Whitepaper da AWS

Criptografar dados de arquivos com o Amazon Elastic File System

Criptografar dados de arquivos com o Amazon Elastic File System: Whitepaper da AWS

Table of Contents

Criptografar dados de arquivos com o Amazon Elastic File System

Data de publicação: 22 de fevereiro de 2021 (Histórico do documento e colaboradores)

Resumo

A segurança vem antes de qualquer outra etapa para a AWS, e oferecemos aos nossos clientes as ferramentas para que isso aconteça em suas empresas também. As regulamentações governamentais e as políticas de conformidade do setor ou da empresa podem exigir que dados de diferentes classificações sejam protegidos usando políticas de criptografia, algoritmos criptográficos e gerenciamento adequado de chaves. Este artigo descreve as práticas recomendadas para criptografar o Amazon Elastic File System (Amazon EFS).

Introdução

O Amazon Elastic File System (Amazon EFS) fornece sistemas de arquivos compartilhados simples, escaláveis, altamente disponíveis e altamente duráveis na nuvem. Os sistemas de arquivos que você cria usando o Amazon EFS são elásticos, permitindo que eles cresçam e diminuam automaticamente à medida que você adiciona e remove dados. Eles podem aumentar de tamanho para petabytes, distribuindo dados em um número irrestrito de servidores de armazenamento em várias zonas de disponibilidade (AZs).

Os dados armazenados nesses sistemas de arquivos podem ser criptografados em repouso e em trânsito usando o Amazon EFS. Para criptografia de dados em repouso, você pode criar sistemas de arquivos criptografados por meio do Console de Gerenciamento da AWS ou da AWS Command Line Interface (AWS CLI). Você também pode criar sistemas de arquivos criptografados programaticamente por meio da API do Amazon EFS ou de um dos SDKs da AWS.

Para criptografia de dados em repouso, o Amazon EFS se integra com o AWS Key Management Service (AWS KMS) para gerenciamento de chaves. Você também pode habilitar a criptografia de dados em trânsito montando o sistema de arquivos e transferindo todo o tráfego NFS por um Transport Layer Security (TLS).

Este artigo descreve as práticas recomendadas de criptografia para o Amazon EFS. Ele descreve como habilitar a criptografia de dados em trânsito na camada de conexão do cliente e como criar um sistema de arquivos criptografados no Console de Gerenciamento da AWS e na AWS CLI.

> **Note**
>
> Usar as APIs e os SDKs para criar um sistema de arquivos criptografados está fora do escopo deste artigo. Para obter mais informações sobre como isso é feito, consulte API do Amazon EFS no Guia do usuário do Amazon EFS ou na documentação do SDK.

Conceitos básicos e terminologia

Esta seção define os conceitos e a terminologia mencionados neste whitepaper.

- Amazon Elastic File System (Amazon EFS): um serviço altamente disponível e altamente durável que fornece armazenamento de arquivos simples, escalável e compartilhado na Nuvem AWS. O Amazon EFS fornece uma interface de sistema de arquivos e uma semântica padrão do sistema de arquivos. Você pode armazenar praticamente uma quantidade ilimitada de dados em um número ilimitado de servidores de armazenamento em várias zonas de disponibilidade.
- AWS Identity and Access Management (IAM): um serviço que permite controlar com segurança o acesso refinado às APIs de serviço da AWS. As políticas são criadas e usadas para limitar o acesso a usuários, grupos e funções individuais. Você pode gerenciar suas chaves do AWS KMS por meio do console do IAM.
- AWS KMS : um serviço gerenciado que facilita a criação e o controle de chaves mestras do cliente (CMKs), as chaves de criptografia usadas para criptografar seus dados. As CMKs do AWS KMS são protegidas por módulos de segurança de hardware (HSMs) validados pelo Cryptographic Module Validation Program FIPS 140-2, exceto nas regiões China (Pequim) e China (Ningxia). O AWS KMS é integrado a outros serviços da AWS que criptografam seus dados. Ele também é totalmente integrado com o AWS CloudTrail para fornecer logs de chamadas de API feitas pelo AWS KMS em seu nome, o que pode ser útil para atender aos requisitos de conformidade ou regulamentares aplicáveis à sua organização.
- Chave mestra do cliente (CMK): representa o topo da hierarquia de chaves. Ela contém material de chave para criptografar e descriptografar dados. O AWS KMS pode gerar esse material de chaves ou você pode gerá-lo e importá-lo para o AWS KMS. As CMKs são específicas para uma conta e região da AWS e podem ser gerenciadas pelo cliente ou pela AWS.
- CMK gerenciada pela AWS: uma CMK gerada pela AWS em seu nome. Uma CMK gerenciada pela AWS é criada quando você habilita a criptografia para um recurso de um serviço integrado da AWS. As políticas de chaves da CMK gerenciadas pela AWS são gerenciadas pela AWS e você não pode alterá-las. Não há cobrança pela criação ou armazenamento de CMKs gerenciadas pela AWS.
- CMK gerenciada pelo cliente: uma CMK que você cria usando o console de gerenciamento da AWS ou API, AWS CLI ou SDKs. Você pode usar uma CMK gerenciada pelo cliente quando precisar de um controle mais granular sobre a CMK.
- Política de chaves do KMS: uma política de recursos que controla o acesso a uma CMK gerenciada pelo cliente. Os clientes definem essas permissões usando a política de chaves ou

uma combinação de políticas do IAM e a política de chaves. Para obter mais informações, consulte Visão geral do gerenciamento de acesso no Guia do desenvolvedor do AWS KMS.

- Chaves de dados : chaves criptográficas geradas pelo AWS KMS para criptografar dados fora do AWS KMS. O AWS KMS permite que entidades autorizadas (usuários ou serviços) obtenham chaves de dados protegidas por uma CMK.
- Transport Layer Security (TLS): sucessor do Secure Sockets Layer (SSL), o TLS é um protocolo criptográfico essencial para criptografar informações trocadas em uma rede.
- Auxiliar de montagem do EFS: um agente cliente Linux (`amazon-efs-utils`) usado para simplificar a montagem de sistemas de arquivos do EFS. Ele pode ser usado para configurar, manter e encaminhar todo o tráfego NFS em um túnel TLS.

Para obter mais informações sobre conceitos básicos e terminologia, consulte Conceitos do AWS Key Management Service no Guia do desenvolvedor do AWS KMS.

Criptografia de dados em repouso

A AWS fornece as ferramentas para você criar um sistema de arquivos criptografados que criptografa todos os seus dados e metadados em repouso usando um algoritmo de criptografia AES-256 padrão do setor. Um sistema de arquivos criptografados é projetado para lidar com criptografia e descriptografia de forma automática e transparente, para que você não precise modificar suas aplicações. Se sua organização estiver sujeita a políticas corporativas ou regulamentares que exijam criptografia de dados e metadados em repouso, recomendamos que você crie um sistema de arquivos criptografados.

Tópicos

Gerenciamento de chaves

O Amazon EFS é integrado ao AWS KMS, que gerencia as chaves de criptografia para sistemas de arquivos criptografados. O AWS KMS também oferece suporte à criptografia por outros serviços da AWS, como Amazon Simple Storage Service (Amazon S3), Amazon Elastic Block Store (Amazon EBS), Amazon Relational Database Service (Amazon RDS), Amazon Aurora, Amazon Redshift, Amazon WorkMail, WorkSpaces, etc. Para criptografar o conteúdo do sistema de arquivos, o Amazon EFS usa o algoritmo Advanced Encryption Standard com o modo XTS e uma chave de 256 bits (XTS-AES-256).

Há três perguntas importantes a serem respondidas ao considerar como proteger dados em repouso adotando qualquer política de criptografia. Essas perguntas são igualmente válidas para dados armazenados em serviços gerenciados e não gerenciados, como o Amazon EBS.

Onde as chaves são armazenadas?

O AWS KMS armazena suas chaves mestras em um armazenamento altamente durável em um formato criptografado para ajudar a garantir que elas possam ser recuperadas quando necessário.

Onde as chaves são usadas?

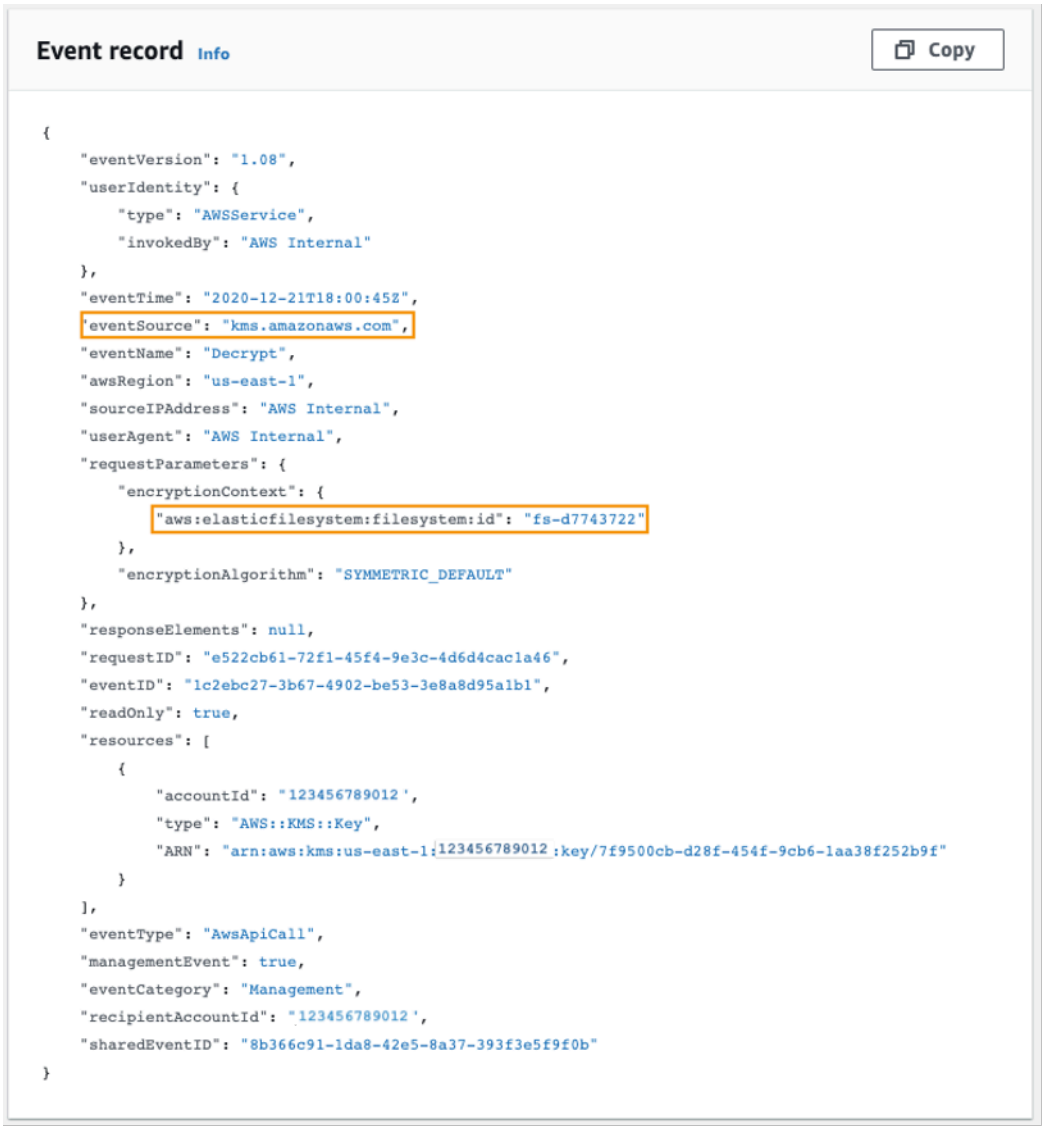
Usar um sistema de arquivos criptografado do Amazon EFS é transparente para os clientes que montam o sistema de arquivos. Todas as operações criptográficas ocorrem dentro do serviço EFS, pois os dados são criptografados antes de serem gravados no disco e descriptografados depois que um cliente emite uma solicitação de leitura.

Quem pode usar as chaves?

As políticas de chaves do AWS KMS controlam o acesso às chaves de criptografia.

Recomendamos combiná-los com políticas do IAM para fornecer outra camada de controle. Cada chave tem uma política de chaves. Se a chave for CMK e gerenciada pela AWS, a AWS gerenciará a política de chaves. Se a chave for CMK e gerenciada pelo cliente, você gerenciará a política de chaves. Essas políticas de chaves são a principal maneira de controlar o acesso às CMKs. Elas definem as permissões que regem o uso e o gerenciamento de chaves.

Ao criar um sistema de arquivos criptografados usando o Amazon EFS, você concede ao Amazon EFS acesso para usar a CMK em seu nome. As chamadas que o Amazon EFS faz para o AWS KMS em seu nome aparecem nos logs do CloudTrail, como se tivessem sido originadas da sua conta da AWS. A captura de tela a seguir mostra o evento de exemplo do CloudTrail para uma chamada do KMS Decrypt feita pelo Amazon EFS.



Log do CloudTrail para KMS Decrypt

Para obter mais informações sobre o AWS KMS e como gerenciar o acesso a chaves de criptografia, consulte Gerenciar o acesso a CMKs do AWS KMS no Guia do desenvolvedor do AWS KMS.

Para obter mais informações sobre como o AWS KMS gerencia a criptografia, consulte o whitepaper AWS KMS Cryptographic Details (Detalhes criptográficos do AWS KMS).

Para obter mais informações sobre como criar um usuário e grupo administrador do IAM, consulte Criar o seu primeiro usuário administrador e um grupo de usuários do IAM no Guia do usuário do IAM.

Criar um sistema de arquivos criptografados

Você pode criar um sistema de arquivos criptografados usando o Console de Gerenciamento da AWS, a AWS CLI, a API do Amazon EFS ou os SDKs da AWS. Você só pode habilitar a criptografia para um sistema de arquivos ao criá-lo.

O Amazon EFS se integra ao AWS KMS para gerenciamento de chaves e usa uma CMK para criptografar o sistema de arquivos. Os metadados do sistema de arquivos, como nomes de arquivos, nomes de diretório e conteúdo de diretório, são criptografados e descriptografados usando uma CMK gerenciada pela AWS.

O conteúdo dos seus arquivos, ou dados do arquivo, é criptografado e descriptografado usando uma CMK de sua escolha. A CMK pode ser de um dos três tipos:

- Uma CMK gerenciada pela AWS para Amazon EFS
- Uma CMK gerenciada pelo cliente da sua conta da AWS
- Uma CMK gerenciada pelo cliente a partir de uma conta diferente da AWS

Sua organização pode estar sujeita a políticas corporativas ou regulatórias que exigem controle total em termos de criação, alternância e exclusão, bem como controle de acesso e política de uso para as CMKs. Nesse caso, recomendamos que você use uma CMK gerenciada pelo cliente. Em outros cenários, você pode usar uma CMK gerenciada pela AWS.

Todos os usuários têm uma CMK gerenciada pela AWS para o Amazon EFS, cujo alias é `aws/elasticfilesystem`. A AWS gerencia essa política de chaves da CMK e você não pode alterá-la. Não há custo para criar e armazenar CMKs gerenciadas pela AWS.

Se você decidir usar uma CMK gerenciada pelo cliente para criptografar seu sistema de arquivos, selecione o alias de chave da CMK gerenciada pelo cliente que você possui. Como alternativa, você pode inserir o nome do recurso da Amazon (ARN) de uma CMK gerenciada pelo cliente que pertence a uma conta diferente. Com uma CMK gerenciada pelo cliente que você possui, você controla quais usuários e serviços podem usar a chave por meio de políticas de chaves e concessões de chave.

Você também controla a vida útil e a alternância dessas chaves escolhendo quando desabilitar, reativar, excluir ou revogar o acesso a elas. Para obter informações sobre como gerenciar o acesso a chaves em outras contas da AWS, consulte Alterar uma política de chaves no Guia do desenvolvedor do AWS KMS.

Para obter mais informações sobre como gerenciar CMKs gerenciadas pelo cliente, consulte Chaves mestras do cliente (CMKs) no Guia do desenvolvedor do AWS KMS.

As seções a seguir discutem como criar um sistema de arquivos criptografados usando o Console de Gerenciamento da AWS e a AWS CLI.

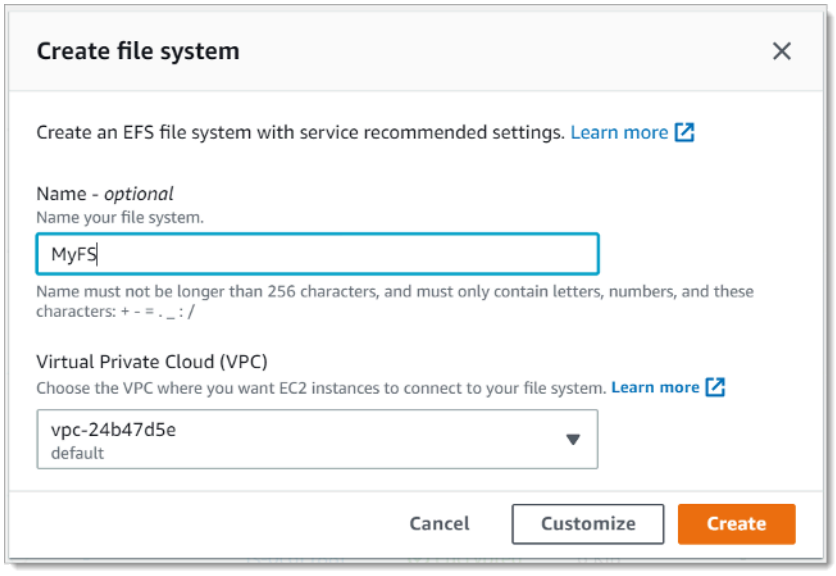
Criar um sistema de arquivos criptografados usando o Console de Gerenciamento da AWS

Use o procedimento a seguir para criar um sistema de arquivos criptografados do Amazon EFS usando o Console de Gerenciamento da AWS.

Etapa 1. Definir as configurações do sistema de arquivos

Nesta etapa, você deve fazer as configurações gerais do sistema de arquivos, incluindo gerenciamento do ciclo de vida, modos de performance e taxa de transferência e criptografia de dados em repouso.

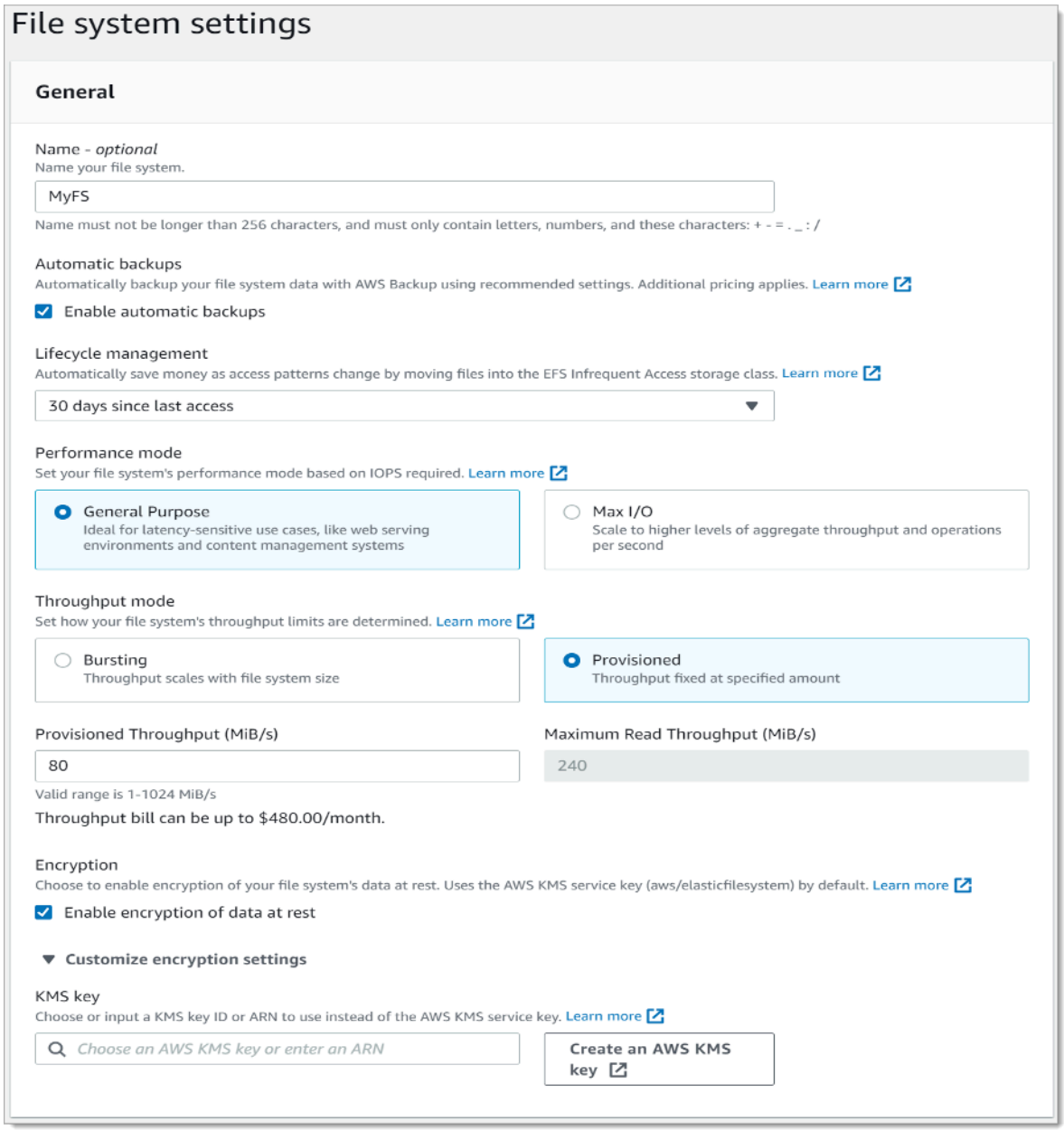
1. Faça login no Console de Gerenciamento da AWS e abra o console do Amazon EFS.
2. Escolha Create file system (Criar sistema de arquivos) para abrir a caixa de diálogo Create file system (Criar sistema de arquivos). Para obter mais informações sobre como criar um sistema de arquivos usando as configurações recomendadas que incluem habilitar a criptografia por padrão, consulte Criar seu sistema de arquivos do Amazon EFS.



Criar sistema de arquivos do EFS

3. (Opcional) Selecione Customize (Personalizar) para criar um sistema de arquivos personalizado em vez de criar um sistema de arquivos usando as configurações recomendadas pelo serviço.

   A página de configurações do sistema de arquivos é exibida.



   Criar sistema de arquivos do EFS: configurações gerais

4. Para as configurações General (Gerais), insira os detalhes a seguir:

   - (Opcional) Insira um Name (Nome) para o sistema de arquivos.

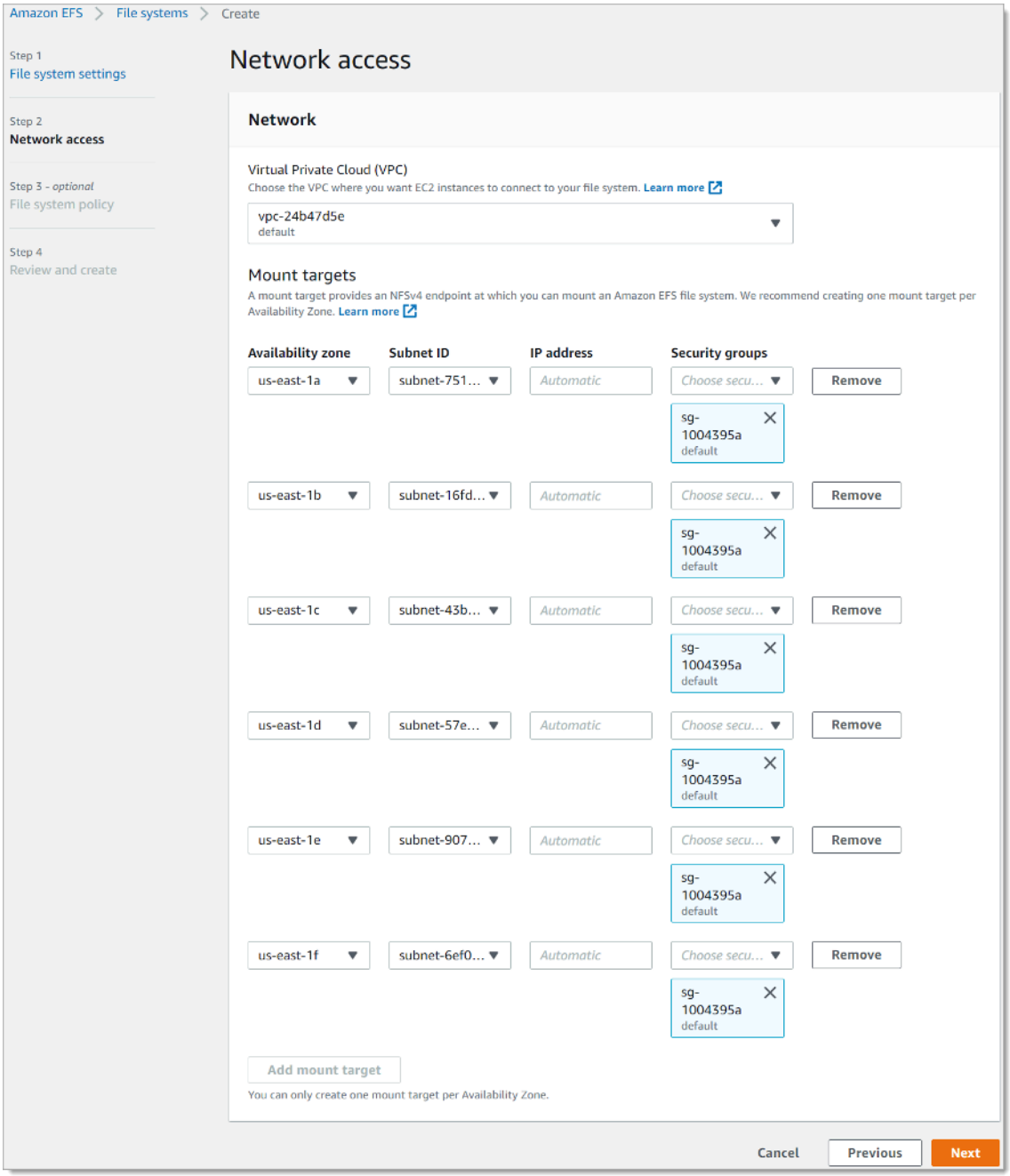
- Backups automáticos são ativados por padrão. É possível desativar backups automáticos desmarcando a caixa de seleção. Para obter mais informações, consulte Usar AWS Backup com Amazon EFS.
- Escolha uma política de gerenciamento do ciclo de vida. O gerenciamento de ciclo de vida útil do Amazon EFS gerencia automaticamente o armazenamento de arquivos econômico dos seus sistemas de arquivos. Quando habilitado, o gerenciamento do ciclo de vida migra os arquivos que não foram acessados por um período definido para a classe de armazenamento de acesso infrequente (IA). Esse período é definido usando a política do ciclo de vida. Se você não quiser que o gerenciamento do ciclo de vida seja ativado, escolha None (Nenhum). Para obter mais informações, consulte Gerenciamento do ciclo de vida do EFS no Guia do usuário do Amazon EFS.
- Escolha um Performance mode (Modo de performance), General Purpose mode (modo de uso geral) ou Max I/O (E/S máx.). Para obter mais informações, consulte Modos de performance no Guia do usuário do Amazon EFS.
- Escolha um Throughput mode (Modo de taxa de transferência), que pode ser o padrão Bursting (Intermitente) ou o Provisioned (Provisionado).
- Se você selecionou Provisioned (Provisionado), o campo Provisioned Throughput (MiB/s) (Taxa de transferência provisionada (MiB/s)) será exibido. Insira a quantidade de taxa de transferência a ser provisionada para o sistema de arquivos. Depois de inserir a taxa de transferência, o console exibirá uma estimativa do custo mensal ao lado do campo. Para obter mais informações, consulte Modos de taxa de transferência no Guia do usuário do Amazon EFS.
- Em Encryption (Criptografia), a criptografia de dados em repouso é habilitada por padrão. Ela usa sua chave de serviço do EFS do AWS Key Management Service (AWS KMS) (`aws/elasticfilesystem`) por padrão. Para escolher uma chave KMS diferente para criptografia, expanda as configurações de criptografia Customize (Personalizar) e escolha uma chave na lista. A outra opção é inserir um ID de chave KMS ou nome do recurso da Amazon (ARN) para a chave KMS a ser usada.

  Se você precisar criar uma chave, escolha Create an AWS Key (Criar uma chave do AWS KMS) para iniciar o console do AWS KMS e criar uma chave.

5. (Opcional) Escolha Add tag (Adicionar etiqueta) para adicionar pares de valores-chave ao sistema de arquivos.
6. Escolha Next (Próximo) para prosseguir para a etapa Network Access (Acesso à rede) no processo de configuração.

Etapa 2. Configurar o acesso à rede

Nesta etapa, você definirá as configurações de rede do sistema de arquivos, incluindo a nuvem privada virtual (VPC) e os destinos de montagem. Para cada destino de montagem, defina a zona de disponibilidade, a sub-rede, o endereço IP e os grupos de segurança.



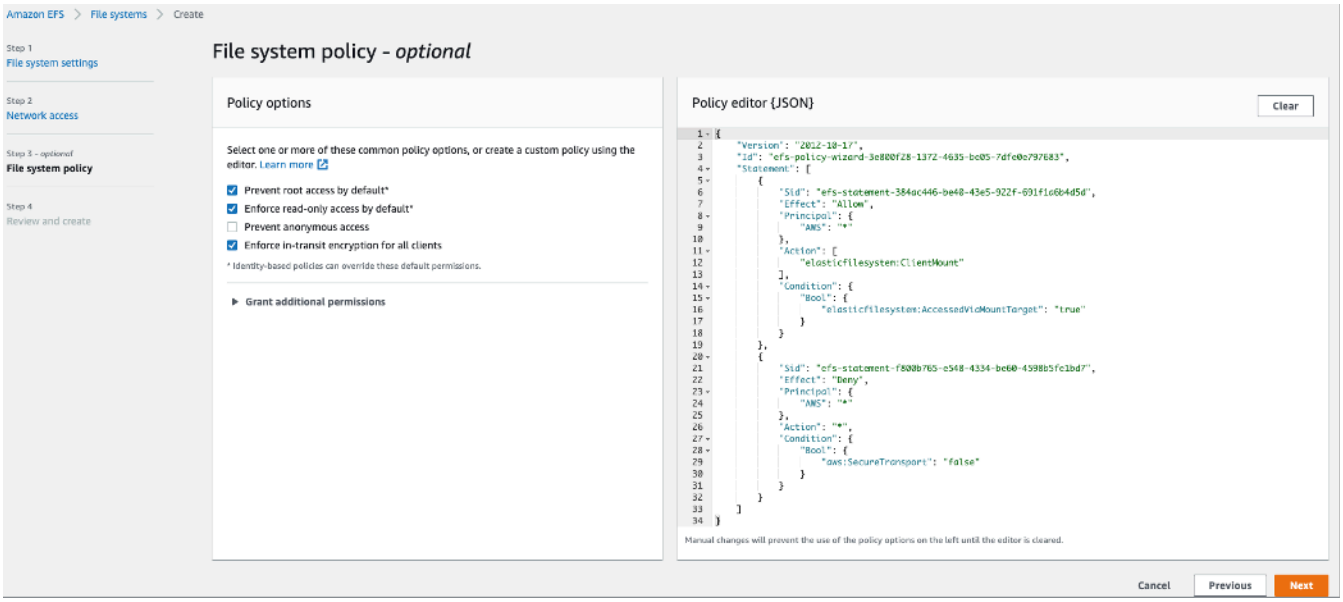
Criar sistema de arquivos do EFS: acesso à rede

1. Escolha a nuvem privada virtual (VPC) na qual deseja que as instâncias do EC2 se conectem ao sistema de arquivos. Para obter mais informações, consulte Gerenciar a acessibilidade de rede do sistema de arquivos no Guia do usuário do Amazon EFS.
   - Zona de disponibilidade: por padrão, um destino de montagem é configurado em cada zona de disponibilidade em uma região da AWS. Se você não quiser um destino de montagem em determinada zona de disponibilidade, escolha Remove (Remover) para excluir o destino de montagem dessa zona. Crie um destino de montagem em todas as zonas de disponibilidade em que deseja acessar seu sistema de arquivos. Não há custos.
   - ID de sub-rede: escolha entre as sub-redes disponíveis em uma zona de disponibilidade. A sub-rede padrão é pré-selecionada. Como prática recomendada, certifique-se de que a sub-rede escolhida seja pública ou privada com base nos seus requisitos de segurança.
   - Endereço IP: por padrão, o Amazon EFS escolhe o endereço IP automaticamente dos endereços disponíveis na sub-rede. Também é possível inserir um endereço IP específico que está na sub-rede. Embora o destino de montagem tenha um único endereço IP, eles são recursos de rede redundantes e altamente disponíveis.
   - Grupos de segurança: é possível especificar um ou mais grupos de segurança para o destino de montagem. Como prática recomendada, verifique se o grupo de segurança é usado apenas para fins de montagem do EFS (porta NFS 2049) e se as regras de entrada permitem somente a porta 2049 de outro intervalo de blocos CIDR da VPC ou utilize o grupo de segurança como fonte dos recursos que precisam acessar o EFS. Para obter mais informações, consulte Uso de grupos de segurança para instâncias do Amazon EC2 e destinos de montagem no Guia do usuário do Amazon EFS.

     Para adicionar outro grupo de segurança ou alterá-lo, selecione Choose security groups (Escolher grupos de segurança) e adicione outro grupo de segurança da lista. Se não desejar usar o grupo de segurança padrão, você pode excluí-lo. Para obter mais informações, consulte Criar grupos de segurança no Guia do usuário do Amazon EFS.
2. Escolha Add mount target (Adicionar destino de montagem) para criar um destino de montagem para uma zona de disponibilidade que não tenha um. Se um destino de montagem estiver configurado para cada zona de disponibilidade, esta opção não estará disponível.
3. Escolha Next (Próximo) para continuar. A página File system policy (Política de sistema de arquivos) é exibida.

Etapa 3. Criar uma política de sistema de arquivos

Nesta etapa, você cria uma política de sistema de arquivos para controlar o acesso do cliente NFS ao sistema de arquivos. Uma política de sistema de arquivos do EFS é uma política de recursos do IAM utilizada para controlar o acesso do cliente NFS ao sistema de arquivos. Para obter mais informações, consulte Usar o IAM para controlar o acesso NFS ao Amazon EFS no Guia do usuário do Amazon EFS.

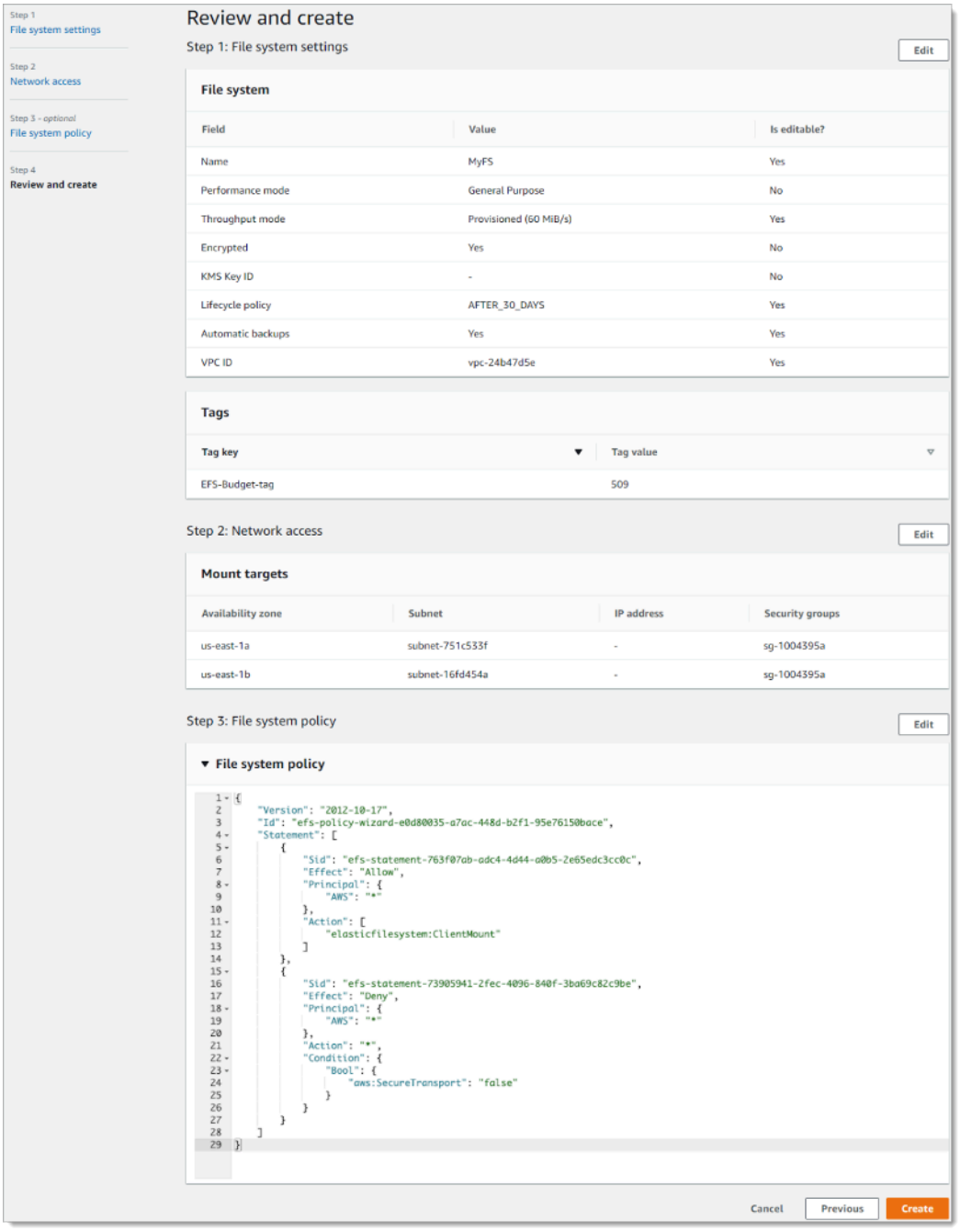


Criar sistema de arquivos do EFS: política do sistema de arquivos

1. Em Policy options (Opções de política), recomendamos que você escolha as seguintes opções de política pré-configuradas disponíveis:
   - Impedir acesso raiz por padrão
   - Impor acesso somente leitura por padrão
   - Impor criptografia em trânsito para todos os clientes
2. Use Grant additional permissions (Conceder permissões adicionais) para conceder permissões do sistema de arquivos a mais entidades principais do IAM, incluindo outra conta da AWS. Escolha Add (Adicionar) e insira o ARN da entidade principal à qual você está concedendo permissões. Depois, escolha as Permissions (Permissões) a serem concedidas.
3. Use o Policy editor (Editor de políticas) para personalizar uma política pré-configurada ou criar sua própria política com base no que você precisa. Quando uma das políticas pré-configuradas é escolhida, a definição de política JSON aparece no editor de políticas.
4. Escolha Next (Próximo) para continuar. A página Review and create (Revisar e criar) é exibida.

Etapa 4. Revisar e criar

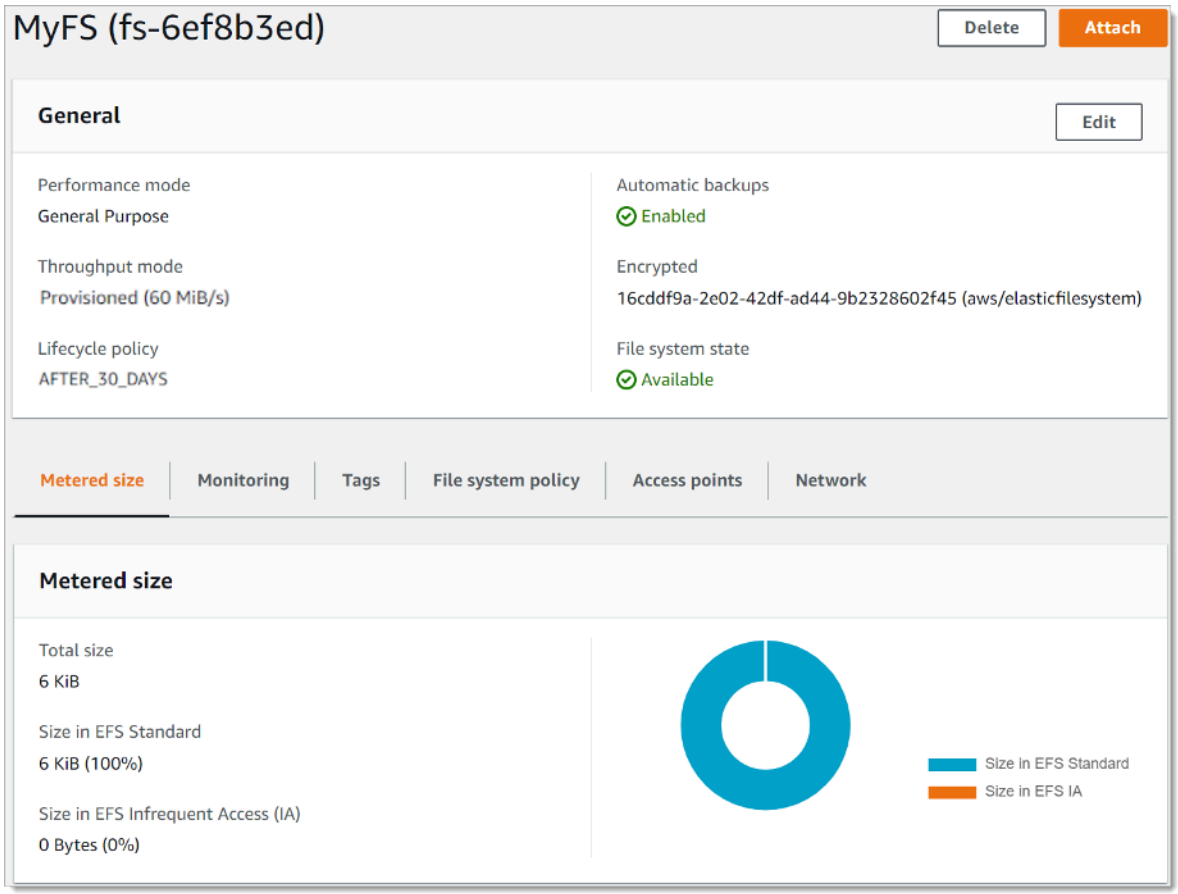
Nesta etapa, você revisará as configurações do sistema de arquivos, fará as modificações necessárias e, depois, criará o sistema de arquivos.



Criar sistema de arquivos do EFS: revisar e criar

1. Revise cada um dos grupos de configuração do sistema de arquivos. É possível fazer alterações em cada grupo nessa etapa, escolhendo a opção Edit (Editar).

2. Escolha Create (Criar) para criar o sistema de arquivos e retornar à página File Systems (Sistemas de arquivos).
3. A página File systems (Sistemas de arquivos) exibe o sistema de arquivos e seus detalhes de configuração, conforme mostrado a seguir.



File Systems (Sistemas de arquivo)

Criar um sistema de arquivos criptografados usando a AWS CLI

Ao usar a AWS CLI para criar um sistema de arquivos criptografados, você pode usar parâmetros adicionais para definir o status de criptografia e a CMK gerenciada pelo cliente. Você deve usar a versão mais recente da AWS CLI. Para obter informações sobre como atualizar a AWS CLI, consulte Instalação, atualização e desinstalação da AWS CLI no Guia do usuário da AWS Command Line Interface.

Na operação `CreateFileSystem`, o parâmetro `--encrypted` é booliano e é necessário para criar sistemas de arquivos criptografados. O `--kms-key-id` é necessário somente quando você usa uma

CMK gerenciada pelo cliente e inclui o alias ou o ARN da chave. Não inclua esse parâmetro se você estiver usando a CMK gerenciada pela AWS.

```
$ aws efs create-file-system \
--creation-token $(uuidgen) \
--performance-mode generalPurpose \
--encrypted \
--kms-key-id user/customer-managedCMKalias
```

Para obter mais informações sobre a criação de sistemas de arquivos do Amazon EFS usando o Console de Gerenciamento da AWS, a AWS CLI, os SDKs da AWS ou a API do Amazon EFS, consulte O que é o Amazon Elastic File SystemGuia do usuário do Amazon EFS.

Aplicar criptografia de dados em repouso

A criptografia tem um efeito mínimo na latência de E/S e na taxa de transferência. A criptografia e a descriptografia são transparentes para usuários, aplicações e serviços. Todos os dados e metadados são criptografados pelo Amazon EFS em seu nome antes de serem gravados no disco, e descriptografados antes de serem lidos pelos clientes. Você não precisa alterar as ferramentas do cliente, as aplicações ou os serviços para acessar um sistema de arquivos criptografados.

Sua organização pode exigir a criptografia de todos os dados que atendem a uma classificação específica ou que estejam associados a determinada aplicação, workload ou ambiente. Você pode usar o AWS Identity and Access Management (IAM) e as políticas baseadas em identidade dele para forçar a criptografia de dados em repouso para seus recursos do sistema de arquivos do Amazon EFS. Usando uma chave de condição do IAM, você pode impedir que os usuários criem sistemas de arquivos do EFS que não estejam criptografados.

Por exemplo, uma política do IAM que permite explicitamente que os usuários criem apenas sistemas de arquivos do EFS criptografados usa a seguinte combinação de efeito, ação e condição:

- O `Effect` é `Allow`.
- O `Action` é `elasticfilesystem:CreateFileSystem`.
- O `Condition` `elasticfilesystem:Encrypted` é `true`.

O exemplo a seguir ilustra uma política baseada em identidade do IAM que autoriza as entidades principais a criar somente sistemas de arquivos criptografados.

```
{
  “Version”: “2012-10-17”,
  “Statement”: [
    {
      “Sid”: “VisualEditior0”,
      “Effect”: “Allow”,
      “Action”: “elasticfilesystem:CreateFileSystem”,
      “Condition”: {
        “Bool”: {
          “elasticfilesystem:Encrypted”: “true”
        }
      },
      “Resource”: “*”
    }
}
```

O atributo `Resource` definido como * significa que a política do IAM se aplica a todos os recursos do EFS criados. Você pode adicionar atributos condicionais adicionais com base em etiquetas para aplicá-lo somente para um subconjunto de recursos do EFS com necessidades de classificação de dados.

Você também pode impor a criação de sistemas de arquivos criptografados do Amazon EFS no nível do AWS Organizations usando políticas de controle de serviço para todas as contas da AWS ou OUs em sua organização. Para obter mais informações sobre políticas de controle de serviço no AWS Organizations, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations.

Criar uma política do IAM exigindo que todos os sistemas de arquivos do EFS sejam criptografados

Você pode criar uma política baseada em identidade do IAM que autoriza os usuários a criar somente sistemas de arquivos criptografados do Amazon EFS usando o console, a AWS CLI ou a API. O procedimento a seguir descreve como criar essa política usando o console do IAM e depois aplicá-la a um usuário em sua conta.

Para criar uma política do IAM para impor sistemas de arquivos do EFS criptografados:

1. Faça login no Console de Gerenciamento da AWS e abra o console do IAM.

2. No painel de navegação, em Access management (Gerenciamento de acesso), escolha Policies (Políticas).
3. Escolha Create policy (Criar política) para exibir a página Criar política.
4. Na guia Visual Editor (Editor visual), insira as seguintes informações:
   - Em Service (Serviço), escolha EFS.
   - Em Actions (Ações), insira `create` no campo de pesquisa e escolha CreateFileSystem.
   - Em Request conditions (Condições de solicitação), clique no link Add condition (Adicionar condição), procure `elasticfilesystem:Encrypted` para a Condition Key (Chave de condição), `Bool` para Operator (Operador) e `true` para Value (Valor).
5. Forneça um Name (nome) e uma Description (Descrição) para a política. Verifique o resumo da política, incluindo a condição de solicitação Encrypted (Criptografada).
6. Escolha Create policy (Criar política) para criar a política.

Para aplicar a política a um usuário em sua conta:

1. No console do IAM, em Access management (Gerenciamento de acesso), escolha Users (Usuários).
2. Selecione o usuário ao qual você deseja aplicar a política.
3. Escolha Add permissions (Adicionar permissões) para exibir a página Add permissions (Adicionar permissões).
4. Escolha Attach existing policies directly (Anexar políticas existentes diretamente).
5. Insira o nome da política do EFS criada no procedimento anterior.
6. Selecione e expanda a política. Escolha {}JSON para verificar o conteúdo da política. Deve se parecer com a seguinte política do JSON:

```
{
  “Version”: “2012-10-17”,
  “Statement”: [
    {
      “Sid”: “VisualEditior0”,
      “Effect”: “Allow”,
      “Action”: “elasticfilesystem:CreateFileSystem”,
      “Condition”: {
        “Bool”: {
          “elasticfilesystem:Encrypted”: “true”
```

```
        }
      },
      “Resource”: “*”
    }
}
```

Detectar sistemas de arquivos não criptografados

Sua organização pode ter um requisito para identificar recursos do Amazon EFS que não estão criptografados. Você pode detectar sistemas de arquivos não criptografados usando o AWS Config Managed Rules. O AWS Config fornece regras gerenciadas da AWS, que são regras predefinidas e personalizáveis que o AWS Config usa para avaliar se os recursos da AWS estão em conformidade com as práticas recomendadas comuns e para sinalizar os recursos que falham nas regras como NON_COMPLIANT.

Você pode usar a regra do AWS Managed Config `efs-encrypted-check` para verificar se o Amazon Elastic File System (Amazon EFS) está configurado para criptografar os dados do arquivo usando o AWS Key Management Service (AWS KMS). Para obter mais informações sobre como configurar e ativar as regras gerenciadas da AWS, consulte Working with AWS Config Managed Rules (Trabalhar com regras gerenciadas do AWS Config).

Criptografia de dados em trânsito

Você pode montar um sistema de arquivos para que todo o tráfego NFS seja criptografado em trânsito usando o Transport Layer Security 1.2 (TLS) com uma cifra AES-256 padrão do setor. O TLS é um conjunto de protocolos criptográficos padrão do setor usado para criptografar informações trocadas pela rede. AES-256 é uma cifra de criptografia de 256 bits usada para transmissão de dados em TLS. Recomendamos configurar a criptografia em trânsito em todos os clientes que acessam o sistema de arquivos.

Você pode usar políticas do IAM para impor a criptografia em trânsito para o acesso do cliente NFS ao Amazon EFS. Quando um cliente se conecta a um sistema de arquivos, o Amazon EFS avalia a política de recurso do IAM do sistema de arquivos, que é chamada de política de sistema de arquivos, com qualquer política do IAM baseada em identidade, a fim de determinar as permissões de acesso apropriadas ao sistema de arquivos que devem ser concedidas. Você pode usar a chave de condição `aws:SecureTransport` na política de recursos do sistema de arquivos para impor que os clientes NFS usem o TLS ao se conectarem a um sistema de arquivos do EFS.

> **Note**
>
> É necessário usar o assistente de montagem do EFS para montar seus sistemas de arquivos do Amazon EFS a fim de usar a autorização do IAM para controlar o acesso por clientes NFS. Para obter mais informações, consulte Montar com autorização do IAM no Guia do usuário do Amazon EFS.

O exemplo a seguir da política do sistema de arquivos do EFS impõe a criptografia em trânsito e tem as seguintes características:

- O `effect` é `allow`.
- O princípio é definido como * para todas as entidades do IAM.
- A ação está definida como `ClientMount`, `ClientWrite` e `ClientRootAccess`.
- A condição para conceder permissões está definida como `SecureTransport`. Somente clientes NFS que usam TLS para se conectar ao sistema de arquivos têm acesso concedido.

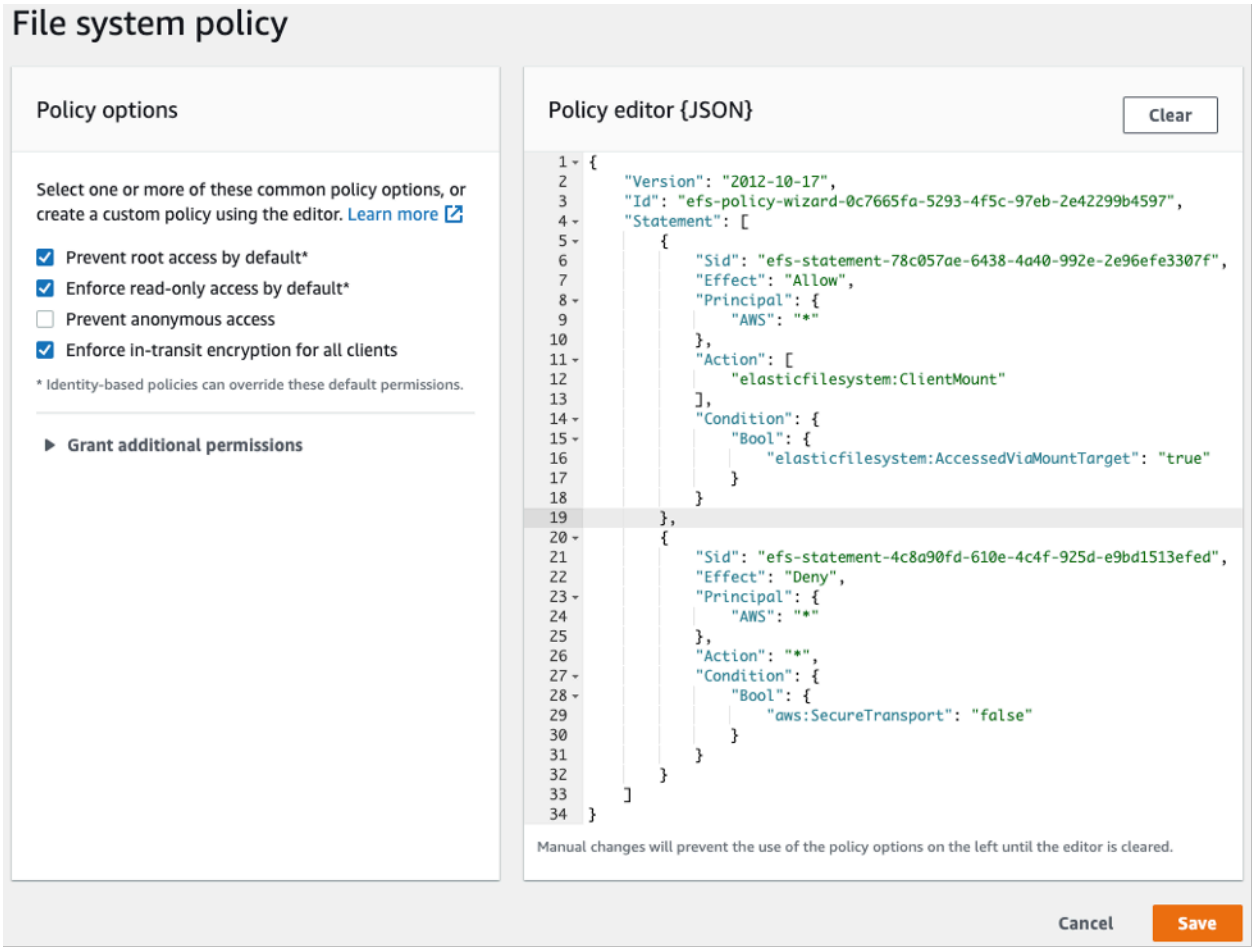
```
{
  “Version”: “2012-10-17”,
```

```
  “Id”: “ExamplePolicy01”,
  “Statement”: [
    {
      “Sid”: “VisualEditior0”,
      “Effect”: “Allow”,
      “Principal”: {
        “AWS”: “*”,
      },
      “Action”: [
“elasticfilesystem:ClientRootAccess”,
“elasticfilesystem:ClientMount”,
“elasticfilesystem:ClientWrite”
      ],
      “Condition”: {
        “Bool”: {
          “aws:SecureTransport”: “true”
        }
      }
    }
  ]
}
```

É possível criar uma política de sistema de arquivos usando o console do Amazon EFS ou usando a AWS CLI.

Para criar uma política do sistema de arquivos usando o console do EFS:

1. Abra o console do Amazon EFS.
2. Escolha File Systems (Sistemas de arquivos).
3. Na página File Systems (Sistemas de arquivos), escolha o sistema para o qual deseja editar ou criar uma política de sistema de arquivos. A página de detalhes desse sistema de arquivos é exibida.
4. Escolha File system policy (Política de sistema de arquivos) e, depois, selecione Edit (Editar). A página File system policy (Política do sistema de arquivos) é exibida.



Criar política do sistema de arquivos

5. Em Policy options (Opções de política), recomendamos que você escolha as seguintes opções de política pré-configuradas disponíveis:

   - Impedir acesso raiz por padrão
   - Impor acesso somente leitura por padrão
   - Impor criptografia em trânsito para todos os clientes

   Se você escolher uma política pré-configurada, o objeto JSON de política será exibido no painel Policy editor (Editor de políticas).

6. Use Grant additional permissions (Conceder permissões adicionais) para conceder permissões do sistema de arquivos a mais entidades principais do IAM, incluindo outra conta da AWS. Escolha Add (Adicionar) e insira o ARN da entidade principal à qual você está concedendo permissões. Depois, escolha as Permissions (Permissões) a serem concedidas.

7. Use o Policy editor (Editor de políticas) para personalizar uma política pré-configurada ou criar sua própria política com base no que você precisa. Quando o editor é usado, as opções de políticas pré-configuradas ficam indisponíveis. Para desfazer as alterações de política, escolha Clear (Limpar).

   Quando você limpa o editor, as políticas pré-configuradas ficam disponíveis novamente.
8. Depois de concluir a edição ou a criação da política, escolha Save (Salvar).

   A página de detalhes do sistema de arquivos é exibida, mostrando a política em File system policy (Política de sistema de arquivos).

   Você também pode criar uma política de sistemas de arquivos de modo programático usando o AWS CloudFormation, SDKs da AWS ou a API do Amazon EFS diretamente. Para obter mais informações sobre a criação de políticas do sistema de arquivos, consulte Creating file system policies (Criar políticas de sistema de arquivos) no Guia do usuário do Amazon EFS.

Configurar a criptografia de dados em trânsito

Para configurar a criptografia de dados em trânsito, recomendamos que você baixe o auxiliar de montagem do EFS em cada cliente. O auxiliar de montagem do EFS é um utilitário de código aberto que a AWS fornece para simplificar o uso do EFS, incluindo a configuração da criptografia de dados em trânsito. O auxiliar de montagem usa as opções de montagem recomendadas pelo EFS por padrão.

O auxiliar de montagem do EFS é compatível com as seguintes distribuições do Linux:

- Amazon Linux 2017.09+
- Amazon Linux 2+
- Debian 9+
- Fedora 28+
- Red Hat Enterprise Linux/CentOS 7+
- Ubuntu 16.04+

Para configurar a criptografia de dados em trânsito:

1. Instale o auxiliar de montagem do EFS:

- Para o Amazon Linux, use este comando:

```
sudo yum install -y amazon-efs-utils
```

- Para outras distribuições Linux, baixe-as do GitHub e instale.

  O pacote amazon-efs-utils instala automaticamente as seguintes dependências: cliente NFS (nfs-utils), Network relay (stunnel), OpenSSL e Python.

2. Monte o sistema de arquivos:

```
sudo mount -t efs -o tls file-system-id
efs-mount-point
```

- `mount -t efs` invoca o auxiliar de montagem do EFS.
- Não é possível usar o nome DNS do sistema de arquivos ou o endereço IP de um destino de montagem ao montar usando o auxiliar de montagem do EFS. Use o ID do sistema de arquivos.
- O auxiliar de montagem do EFS usa as opções de montagem recomendadas pela AWS por padrão. Substituir essas opções de montagem padrão não é recomendado, mas oferecemos a flexibilidade para fazer isso quando surgir a ocasião. Recomendamos testar minuciosamente todas as substituições de opções de montagem para que você entenda como essas alterações afetam o acesso e a performance do sistema de arquivos.
- A tabela a seguir representa as opções de montagem padrão usadas pelo auxiliar de montagem do EFS.

Opção	Descrição
nfsvers=4.1	A versão do protocolo NFS
rsize=1048576	O número máximo de bytes de dados que o cliente NFS pode receber para

Opção	Descrição
	cada solicitação READ de rede)
wsize=1048576	O número máximo de bytes de dados que o cliente NFS pode enviar para cada solicitação WRITE de rede
hard	O comportamento de recuperação do cliente NFS após uma solicitação NFS expirar, para que essas solicitações sejam repetidas indefinidamente até que o servidor responda.

Opção	Descrição
timeo=600	O valor de tempo limite que o cliente NFS usa para aguardar por uma resposta antes de realizar novas tentativas de uma solicitação NFS em décimos de segundos
retrans=2	O número de vezes que o cliente NFS tenta executar novamente uma solicitação antes de tentar executar outra ação de recuperação
noresvport	Diz ao cliente NFS para usar uma nova porta de origem TCP quando uma conexão de rede for restabelecida

- Adicione a seguinte linha ao `/etc/fstab` para remontar automaticamente o sistema de arquivos após qualquer reinicialização do sistema.

```
file-system-id efs-mount-point efs _netdev, tls, iam 0 0
```

Usar criptografia de dados em trânsito

Se sua organização estiver sujeita a políticas corporativas ou regulamentares que exijam criptografia de dados em trânsito, recomendamos o uso de criptografia de dados em trânsito em cada cliente que acessa o sistema de arquivos. A criptografia e a descriptografia são configuradas no nível da conexão e adicionam outra camada de segurança.

A montagem do sistema de arquivos usando o auxiliar de montagem do EFS configura e mantém um túnel TLS 1.2 entre o cliente e o Amazon EFS e encaminha todo o tráfego NFS por esse túnel criptografado. O certificado usado para estabelecer a conexão TLS criptografada é assinado pela Autoridade de Certificação (CA) da Amazon, na qual a maioria das distribuições Linux modernas confiam. O auxiliar de montagem do EFS também gera um processo de vigilância para monitorar todos os túneis seguros para cada sistema de arquivos e garantir que eles estejam em execução.

Depois de usar o auxiliar de montagem do EFS para estabelecer conexões criptografadas com o Amazon EFS, nenhuma outra entrada ou configuração será necessária por parte do usuário. A criptografia é transparente para conexões de usuários e aplicações que acessam o sistema de arquivos.

Depois de montar e estabelecer com êxito uma conexão criptografada a um sistema de arquivos do EFS usando o auxiliar de montagem do EFS, a saída de um comando de montagem mostra que o sistema de arquivos está montado e um túnel criptografado foi estabelecido usando o localhost (127.0.0.1) como relé de rede. Veja o exemplo de saída a seguir.

```
127.0.0.1:/ on efs-mount-point type nfs4
(rw,relatime,vers=4.1,rsize=1048576,wsize=1048576,namlen=255,hard,proto=tcp,port=20059,timeo=6
```

Para mapear um `efs-mount-point` até um sistema de arquivos do EFS, consulte o arquivo mount.log em `/var/log/amazon/efs` e encontre a última operação de montagem bem-sucedida. Isso pode ser feito usando o seguinte comando grep simples.

```
grep -E "Successfully
mounted.*efs-mount-point"
/var/log/amazon/efs/mount.log | tail -1
```

A saída desse comando grep retornará o nome DNS do sistema de arquivos do EFS montado. Veja o exemplo de saída abaixo.

```
2018-03-15 07:03:42,363 - INFO - Successfully mounted
file-system-id.efs.region.amazonaws.com
at efs-mount-point
```

Conclusão

Os dados do sistema de arquivos do Amazon EFS podem ser criptografados em repouso e em trânsito. Você pode criptografar dados em repouso usando CMKs que podem ser controladas e gerenciadas usando o AWS KMS. Criar um sistema de arquivos criptografados é simples: basta marcar uma caixa de seleção no assistente de criação de sistema de arquivos do Amazon EFS no Console de Gerenciamento da AWS ou adicionar um único parâmetro à operação `CreateFileSystem` na AWS CLI, nos SDKs da AWS ou na API do Amazon EFS.

Você pode aplicar a criptografia em repouso e trânsito usando políticas baseadas em identidade do AWS IAM e políticas do sistema de arquivos para fortalecer ainda mais seus requisitos de segurança e ajudar a atender às suas necessidades de conformidade. O uso de um sistema de arquivos criptografados também é transparente para serviços, aplicações e usuários, com efeito mínimo na performance do sistema de arquivos. Você pode criptografar dados em trânsito usando o auxiliar de montagem do EFS para estabelecer um túnel TLS criptografado em cada cliente, criptografando todo o tráfego NFS entre o cliente e o sistema de arquivos do EFS montado. A aplicação da criptografia de dados em repouso do Amazon EFS usando políticas de identidade do IAM e em trânsito usando políticas do sistema de arquivos do EFS está disponível para você sem custo adicional.

Recursos

- Whitepaper de detalhes criptográficos do AWS KMS
- Guia do usuário do Amazon EFS

Histórico do documento e colaboradores

Histórico do documento

Para ser notificado sobre atualizações deste whitepaper, inscreva-se no RSS feed.

update-history-change	update-history-description	update-history-date
Atualizações secundárias	Layout de página ajustado	30 de abril de 2021
Whitepaper atualizado	Adição da aplicação da criptografia em repouso e em trânsito usando o IAM	22 de fevereiro de 2021
Whitepaper atualizado	Adição da criptografia de dados em trânsito	1º de abril de 2018
Publicação inicial	Publicação da seção Criptografar dados em repouso com os sistemas de arquivos criptografados do Amazon EFS	1º de setembro de 2017

> **Note**
>
> Para assinar atualizações RSS, você deve ter um plugin RSS habilitado para o navegador que está usando.

Colaboradores

Dentre os colaboradores deste documento estão:

- Darryl S. Osborne, arquiteto de soluções especializado em armazenamento na AWS
- Joseph Travaglini, gerente sênior de produtos, Amazon EFS
- Peter Buonora, arquiteto-chefe de soluções na AWS

- Siva Rajamani, arquiteto de soluções sênior na AWS