AWS 白皮书

使用 Amazon Elastic File System 加密文件数据

使用 Amazon Elastic File System 加密文件数据: AWS 白皮书

Table of Contents

使用 Amazon Elastic File System 加密文件数据

发布日期：2021 年 2 月 22日（文档历史记录和贡献者）

摘要

安全性是 AWS 的工作重点，我们为客户提供工具，将安全性作为他们企业中的头等大事。政府法规和行业或公司的合规性政策可能会要求使用加密策略、加密算法和适当的密钥管理，来保护不同分类的数据。本白皮书概述了加密 Amazon Elastic File System（Amazon EFS）的最佳实践。

介绍

Amazon Elastic File System（Amazon EFS）在云中提供简单、可扩展、高度可用且具有高持久性的共享文件系统。您使用 Amazon EFS 创建的文件系统具有弹性，使它们可以在您添加和删除数据时自动扩展和缩减。它们的大小会增长到数 PB，从而将数据分布在多个可用区（AZ）中数量不受限制的存储服务器上。

存储在这些文件系统中的数据可以使用 Amazon EFS 进行静态和传输中加密。要对静态数据进行加密，您可以通过 AWS 管理控制台或 AWS Command Line Interface（AWS CLI）创建加密的文件系统。或者，您可以通过 Amazon EFS API 或其中一个 AWS 开发工具包以编程方式创建加密的文件系统。

为了对静态数据进行加密，Amazon EFS 与 AWS Key Management Service（AWS KMS）集成以进行密钥管理。您还可以通过挂载文件系统并通过传输层安全性（TLS）传输所有 NFS 流量，从而启用传输中数据加密。

本白皮书概述了 Amazon EFS 的加密最佳实践。它介绍了如何在客户端连接层启用传输中数据加密，以及如何在 AWS 管理控制台和 AWS CLI 中创建加密的文件系统。

> **Note**
>
> 使用 API 和开发工具包创建加密的文件系统不在本白皮书的讨论范围之内。有关如何执行此操作的更多信息，请参阅 Amazon EFS 用户指南或开发工具包文档中的 Amazon EFS API。

基本概念和术语

本节定义了本白皮书中引用的概念和术语。

- Amazon Elastic File System（Amazon EFS）– 一种高度可用且具有高持久性的服务，可在 AWS 云中提供简单、可扩展的共享文件存储。Amazon EFS 提供标准文件系统接口和文件系统语义。您可以在多个可用区中数量不受限制的存储服务器上存储几乎任意数量的数据。
- AWS Identity and Access Management（IAM）– 使您能够安全地控制对 AWS 服务 API 的精细访问的一项服务。创建策略并将其用于限制对单个用户、组和角色的访问。您可以通过 IAM 控制台管理您的 AWS KMS 密钥。
- AWS KMS – 一项托管式服务，可让您轻松创建和控制客户主密钥（CMK），这是用于加密数据的加密密钥。AWS KMS CMK 由硬件安全模块（HSM）提供保护，而 HSM 通过 FIPS 140-2 加密模块验证计划进行验证，中国（北京）和中国（宁夏）区域除外。AWS KMS 与其他 AWS 服务集成，对您的数据进行加密。它还与 AWS CloudTrail 完全集成，以提供 AWS KMS 代表您进行的 API 调用的日志，这有助于满足适用于您组织的合规性或监管要求。
- 客户主密钥（CMK）– 表示密钥层次结构的顶层。它包含用于加密和解密数据的密钥材料。AWS KMS 可以生成此密钥材料，或者您可以生成密钥材料，然后将其导入 AWS KMS。CMK 特定于 AWS 账户和 AWS 区域，可以由客户管理或 AWS 托管。
- AWS 托管的 CMK – 由 AWS 代表您生成的 CMK。当您为集成 AWS 服务的资源启用加密时，会创建由 AWS 托管的 CMK。AWS 托管的 CMK 密钥策略由 AWS 管理，您无法更改它们。创建或存储 AWS 托管的 CMK 不产生任何费用。
- 客户管理的 CMK – 您使用 AWS 管理控制台或 API、AWS CLI 或开发工具包创建的 CMK。当您需要对 CMK 进行更精细的控制时，可以使用客户管理的 CMK。
- KMS 密钥策略 – 一项资源策略，控制对客户管理的 CMK 的访问。客户使用密钥策略或 IAM 策略与密钥策略的组合来定义这些权限。有关更多信息，请参阅 AWS KMS 开发人员指南中的管理访问权限概述。
- 数据密钥 – 由 AWS KMS 生成的加密密钥，用于加密 AWS KMS 之外的数据。AWS KMS 使授权实体（用户或服务）可以获取受 CMK 保护的数据密钥。
- 传输层安全性（TLS）– TLS 是安全套接字层（SSL）的后继者，是加密通过网络交换的信息所必需的加密协议。
- EFS 挂载帮助程序 – 用于简化 EFS 文件系统挂载的 Linux 客户端代理（`amazon-efs-utils`）。它可用于设置、维护和通过 TLS 隧道路由所有 NFS 流量。

有关基本概念和术语的更多信息，请参阅 AWS KMS 开发人员指南中的 AWS Key Management Service 概念。

静态数据加密

AWS 为您提供了创建加密文件系统的工具，使用行业标准的 AES-256 加密算法对所有静态数据和元数据进行加密。加密的文件系统可以自动和透明地处理加密和解密，因此您不必修改应用程序。如果您组织的政策或监管政策要求对静态数据和元数据进行加密，我们建议您创建一个加密的文件系统。

主题

管理密钥

Amazon EFS 与 AWS KMS 集成，后者管理加密文件系统的加密密钥。AWS KMS 还支持其他 AWS 服务的加密，例如 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 等。为了加密文件系统内容，Amazon EFS 使用具有 XTS 模式和 256 位密钥 (XTS-AES-256) 的高级加密标准算法。

在考虑如何通过采用任何加密策略来保护静态数据时，有三个重要问题需要回答。这些问题同样适用于存储在托管和非托管式服务（例如 Amazon EBS）中的数据。

密钥存储在哪里？

AWS KMS 将您的主密钥以加密格式存储在高度持久的存储中，以帮助确保在需要时可以检索它们。

密钥用在何处？

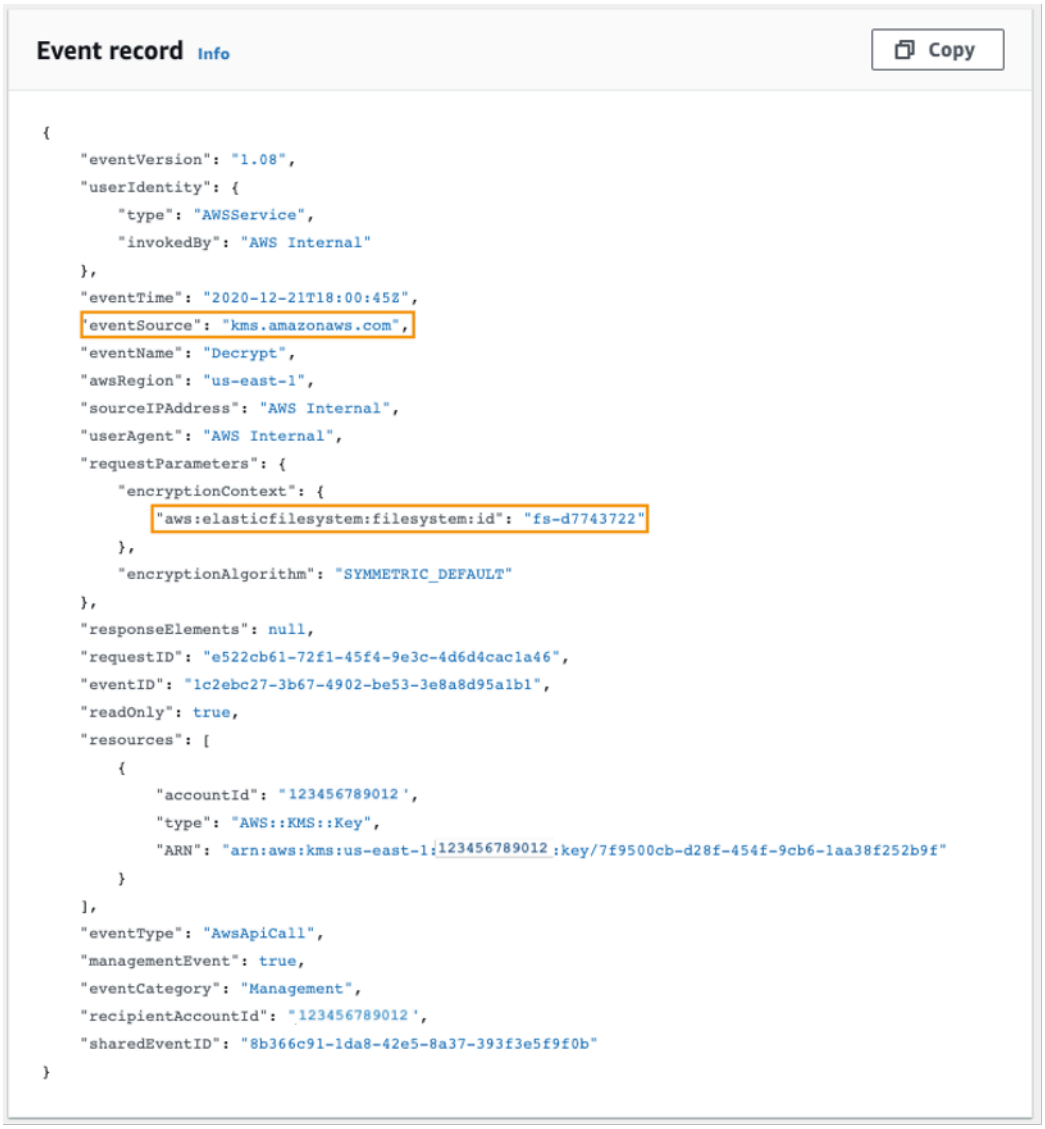
使用加密的 Amazon EFS 文件系统对挂载文件系统的客户端是透明的。因为数据在写入磁盘之前先加密，在客户端发出读取请求后解密，所以所有加密操作都在 EFS 服务内进行。

谁可以使用密钥？

AWS KMS 密钥策略控制对加密密钥的访问。

我们建议您将它们与 IAM 策略结合使用，以提供另一层控制。每个密钥都有密钥策略。如果密钥是 AWS 托管的 CMK，则由 AWS 管理密钥策略。如果密钥是客户管理的 CMK，则由您管理密钥策略。这些密钥策略是控制 CMK 访问的主要方法。它们定义了控制密钥使用和管理的权限。

当您使用 Amazon EFS 创建加密文件系统时，您授予 Amazon EFS 代表您使用 CMK 的访问权限。Amazon EFSS 代表您对 AWS KMS 进行的调用将显示在 CloudTrail 日志中，就像它们源自您的 AWS 账户一样。以下屏幕截图显示了 Amazon EFS 发起的 KMS 解密调用的示例 CloudTrail 事件。



KMS 解密的 CloudTrail 日志

有关 AWS KMS 以及如何管理加密密钥访问权限的更多信息，请参阅 AWS KMS 开发人员指南中的管理对 AWS KMS CMK 的访问。

有关 AWS KMS 如何管理加密的更多信息，请参阅 AWS KMS 加密详情白皮书。

有关如何创建管理员 IAM 用户和组的更多信息，请参阅 IAM 用户指南中的创建您的第一个 IAM 管理员用户和组。

创建加密文件系统

您可以使用 AWS 管理控制台、AWS CLI、Amazon EFS API 或 AWS 开发工具包创建加密的文件系统。您只能在创建文件系统时为其启用加密。

Amazon EFS 与 AWS KMS 集成以进行密钥管理，并使用 CMK 对文件系统进行加密。文件系统元数据（例如文件名、目录名称和目录内容）使用 AWS 托管的 CMK 进行加密和解密。

文件的内容或文件数据将使用您选择的 CMK 进行加密和解密。CMK 分为三种类型：

- 适用于 Amazon EFS 的 AWS 托管 CMK
- 来自您的 AWS 账户的客户管理 CMK
- 来自另一个 AWS 账户的客户管理 CMK

您组织的政策或监管政策可能要求对 CMK 的创建、轮换、删除以及访问控制和使用策略进行完全控制。如果是这样，我们建议您使用客户管理的 CMK。在其他情况下，您可以使用 AWS 托管的 CMK。

所有用户都有适用于 Amazon EFS 的 AWS 托管 CMK，其别名为 `aws/elasticfilesystem`。AWS 管理此 CMK 的密钥策略，您无法对其进行更改。创建和存储 AWS 托管的 CMK 不会产生任何费用。

如果您决定使用客户管理的 CMK 来加密文件系统，请选择您拥有的客户管理 CMK 的密钥别名。或者，您可以输入另一个账户拥有的客户管理 CMK 的 Amazon Resource Name（ARN）。使用您拥有的客户管理 CMK，您可以通过密钥策略和密钥授权来控制哪些用户和服务可以使用密钥。

您还可以通过选择何时禁用、重新启用、删除或撤销对这些密钥的访问权限，从而控制这些密钥的生命周期和轮换。有关管理其他 AWS 账户中密钥的访问权限的信息，请参阅 AWS KMS 开发人员指南中的更改密钥策略。

有关如何管理客户管理的 CMK 的更多信息，请参阅 AWS KMS 开发人员指南中的客户主密钥（CMK）。

以下各节讨论如何使用 AWS 管理控制台和 AWS CLI 创建加密文件系统。

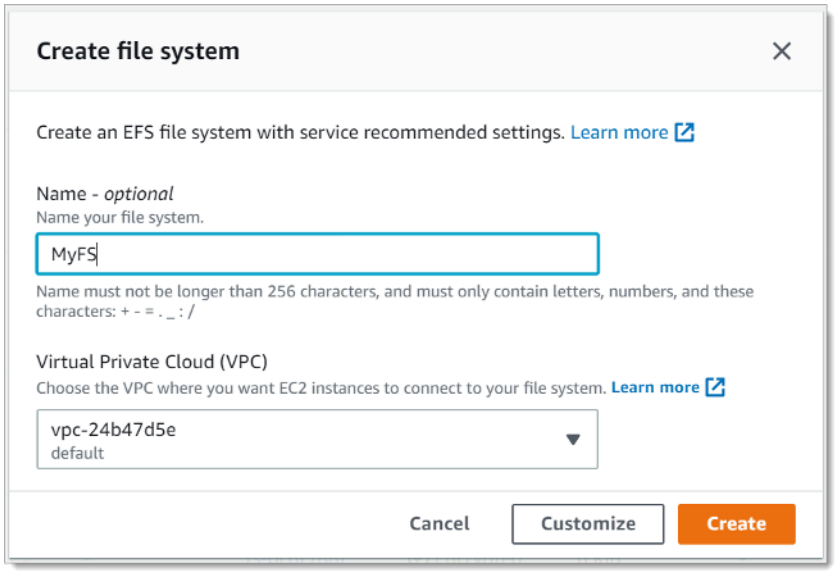
使用 AWS 管理控制台创建加密文件系统

按照以下程序使用 AWS 管理控制台创建加密的 Amazon EFS 文件系统。

步骤 1.配置文件系统设置

在这个步骤中，您配置常规文件系统设置，包括生命周期管理、性能和吞吐量模式以及静态数据加密。

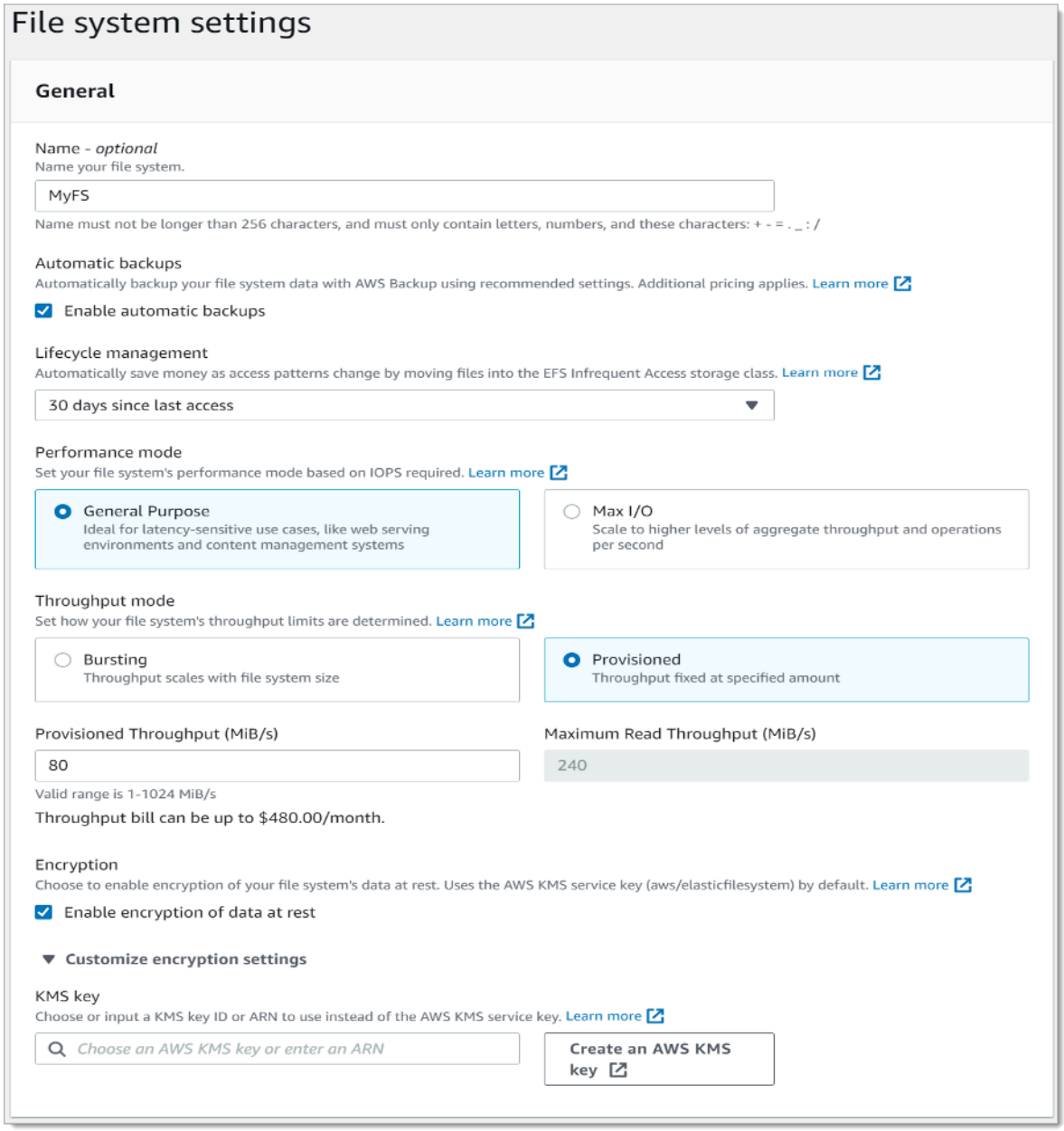
1. 登录 AWS 管理控制台，打开 Amazon EFS 控制台。
2. 选择 Create file system（创建文件系统）以打开 Create file system（创建文件系统）对话框。有关使用推荐设置（包括默认启用加密）创建文件系统的更多信息，请参阅创建您的 Amazon EFS 文件系统。



创建 EFS 文件系统

3. （可选）选择 Customize（自定义）以创建自定义文件系统，而不是使用服务建议的设置创建文件系统。

此时将显示 File system settings（文件系统设置）页面。



创建 EFS 文件系统：常规设置

4. 对于 General（常规）设置，请输入以下详细信息。
   - （可选）输入文件系统的 Name（名称）。
   - 默认情况下，Automatic backups（自动备份）处于打开状态。您可以通过清除复选框来关闭自动备份。有关更多信息，请参阅将 AWS Backup 与 Amazon EFS 结合使用。
   - 选择 Lifecycle management（生命周期管理）策略。Amazon EFS 生命周期管理自动针对您的文件系统管理经济高效的文件存储。启用后，生命周期管理将在一段设定时间内未访问的文件迁移到不常访问（IA）存储类别。您可以使用生命周期策略定义这段时间。如果不希望启用生命周期

管理，请选择 None（无）。有关更多信息，请参阅 Amazon EFS 用户指南 中的 EFS 生命周期管理。

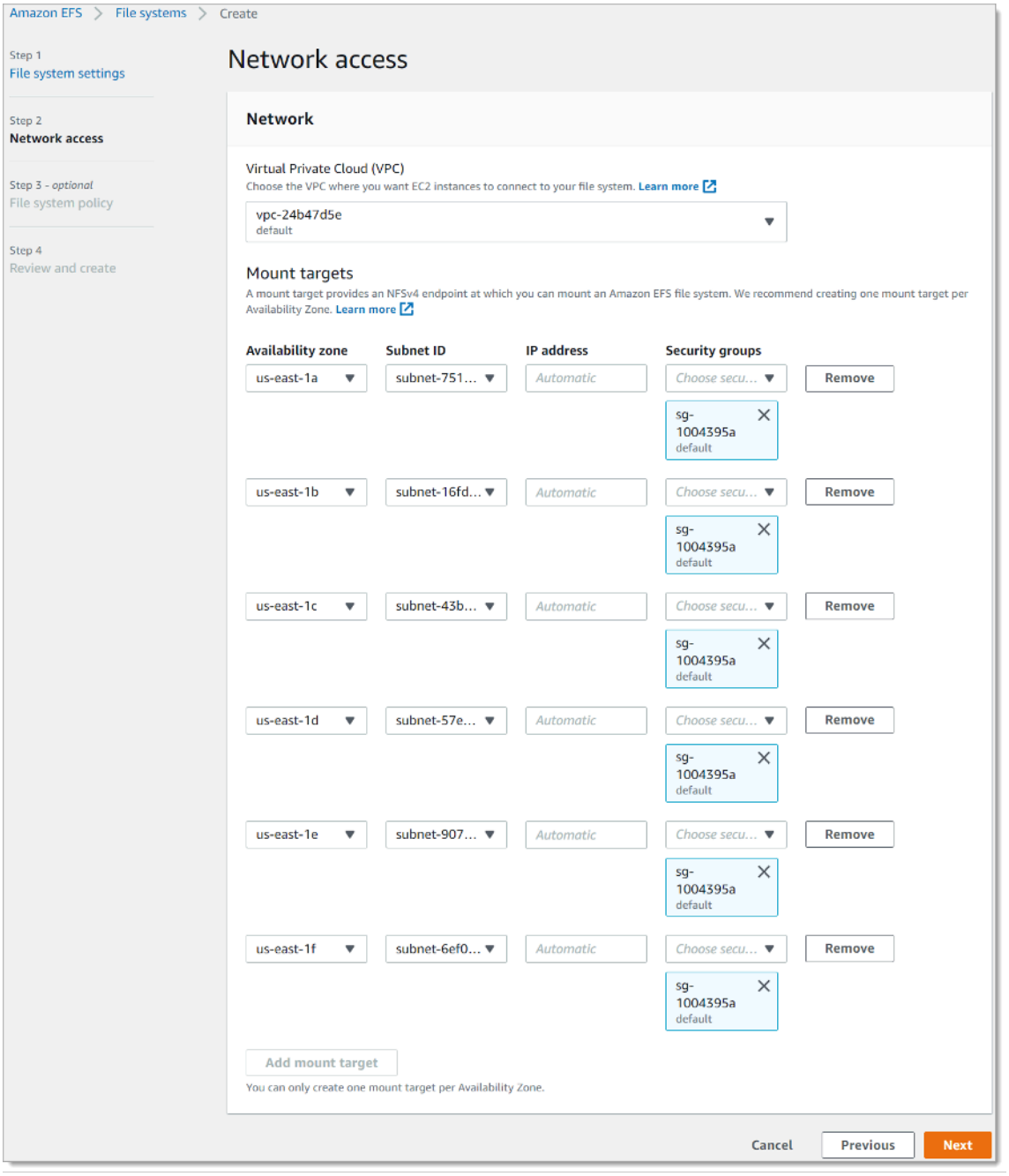
- 选择 Performance mode（性能模式）：默认的 General Purpose mode（通用模式）或 Max I/O（最大 I/O）。有关更多信息，请参阅 Amazon EFS 用户指南中的性能模式。
- 选择 Throughput mode（吞吐量模式）：默认的 Bursting mode（突增模式）或 Provisioned mode（预置模式）。
- 如果选择了 Provisioned（预置），则会显示 Provisioned Throughput (MiB/s)（预置吞吐量 (MiB/s)）字段。输入要为文件系统预置的吞吐量。输入吞吐量后，控制台会在字段旁边显示每月成本的估计值。有关更多信息，请参阅 Amazon EFS 用户指南中的吞吐量模式。
- 对于 Encryption（加密），默认情况下启用静态数据加密。默认情况下，它使用您的 AWS Key Management Service（AWS KMS）EFS 服务密钥（`aws/elasticfilesystem`）。要选择其他用于加密的 KMS 密钥，请展开 Customize encryption settings（自定义加密设置），然后从列表中选择一个密钥。或者，输入要使用的 KMS 密钥的 KMS 密钥 ID 或 Amazon Resource Name (ARN)。

  如果您需要创建新密钥，请选择 Create an AWS KMS key（创建 AWS KMS 密钥）以启动 AWS KMS 控制台并创建新密钥。

5. （可选）选择 Add tag（添加标签）以将键值对添加到文件系统。
6. 选择 Next（下一步）继续执行配置过程中的 Network Access（网络访问）步骤。

步骤 2.配置网络访问

在此步骤中，配置文件系统的网络设置，包括 virtual private cloud (VPC) 和挂载目标。对于每个挂载目标，设置可用区、子网、IP 地址和安全组。



创建 EFS 文件系统：网络访问

1. 选择您希望 EC2 实例连接到文件系统的 Virtual Private Cloud (VPC)。有关详细信息，请参阅 Amazon EFS 用户指南中的管理文件系统网络可访问性。
   - 可用区 – 默认情况下，在 AWS 区域的每个可用区中配置挂载目标。如果您不希望在特定可用区中设置挂载目标，请选择 Remove（删除）以删除该区域的挂载目标。在您计划从中访问文件系统的每个可用区中创建一个挂载目标。无需任何费用。

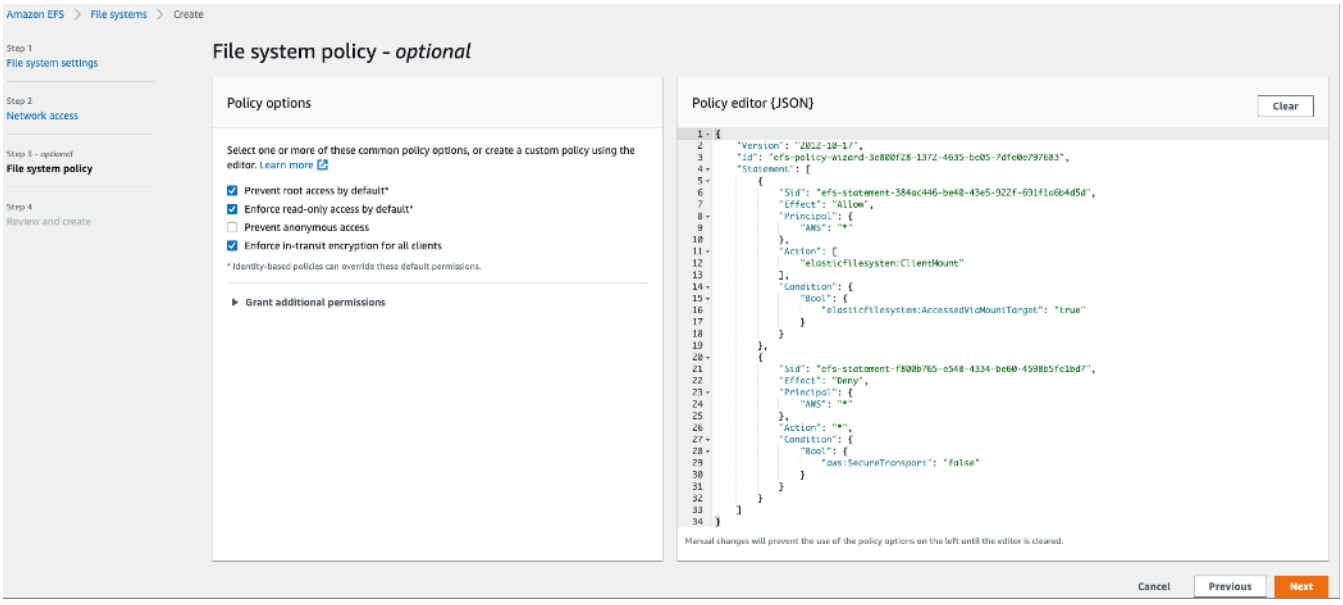
- 子网 ID – 从可用区的可用子网中进行选择。默认子网处于预选中状态。最佳实践是，根据您的安全要求，确保所选子网为公有或私有子网。
- IP 地址 – 默认情况下，Amazon EFS 从子网的可用地址中自动选择 IP 地址。或者，您可以输入子网中的特定 IP 地址。虽然挂载目标只有一个 IP 地址，但它们是冗余、高度可用的网络资源。
- 安全组 – 可以为挂载目标指定一个或多个安全组。作为最佳实践，请确保安全组仅用于 EFS 挂载目的（NFS 端口 2049），并且入站规则仅允许来自其他 VPC CIDR 块范围的端口 2049，或者使用安全组作为需要访问 EFS 的资源的来源。有关更多信息，请参阅 Amazon EFS 用户指南中的使用 Amazon EC2 实例和挂载目标的安全组。

  要添加其他安全组或更改安全组，请选择 Choose security groups（选择安全组），然后从列表中添加另一个安全组。如果您不想使用默认安全组，可以将其删除。有关更多信息，请参阅 Amazon EFS 用户指南中的创建安全组。

2. 选择 Add mount target（添加挂载目标），以便为没有挂载目标的可用区创建挂载目标。如果为每个可用区配置了挂载目标，则此选项不可用。
3. 选择 Next（下一步）以继续。此时将显示 File system policy（文件系统策略）页面。

步骤 3.创建文件系统策略

在此步骤中，创建文件系统策略以控制 NFS 客户端对文件系统的访问。EFS 文件系统策略是用于控制 NFS 客户端对文件系统的访问的 IAM 资源策略。有关更多信息，请参阅 Amazon EFS 用户指南 中的使用 IAM 控制对 Amazon EFS 的 NFS 访问。

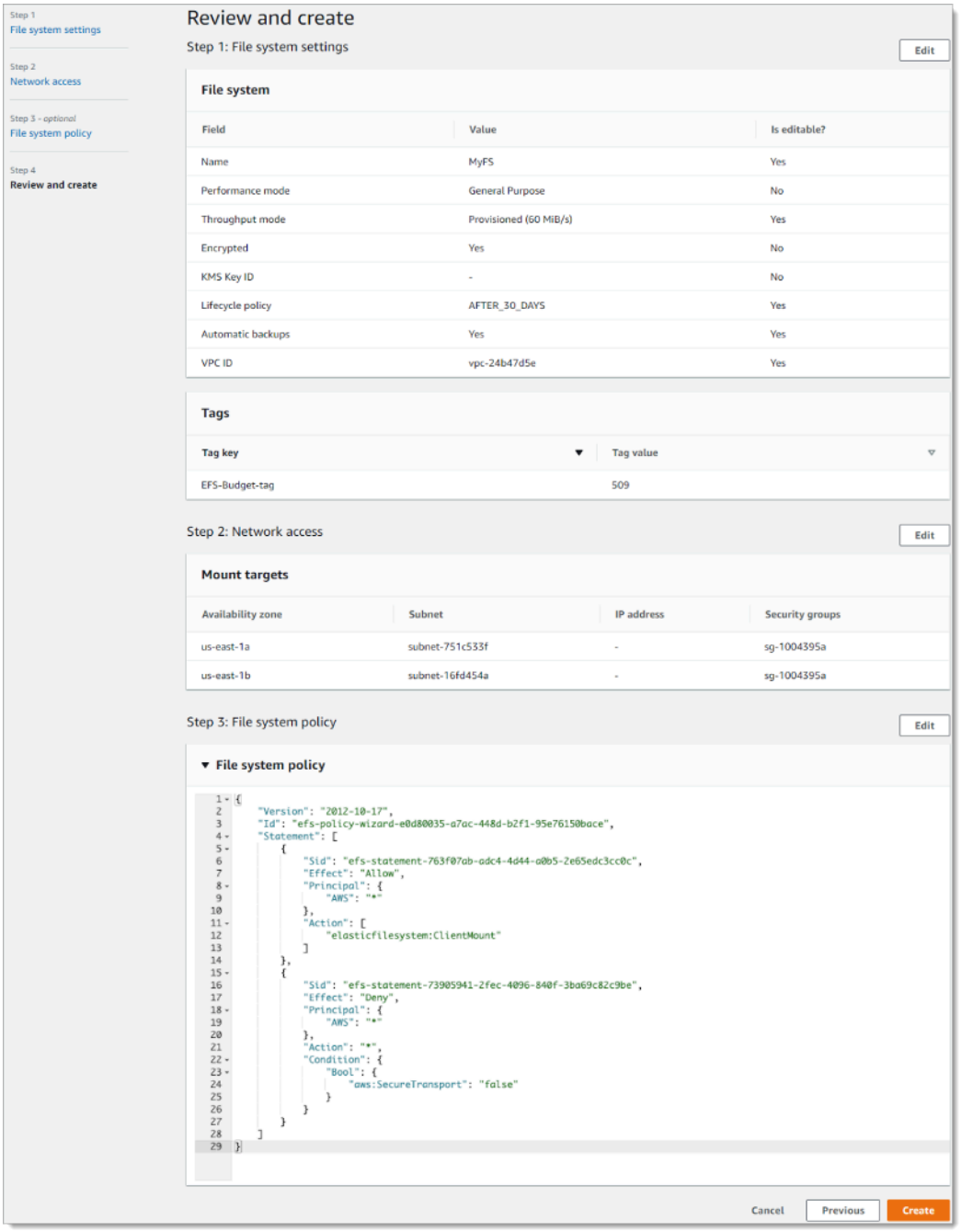


创建 EFS 文件系统：文件系统策略

1. 在 Policy options（策略选项）中，我们建议您选择以下可用的预配置策略选项：
   - 默认情况下阻止根访问
   - 默认情况下强制实施只读访问
   - 为所有客户端强制实施传输中加密
2. 使用 Grant additional permissions（授予额外权限）向其他 IAM 主体（包括另一个 AWS 账户）授予文件系统权限。选择 Add（添加），然后输入要向其授予权限的实体的主体 ARN，然后选择要授予的 Permissions（权限）。
3. 根据您的需求使用 Policy editor（策略编辑器）自定义预配置的策略或创建自己的策略。选择其中一个预配置的策略时，JSON 策略定义将显示在策略编辑器中。
4. 选择 Next（下一步）以继续。此时将显示 Review and create（审核和创建）页面。

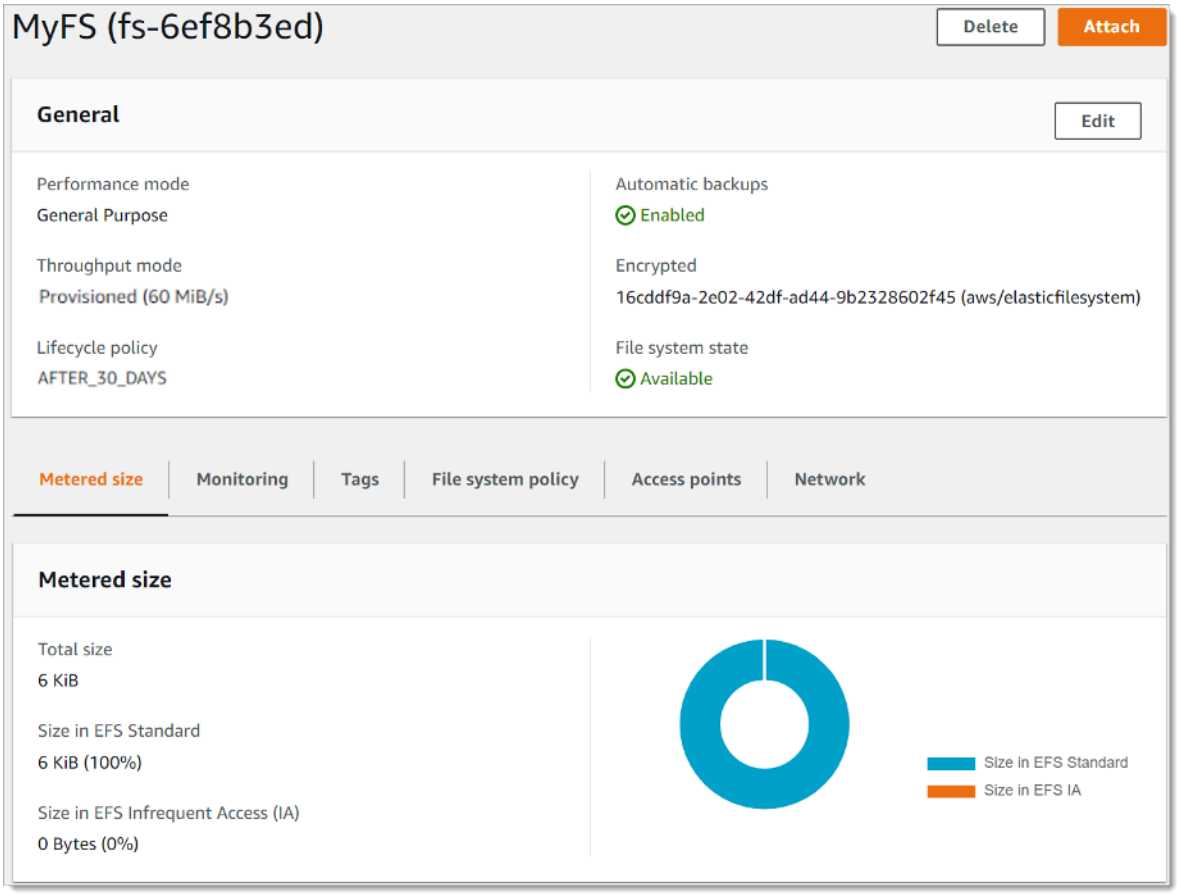
步骤 4.审核和创建

在此步骤中，检查文件系统设置，进行任何修改，然后创建文件系统。



创建 EFS 文件系统：审核和创建

1. 查看每个文件系统配置组。此时您可以通过选择 Edit（编辑）对每个组进行更改。
2. 选择 Create（创建）以创建文件系统并返回到 File systems（文件系统）页。
3. File systems（文件系统）页显示文件系统及其配置详细信息，如下图所示。



文件系统

使用 AWS CLI 创建加密文件系统

使用 AWS CLI 创建加密文件系统时，您可以使用额外参数来设置加密状态和客户管理的 CMK。请确保使用的是最新版本的 AWS CLI。有关如何升级 AWS CLI 的信息，请参阅 AWS 命令行界面用户指南中的安装、更新和卸载 AWS CLI。

在 `CreateFileSystem` 操作中，`--encrypted` 参数是布尔值，是创建加密文件系统所必需的。仅当您使用客户管理的 CMK 且包括密钥的别名或 ARN 时，才需要 `--kms-key-id`。如果您使用的是 AWS 托管的 CMK，请不要包括此参数。

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

有关使用 AWS 管理控制台、AWS CLI、AWS 开发工具包或 Amazon EFS API 创建 Amazon EFS 文件系统的更多信息，请参阅 Amazon EFS 用户指南中的什么是 Amazon Elastic File System。

强制实施静态数据加密

加密对 I/O 延迟和吞吐量的影响微乎其微。加密和解密对用户、应用程序和服务都是透明的。所有数据和元数据在写入磁盘之前由 Amazon EFS 代表您进行加密，并在客户端读取之前先解密。您无需更改客户端工具、应用程序或服务即可访问加密的文件系统。

您的组织可能要求加密符合特定分类条件的所有数据，或者加密与特定应用程序、工作负载或环境关联的所有数据。您可以使用 AWS Identity and Access Management（IAM）基于身份的策略对 Amazon EFS 文件系统资源实施静态数据加密。使用 IAM 条件键， 您可以避免用户创建未加密的 EFS 文件系统。

例如，明确允许用户仅创建加密的 EFS 文件系统的 IAM 策略使用以下效果、操作和条件组合：

- `Effect` 为 `Allow`。
- `Action` 为 `elasticfilesystem:CreateFileSystem`。
- `Condition` `elasticfilesystem:Encrypted` 为 `true`。

以下示例演示了一个基于身份的 IAM 策略，该策略授权主体仅创建加密的文件系统。

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

将 `Resource` 属性设置为 `*` 表示 IAM 策略适用于创建的所有 EFS 资源。您可以添加基于标签的其他条件属性，以便仅对具有数据分类需求的 EFS 资源子集强制使用该属性。

您还可以通过对组织中的所有 AWS 账户或组织单位使用服务控制策略，在 AWS Organizations 级别强制创建加密的 Amazon EFS 文件系统。有关 AWS Organizations 中的服务控制策略的更多信息，请参阅 AWS Organizations 用户指南中的服务控制策略。

创建要求加密所有 EFS 文件系统的 IAM 策略

您可以创建基于身份的 IAM 策略，授权用户使用控制台、AWS CLI 或 API 仅创建加密的 Amazon EFS 文件系统。以下过程介绍如何使用 IAM 控制台创建此类策略，然后将该策略应用于您账户中的用户。

要创建 IAM 策略以强制使用加密的 EFS 文件系统，请执行以下操作：

1. 登录 AWS 管理控制台，并打开 IAM 控制台。
2. 在导航窗格中的 Access Management（访问管理）下面，选择 Policies（策略）。
3. 选择 Create Policy（创建策略）以显示 Create Policy（创建策略）页面。
4. 在 Visual Editor（可视化编辑器）选项卡中，输入以下信息。
   - 对于 Service（服务），请选择 EFS。
   - 对于 Actions（操作），在搜索字段中输入 `create`，然后选择 CreateFileSystem。
   - 对于 Request conditions（请求条件），单击 Add condition（添加条件）链接，为 Condition Key（条件键）搜索 `elasticfilesystem:Encrypted`，为 Operator（运算符）搜索 `Bool`，为 Value（值）搜索 `true`。
5. 为策略提供 Name（名称）和 Description（描述）。验证策略摘要，包括 Encrypted（已加密）请求条件。
6. 选择 Create policy（创建策略）以创建策略。

要将策略应用于您账户中的用户，请执行以下操作：

1. 在 IAM 控制台的 Access management（访问管理）下，选择 Users（用户）。
2. 选择要应用该策略的用户。
3. 选择 Add permissions（添加权限）以显示 Add permissions（添加权限）页面。
4. 选择 Attach existing policies directly（直接附加现有策略）。
5. 输入您在上一过程中创建的 EFS 策略的名称。

6. 选择并展开策略。然后选择 {}JSON 以验证策略内容。它应该与下面的 JSON 策略类似。

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

检测未加密的文件系统

您的组织可能需要识别未加密的 Amazon EFS 资源。您可以使用 AWS Config 托管式规则检测未加密的文件系统。AWS Config 提供 AWS 托管式规则，这些规则是预定义且可自定义的规则，AWS Config 使用这些规则来评估您的 AWS 资源是否符合通用最佳实践，将不符合规则的资源标记为 NON_COMPLIANT。

您可以使用 AWS 托管式配置规则 `efs-encrypted-check` 检查 Amazon Elastic File System（Amazon EFS）是否配置为使用 AWS Key Management Service（AWS KMS）加密文件数据。有关设置和激活 AWS 托管规则的更多信息，请参阅使用 AWS Config 托管式规则。

传输中数据加密

您可以挂载文件系统，以便在传输过程中使用传输层安全性 1.2（TLS）和行业标准 AES-256 密码对所有 NFS 流量进行加密。TLS 是一组行业标准的加密协议，用于加密通过网络交换的信息。AES-256 是一种 256 位加密密码，用于 TLS 中的数据传输。我们建议对访问文件系统的每台客户端设置传输中加密。

您可以使用 IAM 策略对访问 Amazon EFS 的 NFS 客户端强制实施传输中加密。当客户端连接到文件系统时，Amazon EFS 会评估文件系统的 IAM 资源策略（称为文件系统策略）以及任何基于身份的 IAM 策略，确定要授予的相应文件系统访问权限。您可以在文件系统资源策略中使用 `aws:SecureTransport` 条件键来强制 NFS 客户端在连接到 EFS 文件系统时使用 TLS。

> **Note**
>
> 必须使用 EFS 挂载帮助程序挂载 Amazon EFS 文件系统，从而使用 IAM 授权来控制 NFS 客户端的访问。有关更多信息，请参阅 Amazon EFS 用户指南中的使用 IAM 授权挂载。

以下示例 EFS 文件系统策略强制实施传输中加密，并具有以下特征：

- `effect` 为 `allow`。
- 所有 IAM 实体的主体设置为 `*`。
- 操作设置为 `ClientMount`、`ClientWrite` 和 `ClientRootAccess`。
- 授予权限的条件设置为 `SecureTransport`。仅向使用 TLS 连接到文件系统的 NFS 客户端授予访问权限。

```
{
  “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”
        }
      }
    }
  ]
}
```

您可以使用 Amazon EFS 控制台或 AWS CLI 创建文件系统策略。

要使用 EFS 控制台创建文件系统策略，请执行以下操作：

1. 打开 Amazon EFS 控制台。
2. 选择 File Systems（文件系统）。
3. 在 File systems（文件系统）页面上，选择要为其编辑或创建文件系统策略的文件系统。此时将显示该文件系统的详细信息页面。
4. 选择 File system policy（文件系统策略），然后选择 Edit（编辑）。 此时将显示 File system policy（文件系统策略）页面。

创建文件系统策略

5. 在 Policy options（策略选项）中，我们建议您选择以下可用的预配置策略选项：

   - 默认情况下阻止根访问
   - 默认情况下强制实施只读访问
   - 为所有客户端强制实施传输中加密

   如果选择预配置的策略，策略 JSON 对象将显示在 Policy editor（策略编辑器）面板中。

6. 使用 Grant additional permissions（授予额外权限）向其他 IAM 主体（包括另一个 AWS 账户）授予文件系统权限。选择 Add（添加），然后输入要向其授予权限的实体的主体 ARN，然后选择要授予的 Permissions（权限）。

7. 根据您的需求使用 Policy editor（策略编辑器）自定义预配置的策略或创建自己的策略。使用编辑器时，预配置的策略选项将变得不可用。要撤销策略更改，请选择 Clear（清除）。

   清除编辑器后，预配置的策略将再次变为可用。

8. 完成编辑或创建策略后，选择 Save（保存）。

   此时将显示文件系统的详细信息页面，其中显示 File system policy（文件系统策略）中的策略。

   也可以直接使用 AWS CloudFormation、AWS 开发工具包或 Amazon EFS API 以编程方式创建文件系统策略。有关创建文件系统策略的更多信息，请参阅 Amazon EFS 用户指南中的创建文件系统策略。

设置传输中数据加密

要设置传输中数据加密，建议您在每个客户端下载 EFS 挂载帮助程序。EFS 挂载帮助程序是 AWS 提供的开源实用程序，用于简化 EFS 的使用，包括设置传输中数据加密。默认情况下，挂载帮助程序使用 EFS 推荐的挂载选项。

以下 Linux 发行版支持 EFS 挂载帮助程序：

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

要设置传输中数据加密，请执行以下操作：

1. 安装 EFS 挂载帮助程序：
   - 对于 Amazon Linux，请使用以下命令：

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

   - 对于其他 Linux 发行版，请从 GitHub 下载并安装。

     amazon-efs-utils 软件包会自动安装以下依赖项：NFS 客户端（nfs-utils）、网络中继（stunnel）、OpenSSL 和 Python。
2. 挂载文件系统：

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

- `mount -t efs` 调用 EFS 挂载帮助程序。
- 使用 EFS 挂载帮助程序挂载时，不支持使用文件系统的 DNS 名称或挂载目标的 IP 地址，请改用文件系统 ID。
- 默认情况下，EFS 挂载帮助程序使用 AWS 推荐的挂载选项。不建议覆盖这些默认的挂载选项，但我们提供了在必要时进行覆盖的灵活性。我们建议彻底测试所有挂载选项覆盖，以便了解这些更改对文件系统访问权限和性能的影响。
- 下表显示了 EFS 挂载帮助程序使用的默认挂载选项。

选项	描述
nfsvers=4.1	NFS 协议的版本
rsize=1048576	NFS 客户端对每个网络 READ 请求可以接收的数据最大字节数
wsize=1048576	NFS 客户端对每个网络 WRITE 请求可以发送的数据最大字节数
hard	NFS 客户端在 NFS 请求超时之后的恢复行为，这样 NFS 请求在服务器回复之前会无限重试

选项	描述
timeo=600	NFS 客户端在重试 NFS 请求之前等待响应的超时值，以分秒计算
retrans=2	NFS 客户端重试请求的次数，超过此次数之后将尝试进一步的恢复操作
noresvport	告知 NFS 客户端在重新建立网络连接时，使用新 TCP 源端口。

- 将以下行添加到 `/etc/fstab`，以便在系统重新启动后自动重新挂载文件系统。

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

使用传输中数据加密

如果您组织的政策或监管政策要求对传输中数据进行加密，我们建议对访问文件系统的每个客户端上的传输中数据进行加密。在连接级别配置加密和解密，并增加了另一层安全性。

使用 EFS 挂载帮助程序挂载文件系统，在客户端和 Amazon EFS 之间设置并维护一个 TLS 1.2 隧道，并通过这个加密隧道路由所有 NFS 流量。用于建立加密 TLS 连接的证书由亚马逊证书颁发机构（CA）签名，并受到大多数现代 Linux 发行版的信任。EFS 挂载帮助程序还会生成一个监视程序进程来监视每个文件系统的所有安全隧道并确保它们正在运行。

使用 EFS 挂载帮助程序建立与 Amazon EFS 的加密连接后，无需其他用户输入或配置。加密对访问文件系统的用户连接和应用程序是透明的。

使用 EFS 挂载帮助程序成功挂载并建立与 EFS 文件系统的加密连接后，挂载命令的输出显示文件系统已挂载，并且已使用 localhost（127.0.0.1）作为网络中继建立加密隧道。请参阅以下示例输出。

```
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
```

要将 `efs-mount-point` 映射至 EFS 文件系统，请在 `/var/log/amazon/efs` 中查询 mount.log 文件，然后查找上次成功的挂载操作。这可以使用以下简单的 grep 命令来完成。

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

此 grep 命令的输出将返回挂载的 EFS 文件系统的 DNS 名称。请参阅下面的示例输出。

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

结论

Amazon EFS 文件系统数据可以静态加密和传输中加密。您可以使用 CMK 对数据进行静态加密，使用 AWS KMS 控制和管理 CMK。创建加密文件系统非常简单，只需在 AWS 管理控制台的 Amazon EFS 文件系统创建向导中选中复选框，或者在 AWS CLI、AWS 开发工具包或 Amazon EFS API 中为 `CreateFileSystem` 操作添加一个参数。

您可以使用 AWS IAM 基于身份的策略和文件系统策略强制实施静态加密和传输中加密，以进一步增强安全要求并帮助满足合规性需求。使用加密的文件系统对服务、应用程序和用户也是透明的，对文件系统性能的影响微乎其微。您可以使用 EFS 挂载帮助程序在每个客户端上建立加密的 TLS 隧道，对客户端和挂载的 EFS 文件系统之间的所有 NFS 流量进行加密，从而对传输中的数据进行加密。您可以使用 IAM 身份策略对静态的 Amazon EFS 数据进行加密，也可以使用 EFS 文件系统策略对传输中的数据进行加密，无需额外付费。

资源

- AWS KMS 加密详情白皮书
- Amazon EFS 用户指南

文档历史记录和贡献者

文档历史记录

要获得有关此白皮书的更新通知，请订阅 RSS 源。

更新-历史记录-更改	更新-历史记录-描述	更新-历史记录-日期
次要更新	调整了页面布局	2021 年 4 月 30 日
更新了白皮书	增加了使用 IAM 强制实施静态加密和传输中加密	2021 年 2 月 22日
更新了白皮书	增加了传输中数据加密	2018 年 4 月 1 日
初次发布	发布了使用 Amazon EFS 加密文件系统加密静态数据	2017 年 9 月 1 日

> **Note**
>
> 要订阅 RSS 更新，您必须为正在使用的浏览器启用 RSS 插件。

贡献者

本文档的贡献者包括：

- AWS 存储专家和解决方案构架师 Darryl S. Osborne
- Amazon EFS 高级产品经理 Joseph Travaglini
- AWS 首席解决方案构架师 Peter Buonora
- AWS 高级解决方案构架师 Siva Rajamani