# Baseline de Segurança para Amazon EC2

## Objetivo

Estabelecer um padrão de segurança consistente para proteger os ativos da organização contra ameaças cibernéticas.

## Introdução

Amazon EC2 (Elastic Compute Cloud) é um serviço central da plataforma Amazon Web Services (AWS) que oferece capacidade computacional escalável na nuvem. EC2 permite aos usuários executar aplicações em um ambiente computacional virtualizado, conhecido como instâncias, o que facilita o escalonamento da capacidade computacional com a mudança das necessidades de negócio.

## Escopo

Este documento se aplica ao Amazon EC2 e todos os controles aqui descritos são obrigatórios.

## Visão Geral dos Controles

|  |  |  |  |
| --- | --- | --- | --- |
| **Controle** | **Racional** | **Aplicabilidade** | **Local de Aplicação do Controle** |
| Implemente Política de Endpoint para Restringir Volumes e Instâncias Não Criptografadas | Aplicar políticas de endpoint personalizadas para restringir a criação de volumes e instâncias não criptografadas aumenta a segurança dos dados, garantindo que todas as novas instâncias e volumes estejam criptografados por padrão. | <TBD> | <TBD> |
| Use o Amazon Inspector para Avaliar Vulnerabilidades em Instâncias EC2 | O Amazon Inspector ajuda a identificar automaticamente vulnerabilidades de software e exposições de rede em instâncias EC2, permitindo a rápida detecção e remediação de potenciais ameaças à segurança. |  |  |
| Encripte Volumes e Snapshots do EBS | A criptografia de volumes e snapshots do EBS protege os dados em repouso dentro da nuvem, garantindo que informações sensíveis estejam seguras contra acessos não autorizados, mesmo que os meios físicos sejam comprometidos. |  |  |
| Atualize o Agente EC2Launch v2 para a Versão Mais Recente em Instâncias Windows EC2 | Atualizar para a versão mais recente do agente EC2Launch v2 em instâncias Windows EC2 garante que você esteja utilizando as funcionalidades mais avançadas para configuração e gerenciamento de instâncias, além de melhorar a segurança e o desempenho. |  |  |
| Garanta o Uso de AMIs Seguras e Configurações de Lançamento Conformes com o Baseline de Segurança | Garantir que todas as novas instâncias EC2 sejam lançadas utilizando AMIs que estejam em conformidade com os padrões de segurança atualizados é crucial para a proteção contra vulnerabilidades conhecidas. Este controle foca em orientar os usuários na seleção de AMIs seguras e na implementação de configurações de lançamento que respeitem as melhores práticas e políticas de segurança da empresa. |  |  |

## Detalhamento dos Controles

Implemente Política de Endpoint para Restringir Volumes e Instâncias Não Criptografadas

* Controle ID: EC2\_001
* Racional: Aplicar políticas de endpoint personalizadas para restringir a criação de volumes e instâncias não criptografadas aumenta a segurança dos dados, garantindo que todas as novas instâncias e volumes estejam criptografados por padrão.
* Riscos Mitigados: Mitiga o risco de exposição de dados sensíveis e não autorizados, fortalecendo a postura de segurança da infraestrutura de nuvem.
* Auditoria:
  + Acesse o console da AWS e vá para o serviço VPC.
  + No painel de navegação, clique em 'Endpoints'.
  + Selecione o endpoint relevante e visualize a política de endpoint em vigor.
  + Verifique se a política inclui regras que proíbam a criação de volumes e instâncias EC2 não criptografadas.
* Remediação:
  + Acesse o console da AWS e vá para o serviço VPC.
  + No painel de navegação, clique em 'Endpoints' e depois selecione o endpoint que você deseja configurar.
  + Clique em 'Modificar política' para editar a política de endpoint existente.
  + Insira uma política que especifique a restrição de criar e lançar volumes e instâncias EC2 não criptografadas, como mostrado no exemplo abaixo:

|  |
| --- |
| {  "Version": "2012-10-17",  "Statement": [  {  "Effect": "Deny",  "Action": [  "ec2:RunInstances",  "ec2:CreateVolume"  ],  "Resource": "\*",  "Condition": {  "Bool": {"ec2:Encrypted": "false"}  }  }  ]  } |

* + Salve e aplique a política.
* Referências:
  + [Documentação oficial da AWS sobre criação de políticas de endpoint](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-access.html#vpc-endpoints-policies)

Use o Amazon Inspector para Avaliar Vulnerabilidades em Instâncias EC2

* Controle ID: EC2\_002
* Racional: O Amazon Inspector ajuda a identificar automaticamente vulnerabilidades de software e exposições de rede em instâncias EC2, permitindo a rápida detecção e remediação de potenciais ameaças à segurança.
* Riscos Mitigados: Mitiga o risco de exploração de vulnerabilidades desconhecidas e não gerenciadas, fortalecendo a segurança das instâncias EC2.
* Auditoria:
  + Acesse o console da AWS e vá para o serviço Amazon Inspector.
  + Verifique se há uma configuração de avaliação existente para as instâncias EC2.
  + Revise os relatórios de avaliação recentes para identificar qualquer sinal de vulnerabilidade ou exposição de rede.
  + Assegure-se de que as avaliações estão sendo executadas regularmente conforme configurado.
* Remediação:
  + Acesse o console da AWS e vá para o serviço Amazon Inspector.
  + Se necessário, crie uma nova configuração de avaliação:
  + Clique em 'Assessment templates' e depois em 'Create'.
  + Selecione o modelo apropriado para as instâncias EC2 ou crie um modelo personalizado.
  + Configure o cronograma de avaliação para executar análises regularmente.
  + Inicie uma avaliação imediatamente para verificar o estado atual das instâncias EC2.
  + Revise os resultados das avaliações e tome as medidas necessárias para remediar quaisquer vulnerabilidades ou exposições identificadas.
* Referências:
  + [Melhores práticas para Amazon EC2 na documentação da AWS](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-best-practices.html)
  + [Guia do usuário do Amazon Inspector](https://docs.aws.amazon.com/inspector/latest/userguide/inspector\_introduction.html)

Encripte Volumes e Snapshots do EBS

* Controle ID: EC2\_003
* Racional: A criptografia de volumes e snapshots do EBS protege os dados em repouso dentro da nuvem, garantindo que informações sensíveis estejam seguras contra acessos não autorizados, mesmo que os meios físicos sejam comprometidos.
* Riscos Mitigados: Mitiga o risco de exposição de dados sensíveis, aumentando a segurança dos dados armazenados em volumes EBS e seus respectivos snapshots.
* Auditoria:
  + Acesse o console da AWS e vá para o serviço EC2.
  + No painel de navegação, clique em 'Volumes' e 'Snapshots' para revisar os existentes.
  + Verifique se todos os volumes e snapshots listados estão criptografados. Isso pode ser identificado pelo status de criptografia na coluna de informações de cada recurso.
* Remediação:
  + Acesse o console da AWS e vá para o serviço EC2.
  + Para criar um novo volume EBS criptografado:
    - Clique em 'Create Volume', selecione os parâmetros desejados, e assegure-se de marcar a opção 'Encrypt this volume'.
    - Escolha uma chave de criptografia gerida pela AWS (AWS-managed key) ou selecione uma chave de criptografia personalizada que você gerencia (customer-managed key).
  + Para criptografar um volume EBS existente que não está criptografado, você precisará criar um snapshot criptografado do volume e, então, criar um novo volume a partir desse snapshot criptografado.
  + Para snapshots, certifique-se de que, ao criar um novo snapshot, a opção de criptografia esteja habilitada.
* Referências:
  + [Melhores práticas para Amazon EC2 na documentação da AWS](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-best-practices.html)
  + [Guia de criptografia de volumes EBS](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html)

Atualize o Agente EC2Launch v2 para a Versão Mais Recente em Instâncias Windows EC2

* Controle ID: EC2\_004
* Racional: Atualizar para a versão mais recente do agente EC2Launch v2 em instâncias Windows EC2 garante que você esteja utilizando as funcionalidades mais avançadas para configuração e gerenciamento de instâncias, além de melhorar a segurança e o desempenho.
* Riscos Mitigados: Mitiga o risco associado a falhas de segurança e problemas de desempenho que podem ocorrer com versões desatualizadas do agente, além de garantir compatibilidade com as últimas atualizações do Windows.
* Auditoria:
  + Acesse o console da AWS e vá para o serviço EC2.
  + Selecione as instâncias Windows que deseja verificar.
  + Conecte-se às instâncias via Remote Desktop Protocol (RDP).
  + Verifique a versão do agente EC2Launch v2 instalada, acessando o diretório onde o agente está instalado ou consultando através do Painel de Controle -> Programas.
* Remediação:
  + Acesse o console da AWS e vá para o serviço EC2.
  + Conecte-se às instâncias Windows que necessitam de atualização do agente EC2Launch v2 via RDP.
  + Acesse o site da AWS ou o console de gerenciamento EC2 para baixar a versão mais recente do EC2Launch v2.
  + Execute o instalador para atualizar o agente na instância.
  + Siga as instruções de instalação fornecidas pela AWS para garantir que o agente seja atualizado corretamente.
  + Reinicie a instância, se necessário, para completar a atualização.
* Referências:
  + [Melhores práticas para Windows na Amazon EC2 na documentação da AWS](https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/windows-ec2-best-practices.html)
  + [Documentação do EC2Launch v2](https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2launch-v2.html)

Garanta o Uso de AMIs Seguras e Configurações de Lançamento Conformes com o Baseline de Segurança

* Controle ID: EC2\_005
* Racional: Garantir que todas as novas instâncias EC2 sejam lançadas utilizando AMIs que estejam em conformidade com os padrões de segurança atualizados é crucial para a proteção contra vulnerabilidades conhecidas. Este controle foca em orientar os usuários na seleção de AMIs seguras e na implementação de configurações de lançamento que respeitem as melhores práticas e políticas de segurança da empresa.
* Riscos Mitigados: Mitiga o risco de ataques explorando vulnerabilidades conhecidas em instâncias EC2, que podem ser evitados através da correta utilização de AMIs seguras e configurações de lançamento adequadas.
* Auditoria:
  + Acesse o console da AWS e vá para o serviço EC2.
  + Verifique se as instâncias lançadas estão utilizando AMIs aprovadas e atualizadas.
  + Confirme que as configurações de lançamento, incluindo grupos de segurança, políticas de IAM e outras configurações de rede, estão em conformidade com as políticas internas de segurança.
  + Utilize ferramentas de conformidade e segurança para avaliar periodicamente as instâncias quanto à aderência aos padrões de segurança.
* Remediação:
  + Eduque os usuários sobre a importância de selecionar AMIs seguras e atualizadas disponibilizadas pelo time responsável.
  + Estabeleça procedimentos claros para a configuração de lançamento de novas instâncias, incluindo a seleção de grupos de segurança, configurações de rede e políticas de IAM apropriadas.
  + Implemente políticas de grupo ou utilize ferramentas de gestão de configuração, como Ansible, Chef, ou Puppet, para assegurar a manutenção das configurações de segurança após o lançamento das instâncias.
  + Monitore e audite regularmente o uso de AMIs e as configurações de lançamento para garantir conformidade contínua com os requisitos de segurança.
* Referências:
  + [Melhores práticas para Windows na Amazon EC2 na documentação da AWS](https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/windows-ec2-best-practices.html)
  + [Guia de Segurança na Amazon EC2](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security.html)

## Histórico de alterações

|  |  |  |  |
| --- | --- | --- | --- |
| **Versão** | **Data de Publicação** | **Descrição** | **Alterações** |
| 1.0 | 14/04/2024 | Inclusão inicial de controles de segurança para EC2 | * Controles incluídos: ec2\_endpoint\_control\_001 Política de Endpoint Personalizada * ec2\_endpoint\_control\_002 Amazon Inspector para Vulnerabilidades * ec2\_endpoint\_control\_003 Criptografia de Volumes e Snapshots do EBS * ec2\_endpoint\_control\_004 Atualização do Agente EC2Launch v2 * ec2\_endpoint\_control\_005 Uso de AMIs Seguras * Controles excluídos: None * Controles alterados: None" |