



Análise semanal LATAMSEC • semana de 29 de setembro a 6 de outubro de 2026

631 operadores de Kubernetes auditados. Um em vinte pede privilégio de administrador do cluster

A Unit 42 comparou o privilégio que cada operador de Kubernetes documenta precisar com o privilégio que ele de fato recebe no cluster. Pouco mais de 5% pedem permissão excessiva, com caminho até administrador. Somando a isso chave de acesso com anos de idade, segredo em repositório sem revogação e uma proporção estimada de 82 identidades de máquina por pessoa, o que aparece é a credencial que nenhum processo de revisão de acesso alcança.

Unit 42, 29/09/2026

631 operadores auditados

5% pedem cluster-admin

82 identidades de máquina por pessoa

Leitura LGPD

O que esta análise mostra: a Unit 42 auditou 631 operadores de Kubernetes em 29 de setembro e encontrou privilégio excessivo em pouco mais de 5% deles, com caminho implícito até administrador do cluster, além de 16 casos de alto risco e uma falha concreta, a CVE-2026-6389, CVSS 8.8, na plataforma Turbonomic da IBM. O dado não está sozinho. A telemetria de nuvem da Datadog aponta 59% dos usuários IAM da AWS com chave de acesso de mais de um ano, 55% das contas de serviço do Google Cloud na mesma situação e 19,4% das instâncias EC2 com privilégio excessivo. O relatório da GitGuardian contabiliza cerca de 29 milhões de segredos expostos em repositórios públicos, alta de 34%, e registra que 64% dos segredos válidos detectados em 2022 seguiam sem revogação em 2026. A CyberArk estima 82 identidades de máquina por identidade humana, 42% delas com acesso privilegiado. A conclusão prática é que nenhum desses quatro números se resolve com revisão trimestral de acesso: o controle precisa ser escopo mínimo por padrão, credencial de vida curta por federação e prazo de validade automático.

Toda organização sabe quantas pessoas têm acesso de administrador. Quase nenhuma sabe quantos programas têm. E é o segundo número que cresce sozinho.

A semana trouxe uma medição que dá tamanho ao problema. A Unit 42 auditou 631 operadores de Kubernetes, o tipo de componente que é instalado com um comando e passa a viver dentro do plano de controle do cluster, e comparou o privilégio que cada um documenta precisar com o privilégio que de fato recebe. Pouco mais de 5% pedem permissão excessiva, com caminho implícito até administrador do cluster. Dezesesseis foram classificados como alto risco, incluindo leitura de segredo em todo o cluster.

Essa análise junta esse dado com outros três, porque isolado ele parece um problema de Kubernetes. Não é. É o mesmo problema em quatro superfícies.

1. O operador que pede mais do que usa

O trabalho da Unit 42, publicado em 29 de setembro por Lior Yakim, parte de uma observação de engenharia e não de segurança: quem escreve operador quer que a instalação funcione na primeira tentativa, em qualquer cluster. O caminho mais curto para isso é pedir permissão com curinga. O manifesto entra, o operador roda, ninguém revisa.

A consequência é que o alcance de um comprometimento passa a ser definido pelo RBAC do operador, não pela função dele. Um operador de banco de dados que recebeu leitura de Secret em escopo de cluster entrega, se for comprometido, toda a credencial que existe no cluster, inclusive as que não têm relação nenhuma com banco de dados.

A pesquisa veio com ferramenta aberta, o OperTraitor, que coleta a configuração de RBAC dos operadores instalados e dos publicados no OperatorHub e devolve nota de 1 a 10 baseada na diferença entre o privilégio necessário e o concedido. E veio com um caso concreto: a CVE-2026-6389, de severidade alta e CVSS 8.8, na plataforma Turbonomic da IBM.

Medida	Resultado
Operadores analisados	631
Classificados como alto risco	16
Com privilégio excessivo, incluindo caminho a cluster-admin	pouco mais de 5%
Escala da nota do OperTraitor	1 a 10, pela diferença entre necessário e concedido

2. A chave que ninguém aposenta

O segundo dado vem do levantamento de telemetria de nuvem da Datadog, e ele é mais incômodo porque não depende de ninguém errar o manifesto. Depende de ninguém apagar nada.

- 59% dos usuários IAM da AWS têm chave de acesso com mais de um ano, e mais da metade dessas chaves não foi usada nos últimos 90 dias.
- 55% das contas de serviço do Google Cloud têm chave com mais de um ano. Em aplicações do Entra ID, 40%.
- Chave com mais de três anos subiu de 21% para 25% na AWS e de 22% para 25% no Google Cloud. Com mais de cinco anos, subiu de 8% para 10% na AWS e de 6% para 10% no Azure.
- 19,4% das instâncias EC2 estão com privilégio excessivo. Em 3,8% o excesso permite movimento lateral e em 2,4% permite escalada de privilégio.
- 23% das máquinas virtuais do Google Cloud estão excessivamente permissivas, e 17% têm privilégio administrativo completo.

Tem um sinal bom no mesmo levantamento: 61% das organizações já usam só federação de identidade, acima dos 54% do ano anterior. Mas 39% ainda mantêm usuários IAM com credencial estática, e 21% dependem exclusivamente deles. A chave estática não é mais o padrão e continua sendo a maioria do estrago.

3. O segredo que já está publicado

Credencial de máquina vaza por um caminho que credencial de pessoa não tem: ela é escrita em arquivo, e arquivo vai para repositório. O relatório anual da GitGuardian mediu isso em 2026 e os números não melhoraram.

- Cerca de 29 milhões de segredos expostos em repositórios públicos do GitHub, 34% mais que no ano anterior.
- Vazamento de credencial de serviço de IA cresceu 81% em um ano, chegando a 1.275.105 ocorrências.
- 64% dos segredos válidos detectados em 2022 continuavam sem revogação em 2026. Essa é a estatística que importa: o problema não é a detecção, é o que acontece depois dela.
- Cerca de 60% das violações de política envolvem credencial de vida longa.
- Repositório interno tem aproximadamente seis vezes mais chance de guardar segredo em código do que repositório público, porque ninguém imagina que ele vai sair de lá.
- Em arquivos de configuração de MCP analisados, 24.008 segredos únicos. Commit assistido por IA vaza segredo em 3,2% dos casos, contra 1,5% da linha de base.

4. A proporção

O quarto dado é o que explica por que a revisão trimestral de acesso nunca alcança isso. O levantamento da CyberArk com 2.600 tomadores de decisão em 20 países estima 82 identidades de máquina por identidade humana, e aponta que 42% delas têm acesso privilegiado ou a dado sensível.

Vale a ressalva: esse número é autodeclarado em pesquisa, não medido em telemetria, e serve como ordem de grandeza e não como inventário. Mesmo assim, a aritmética muda a conversa. Um processo de revisão de acesso desenhado para 500 pessoas não funciona para 41 mil identidades de máquina, por mais disciplinado que seja o responsável.

O que a nuvem já faz sozinha, e até onde

Há uma camada automática que muita equipe não sabe que existe. A Unit 42 documentou em 21 de setembro como a AWS reage quando uma chave de acesso aparece em repositório público: a política gerenciada

`AWSCompromisedKeyQuarantineV3` é anexada ao principal, em teste próprio cerca de dez segundos depois do push, e o aviso do GitHub chega um segundo depois. Política anexada, alerta do GitHub, alerta no AWS Health e caso aberto no suporte, tudo dentro de mais ou menos um minuto.

A linhagem da política mostra a corrida: a primeira versão, de agosto de 2020, negava 28 ações. A segunda, de abril de 2021, foi a 61 permissões em 17 serviços. A terceira, de agosto de 2024, incorpora a anterior e acrescenta alvos novos, incluindo Amazon Bedrock e ECS.

O limite precisa ficar claro, porque é onde a falsa sensação de segurança mora: quarentena não é revogação. A chave continua autenticando. O que a política faz é negar explicitamente o conjunto de ações mais usado em abuso. Tudo que não está na lista de negação permanece disponível. A quarentena compra tempo para a equipe revogar, e não substitui a revogação.

O roteiro de correção

A boa notícia é que nada aqui depende de produto novo. Depende de decisão de configuração, e a documentação oficial já diz qual.

Controle	O que fazer	De onde vem
Escopo de RBAC	Preferir Role e RoleBinding a ClusterRole e ClusterRoleBinding. Operador em namespace, não em cluster, sempre que a arquitetura permitir.	Boas práticas de RBAC do Kubernetes
Curinga	Nenhum curinga em verbo ou recurso. Restringir com rigor escalate, bind e impersonate.	Boas práticas de RBAC do Kubernetes
Segredo	Minimizar get, list e watch sobre Secret, restringindo por resourceName em vez de liberar o tipo.	Boas práticas de RBAC do Kubernetes
Conta de serviço	Uma por carga de trabalho. Nunca a conta default em produção.	Boas práticas de RBAC do Kubernetes
Credencial de carga	Trocar chave estática por federação. Na AWS, EKS Pod Identity ou IRSA: o token projetado expira em uma hora e o EKS rejeita token com mais de 90 dias. No Google Cloud e no Azure, Workload Identity Federation e Entra Workload ID.	Documentação de contas de serviço do EKS
Idade de chave	Tratar idade máxima de credencial como indicador de serviço, com inventário e prazo. Sem inventário, 25% do parque passa de três anos sem ninguém notar.	Telemetria da Datadog
Revogação	Varredura de segredo é só a metade. O indicador que conta é tempo entre detecção e revogação, e o alvo é hora, não trimestre.	Relatório da GitGuardian
Observação	Log de auditoria do Kubernetes como fonte de comportamento de conta de serviço. Conta que começa a ler recurso novo é sinal.	Recomendação da Unit 42
Saída de rede	NetworkPolicy bloqueando saída não autorizada, com atenção especial a operador e agente de IA dentro do cluster.	Recomendação da Unit 42

Para quem precisa de referência externa em auditoria, o guia de endurecimento de Kubernetes publicado pela NSA em conjunto com a CISA, na versão 1.2, cobre RBAC, autenticação, autorização e log de auditoria, e é citável em documento de conformidade.

O que muda para quem opera no Brasil

- **O inventário vem antes de qualquer controle.** A pergunta inicial não é qual ferramenta comprar. É quantas credenciais de máquina existem, onde estão, qual a idade da mais velha e quem é o dono de cada uma. Na maioria das operações de porte médio essa lista não existe em lugar nenhum.
- **Revisão de acesso trimestral não cobre identidade de máquina.** O processo foi desenhado para gente que entra e sai da empresa. Credencial de serviço não pede demissão, então ela precisa de prazo de validade automático, não de revisão humana.
- **O artigo 46 da LGPD é a conversa que vem.** A lei exige medida de segurança adequada, sem detalhar qual. Chave de acesso de cinco anos, sem uso nos últimos 90 dias e com privilégio administrativo é difícil de defender como medida adequada diante de um incidente. Essa é leitura nossa e não decisão publicada: até agora não há decisão da ANPD tratando especificamente de credencial de máquina.
- **Existe um vazio de dado regional, e ele atrapalha.** Não encontramos levantamento com número sobre identidade de máquina, conta de serviço ou higiene de credencial específico do Brasil ou da América Latina. O que há de regional é

genérico: credencial comprometida como método de entrada mais comum e portal de acesso remoto como tecnologia mais visada. Quem tem esse dado internamente está em vantagem para medir o próprio risco, e deveria produzi-lo.

Leitura LATAMSEC

Há um padrão nos quatro conjuntos de dados desta semana. Em todos, o privilégio excessivo não foi concedido por descuido de uma pessoa, e sim por um atalho razoável de engenharia: curinga no manifesto para a instalação funcionar, chave estática porque federação dá trabalho de configurar, segredo em arquivo porque o pipeline precisa dele, conta de serviço reaproveitada porque criar outra exige ticket.

Isso significa que a correção também não é disciplina individual. É padrão de plataforma. Se criar conta de serviço com escopo mínimo é mais difícil que reaproveitar a existente, o resultado está decidido antes de qualquer política entrar em vigor.

Quatro perguntas para levar à próxima reunião de arquitetura.

Para quem opera cluster: quantos operadores estão instalados com ClusterRole hoje, e quantos deles precisam disso para funcionar?

Para quem responde pela nuvem: qual é a idade da credencial de máquina mais velha ainda ativa, e quem é a pessoa responsável por ela?

Para quem responde pelo pipeline: qual é o tempo médio entre detectar segredo em repositório e revogar a credencial? Se a resposta não existe, o número provavelmente se parece com os 64% sem revogação.

Para o comitê de risco: a política de acesso privilegiado da empresa menciona identidade de máquina, ou fala só de usuário nomeado? Se for a segunda, ela cobre pouco mais de 1% do problema.

Três evidências que um conselho pode exigir

Evidência 1	Lista dos operadores instalados com permissão em escopo de cluster, com justificativa por item O OperTraitor da Unit 42 produz essa lista com nota de 1 a 10 pela diferença entre privilégio necessário e concedido. Sem a lista, o alcance de um comprometimento é desconhecido.
Evidência 2	Idade da credencial de máquina mais velha ainda ativa, por provedor de nuvem A referência pública é desconfortável: 25% das chaves na AWS e no Google Cloud passam de três anos, e 10% passam de cinco. Quem não tem o número tem o problema.
Evidência 3	Tempo médio entre detectar segredo em repositório e revogar a credencial Varredura sem revogação não reduz risco. O dado de referência da GitGuardian é que 64% dos segredos válidos de 2022 continuavam ativos em 2026.

Fontes

- 01 **Unit 42** OperTraitors: How Kubernetes Operators Betray Your Security Posture, com os 631 operadores analisados, os 16 de alto risco, a ferramenta OperTraitor e a CVE-2026-6389.
<https://unit42.paloaltonetworks.com/agentic-ai-kubernetes-operator-risks/>
- 02 **Unit 42** From Exposure to Lockdown: How AWS Neutralizes Compromised IAM Credentials through Managed Policies, com a linhagem da política de quarentena, o tempo de reação medido e o limite do mecanismo.
<https://unit42.paloaltonetworks.com/detecting-exposed-aws-iam-credentials/>
- 03 **Datadog** State of Cloud Security 2025, com a idade das chaves de acesso, o privilégio excessivo em EC2 e a adoção de federação.
<https://www.datadoghq.com/state-of-cloud-security/>
- 04 **GitGuardian** The State of Secrets Sprawl 2026, com os 29 milhões de segredos expostos, a alta de 81% em credencial de IA e os 64% sem revogação.
<https://blog.gitguardian.com/the-state-of-secrets-sprawl-2026-pr/>
- 05 **CyberArk** 2025 Identity Security Landscape, com a proporção de 82 identidades de máquina por pessoa e os 42% com acesso privilegiado.
<https://www.cyberark.com/press/machine-identities-outnumber-humans-by-more-than-80-to-1-new-report-exposes-the-exponential-threats-of-fragmented-identity-security/>
- 06 **Kubernetes** Role Based Access Control Good Practices, com as regras de escopo, curinga, verbos sensíveis e conta de serviço por carga de trabalho.
<https://kubernetes.io/docs/concepts/security/rbac-good-practices/>
- 07 **AWS** Grant Kubernetes workloads access to AWS using Kubernetes Service Accounts, com a validade de uma hora do token projetado, o limite de 90 dias e as opções IRSA e EKS Pod Identity.
<https://docs.aws.amazon.com/eks/latest/userguide/service-accounts.html>
- 08 **NSA e CISA** Kubernetes Hardening Guidance, versão 1.2, referência externa citável em auditoria para RBAC, autenticação, autorização e log.
https://media.defense.gov/2022/Aug/29/2003066362/1/1/0/CTR_KUBERNETES_HARDENING_GUIDANCE_1.2_20220829.PDF

LATAMSEC · análise semanal publicada em 6 de outubro de 2026 em latamsec.com.br/recursos/identidades-nao-humanas-privilegio-excessivo/. Os números desta análise são dos relatórios citados na seção de fontes e valem na data de publicação.