As 10 melhores práticas de segurança para proteger backups em AWS

AWS Recomendações

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Recomendações: As 10 melhores práticas de segurança para proteger backups em AWS

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens de marcas da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

As 10 melhores práticas de segurança para proteger backups em AWS

Ibukun (IB) Oyewumi, Amazon Web Services (AWS)

Maio de 2022 (histórico do documento)

A segurança é uma responsabilidade compartilhada entre a Amazon Web Services (AWS) e os clientes. Os clientes solicitaram maneiras de proteger seus backups em AWS. Como as práticas de segurança evoluem constantemente para mitigar novos riscos, é importante realizar avaliações de risco regulares para determinar a aplicabilidade dos controles de segurança e implemente várias camadas de controles para reduzir os riscos aos seus dados.

Este documento o guiará por uma lista selecionada das 10 principais práticas recomendadas de segurança para proteger seus dados e operações de backup em. AWS Embora este guia se concentre em dados e operações de backup com o serviço AWS Backup, essas práticas recomendadas de segurança podem ser usadas com outras soluções de backup, por exemplo, as ferramentas de backup do AWS Marketplace.

Práticas recomendadas

Ao proteger os backups AWS, recomendamos usar a seguinte abordagem:

Tópicos

Etapa 1. Implementar uma estratégia de backup

Uma estratégia abrangente de backup é uma parte essencial do plano de proteção de dados de uma organização para resistir, se recuperar e reduzir qualquer impacto que possa ser causado por um evento de segurança. Crie uma estratégia de backup abrangente que defina quais e com que frequência os dados devem ser copiados e como as tarefas de backup e recuperação serão monitoradas.

Ao desenvolver uma estratégia abrangente para fazer backup e restaurar dados, primeiro identifique as interrupções que possam ocorrer e seu impacto potencial nos negócios.

Seu objetivo é criar uma estratégia de recuperação que restaure sua workload ou evite tempo de inatividade dentro de objetivos de recuperação, objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO) aceitáveis. O RTO é o atraso aceitável entre a interrupção e a restauração do serviço. O RPO é o período de tempo aceitável desde o último ponto de recuperação de dados. Considere uma estratégia de backup granular que inclua todos os itens a seguir:

- Cadência de backup contínua
- Point-in-Time Recuperação (PITR)

- Recuperação em nível de arquivo
- Recuperação em nível de dados de aplicações
- Recuperação em nível de volume
- Recuperação em nível de instância

Ransomware

Uma estratégia de backup bem projetada deve incluir ações que possam proteger e recuperar seus recursos de ataques de ransomware, com requisitos detalhados de recuperação para suas aplicações e dependências de dados. Por exemplo, ao estabelecer controles preventivos e de detecção para reduzir o risco de ransomware, certifique-se de também criar o nível adequado de granularidade para padrões de cópia e restauração entre contas Região da AWS ou contas, a fim de garantir que os administradores não restaurem dados de backup corrompidos após o evento de segurança.

Requisitos de retenção

Em alguns setores, ao desenvolver uma estratégia de backup, também é necessário considerar as regulamentações para os requisitos de retenção de dados. Certifique-se de que sua estratégia de backup tenha sido projetada com requisitos de retenção suficientes para atender às suas necessidades normativas para cada nível de classificação de dados e tipo de recurso.

Compliance

Consulte suas equipes de conformidade de segurança para validar se seus recursos e operações de backup devem ser incluídos ou segmentados do escopo de seus programas de conformidade. Incluir backup e recuperação como parte essencial de seu programa de segurança ajudará a entender onde estão os dados em seu ambiente e a definir adequadamente o escopo de conformidade.

Para obter as melhores práticas de arquitetura para projetar e operar cargas de trabalho confiáveis, seguras, eficientes e econômicas na nuvem, consulte Abordagens de backup e recuperação usando AWS e Reliability Pillar — AWS Well-Architected Framework.

Etapa 2. Incorporar o backup na DR e no BCP

Recuperação de desastres (DR) é o processo de preparação para, resposta a e recuperação de um desastre. Parte importante de sua estratégia de resiliência, o plano de DR diz respeito à forma como

sua workload responde em caso de desastre. Um desastre pode ser uma falha técnica, uma ação humana ou um evento natural. O Plano de continuidade de negócios (BCP) descreve como uma organização pretende continuar com as operações comerciais normais durante uma interrupção não planejada.

Seu plano de DR deve ser um subconjunto do BCP da organização. O BCP também deve incluir AWS Backup procedimentos. Por exemplo, um evento de segurança que afeta os dados de produção pode exigir que você invoque um plano de DR usado AWS Backup para fazer o failover para fazer backup de dados de outro Região da AWS. Certifique-se de que seus funcionários estejam familiarizados e tenham praticado o uso AWS Backup junto com seus procedimentos organizacionais, para que, em caso de desastre, sua organização possa continuar suas operações normais com pouca ou nenhuma interrupção no serviço. Mais informações sobre o uso AWS Backup são fornecidas em outras seções deste guia.

Etapa 3. Automatize as operações de backup

Os planos de backup e as atribuições de recursos da sua organização devem ser configurados para refletir as políticas de proteção de dados da empresa. Ao automatizar e implantar políticas de backup ou planos de backup em toda a organização, é possível padronizar e escalar sua estratégia de backup. Você pode usar o AWS Organizations para automatizar centralmente as políticas de backup para implementar, configurar, gerenciar e controlar a atividade de backup em recursos do AWS Backup compatíveis ao programar operações de backup.

Para melhorar a produtividade e governar as operações de infraestrutura em ambientes com várias contas, considere implementar a infraestrutura como código (IaC) e a arquitetura orientada por eventos como partes essenciais de sua estratégia de transformação digital e backup. A automação de backups oferece os seguintes benefícios:

- Reduz a sobrecarga manual decorrente da configuração demorada dos backups
- Minimiza o risco de erros
- Fornece visibilidade na detecção de desvios
- Melhora a conformidade com a política de backup em várias AWS cargas de trabalho ou contas

A implementação de políticas de backup como código pode ajudar você a cumprir os regulamentos de proteção de dados:

- Configurando requisitos diferentes para seus tipos de recursos

- Dimensionando sua estratégia de proteção de dados corporativos
- Implementando regras de ciclo de vida para especificar quanto tempo falta para que um ponto de recuperação faça a transição para o armazenamento de baixa atividade (frio) ou seja excluído, o que pode ajudar a otimizar seus custos

Ao automatizar suas operações de backup, você pode escalar as opções de atribuição de recursos usando AWS tags e recursos IDs para identificar automaticamente os AWS recursos que armazenam dados para seus aplicativos essenciais aos negócios e proteger seus dados usando backups imutáveis. Isso pode ajudar a priorizar os controles de segurança, como permissões de acesso e planos ou políticas de backup.

Etapa 4: Implementar mecanismos de controle de acesso

Ao pensar em segurança na nuvem, sua estratégia básica deve começar com uma base sólida de identidade para garantir que o usuário tenha as permissões corretas para acessar os dados. A autenticação e a autorização apropriadas podem ajudar a reduzir o risco de eventos de segurança. O modelo de responsabilidade compartilhada exige que AWS os clientes implementem políticas de controle de acesso. Para criar e gerenciar políticas de acesso em grande escala, é possível usar o AWS Identity and Access Management (IAM).

Ao configurar os direitos e permissões de acesso, implemente o princípio do privilégio mínimo de modo que cada usuário ou sistema que acesse seus dados de backup ou o seu cofre receba somente as permissões necessárias para cumprir suas funções. Use AWS Backup para definir políticas de acesso em cofres de backup para proteger suas cargas de trabalho na nuvem.

Por exemplo, ao implementar políticas de controle de acesso, você pode conceder aos usuários acesso para criar planos de backup e backups sob demanda, limitando a capacidade dos usuários excluírem pontos de recuperação. Usando políticas de acesso ao cofre, você pode compartilhar um cofre de backup de destino com uma função de origem Conta da AWS ou IAM, conforme exigido pelas necessidades da sua empresa. Você também pode usar políticas de acesso para compartilhar um cofre de backup com uma ou mais contas ou com toda a sua organização no AWS Organizations. Para obter mais informações, consulte a documentação do AWS Backup.

À medida que você escala suas cargas de trabalho ou migra para AWS, talvez seja necessário gerenciar centralmente as permissões para seus cofres e operações de backup. Use políticas de controle de serviço (SCPs) para implementar o controle centralizado sobre o máximo de permissões disponíveis para todas as contas em sua organização. SCPs oferecem defesa aprofundada e

garantem que seus usuários permaneçam dentro das diretrizes de controle de acesso definidas. Para obter mais informações, consulte Gerenciar o acesso a backups usando políticas de controle de serviços com o AWS Backup.

Para reduzir os riscos de segurança, como acesso não intencional aos seus recursos e dados de backup, use o IAM Access Analyzer para identificar qualquer função AWS Backup do IAM compartilhada com o seguinte:

- Uma entidade externa, como um Conta da AWS
- Um usuário raiz
- Um usuário ou perfil do IAM
- Um usuário federado
- Um AWS service (Serviço da AWS)
- Um usuário anônimo
- Qualquer outra entidade que possa ser usada para criar um filtro

Etapa 5. Criptografar os dados de backup e o cofre

Cada vez mais as organizações precisam melhorar sua estratégia de segurança de dados, e talvez precisem atender a regulamentações de proteção de dados à medida que se expandem na nuvem. A implementação correta de métodos de criptografia pode fornecer uma camada adicional de proteção acima dos mecanismos básicos de controle de acesso. Essa camada adicional proporcionará uma mitigação se suas políticas primárias de controle de acesso falharem.

Por exemplo, se você configurar políticas de controle de acesso excessivamente permissivas em seus dados do AWS Backup , seu sistema ou processo de gerenciamento de chaves podem minimizar parte do impacto de um evento de segurança. Isso ocorre porque há mecanismos de autorização separados para acessar seus dados e a chave de criptografia, o que significa que os dados de backup podem ser visualizados somente como texto cifrado.

Para aproveitar ao máximo a Nuvem AWS criptografia, criptografe dados em trânsito e em repouso. Para proteger os dados em trânsito, AWS usa chamadas de API publicadas para acessar AWS Backup pela rede usando o protocolo TLS para fornecer criptografia entre você, seu aplicativo e o AWS Backup serviço. Para proteger os dados em repouso, você pode usar o AWS cloud-native AWS Key Management Service(AWS KMS) ou. AWS CloudHSM Um modelo de segurança de hardware (HSM) baseado em nuvem, o AWS CloudHSM usa o Advanced Encryption Standard (AES) com

chaves de 256 bits (AES-256), um algoritmo robusto adotado pelo setor para criptografar dados. Avalie seus requisitos regulatórios e de governança de dados e selecione o serviço de criptografia apropriado para criptografar seus dados na nuvem e os cofres de backup.

A configuração da criptografia difere dependendo do tipo de recurso e das operações de backup entre contas ou regiões. Certos tipos de recursos são compatíveis com a capacidade de criptografar seus backups usando uma chave de criptografia diferente da chave usada para criptografar o recurso de origem. Como você é responsável por gerenciar os controles de acesso para determinar quem pode acessar seus AWS Backup dados ou as chaves de criptografia do cofre e sob quais condições, use a linguagem de política oferecida por AWS KMS para definir controles de acesso nas chaves. Você também pode usar o AWS Backup Audit Manager para confirmar se o backup está criptografado corretamente. Para obter mais informações, consulte Criptografia para backups no AWS Backup.

É possível usar chaves multirregião do AWS KMS para replicar chaves de uma região para outra. As chaves multirregião foram projetadas para simplificar o gerenciamento da criptografia quando seus dados criptografados precisam ser copiados para outras regiões para recuperação de desastres. Avalie a necessidade de implementar AWS KMS chaves multirregionais como parte de sua estratégia geral de backup.

Etapa 6. Proteger os backups usando armazenamento imutável

As organizações podem usar armazenamento imutável para gravar dados no estado Write Once Read Many (WORM). No estado WORM, os dados podem ser gravados uma vez, lidos e usados sempre que necessário após serem confirmados ou gravados na mídia de armazenamento. O armazenamento imutável ajuda a garantir que a integridade dos dados seja mantida. Ele também oferece proteção contra:

- Exclui
- Sobreposições
- Acesso inadvertido e não autorizado
- Comprometimento por ransomware

O armazenamento imutável oferece um mecanismo eficiente para lidar com possíveis eventos de segurança que possam ter impactos reais em suas operações comerciais.

Você pode usar o armazenamento imutável para melhorar a governança quando combinado com fortes restrições de SCP. Você também pode usar o armazenamento imutável em um modo WORM de conformidade quando alguma lei (como uma retenção legal) exigir acesso a dados imutáveis.

Para manter a disponibilidade e a integridade dos dados, você pode usar o AWS Backup Vault Lock para proteger seus backups. Quando você usa o AWS Backup Vault Lock, entidades não autorizadas não podem apagar, alterar ou corromper seus dados de clientes ou empresas durante o período de retenção exigido. AWS Backup O Vault Lock ajuda você a cumprir as políticas de proteção de dados da sua organização evitando o seguinte:

- Exclusões por usuários privilegiados (incluindo o usuário Conta da AWS root)
- Alterações nas configurações do ciclo de vida de backup
- Atualizações que alteram seu período de retenção definido

AWS Backup O Vault Lock garante a imutabilidade e adiciona uma camada adicional de defesa que protege os backups (pontos de recuperação) em seus cofres de backup. Isso é especialmente útil em setores altamente regulamentados que têm necessidades rigorosas de integridade para backups e arquivamentos. AWS Backup O Vault Lock garante que seus dados sejam preservados junto com um backup para recuperação em caso de ações não intencionais ou maliciosas.

Important

- AWS Backup O Vault Lock ainda não foi avaliado quanto à conformidade com a regra 17a-4 (f) da Securities and Exchange Commission (SEC) e com a Commodity Futures Trading Commission (CFTC) no regulamento 17 C.F.R. 1.31 (b) - (c).
- AWS Backup O Vault Lock entra em vigor imediatamente. Isso oferece a você um período mínimo de reflexão de três dias (72 horas) para excluir ou atualizar sua configuração antes que ela bloqueie permanentemente seu cofre. Você pode, opcionalmente, estender a duração desse período de reflexão. Use esse período de reflexão para testar o AWS Backup Vault Lock em relação às suas cargas de trabalho e casos de uso. Depois que seu período de reflexão expirar, nem você AWS Support poderá excluir ou alterar o AWS Backup Vault Lock ou o conteúdo do seu cofre trancado. Para obter mais informações, consulte a documentação do AWS Backup Vault Lock.

Etapa 7. Implementar monitoramento e alertas de backup

Os trabalhos de backup podem falhar. Um trabalho com falha, como uma tarefa de backup, restauração ou cópia, pode afetar as etapas subsequentes de um processo. Quando o trabalho de backup inicial falha, há uma grande probabilidade de que outras tarefas subsequentes também falhem. Nesse cenário, você pode entender melhor o curso dos eventos por meio de monitoramento e notificação. O monitoramento e os alertas podem fornecer reconhecimento organizacional para seus trabalhos de backup, o que ajuda você a responder às falhas de backup.

A ativação e a configuração de notificações para monitorar trabalhos do AWS Backupoferece os seguintes benefícios:

- Permite que você conheça suas atividades de backup
- Ajuda a garantir que você cumpra os contratos essenciais de nível de serviço () SLAs
- Melhora seu monitoramento business-as-usual
- Ajuda a cumprir obrigações de conformidade

Você pode implementar o monitoramento de backup para suas cargas de trabalho por meio da integração AWS Backup com outros sistemas Serviços da AWS e de emissão de tíquetes para realizar fluxos automatizados de investigação e escalonamento. Por exemplo, você pode fazer o seguinte:

- Use CloudWatch a Amazon para rastrear métricas, criar alarmes e visualizar painéis.
- Use EventBridge a Amazon para monitorar AWS Backup processos e eventos.
- Usar o AWS CloudTrail para monitorar chamadas à API do AWS Backup com informações detalhadas sobre a hora, IP de origem, usuários e contas que fazem essas chamadas.
- Use o Amazon Simple Notification Service (Amazon SNS) para assinar tópicos AWS Backup relacionados, como eventos de backup, restauração e cópia.

Você pode usar o AWS Backup Audit Manager para gerar automaticamente evidências de seus relatórios diários de auditoria de backup para cada conta e região. Você também pode escalar seu monitoramento de backup em várias contas usando um conjunto de modelos e painéis de automação (conhecido como solução de observador de backup) para obter relatórios multirregionais agregados diários entre contas. AWS Backup

Etapa 8. Configuração de backup de auditoria

Para garantir que o programa de backup esteja funcionando como deveria e para identificar e corrigir quaisquer anomalias nos processos de backup, audite a conformidade das AWS Backup políticas em relação aos controles definidos, como a frequência de backup definida. Para encontrar e investigar operações ou recursos de backup que não estejam em conformidade com seus requisitos de negócios, acompanhe de forma contínua e automática sua atividade de backup e gere relatórios automáticos.

AWS Backup O Audit Manager fornece controles de conformidade integrados e personalizáveis que se alinham aos requisitos regulatórios e de conformidade de seus negócios. Você pode usar controles pré-construídos e personalizáveis como estruturas de auditoria para avaliar sua práticas de AWS Backup . Os controles incluem:

- Recursos de backup protegidos por planos de backup
- Frequência mínima e retenção mínima do plano de backup
- Ponto de recuperação de backup criptografado
- Exclusão manual do ponto de recuperação de backup
- Retenção mínima do ponto de recuperação de backup
- Cópia entre regiões
- Cópia entre contas
- Bloqueio do cofre de backups

Para automação de infraestrutura como código (IaC), você pode usar o AWS Backup Audit Manager com. AWS CloudFormation

AWS Security Hub CSPMfornece uma visão abrangente do seu estado de segurança em AWS. Ele também ajuda a verificar seu ambiente em relação às práticas recomendadas de segurança e aos padrões do setor, como os Controles de Práticas Recomendadas de Segurança Básica da AWS. Se você usa o Security Hub CSPM em seu ambiente de nuvem, recomendamos que você habilite o padrão AWS Foundational Security Best Practices, pois ele inclui controles de detetive que podem ajudar a proteger os backups. AWSA maioria dos controles de detetive no AWS Backup Audit Manager e no Security Hub CSPM também está disponível como AWS Config regras gerenciadas.

Etapa 9. Testar os recursos de recuperação de dados

Sua estratégia de backup deve incluir o teste dos backups. Uma estratégia de backup não será eficaz se os dados de backup não puderem ser restaurados. Teste regularmente sua capacidade de encontrar pontos de recuperação específicos e restaurá-los.

Embora copie AWS Backup automaticamente as tags dos recursos que protege para os pontos de recuperação, por padrão, as tags não são copiadas dos pontos de recuperação para os recursos restaurados correspondentes. Para escalar seu gerenciamento de inventário e localizar pontos de recuperação, considere o uso de AWS Backup eventos para iniciar um processo de replicação de tags em recursos criados por trabalhos de AWS Backup restauração.

Você pode iniciar seu fluxo de trabalho de recuperação de dados estabelecendo padrões de recuperação de dados e depois testando-os regularmente. Para aumentar a confiança em sua capacidade de recuperar dados de backup, crie um processo básico e repetível para realizar testes contínuos de recuperação de dados. Por exemplo, é possível criar um padrão para testar uma operação de restauração entre contas e regiões a partir de um cofre central de backup de DR criptografado com uma chave do AWS KMS gerenciada pelo cliente para um cofre de backup da conta de origem criptografado com uma chave do AWS KMS gerenciada pelo cliente diferente.

Se você não testa essas operações de restauração com frequência, talvez descubra que suas suposições sobre AWS KMS criptografia para operações entre contas e regiões estão incorretas. Muitas vezes, o único padrão de recuperação de backup que realmente funciona é o caminho que você costuma testar com frequência. Por meio de testes de rotina dos tipos de recursos de backup compatíveis, é possível identificar avisos antecipados que poderiam causar distúrbios futuros e perda de dados essenciais. Se possível, mantenha um número limitado, mas viável, de caminhos e padrões de recuperação para evitar desperdício de espaço de armazenamento, otimizar custos e economizar tempo. Resolver o problema quando um teste de recuperação falha é mais fácil do que perder dados valiosos ou críticos.

Etapa 10. Incorporar o backup no plano de resposta a incidentes

Simulações de resposta a incidentes de segurança (SIRS) são eventos internos que oferecem uma oportunidade estruturada de praticar seu plano e procedimentos de resposta a incidentes em um cenário realista. É importante testar seus dados e operações de backup em atividades criativas do SIRS para testar a si mesmo contra o inesperado. Isso ajuda você a validar a preparação da sua organização e a desenvolver conforto para lidar com situações raras e inesperadas. Suas

simulações devem ser realistas e envolver equipes organizacionais multifuncionais que precisam responder aos eventos.

Comece com exercícios básicos de simulação e trabalhe com um evento completo e complexo em mente. Por exemplo, é possível criar um modelo realista que consiste em uma nuvem privada virtual (VPC) e recursos associados que simulam a superexposição inadvertida de informações ou uma possível violação de dados causada por alterações nas políticas e nas listas de controle de acesso. Para avaliar a performance do seu plano de resposta a incidentes, documente as lições aprendidas e identifique as melhorias que precisam ser feitas nos futuros procedimentos de resposta.

Você pode usar AWS Backup para configurar backups automatizados em nível de instância como Amazon Machine Images (AMIs) e backups em nível de volume como instantâneos em vários. Contas da AWS Isso pode ajudar sua equipe de resposta a incidentes a aprimorar seus processos forenses, como coleta forense automatizada de discos, fornecendo um ponto de restauração que poderia reduzir o escopo e o impacto de possíveis eventos de segurança, como ransomware.

Próximas etapas

Este guia abordou as 10 principais práticas e controles de segurança para proteger seus dados de backup em AWS. Recomendamos usar essas práticas recomendadas para projetar e implementar uma estratégia e uma arquitetura de backup e recuperação, com várias camadas de controles, capazes de escalar e atender às necessidades de sua empresa. Para obter mais informações sobre AWS Backup, consulte a AWS Backup documentação.

Em caso de dúvidas sobre este guia, inicie um novo tópico no fórum do AWS Backup ou entre em contato com AWS Support.

Recursos

AWS Orientação prescritiva

- Abordagens de backup e recuperação na AWS (guia)

AWS documentação

- AWS Backup
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- Amazon EventBridge
- IAM
- AWS KMS
- AWS Organizations
- AWS Security Hub CSPM
- Amazon SNS

Publicações no blog

- Automatize o backup centralizado em grande escala usando Serviços da AWSAWS Backup
- Arquitetura de recuperação de desastres (DR) ativada AWS, Parte I: Estratégias para recuperação na nuvem
- A importância da criptografia e como AWS pode ajudar
- Melhore a postura de segurança de seus backups com o AWS Backup Vault Lock
- Monitore, avalie e demonstre a conformidade do Backup com o AWS Backup Audit Manager
- Crie e compartilhe backups criptografados entre contas e regiões usando AWS Backup
- Simplifique a auditoria de suas políticas de proteção de dados com o AWS Backup Audit Manager

- Gerenciando o acesso aos backups usando políticas de controle de serviços com AWS Backup
- Obtenha relatórios multirregionais agregados diários entre contas AWS Backup

GitHub repositórios

Os repositórios de código a seguir fornecem uma solução de gerenciamento e implantação para implementar backup e recuperação AWS Backup em toda a AWS Organizations organização, abrangendo várias contas e. Regiões da AWS

- Implemente AWS Backup usando AWS
- Implemente AWS Backup usando pipelines de CI/CD

Histórico do documento

A tabela a seguir descreve alterações significativas feitas neste guia. Se desejar receber notificações sobre futuras atualizações, inscreva-se em um feed RSS.

Alteração	Descrição	Data
Publicação inicial	—	13 de maio de 2022

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.