Documento técnico de AWS

Cifrado de datos de archivos con Amazon Elastic File System

Cifrado de datos de archivos con Amazon Elastic File System: Documento técnico de AWS

Table of Contents

Cifrado de datos de archivos con Amazon Elastic File System

Fecha de publicación: 22 de febrero de 2021 (Historial de revisión y colaboradores)

Resumen

La seguridad es el trabajo cero para AWS y les damos a nuestros clientes las herramientas para hacer la seguridad como trabajo cero en su empresa. Las regulaciones gubernamentales y las políticas de conformidad de la industria o la empresa pueden requerir que los datos de diferentes clasificaciones se protejan mediante el uso de políticas de cifrado, algoritmos criptográficos y una administración de claves adecuada. En este documento se describen las prácticas recomendadas para cifrar Amazon Elastic File System (Amazon EFS).

Introducción

Amazon Elastic File System (Amazon EFS) proporciona sistemas de archivos compartidos sencillos, escalables, de alta disponibilidad y muy duraderos en la nube. Los sistemas de archivos que crea con Amazon EFS son elásticos, lo que les permite crecer y reducirse automáticamente a medida que agrega y elimina datos. Pueden crecer en tamaño a petabytes, distribuyendo los datos en una cantidad ilimitada de servidores de almacenamiento en varias zonas de disponibilidad (AZ).

Los datos almacenados en estos sistemas de archivos se pueden cifrar en reposo y en tránsito mediante Amazon EFS. Para el cifrado de datos en reposo, puede crear sistemas de archivos cifrados a través de la consola de administración de AWS o deAWS Command Line Interface (AWS CLI). O bien, puede crear sistemas de archivos cifrados mediante programación a través de la API de Amazon EFS o uno de los SDK de AWS.

Para el cifrado de datos en reposo, Amazon EFS se integra con AWS Key Management Service (AWS KMS) para la administración de claves. También puede habilitar el cifrado de datos en tránsito montando el sistema de archivos y transfiriendo todo el tráfico NFS a través de Seguridad de la capa de transporte (TLS).

En este documento se describen las prácticas recomendadas de cifrado para Amazon EFS. Describe cómo habilitar el cifrado de datos en tránsito en la capa de conexión del cliente y cómo crear un sistema de archivos cifrados en la consola de administración de AWS y en AWS CLI.

> **Note**
>
> El uso de las API y los SDK para crear un sistema de archivos cifrados está fuera del alcance de este documento. Para obtener más información sobre cómo hacerlo, consulte la API de Amazon EFS en la Guía del usuario de Amazon EFS o en la documentación del SDK.

Conceptos básicos y terminología

En esta sección se definen los conceptos y la terminología que se mencionan en este documento técnico.

- Amazon Elastic File System (Amazon EFS): un servicio de alta disponibilidad y durabilidad que proporciona almacenamiento de archivos en la nube de AWS compartido, escalable y sencillo. Amazon EFS proporciona una interfaz de sistema de archivos estándar y una semántica del sistema de archivos. Puede almacenar una cantidad prácticamente ilimitada de datos en un número ilimitado de servidores de almacenamiento en varias zonas de disponibilidad.
- AWS Identity and Access Management (IAM): un servicio que le permite controlar de forma segura el acceso detallado a las API de servicios de AWS. Las políticas se crean y utilizan para limitar el acceso a usuarios, grupos y roles individuales. Puede administrar sus claves de AWS KMS a través de la consola de IAM.
- AWS KMS: un servicio administrado que facilita la creación y el control de las claves maestras del cliente (CMK), las claves de cifrado utilizadas para cifrar los datos. Las CMK de AWS KMS están protegidas por módulos de seguridad de hardware (HSM) validados por el Programa de validación de módulos criptográficos FIPS 140-2 excepto en las regiones China (Pekín) y China (Ningxia). AWS KMS se integra con otros servicios de AWS que cifran sus datos. También está completamente integrado con AWS CloudTrail para proporcionar registros de las llamadas a la API realizadas por AWS KMS en su nombre, lo que puede resultar útil para cumplir con los requisitos de conformidad o normativos aplicables a su organización.
- Clave maestra del cliente (CMK): representa la parte superior de la jerarquía de claves. Contiene material clave para cifrar y descifrar datos. AWS KMS puede generar este material clave o puede generarlo y, a continuación, importarlo en AWS KMS. Las CMK son específicas de una cuenta de AWS y una región de AWS y las puede administrar el cliente o AWS.
- CMK administrada por AWS: una CMK generada por AWS en su nombre. Una CMK administrada por AWS se crea cuando se habilita el cifrado para un recurso de un servicio de AWS integrado. AWS administra las políticas clave de CMK administradas por AWS y no puede cambiarlas. No se aplican cargos por la creación o el almacenamiento de CMK administradas por AWS.
- CMK administrada por el cliente: una CMK que se crea mediante la API o la consola de administración de AWS, AWS CLI o los SDK. Puede usar una CMK administrada por el cliente cuando necesite un control más específico sobre la CMK.
- Política de claves de KMS: política de recursos que controla el acceso a una CMK administrada por el cliente. Los clientes definen estos permisos mediante la política clave o una combinación de

políticas de IAM y la política clave. Para obtener más información, consulte Información general sobre la administración del acceso en la Guía para desarrolladores de AWS KMS.

- Claves de datos: claves criptográficas generadas por AWS KMS para cifrar datos fuera de AWS KMS. AWS KMS permite a las entidades autorizadas (usuarios o servicios) obtener claves de datos protegidas mediante una CMK.
- Seguridad de la capa de transporte (TLS): el sucesor de la capa de sockets seguros (SSL), TLS es un protocolo criptográfico esencial para cifrar la información que se intercambia a través de una red.
- Ayudante de montaje de EFS: un agente cliente Linux (`amazon-efs-utils`) que se utiliza para simplificar el montaje de sistemas de archivos EFS. Se puede usar para configurar, mantener y dirigir todo el tráfico NFS a través de un túnel TLS.

Para obtener más información sobre los conceptos básicos y la terminología, consulte Conceptos de AWS Key Management Service en la Guía para desarrolladores de AWS KMS.

Cifrado de datos en reposo

AWS proporciona las herramientas para crear un sistema de archivos cifrados que cifre todos los datos y metadatos en reposo mediante un algoritmo de cifrado AES-256 estándar del sector. Un sistema de archivos cifrados se ha diseñado para administrar el cifrado y el descifrado de forma automática y transparente, para no tener que modificar las aplicaciones. Si la organización está sujeta a políticas corporativas o regulatorias que requieren el cifrado de datos y metadatos en reposo, recomendamos crear un sistema de archivos encriptado.

Temas

Administración de claves

Amazon EFS se integra con AWS KMS, que administra las claves de cifrado de los sistemas de archivos cifrados. AWS KMStambién admite el cifrado de otros servicios de 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 cifrar el contenido del sistema de archivos, Amazon EFS utiliza el algoritmo estándar de cifrado avanzado con modo XTS y una clave de 256 bits (XTS-AES-256).

Hay tres preguntas importantes que responder al considerar cómo proteger los datos en reposo mediante la adopción de cualquier política de cifrado. Estas preguntas son igualmente válidas para los datos almacenados en servicios administrados y no administrados, como Amazon EBS.

¿Dónde se guardan las llaves?

AWS KMS almacena sus claves maestras en un almacenamiento altamente duradero en un formato cifrado para garantizar que su recuperación cuando sea necesario.

¿Dónde se usan las claves?

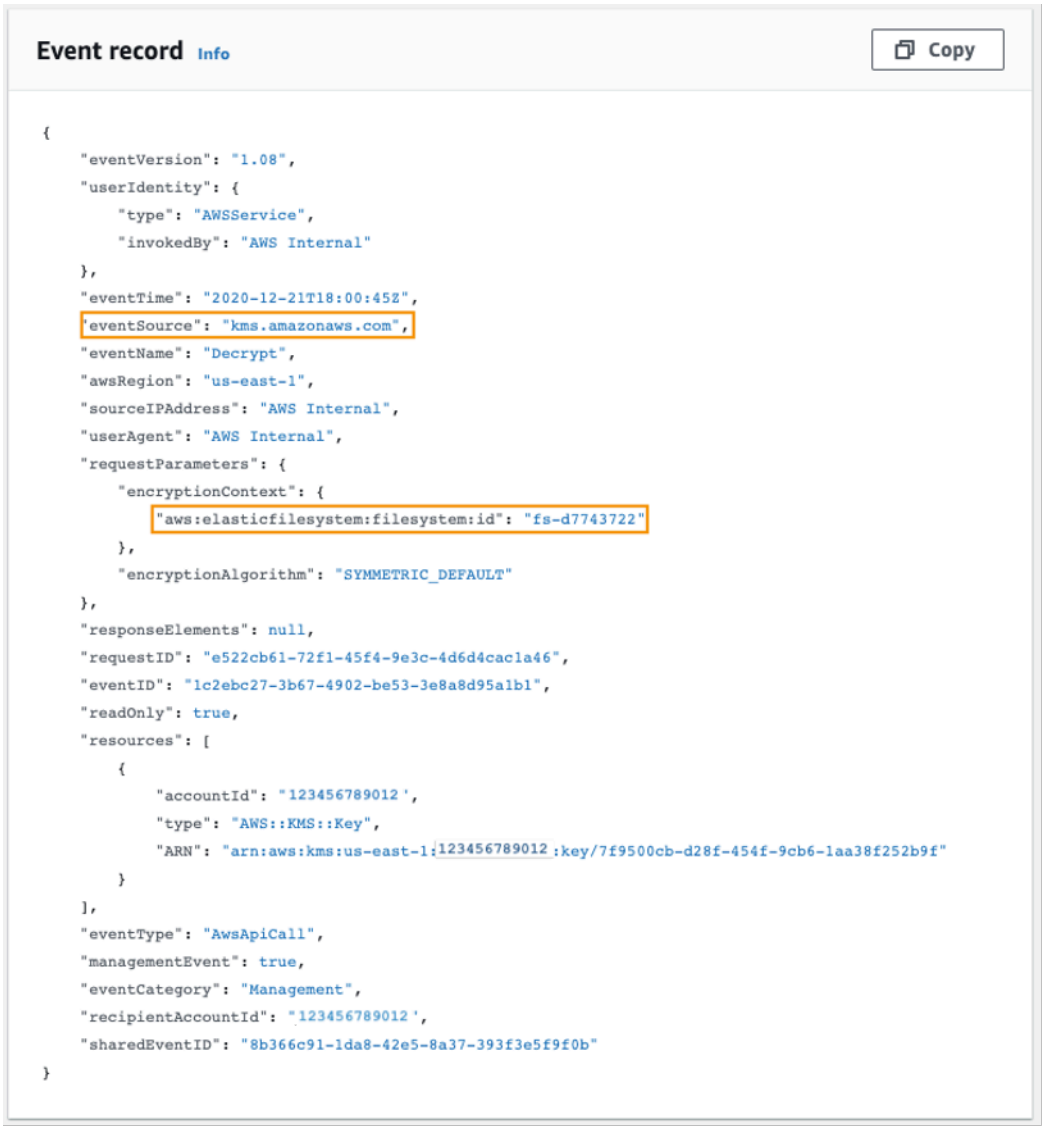
El uso de un sistema de archivos cifrado de Amazon EFS es transparente para los clientes que montan el sistema de archivos. Todas las operaciones criptográficas se producen dentro del servicio EFS, ya que los datos se cifran antes de escribirse en el disco y se descifran después de que un cliente emita una solicitud de lectura.

¿Quién puede usar las claves?

Las políticas de claves de AWS KMS controlan el acceso a las claves de cifrado

Le recomendamos que las combine con las políticas de IAM para proporcionar otra capa de control. Cada clave tiene una política de claves. Si la clave es una CMK administrada por AWS, AWS administra la política de claves. Si la clave es una CMK administrada por el cliente, el usuario administra la política de claves. Estas políticas de claves son la forma principal de controlar el acceso a las CMK. Definen los permisos que rigen el uso y la administración de las claves.

Cuando se crea un sistema de archivos cifrados con Amazon EFS, se concede a Amazon EFS acceso para utilizar la CMK en su nombre. Las llamadas que Amazon EFSS hace a AWS KMS en su nombre aparecen en los registros de CloudTrail como si se hubieran originado en la cuenta de AWS. En la siguiente captura de pantalla se muestra el evento de ejemplo de CloudTrail para una llamada de KMS Decrypt realizada por Amazon EFS.



Registro de CloudTrail para KMS Decrypt

Para obtener más información sobre AWS KMS y cómo administrar el acceso a las claves de cifrado, consulte Administración de acceso a las CMK de AWS KMS en la Guía para desarrolladores de AWS KMS.

Para obtener más información sobre cómo AWS KMS administra la criptografía, consulte el documento técnico Detalles criptográficos de AWS KMS.

Para obtener más información sobre cómo crear un grupo y usuario administrador de IAM, consulte Creación del primer usuario administrador de IAM y grupo de usuarios en la Guía del usuario de IAM.

Creación de un sistema de archivos cifrado

Puede crear un sistema de archivos cifrados mediante la consola de administración de AWS, AWS CLI, la API de Amazon EFS o los SDK de AWS. Solo se puede habilitar el cifrado para un sistema de archivos cuando se crea.

Amazon EFS se integra con AWS KMS para la administración de claves y utiliza una CMK para cifrar el sistema de archivos. Los metadatos del sistema de archivos, como los nombres de archivos, los nombres de directorios y el contenido del directorio, se cifran y descifran mediante una CMK administrada por AWS.

El contenido de los archivos o datos de archivo, se cifra y descifra mediante una CMK que se elija. La CMK puede ser de tres tipos:

- Una CMK administrada por AWS para Amazon EFS
- Una CMK administrada por el cliente desde su cuenta de AWS
- Una CMK administrada por el cliente desde una cuenta de AWS diferente

La organización puede estar sujeta a políticas corporativas o regulatorias que requieran un control total en términos de creación, rotación y eliminación, así como la política de uso y control de acceso para las CMK. Si así fuera, recomendamos utilizar una CMK administrada por el cliente. En otros escenarios, se puede usar una CMK administrada por AWS.

Todos los usuarios tienen una CMK administrada por AWS para Amazon EFS, cuyo alias es `aws/elasticfilesystem`. AWS administra la política de claves de esta CMK y no puede cambiarla. La creación y el almacenamiento de CMK administradas por AWS no tienen ningún coste.

Si se decide utilizar una CMK administrada por el cliente para cifrar el sistema de archivos, hay que seleccionar el alias de clave de la CMK administrada por el cliente de la que se sea propietario. Como alternativa, se puede introducir el nombre de recurso de Amazon (ARN) de una CMK administrada por el cliente que sea propiedad de otra cuenta. Con una CMK administrada por el cliente propia, se controla qué usuarios y servicios pueden usar la clave a través de políticas de claves y concesiones de claves.

También se puede controlar la duración y la rotación de estas claves eligiendo cuándo deshabilitarlas, volver a habilitarlas, eliminarlas o revocar el acceso a ellas. Para obtener información sobre cómo administrar el acceso a las claves en otras cuentas de AWS, consulte Cambiar una política de claves en la Guía para desarrolladores de AWS KMS.

Para obtener más información sobre cómo administrar las CMK administradas por el cliente, consulte Claves maestras de clientes (CMK) en la Guía para desarrolladores de AWS KMS.

En las siguientes secciones se explica cómo crear un sistema de archivos cifrados con la consola de administración de AWS y con AWS CLI.

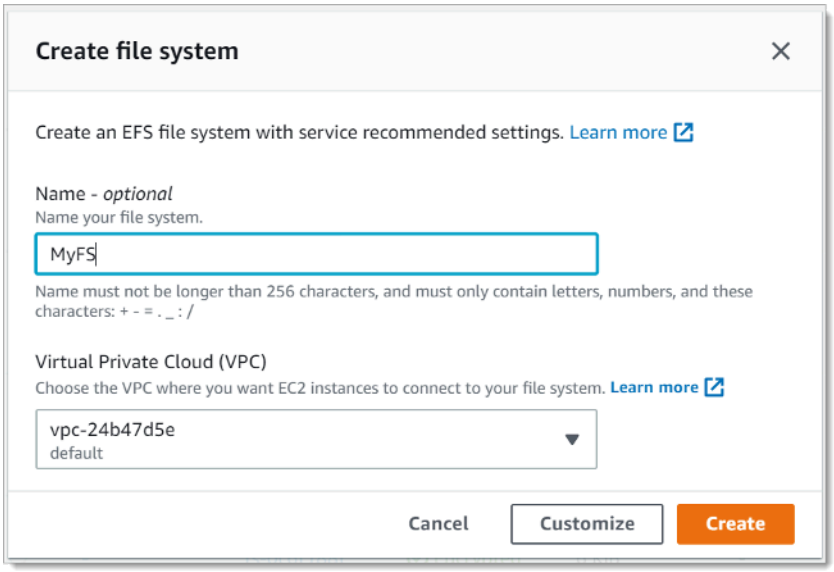
Creación de un sistema de archivos cifrados mediante la consola de administración de AWS

Utilice el siguiente procedimiento para crear un sistema de archivos cifrados de Amazon EFS mediante la consola de administración de AWS.

Paso 1. Definir la configuración del sistema de archivos

En este paso, se define la configuración general del sistema de archivos, incluida la administración del ciclo de vida, los modos de rendimiento y desempeño y el cifrado de datos en reposo.

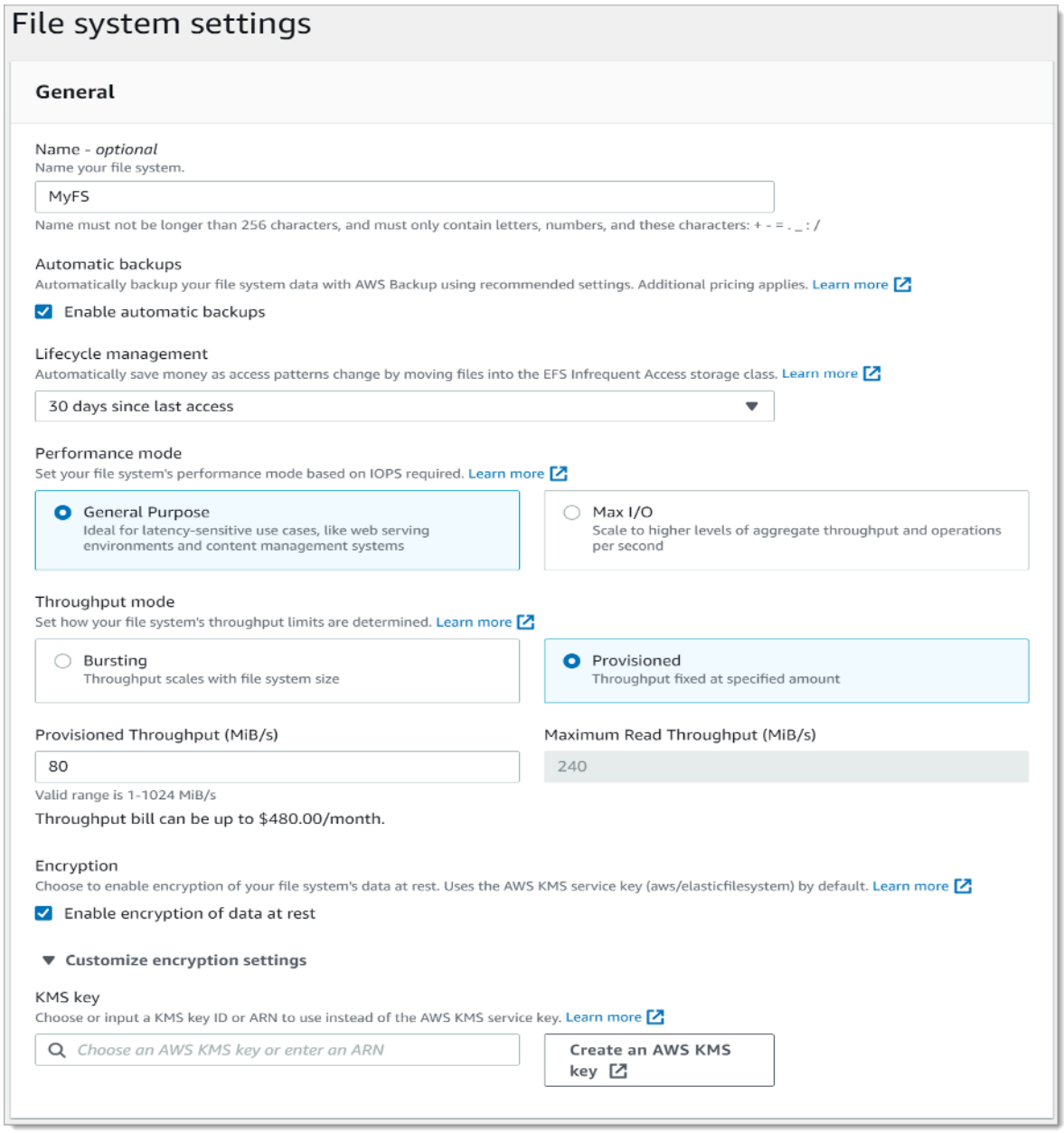
1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon EFS.
2. Seleccione Create file system (Crear sistema de archivos) para abrir el cuadro de diálogo Create file system (Crear sistema de archivos). Para obtener más información sobre la creación de un sistema de archivos mediante el uso de la configuración recomendada que incluye habilitar el cifrado de forma predeterminada, consulte Cree su sistema de archivos de Amazon EFS.



Crear sistema de archivos de EFS

3. (Opcional) Seleccione Customize (Personalizar) para crear un sistema de archivos personalizado en lugar de crear un sistema de archivos con la configuración recomendada del servicio.

Aparece la página File system settings (Configuración del sistema de archivos).



Crear sistema de archivos de EFS: configuración general

4. En la configuración General, escriba los siguientes detalles.
   - (Opcional) Ingrese un nombre para el sistema de archivos.
   - Las copias de seguridad automáticas están activadas de forma predeterminada. Puede desactivar las copias de seguridad automáticas desmarcando la casilla de verificación. Para obtener más información, consulte Uso de AWS Backup con Amazon EFS.

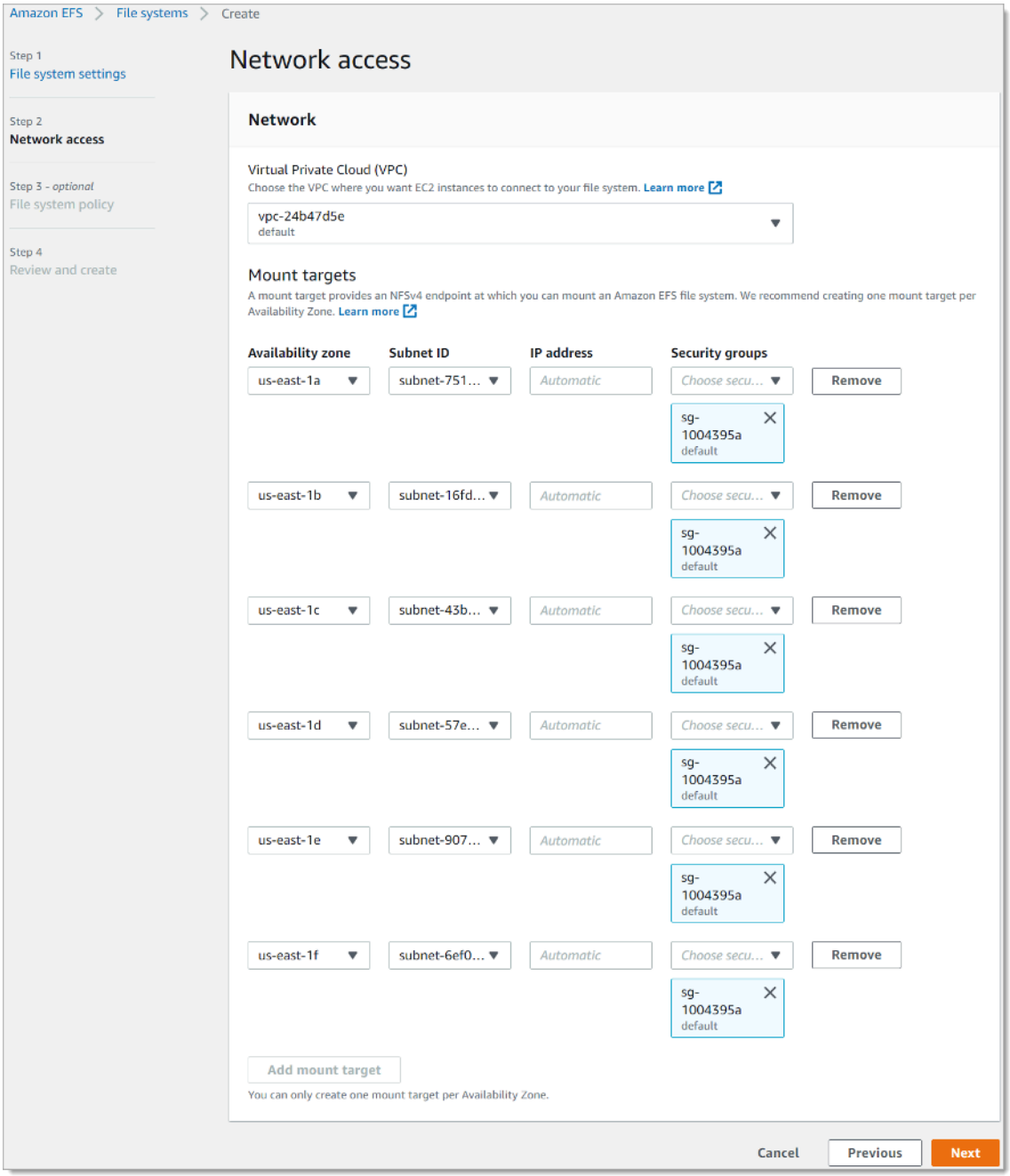
- Elija una política de administración del ciclo de vida. La administración del ciclo de vida de Amazon EFS administra automáticamente el almacenamiento económico de los archivos para sus sistemas de archivos. Cuando está habilitada, la administración del ciclo de vida migra los archivos a los que no se ha obtenido acceso durante un periodo determinado a la clase de almacenamiento Acceso poco frecuente (IA). Para definir dicho periodo, utilice una política de ciclo de vida. Si no desea activar la administración del ciclo de vida, seleccione None (Ninguna). Para obtener más información, consulte Administración del ciclo de vida de EFS en la Guía del usuario de Amazon EFS.
- Elija un modo de rendimiento, ya sea el modo predeterminado General Purpose (Uso general) o Max I/O (E/S máx.). Para obtener más información, consulte Modos de rendimiento en la Guía del usuario de Amazon EFS.
- Elija un modo de desempeño, ya sea el modo predeterminado Bursting (Por ráfagas) o el modo Provisioned (Aprovisionado).
- Si se ha seleccionado Provisioned (Aprovisionado), se muestra el campo Provisioned Throughput (MiB/s) (Rendimiento aprovisionado (MIB/s)). Introduzca la cantidad de desempeño que se va a aprovisionar para el sistema de archivos. Después de introducir el desempeño, la consola muestra una estimación del coste mensual junto al campo. Para obtener más información, consulte Modos de rendimiento en la Guía del usuario de Amazon EFS.
- En Encryption (Cifrado), el cifrado de datos en reposo está habilitado de forma predeterminada. Utiliza la clave del servicio de EFS de AWS Key Management Service (AWS KMS) (`aws/elasticfilesystem`) de forma predeterminada. Para utilizar una clave de KMS diferente en el cifrado, amplíe Customize encryption settings (Personalizar configuración de cifrado) y elija una clave de la lista. O bien introduzca un ID de clave de KMS o el nombre de recurso de Amazon (ARN) de la clave de KMS que desee utilizar.

  Si tiene que crear una clave nueva, seleccione Create an AWS KMS key (Crear una clave de AWS KMS) para lanzar la consola de AWS KMS y crear una clave nueva.

5. (Opcional) Seleccione Add tag (Añadir etiqueta) para añadir pares clave-valor al sistema de archivos.
6. Seleccione Next (Siguiente) para continuar con el paso Network Access (Acceso a la red) del proceso de configuración.

Paso 2. Paso 2: configurar el acceso a la red

En este paso, se configuran los ajustes de red del sistema de archivos, incluida la nube privada virtual (VPC) y los destinos de montaje. En cada uno de los destinos de montaje, establezca la zona de disponibilidad, la subred, la dirección IP y los grupos de seguridad.



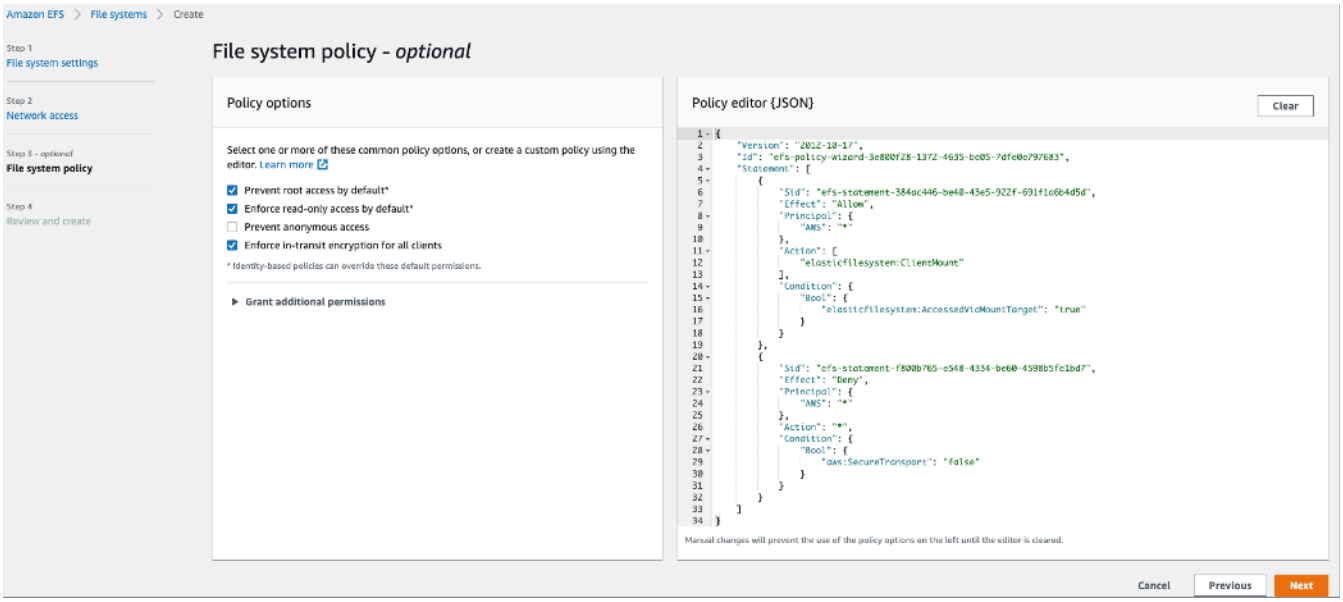
Crear sistema de archivos de EFS: acceso a la red

1. Elija la Virtual Private Cloud (VPC) en la que desea que las instancias de EC2 se conecten al sistema de archivos. Para obtener más información, consulte Administración de la accesibilidad de la red del sistema de archivos en la Guía del usuario de Amazon EFS.
   - Availability zone (Zona de disponibilidad): de forma predeterminada, se configura un destino de montaje en cada una de las zonas de disponibilidad de una región de AWS. Si no desea un destino de montaje en una zona de disponibilidad determinada, seleccione Remove (Quitar) para eliminar el destino de montaje de dicha zona. Crear un destino de montaje en todas las zonas de disponibilidad a las que prevea acceder desde su sistema de archivos no supone ningún coste.
   - Subnet ID (ID de subred): seleccione una de las subredes disponibles en una zona de disponibilidad. La subred predeterminada está preseleccionada. Como práctica recomendada, asegúrese de que la subred elegida sea pública o privada en función de sus requisitos de seguridad.
   - IP Address (Dirección IP): de forma predeterminada, Amazon EFS selecciona la dirección IP automáticamente de las direcciones disponibles en la subred. O bien puede introducir una dirección IP concreta que esté en la subred. Aunque los destinos de montaje tienen una única dirección IP, son recursos de red redundantes de alta disponibilidad.
   - Security groups (Grupos de seguridad): puede especificar uno o varios grupos de seguridad en el destino de montaje. Como práctica recomendada, asegúrese de que el grupo de seguridad solo se use para fines de montaje de EFS (puerto NFS 2049) y que las reglas de entrada solo permitan el puerto 2049 de otro rango de bloques de CIDR de VPC o use Grupo de seguridad como origen de los recursos que necesitan acceder a EFS. Para obtener más información, consulte Uso de grupos de seguridad para instancias Amazon EC2 y destinos de montaje en la Guía del usuario de Amazon EFS.

     Para añadir otro grupo de seguridad o cambiarlo, seleccione Choose security groups (Elegir grupos de seguridad) y añada otro grupo de seguridad de la lista. Si no desea utilizar el grupo de seguridad predeterminado, puede eliminarlo. Para obtener más información, consulte Creación de grupos de seguridad en la Guía del usuario de Amazon EFS.
2. Elija Add mount target (Añadir destino de montaje) para crear un destino de montaje en una zona de disponibilidad que no tenga uno. Si se configura un destino de montaje en cada una de las zonas de disponibilidad, esta opción no está disponible.
3. Elija Next (Siguiente) para continuar. Aparece la página File system policy (Política de sistema de archivos).

Paso 3. Crear una política del sistema de archivos

En teste paso, cree una política de sistema de archivos para controlar el acceso del cliente NFS al sistema de archivos. Una política de sistema de archivos de EFS es una política de recursos de IAM que se utiliza para controlar el acceso del cliente NFS al sistema de archivos. Para obtener más información, consulte Uso de IAM para controlar el acceso de NFS a Amazon EFS en la Guía del usuario de Amazon EFS.

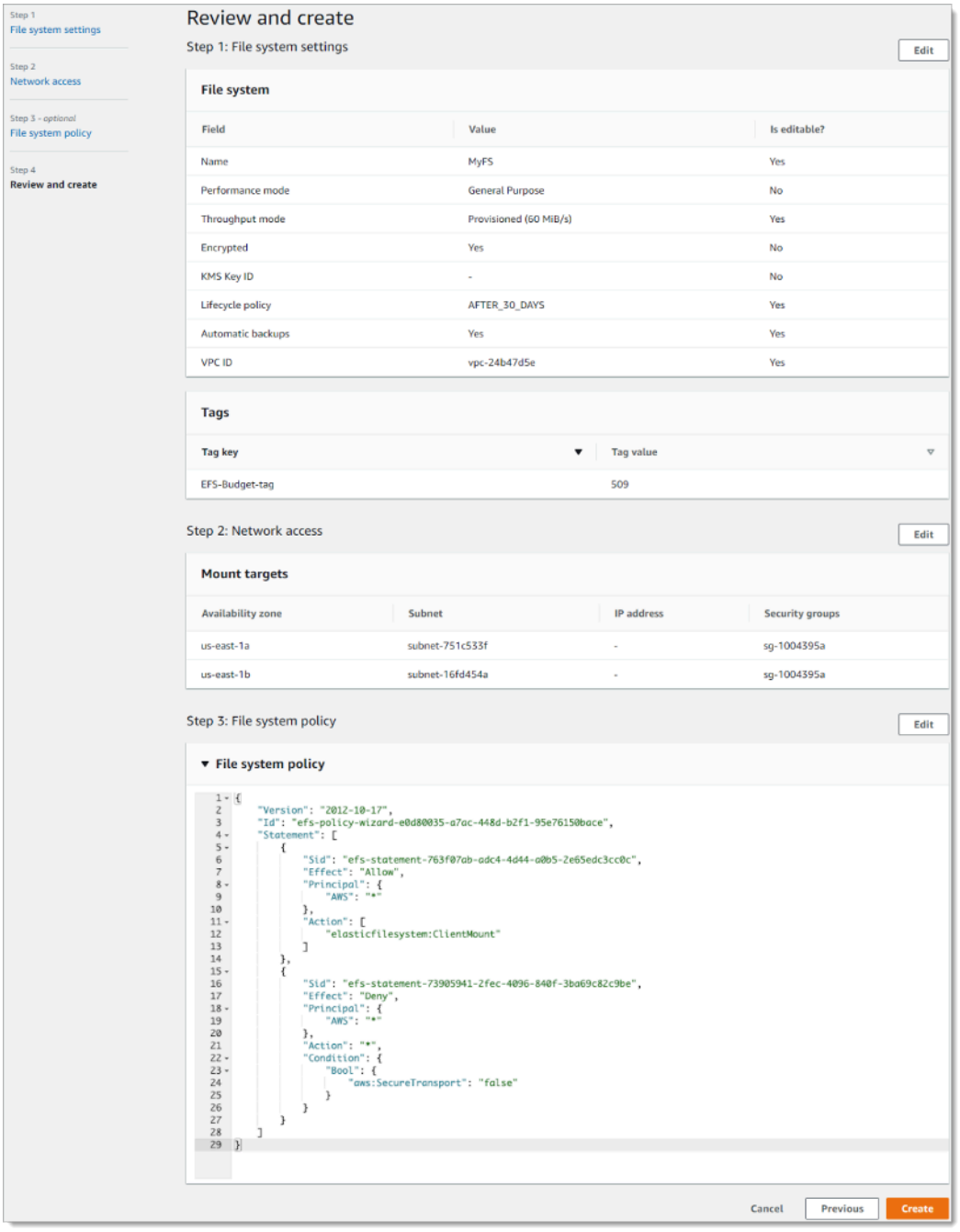


Crear sistema de archivos de EFS: política del sistema de archivos

1. En Policy options (Opciones de política), le recomendamos que elija las siguientes opciones de políticas preconfiguradas disponibles:
   - Impedir el acceso raíz de forma predeterminada
   - Imponer el acceso de solo lectura de forma predeterminada
   - Imponer el cifrado en tránsito para todos los clientes
2. Use Grant additional permissions (Otorgar permisos adicionales) para conceder permisos del sistema de archivos a entidades principales de IAM adicionales, incluida otra cuenta de AWS. Elija Add (Agregar), luego ingrese el ARN principal de la entidad a la que le está otorgando permisos y, a continuación, elija los permisos que se vayan a otorgar.
3. Utilice el editor de políticas para personalizar una política preconfigurada o crear su propia política basándose en los requisitos. Al elegir una de las políticas preconfiguradas, la definición de política JSON aparece en el editor de políticas.
4. Elija Next (Siguiente) para continuar. Aparece la página Review and create (Revisar y crear).

Paso 4. Revisar y crear

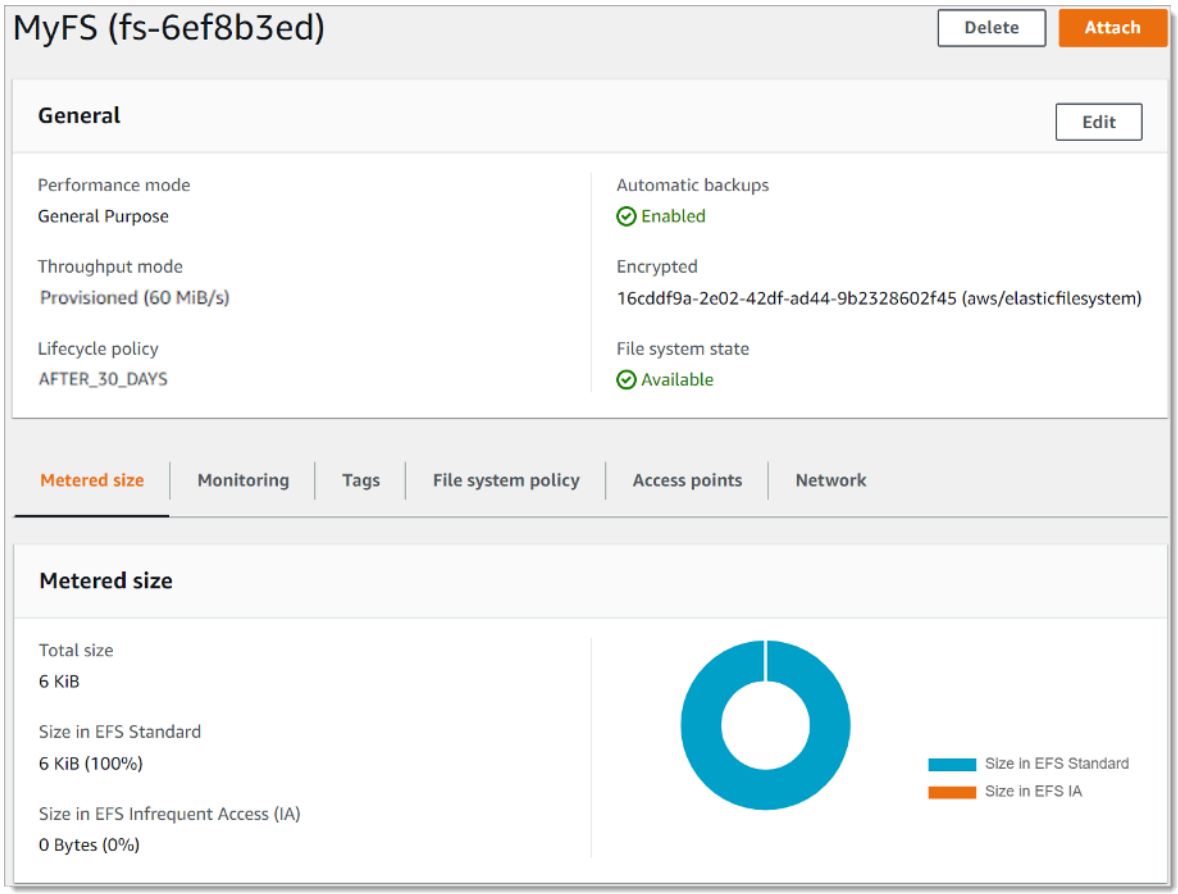
En este paso, revise la configuración del sistema de archivos, realice las modificaciones que desee y, a continuación, cree el sistema de archivos.



Crear sistema de archivos de EFS: revisar y crear

1. Revise cada uno de los grupos de configuración del sistema de archivos. Puede realizar cambios en los grupos en este momento seleccionando Edit (Editar).

2. Seleccione Create (Crear) para crear el sistema de archivos y volver a la página File systems (Sistemas de archivos).
3. La página File systems (Sistemas de archivos) muestra el sistema de archivos y los detalles de su configuración, como se muestra en la siguiente imagen.



Sistemas de archivos

Creación de un sistema de archivos cifrados mediante AWS CLI

Cuando utilice AWS CLI para crear un sistema de archivos cifrados, puede usar parámetros adicionales para establecer el estado de cifrado y la CMK administrada por el cliente. Asegúrese de que utiliza la última versión de AWS CLI. Para obtener información sobre cómo actualizar AWS CLI, consulte Instalación, actualización y desinstalación de AWS CLI en la Guía del usuario de la interfaz de línea de comandos de AWS.

En la operación `CreateFileSystem`, el parámetro `--encrypted` es booleano y es necesario para crear sistemas de archivos cifrados. Solo se requiere `--kms-key-id` cuando se utiliza una

CMK administrada por el cliente y se incluye el alias o el ARN de la clave. No se debe incluir este parámetro si se utiliza la CMK administrada de AWS.

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

Para obtener más información sobre la creación de sistemas de archivos de Amazon EFS con la consola de administración de AWS, AWS CLI, los SDK de AWS o la API de Amazon EFS, consulte la Guía del usuario de Amazon Elastic File System Amazon EFS.

Aplicación del cifrado de datos en reposo

El cifrado tiene un efecto mínimo en la latencia y el rendimiento de E/S. El cifrado y el descifrado son transparentes para los usuarios, las aplicaciones y los servicios. Amazon EFS cifra todos los datos y metadatos en su nombre antes de que se escriban en el disco y se descifran antes de que los clientes los lean. No es necesario cambiar las herramientas, las aplicaciones o los servicios del cliente para acceder a un sistema de archivos cifrados.

Su organización podría necesitar el cifrado en reposo de todos los datos que cumplan una clasificación específica o que se asocien a una determinada aplicación, carga de trabajo o entorno. Puede utilizar políticas basadas en identidad AWS Identity and Access Management (IAM) para imponer el cifrado de los datos en reposo para los recursos del sistema de archivos de Amazon EFS. Con una clave de condición de IAM, puede evitar que los usuarios creen sistemas de archivos EFS que no estén cifrados.

Por ejemplo, una política de IAM que permite explícitamente a los usuarios crear solo sistemas de archivos EFS cifrados utiliza la siguiente combinación de efecto, acción y condición:

- El valor de `Effect` es `Allow`.
- El valor de `Action` es `elasticfilesystem:CreateFileSystem`.
- El valor de `Condition elasticfilesystem:Encrypted` es `true`.

El siguiente ejemplo ilustra una política basada en identidad de IAM que autoriza a las entidades principales a crear solo sistemas de archivos cifrados.

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

El atributo `Resource` establecido en * significa que la política de IAM se aplica a todos los recursos de EFS creados. Puede agregar atributos condicionales adicionales basados en etiquetas para aplicarlos solo para un subconjunto de recursos de EFS con necesidades de clasificación de datos.

También puede aplicar la creación de sistemas de archivos cifrados de Amazon EFS a nivel AWS Organizations mediante el uso de políticas de control de servicios para todas las cuentas de AWS o unidades organizativas de su organización. Para obtener más información sobre las políticas de control de servicios en AWS Organizations, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations.

Creación de una política de IAM que requiere el cifrado de todos los sistemas de archivos de EFS

Puede crear una política basada en identidad de IAM que autorice a los usuarios a crear solo sistemas de archivos cifrados de Amazon EFS mediante la consola, AWS CLI o la API. En el siguiente procedimiento se describe cómo crear una política de este tipo mediante la consola de IAM y, a continuación, aplicar la política a un usuario de su cuenta.

Para crear una política de IAM para aplicar sistemas de archivos de EFS cifrados:

1. Inicie sesión en la consola de administración de AWS y abra la consola de IAM.

2. En el panel de navegación, en Access management (Administración de acceso), elija Policies (Políticas).
3. Elija Create policy (Crear política) para mostrar la página Create policy (Crear política).
4. En la pestaña Visual Editor (Editor visual), ingrese la siguiente información.
   - ParaService (Servicio), elija EFS.
   - En Actions (Acciones), ingrese `create` en el campo de búsqueda y, a continuación, elija CreateFileSystem.
   - En Request conditions (Condiciones de solicitud), haga clic en el enlace Add condition (Agregar condición), busque `elasticfilesystem:Encrypted` para Condition Key (Clave de condición), `Bool` para Operator (Operador) y `true` para Value (Valor).
5. Proporcione un nombre y una descripción para la política. Verifique el resumen de la política, incluida la condición de solicitud Encrypted (Cifrada).
6. Elija Create policy (Crear política) para crear la política.

Para aplicar la política a un usuario de su cuenta:

1. En la consola de IAM, en Access management (Administración de acceso), elija Users (Usuarios).
2. Seleccione el usuario al que desea aplicar la política.
3. Elija Add permissions (Agregar permisos) para mostrar la página Add permissions (Agregar permisos).
4. Elija Attach existing policies directly (Asociar directamente políticas existentes).
5. Ingrese el nombre de la política de EFS que creó en el procedimiento anterior.
6. Seleccione y expanda la política. A continuación, elija {} JSON para verificar el contenido de la política. Debe tener el aspecto de la política de JSON que se incluye a continuación.

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

```
            “elasticfilesystem:Encrypted”: “true”
          }
        },
        “Resource”: “*”
      }
}
```

Detección de sistemas de archivos no cifrados

Es posible que su organización tenga la obligación de identificar los recursos de Amazon EFS que no estén cifrados. Puede detectar sistemas de archivos sin cifrar mediante las reglas administradas de AWS Config. AWS Config proporciona reglas administradas de AWS, que son reglas predefinidas y personalizables que AWS Config utiliza para evaluar si sus recursos de AWS cumplen con las prácticas recomendadas comunes y marcar los recursos que no cumplen las reglas como NON_COMPLIANT.

Puede utilizar la regla de AWS Managed Config `efs-encrypted-check` para comprobar si Amazon Elastic File System (Amazon EFS) está configurado para cifrar los datos del archivo mediante AWS Key Management Service (AWS KMS). Para obtener más información sobre cómo configurar y activar las reglas administradas de AWS, consulte Trabajo con reglas administradas de AWS Config.

Cifrado de datos en tránsito

Puede montar un sistema de archivos para que todo el tráfico NFS se cifre en tránsito mediante Seguridad de la capa de transporte 1.2 (TLS) con un cifrado AES-256 estándar del sector. TLS es un conjunto de protocolos criptográficos estándar del sector que se utilizan para cifrar la información que se intercambia a través de la red. AES-256 es un cifrado de 256 bits que se utiliza para la transmisión de datos en TLS. Recomendamos configurar el cifrado en tránsito en cada cliente que acceda al sistema de archivos.

Puede utilizar políticas de IAM para aplicar el cifrado en tránsito para el acceso de los clientes de NFS a Amazon EFS. Cuando un cliente se conecta a un sistema de archivos, Amazon EFS evalúa la política de recursos de IAM del sistema de archivos, conocida como política del sistema de archivos, junto con las políticas de IAM basadas en la identidad de para determinar los permisos de acceso del sistema de archivos que se deben conceder. Puede usar la clave de condición `aws:SecureTransport` en la política de recursos del sistema de archivos para obligar a los clientes NFS a usar TLS al conectarse a un sistema de archivos EFS.

> **Note**
>
> Debe utilizar el ayudante de montaje EFS para montar sus sistemas de archivos de Amazon EFS con el fin de utilizar la autorización de IAM para controlar el acceso de los clientes NFS. Para obtener más información, consulte Montaje con autorización de IAM en la Guía del usuario de Amazon EFS.

El siguiente ejemplo de política del sistema de archivos EFS impone el cifrado en tránsito y tiene las siguientes características:

- El valor de `effect` es `allow`.
- El principio se establece en * para todas las entidades de IAM.
- La acción se establece en `ClientMount`, `ClientWrite`, `ClientRootAccess`.
- La condición para conceder permisos se establece en `SecureTransport`. Solo se concede acceso a los clientes NFS que utilizan TLS para conectarse al sistema de archivos.

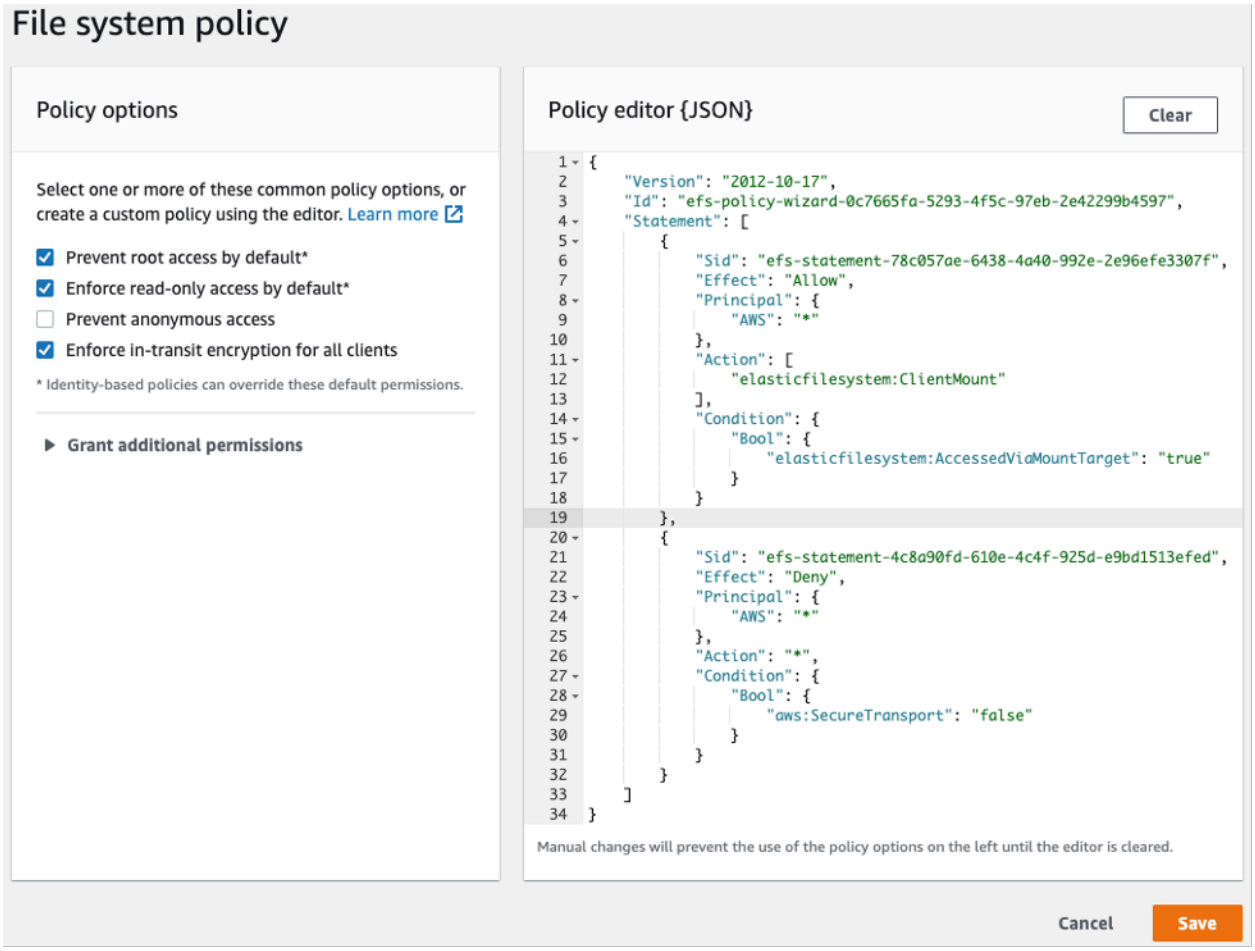
```
{
  “Version”: “2012-10-17”,
```

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

Puede crear una política de sistema de archivos mediante la consola de Amazon EFS o mediante AWS CLI.

Para crear una política del sistema de archivos mediante la consola de EFS:

1. Abra la consola de Amazon EFS.
2. Seleccione File systems (Sistemas de archivos).
3. En la página File systems (Sistemas de archivos), elija el sistema de archivos para el que desea editar o crear una política de sistema de archivos. Se muestra la página de detalles de dicho sistema de archivos.
4. Seleccione File system policy (Política de sistema de archivos) y, a continuación, Edit (Editar). Aparece la página File system policy (Política del sistema de archivos).



Crear política del sistema de archivos

5. En Policy options (Opciones de política), le recomendamos que elija las siguientes opciones de política preconfiguradas disponibles:

   - Impedir el acceso raíz de forma predeterminada
   - Imponer el acceso de solo lectura de forma predeterminada
   - Imponer el cifrado en tránsito para todos los clientes

   Si elige una política preconfigurada, el objeto JSON de la política se muestra en el panel Policy editor (Editor de políticas).

6. Use Grant additional permissions (Otorgar permisos adicionales) para conceder permisos del sistema de archivos a entidades principales de IAM adicionales, incluida otra cuenta de AWS. Elija Add (Agregar), luego ingrese el ARN principal de la entidad a la que le está otorgando permisos y, a continuación, elija los permisos que se vayan a otorgar.

7. Utilice el editor de políticas para personalizar una política preconfigurada o crear su propia política basándose en los requisitos. Al utilizar el editor, las opciones de políticas preconfiguradas dejan de estar disponibles. Para deshacer los cambios en las políticas, seleccione Clear (Borrar).

   Al borrar el editor, las políticas preconfiguradas vuelven a estar disponibles.
8. Tras finalizar la edición o creación de la política, seleccione Save (Guardar).

   Aparece la página de detalles del sistema de archivos, en la que se muestra la política en File system policy (Política de sistema de archivos).

   También puede crear una política de sistema de archivos mediante programación utilizando AWS CloudFormation, los SDK de AWS o la API de Amazon EFS directamente. Para obtener más información sobre la creación de políticas del sistema de archivos, consulte Creación de políticas del sistema de archivos en la Guía del usuario de Amazon EFS.

Configuración del cifrado de datos en tránsito

Para configurar el cifrado de los datos en tránsito, le recomendamos que descargue el ayudante de montaje EFS en cada cliente. El ayudante de montaje de EFS es una utilidad de código abierto que AWS proporciona para simplificar el uso de EFS, incluida la configuración del cifrado de datos en tránsito. El ayudante de montaje utiliza las opciones de montaje recomendadas por EFS de forma predeterminada.

El ayudante de montaje de EFS se admite en las siguientes distribuciones de Linux:

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

Para configurar el cifrado de los datos en tránsito:

1. Instale el ayudante de montaje de EFS:

- En Amazon Linux, use este comando:

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

- En ara otras distribuciones de Linux, descárguelo de GitHub e instálelo.

  El paquete amazon-efs-utils instala automáticamente las siguientes dependencias: cliente NFS (nfs-utils), retransmisión de red (stunnel), OpenSSL y Python.

2. Monte el sistema de archivos:

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

- `mount -t efs` invoca al ayudante de montaje de EFS.
- No se admite el uso del nombre DNS del sistema de archivos o la dirección IP de un destino de montaje cuando se monta con el ayudante de montaje de EFS; en su lugar, use el identificador del sistema de archivos.
- El ayudante de montaje EFS utiliza las opciones de montaje recomendadas por AWS de forma predeterminada. No se recomienda anular estas opciones de montaje predeterminadas, pero proporcionamos la flexibilidad de hacerlo cuando surja la ocasión. Le recomendamos que pruebe a fondo cualquier anulación de las opciones de montaje para que comprenda cómo afectan estos cambios al acceso al sistema de archivos y al rendimiento.
- La siguiente tabla representa las opciones de montaje predeterminadas que utiliza el ayudante de montaje de EFS.

Opción	Descripción
nfsvers=4.1	La versión del protocolo NFS
rsize=1048576	El número máximo de bytes de datos que el cliente NFS puede

Opción	Descripción
	recibir para cada solicitud READ de red
wsize=1048576	El número máximo de bytes de datos que el cliente NFS puede enviar para cada solicitud WRITE de red
hard	El comportamiento de recuperación del cliente NFS después de que se agote el tiempo de espera de una solicitud NFS, de modo que las solicitudes de NFS se vuelven a intentar indefinidamente hasta que el servidor responde.

Opción	Descripción
timeo=600	El valor de tiempo de espera que utiliza el cliente NFS para esperar una respuesta antes de que vuelva a intentar una solicitud NFS en décimas de segundo
retrans=2	El número de veces que el cliente de NFS reintenta una solicitud antes de intentar una acción de recuperación adicional.
noresvport	Indica al cliente NFS que use un nuevo puerto de origen TCP cuando se restablece una conexión de red

- Agregue la siguiente línea a `/etc/fstab` para volver montar automáticamente el sistema de archivos después de reiniciar el sistema.

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

Utilización del cifrado de datos en tránsito

Si su organización está sujeta a políticas corporativas o regulatorias que requieren el cifrado de los datos en tránsito, le recomendamos usar el cifrado de los datos en tránsito en cada cliente que acceda al sistema de archivos. El cifrado y el descifrado se configuran en el nivel de conexión y agregan otra capa de seguridad.

El montaje del sistema de archivos con el ayudante de montaje de EFS configura y mantiene un túnel TLS 1.2 entre el cliente y Amazon EFS, y dirige todo el tráfico de NFS a través de este túnel cifrado. El certificado utilizado para establecer la conexión TLS cifrada está firmado por la Autoridad de Certificación (CA) de Amazon y la mayoría de las distribuciones de Linux modernas confían en él. El ayudante de montaje de EFS también genera un proceso de vigilancia para supervisar todos los túneles seguros a cada sistema de archivos y garantizar que se estén ejecutando.

Después de utilizar el ayudante de montaje de EFS para establecer conexiones cifradas con Amazon EFS, no se requiere ninguna otra entrada o configuración del usuario. El cifrado es transparente para las conexiones de usuario y las aplicaciones que acceden al sistema de archivos

Después de montar y establecer correctamente una conexión cifrada a un sistema de archivos de EFS mediante el ayudante de montaje de EFS, el resultado de un comando mount muestra que el sistema de archivos está montado y que se ha establecido un túnel cifrado utilizando el host local (127.0.0.1) como retransmisión de red. Consulte el siguiente ejemplo de resultado.

```
     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 asignar un `efs-mount-point` a un sistema de archivos de EFS, consulte el archivo mount.log en `/var/log/amazon/efs` y busque la última operación de montaje correcta. Esto se puede hacer con el siguiente comando grep simple.

```
     grep -E "Successfully
     mounted.*efs-mount-point"
```

```
/var/log/amazon/efs/mount.log | tail -1
```

El resultado de este comando grep devolverá el nombre DNS del sistema de archivos EFS montado. Consulte el resultado de ejemplo a continuación.

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

Conclusión

Los datos del sistema de archivos de Amazon EFS se pueden cifrar en reposo y en tránsito. Puede cifrar los datos en reposo mediante CMK, que puede controlar y administrar con AWS KMS. La creación de un sistema de archivos cifrados es tan simple como seleccionar una casilla de verificación en el asistente de creación del sistema de archivos de Amazon EFS en la consola de administración de AWS o agregar un único parámetro a la operación de `CreateFileSystem` en AWS CLI, los SDK de AWS o la API de Amazon EFS.

Puede aplicar el cifrado en reposo y en tránsito mediante las políticas basadas en identidad y las políticas del sistema de archivos de AWS IAM para reforzar aún más sus requisitos de seguridad y ayudar a satisfacer sus necesidades de conformidad. El uso de un sistema de archivos cifrado también es transparente para los servicios, las aplicaciones y los usuarios, con un efecto mínimo en el rendimiento del sistema de archivos. Puede cifrar los datos en tránsito mediante el ayudante de montaje EFS para establecer un túnel TLS cifrado en cada cliente, cifrando todo el tráfico NFS entre el cliente y el sistema de archivos EFS montado. La aplicación del cifrado de los datos de Amazon EFS en reposo mediante políticas de identidad de IAM y en tránsito mediante políticas del sistema de archivos EFS está disponible para sin coste adicional.

Recursos

- Documento técnico Detalles criptográficos de AWS KMS
- Guía del usuario de Amazon EFS:

Historial de revisión y colaboradores

Historial de revisión

Para recibir notificaciones sobre las actualizaciones de este documento técnico, suscríbase a la fuente RSS.

update-history-change	update-history-description	update-history-date
Actualizaciones menores	Diseño de página ajustado.	30 de abril de 2021
Documento técnico actualizado	Aplicación adicional del cifrado en reposo y en tránsito mediante IAM	22 de febrero de 2021
Documento técnico actualizado	Se ha añadido el cifrado de datos en tránsito	1 de abril de 2018
Publicación inicial	Cifre datos en reposo con los sistemas de archivos cifrados de Amazon EFS publicado	1 de septiembre de 2017

> **Note**
>
> Para suscribirse a las actualizaciones de RSS, debe disponer de un complemento de RSS habilitado para el navegador que utilice.

Colaboradores

Entre los colaboradores de este documento, están las siguientes personas:

- Darryl S. Osborne, arquitecto de soluciones especializado en almacenamiento, AWS
- Joseph Travaglini, director sénior de productos, Amazon EFS
- Peter Buonora, arquitecto principal de soluciones, AWS

- Siva Rajamani, arquitecto sénior de soluciones, AWS