA, MFA, PAM, jump server, segmentação, gravação de sessão, logs e procedimentos de emergência. Nenhum componente isolado resolve todo o problema.

1. O QUE É PAM

PAM significa *Privileged Access Management*. É o conjunto de processos e tecnologias para descobrir, proteger, conceder, monitorar e revisar acessos privilegiados.

Contas privilegiadas incluem administradores de domínio, root, administradores locais, contas de serviço, contas de equipamentos, credenciais de aplicações e acessos de fornecedores.

O PAM pode armazenar segredos em cofre, rotacionar senhas, intermediar sessões, aplicar aprovação, limitar tempo e gerar auditoria.

2. POR QUE CONTAS PRIVILEGIADAS SÃO CRÍTICAS

Uma conta comum acessa recursos limitados. Uma conta privilegiada pode alterar configuração, criar usuários, desabilitar proteção, modificar lógica ou interromper serviços.

Em OT, privilégios podem alcançar sistemas que controlam processo. O impacto inclui indisponibilidade, perda de visibilidade e alteração de parâmetros.

O risco aumenta quando contas são compartilhadas, não expiram ou permanecem válidas após o término de um contrato.

3. DESCOBERTA DE CONTAS PRIVILEGIADAS

O primeiro passo é identificar contas em diretórios, servidores, bancos, firewalls, switches, aplicações e dispositivos.

A descoberta automática funciona melhor em sistemas padronizados. IEDs, RTUs e equipamentos embarcados podem exigir inventário manual ou APIs específicas.

O inventário deve indicar proprietário, finalidade, sistema, privilégio, autenticação, última utilização e ciclo de vida.

Contas sem proprietário ou não utilizadas precisam ser investigadas antes da remoção.

4. COFRE DE CREDENCIAIS

O cofre armazena senhas, chaves SSH, tokens e outros segredos de forma controlada.

Usuários não precisam conhecer a senha quando a sessão é intermediada. O PAM recupera a credencial e inicia o acesso.

O cofre precisa de criptografia, controle de acesso, backup, alta disponibilidade e proteção das chaves mestras.

A indisponibilidade do cofre não pode impedir resposta a incidentes sem procedimento de contingência.

5. CHECKOUT E CHECK-IN

Em modelos de checkout, o usuário solicita uma credencial por período. O sistema registra quem acessou e pode rotacionar depois do uso.

Check-in encerra a autorização. Sessões ainda abertas precisam ser tratadas.

Em ambientes críticos, a preferência é intermediar a sessão sem revelar o segredo. Quando a credencial é exibida, existe risco de cópia e uso fora do PAM.

6. ROTAÇÃO DE SENHAS

O PAM pode alterar senhas automaticamente após uso ou em intervalos definidos.

A rotação exige integração compatível. Equipamentos legados podem não possuir API ou podem armazenar a senha em várias aplicações.

Alterar sem atualizar dependências pode interromper serviços. Contas de serviço precisam de análise específica.

A rotação deve ser testada em cada tipo de ativo antes da produção.

7. CONTAS DE SERVIÇO

Contas de serviço executam aplicações, tarefas e integrações. Elas costumam possuir senhas estáticas e privilégios elevados.

O projeto deve identificar dependências e substituir senhas embutidas por mecanismos seguros quando possível.

Rotação precisa atualizar serviços, arquivos de configuração e clusters. O impacto deve ser monitorado.

Contas gerenciadas pelo sistema operacional ou certificados podem reduzir uso de senhas tradicionais.

Acesso privilegiado deve existir somente quando necessário.

Identidade individual, aprovação, janela, cofre, rotação e menor privilégio reduzem contas permanentes e melhoram a rastreabilidade.

Conhecer a solução de Zero Trust Network Access

8. JUST-IN-TIME

Just-in-time concede privilégio apenas durante uma janela aprovada.

O usuário pode receber associação temporária a um grupo ou acesso intermediado. Após o período, a autorização é removida.

Isso reduz contas administrativas permanentes. A integração com diretório e aplicações precisa ser confiável.

O horário deve ser sincronizado e a expiração monitorada.

9. JUST ENOUGH ADMINISTRATION

Just enough administration limita o conjunto de operações permitidas.

Em vez de entregar administração total, o usuário recebe comandos ou funções necessários à tarefa.

A implementação é mais simples em plataformas com modelos de função e APIs. Equipamentos OT proprietários podem oferecer apenas perfis amplos.

Quando granularidade não existe, segmentação, supervisão e gravação ganham importância.

10. APROVAÇÃO DE ACESSO

Solicitações podem exigir justificativa, ativo, período, chamado e aprovador.

A aprovação deve refletir risco. Acesso de emergência pode ter fluxo acelerado, mas precisa de revisão posterior.

Aprovações genéricas por longos períodos tornam o controle apenas formal.

Integração com sistema de chamados ajuda a relacionar sessão e atividade autorizada.

11. MFA PARA ACESSO PRIVILEGIADO

MFA deve proteger o login no PAM, VPN, ZTNA e jump server.

O artigo sobre MFA e 2FA aborda métodos, resistência a phishing e contingência.

MFA não corrige uma sessão excessivamente ampla. Ele confirma identidade, mas autorização e segmentação continuam necessárias.

12. O QUE É JUMP SERVER

Jump server é um sistema intermediário pelo qual administradores acessam ativos de outra zona.

Ele concentra ferramentas, clientes e registros. O usuário conecta ao jump server e, a partir dele, ao destino autorizado.

A estação deve ser endurecida e dedicada. Uso para e-mail, navegação geral ou tarefas administrativas aumenta risco.

Em OT, jump servers podem ficar em uma DMZ industrial ou zona de acesso remoto.

13. O QUE É BASTION HOST

Bastion host é um sistema reforçado colocado em posição exposta ou de fronteira para intermediar acesso.

O termo é comum em nuvem e redes segmentadas. Um bastion pode oferecer SSH, RDP ou proxy administrativo.

Jump server e bastion host podem desempenhar funções semelhantes, mas o bastion enfatiza endurecimento e exposição controlada na fronteira.

14. PAM VERSUS JUMP SERVER

PAM gerencia identidade, credenciais, aprovação e auditoria. Jump server fornece o ponto intermediário de conexão.

Um jump server sem PAM pode centralizar acesso, mas ainda utilizar contas compartilhadas e senhas conhecidas.

Um PAM sem isolamento de rede pode gerenciar credenciais, mas permitir caminhos alternativos diretos.

A arquitetura ideal integra os dois e bloqueia rotas que contornam o controle.

15. SESSION BROKERING

Session brokering cria a conexão ao destino em nome do usuário.

O PAM injeta a credencial sem revelá-la. Pode suportar RDP, SSH, web e outros protocolos.

Protocolos industriais e ferramentas proprietárias podem não ser facilmente intermediados. Nesses casos, o acesso ocorre a partir de uma estação de engenharia controlada.

16. GRAVAÇÃO DE SESSÕES

Sessões podem ser gravadas em vídeo, comandos, texto ou eventos.

A gravação apoia auditoria, investigação e treinamento. Precisa possuir retenção, integridade, acesso restrito e pesquisa.

Informações sensíveis podem aparecer na tela. A política deve considerar privacidade e requisitos legais.

A gravação não substitui supervisão em atividades críticas. Algumas intervenções podem exigir acompanhamento em tempo real.

17. REGISTRO DE COMANDOS

Em SSH, o sistema pode registrar comandos. Em RDP, gravação visual é mais comum.

Comandos digitados dentro de aplicações gráficas podem não ser visíveis em logs textuais.

O objetivo é construir evidência suficiente para responder quem acessou, quando, qual ativo e o que realizou.

18. ACESSO DE FORNECEDORES

Fornecedores devem possuir identidades individuais e contratos associados. Contas genéricas como “vendor” impedem atribuição.

O acesso precisa ser ativado apenas quando necessário, com janela, ativo e responsável interno.

A VPN não deve liberar toda a rede. O usuário deve chegar ao PAM ou jump server e somente aos destinos aprovados.

Arquivos transferidos precisam de controle e análise. Ferramentas remotas não autorizadas devem ser bloqueadas.

VPN ampla não é arquitetura de acesso remoto.

Fornecedores e administradores devem chegar a um PAM ou jump server e somente aos ativos, protocolos e períodos aprovados.

Conhecer o serviço de Projeto de Telecomunicações

19. ACESSO REMOTO EM SUBESTAÇÕES

A arquitetura pode incluir VPN ou ZTNA na borda, MFA, PAM na zona central e jump server na DMZ OT.

A partir do jump server, o usuário acessa estações de engenharia, servidores SCADA ou interfaces autorizadas.

IEDs e RTUs não devem ser expostos diretamente à internet ou à rede corporativa. O Projeto de Telecomunicações deve representar todos os fluxos.

20. ESTAÇÕES DE ENGENHARIA

Ferramentas de proteção, PLC, SCADA e rede podem exigir software específico. Uma estação de engenharia controlada reduz instalação dessas ferramentas em notebooks externos.

A estação precisa de hardening, EDR quando compatível, controle de software, backup e acesso restrito.

Projetos e arquivos transferidos devem possuir versionamento. A sessão remota precisa registrar atividade.

21. TRANSFERÊNCIA DE ARQUIVOS

Fornecedores podem precisar enviar firmware, projetos e logs.

A transferência deve ocorrer por repositório controlado, com análise antimalware, hash e aprovação.

Copiar diretamente do computador externo para o ativo OT reduz controle. A DMZ pode hospedar uma área de transferência intermediária.

Mídias removíveis seguem procedimento próprio.

22. CONTROLE DE CLIPBOARD E DISPOSITIVOS

Sessões RDP podem permitir clipboard, discos e impressoras. Esses recursos devem ser limitados.

O bloqueio completo pode impedir uma tarefa legítima; a liberação ampla facilita exfiltração e malware.

Perfis devem diferenciar administração rotineira, suporte e emergência.

23. PROTOCOLOS DE ACESSO

SSH, RDP, HTTPS, VNC, WinRM e ferramentas proprietárias podem fazer parte.

Cada protocolo precisa de origem, destino e porta definidos. Protocolos inseguros devem ser substituídos ou encapsulados.

O PAM deve registrar quando não consegue intermediar completamente um protocolo.

24. ACESSO A EQUIPAMENTOS DE REDE

Switches, roteadores e firewalls podem utilizar TACACS+, RADIUS, SSH e perfis de comando.

O RADIUS e 802.1X atende autenticação e accounting. TACACS+ pode oferecer controle granular de comandos em equipamentos compatíveis.

Credenciais locais de emergência precisam ser protegidas e rotacionadas.

25. ACESSO A IEDS E RTUS

IEDs e RTUs podem possuir contas locais e ferramentas proprietárias. Integração direta com PAM pode ser limitada.

O controle pode ocorrer pela estação de engenharia, cofre de senha, janela de rede e gravação de sessão.

A RTU e o IED precisam permanecer em zonas restritas.

26. CONTAS COMPARTILHADAS LEGADAS

Alguns equipamentos permitem apenas uma conta administrativa. O PAM pode custodiar e rotacionar a senha.

A sessão intermediada atribui o acesso ao usuário individual, mesmo que o destino use uma conta compartilhada.

Fora do PAM, o acesso direto deve ser bloqueado. Caso contrário, a auditoria pode ser contornada.

27. BREAK-GLASS

Break-glass é o acesso emergencial utilizado quando os controles normais estão indisponíveis.

Credenciais devem ser armazenadas com proteção forte, dupla custódia ou processo equivalente. O uso gera alerta e revisão obrigatória.

Testar o procedimento é necessário. Um segredo que não funciona ou um cofre inacessível durante falha não oferece contingência.

28. ALTA DISPONIBILIDADE DO PAM

PAM pode se tornar componente crítico. Servidores, cofres, bancos, conectores e jump servers precisam de redundância conforme o risco.

A arquitetura deve prever perda de site, rede e identidade. Backups precisam ser protegidos e restauráveis.

O failover não pode perder logs ou permitir acesso sem política.

29. DEPENDÊNCIAS DE IDENTIDADE

Active Directory, LDAP, PKI, MFA, DNS e NTP podem ser dependências.

A perda do diretório não deve resultar automaticamente em acesso irrestrito. Contas de contingência precisam ser limitadas.

O servidor NTP sustenta validade de tokens, certificados e logs.

30. SEGMENTAÇÃO E BLOQUEIO DE CAMINHOS ALTERNATIVOS

PAM só é efetivo quando acessos diretos são bloqueados. Firewalls devem permitir administração a partir dos jump servers autorizados.

Redes de gestão precisam ser separadas das redes de processo. Usuários não devem rotear diretamente de seus notebooks aos ativos.

O Zero Trust Network Access pode limitar acesso por identidade, dispositivo e aplicação.

31. HARDENING DO JUMP SERVER

O jump server deve ser dedicado, atualizado e monitorado. Serviços desnecessários, navegadores e ferramentas não aprovadas devem ser removidos.

O hardening de servidores e endpoints fornece uma base.

Sessões administrativas no próprio jump server precisam ser separadas das sessões intermediadas. Contas de serviço e agentes devem seguir menor privilégio.

32. EDR NO JUMP SERVER

EDR pode proteger o jump server e estações de engenharia, desde que compatível com desempenho e aplicações.

O artigo sobre EDR e XDR em OT detalha testes e exceções.

Alertas críticos podem bloquear sessão, mas a política deve considerar disponibilidade e operação.

33. LOGS E SIEM

PAM deve registrar solicitação, aprovação, login, destino, sessão, comando, transferência e encerramento.

Logs precisam ser enviados para o SIEM sem depender apenas do próprio PAM.

Eventos relevantes incluem acesso fora da janela, falha repetida, uso de break-glass, criação de conta e mudança de política.

34. RETENÇÃO E INTEGRIDADE

Gravações podem ocupar grande espaço. A retenção deve considerar risco, contrato e investigação.

Arquivos precisam de proteção contra alteração e acesso limitado. Metadados ajudam pesquisa sem abrir todo o vídeo.

O horário deve ser consistente. Diferenças entre PAM, jump server e destino dificultam correlação.

35. PROCESSO DE CONCESSÃO

A concessão deve começar por solicitação com justificativa. O aprovador valida necessidade, ativo e período.

O usuário autentica com MFA e inicia a sessão. Ao final, acesso expira, credencial é rotacionada e logs são revisados conforme risco.

Atividades de alto impacto podem exigir duas pessoas ou supervisão.

36. REVISÃO PERIÓDICA

Contas, grupos, fornecedores e políticas precisam de recertificação.

A revisão identifica acessos que permaneceram após mudança de função ou contrato.

Métricas incluem contas privilegiadas, sessões, acessos emergenciais, falhas, credenciais não rotacionadas e caminhos diretos.

37. PROJETO E DOCUMENTAÇÃO

O projeto deve incluir arquitetura, zonas, fluxos, ativos, contas, protocolos, aprovação, gravação, retenção e contingência.

Também precisa definir integrações com diretório, MFA, SIEM, chamados e PKI.

Matriz de acesso relaciona função, usuário, origem, destino, privilégio e janela.

38. IMPLANTAÇÃO POR ETAPAS

O inventário e o bloqueio de caminhos diretos devem preceder a expansão.

Pode-se começar por fornecedores e servidores de maior risco, depois equipamentos de rede e aplicações.

A mudança precisa de comunicação, treinamento e plano de retorno. PAM mal implantado pode interromper manutenção.

39. COMISSIONAMENTO E ACEITE

Os testes devem validar autorização, sessão, credencial, gravação, contingência e integração.

O roteiro mínimo inclui:

O aceite deve comprovar que a operação consegue realizar manutenção legítima sem manter privilégios permanentes.

O aceite precisa provar o controle e a contingência.

Aprovação, MFA, rotação, gravação, transferência de arquivos, falhas, break-glass, logs e bloqueio de caminhos diretos devem ser exercitados.

Conhecer o serviço de Comissionamento e Aceite Técnico

40. DIAGNÓSTICO DE FALHAS

Falha de login pode envolver identidade, MFA, aprovação, política ou credencial do destino. Sessão que abre e fecha pode indicar protocolo, licença ou timeout.

Rotação que falha exige verificar permissão, conectividade e dependências. Gravação ausente aponta agente, armazenamento ou política.

A análise deve usar logs do PAM, jump server, firewall e destino.

41. ERROS COMUNS

Erros frequentes incluem instalar jump server sem bloquear acesso direto, custodiar senhas mas revelá-las a todos e manter aprovações longas.

Também são comuns contas compartilhadas, gravação sem revisão, break-glass não testado e fornecedores usando VPN ampla.

Outro erro é tornar o PAM ponto único de falha sem contingência segura.

42. CONCLUSÃO

PAM, jump server e bastion host reduzem o risco de administração remota ao centralizar identidades, credenciais, caminhos e evidências.

Em OT, o controle precisa equilibrar segurança e disponibilidade. Acesso temporário, MFA, segmentação, gravação, break-glass e testes de falha permitem apoiar manutenção sem manter rotas e privilégios permanentes.

[1] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-53 Rev. 5 — Security and Privacy Controls for Information Systems and Organizations.

[2] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-82 Rev. 3 — Guide to Operational Technology Security. Gaithersburg, 2023.

[3] CISA. Cybersecurity Performance Goals — Identity and access management guidance.

[4] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 62443 series — Security for industrial automation and control systems.

[5] MITRE. ATT&CK for ICS — Valid Accounts and Remote Services techniques.

O que é PAM? PAM é a gestão de acessos privilegiados, incluindo descoberta, cofre, concessão, monitoramento, rotação e auditoria.**O que é jump server?** É um sistema intermediário usado para acessar ativos de outra zona de rede.**O que é bastion host?** É um host endurecido colocado em uma fronteira para intermediar acesso administrativo controlado.**PAM e jump server são a mesma coisa?** Não. PAM gerencia identidade e credenciais; jump server fornece o caminho intermediário. Eles podem ser integrados.**PAM pode gravar sessões?** Sim. Pode registrar vídeo, comandos, eventos e transferência, conforme protocolo e solução.**Como fornecedores devem acessar OT?** Com identidade individual, MFA, janela aprovada, PAM ou jump server e acesso somente aos destinos necessários.**O que é just-in-time?** É a concessão temporária de privilégio apenas durante o período necessário.**O que é break-glass?** É um acesso emergencial protegido e auditado usado quando os controles normais estão indisponíveis.**PAM rotaciona senhas de equipamentos?** Pode rotacionar quando existe integração compatível. Equipamentos legados exigem testes e procedimentos específicos.**Como testar uma implantação PAM?** Devem ser testados aprovação, MFA, rotação, sessão, gravação, logs, falhas, break-glass e bloqueio de acesso direto.

Soluções relacionadas

Serviços relacionados

Artigos e materiais técnicos relacionados

Sobre a A3A Engenharia de Sistemas

Com 30 anos de história, a A3A Engenharia de Sistemas se consolidou como referência em serviços de Engenharia, oferecendo soluções integradas de Telecomunicações, Segurança Eletrônica, Segurança Digital e Instalações Elétricas.

A empresa atua em todas as etapas do ciclo de Engenharia, desde a elaboração de projetos e consultoria técnica até a implantação, manutenção e retrofit de sistemas, sempre em conformidade com as normas técnicas e melhores práticas do setor.

A3A® Engenharia de Sistemas