Laporan Resmi AWS

Mengenkripsi Data File dengan Amazon Elastic File System

Mengenkripsi Data File dengan Amazon Elastic File System: Laporan Resmi AWS

Table of Contents

Mengenkripsi Data File dengan Amazon Elastic File System

Tanggal publikasi: 22 Februari 2021 (Riwayat Dokumen dan Kontributor)

Abstrak

Keamanan adalah pekerjaan prioritas untuk AWS dan kami memberi pelanggan alat untuk menjalankan keamanan sebagai pekerjaan prioritas di korporasi mereka. Peraturan pemerintah dan kebijakan kepatuhan industri atau perusahaan mungkin mengharuskan data klasifikasi yang berbeda-beda diamankan dengan menggunakan kebijakan enkripsi, algoritme kriptografi, dan manajemen kunci yang tepat. Laporan ini menguraikan praktik terbaik untuk mengenkripsi Amazon Elastic File System (Amazon EFS).

Pengantar

Amazon Elastic File System (Amazon EFS) menyediakan sistem file bersama yang sederhana, dapat diskalakan, berketersediaan tinggi, dan sangat berdaya tahan di cloud. Sistem file yang Anda buat menggunakan Amazon EFS bersifat elastis, sehingga memungkinkannya tumbuh dan menyusut secara otomatis saat Anda menambahkan dan menghapus data. Sistem file ini dapat bertambah ukurannya hingga petabita, dan mendistribusikan data di sejumlah server penyimpanan yang tidak terbatas di banyak Zona Ketersediaan (AZ).

Data yang disimpan dalam sistem file ini dapat dienkripsi saat at rest dan in transit menggunakan Amazon EFS. Untuk enkripsi data at rest, Anda dapat membuat sistem file terenkripsi melalui Konsol Manajemen AWS atau AWS Command Line Interface (AWS CLI). Atau Anda dapat membuat sistem file terenkripsi secara terprogram melalui API Amazon EFS atau salah satu SDK AWS.

Untuk enkripsi data at rest, Amazon EFS terintegrasi dengan AWS Key Management Service (AWS KMS) untuk manajemen kunci. Anda juga dapat mengaktifkan enkripsi data in transit dengan memasang sistem file dan mentransfer semua lalu lintas NFS melalui Keamanan Lapisan Pengangkutan (TLS).

Laporan ini menguraikan praktik terbaik enkripsi untuk Amazon EFS. Laporan ini menjelaskan cara mengaktifkan enkripsi data in transit di lapisan koneksi klien, dan cara membuat sistem file terenkripsi di Konsol Manajemen AWS dan di AWS CLI.

> **Note**
>
> Bahasan tentang menggunakan API dan SDK untuk membuat sistem file terenkripsi berada di luar cakupan laporan ini. Untuk informasi selengkapnya tentang cara melakukannya, lihat API Amazon EFS dalam Panduan Pengguna Amazon EFS atau dokumentasi SDK.

Konsep dan Terminologi Dasar

Bagian ini mendefinisikan konsep dan terminologi yang direferensikan dalam laporan resmi ini.

- Amazon Elastic File System (Amazon EFS) – Layanan yang berketersediaan tinggi dan sangat berdaya tahan yang menyediakan penyimpanan file bersama yang sederhana dan dapat diskalakan di AWS Cloud. Amazon EFS menyediakan antarmuka sistem file dan semantik sistem file standar. Anda dapat menyimpan jumlah data yang hampir tidak terbatas di sejumlah server penyimpanan yang tidak terbatas di beberapa Zona Ketersediaan.
- AWS Identity and Access Management (IAM) – Layanan yang memungkinkan Anda mengontrol akses terperinci ke API layanan AWS dengan aman. Kebijakan dibuat dan digunakan untuk membatasi akses ke pengguna, grup, dan peran individual. Anda dapat mengelola kunci AWS KMS melalui konsol IAM.
- AWS KMS – Layanan terkelola yang memudahkan Anda untuk membuat dan mengontrol kunci utama pelanggan (CMK), kunci enkripsi yang digunakan untuk mengenkripsi data Anda. AWS KMS CMK dilindungi oleh modul keamanan perangkat keras (HSM) yang divalidasi oleh Program Validasi Modul Kriptografi FIPS 140-2 kecuali di Wilayah Tiongkok (Beijing) dan Tiongkok (Ningxia). AWS KMS terintegrasi dengan layanan AWS lain yang mengenkripsi data Anda. Layanan ini juga terintegrasi sepenuhnya dengan AWS CloudTrail untuk menyediakan log panggilan API yang dibuat oleh AWS KMS atas nama Anda, yang dapat membantu memenuhi persyaratan kepatuhan atau peraturan yang berlaku untuk organisasi Anda.
- Kunci utama pelanggan (CMK) – Merupakan bagian atas hierarki kunci Anda. Ini berisi material kunci untuk mengenkripsi dan mendekripsi data. AWS KMS dapat menghasilkan materi kunci ini, atau Anda dapat membuatnya dan kemudian mengimpornya ke AWS KMS. CMK ditujukan khusus untuk akun AWS dan Wilayah AWS dan dapat dikelola pelanggan atau dikelola AWS.
- CMK yang dikelola AWS – CMK yang dihasilkan oleh AWS atas nama Anda. CMK yang dikelola AWS dibuat saat Anda mengaktifkan enkripsi untuk sumber daya layanan AWS terintegrasi. Kebijakan kunci CMK yang dikelola AWS akan dikelola oleh AWS dan Anda tidak dapat mengubahnya. Tidak ada biaya untuk pembuatan atau penyimpanan CMK yang dikelola AWS.
- CMK yang dikelola pelanggan – CMK yang Anda buat dengan menggunakan Konsol Manajemen AWS atau API, AWS CLI, atau SDK. Anda dapat menggunakan CMK yang dikelola pelanggan saat Anda membutuhkan kontrol yang lebih terperinci atas CMK.
- Kebijakan Kunci KMS – Kebijakan sumber daya yang mengontrol akses ke CMK yang dikelola pelanggan. Pelanggan menentukan izin ini menggunakan kebijakan kunci atau kombinasi

kebijakan IAM dan kebijakan kunci. Untuk informasi selengkapnya, lihat Gambaran Umum tentang Mengelola Akses dalam Panduan Developer AWS KMS.

- Kunci data – Kunci kriptografi yang dihasilkan oleh AWS KMS untuk mengenkripsi data di luar AWS KMS. AWS KMS memungkinkan entitas resmi (pengguna atau layanan) untuk mendapatkan kunci data yang dilindungi oleh CMK.
- Keamanan Lapisan Pengangkutan (TLS) – Penerus Lapisan Soket Aman (SSL), TLS adalah protokol kriptografi yang penting untuk mengenkripsi informasi yang dipertukarkan melalui jaringan.
- EFS mount helper – Agen klien Linux (`amazon-efs-utils`) yang digunakan untuk menyederhanakan pemasangan sistem file EFS. Hal ini dapat digunakan untuk penyiapan, pemeliharaan, dan perutean semua lalu lintas NFS melalui terowongan TLS.

Untuk informasi selengkapnya tentang konsep dan terminologi dasar, lihat Konsep AWS Key Management Service dalam Panduan Developer AWS KMS.

Enkripsi Data at Rest

AWS menyediakan alat bagi Anda untuk membuat sistem file terenkripsi yang mengenkripsi semua data dan metadata Anda saat at rest menggunakan algoritme enkripsi AES-256 standar industri. Sistem file terenkripsi dirancang untuk menangani enkripsi dan dekripsi secara otomatis dan transparan, sehingga Anda tidak perlu memodifikasi aplikasi Anda. Jika organisasi Anda tunduk pada kebijakan korporasi atau peraturan yang mewajibkan enkripsi data dan metadata saat at rest, sebaiknya Anda membuat sistem file terenkripsi.

Topik

Mengelola Kunci

Amazon EFS terintegrasi dengan AWS KMS, yang mengelola kunci enkripsi untuk sistem file terenkripsi. AWS KMS juga mendukung enkripsi oleh layanan AWS lainnya seperti 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, dll. Untuk mengenkripsi konten sistem file, Amazon EFS menggunakan algoritme Advanced Encryption Standard dengan Mode XTS dan kunci 256-bit (XTS-AES-256).

Ada tiga pertanyaan penting untuk dijawab ketika mempertimbangkan bagaimana mengamankan data at rest dengan mengadopsi kebijakan enkripsi apa pun. Pertanyaan-pertanyaan ini sama-sama berlaku untuk data yang disimpan dalam layanan terkelola dan tidak terkelola seperti Amazon EBS.

Di mana kunci disimpan?

AWS KMS menyimpan kunci utama Anda dalam penyimpanan yang sangat berdaya tahan dalam format terenkripsi untuk membantu memastikan bahwa kunci tersebut dapat diambil jika diperlukan.

Di mana kunci digunakan?

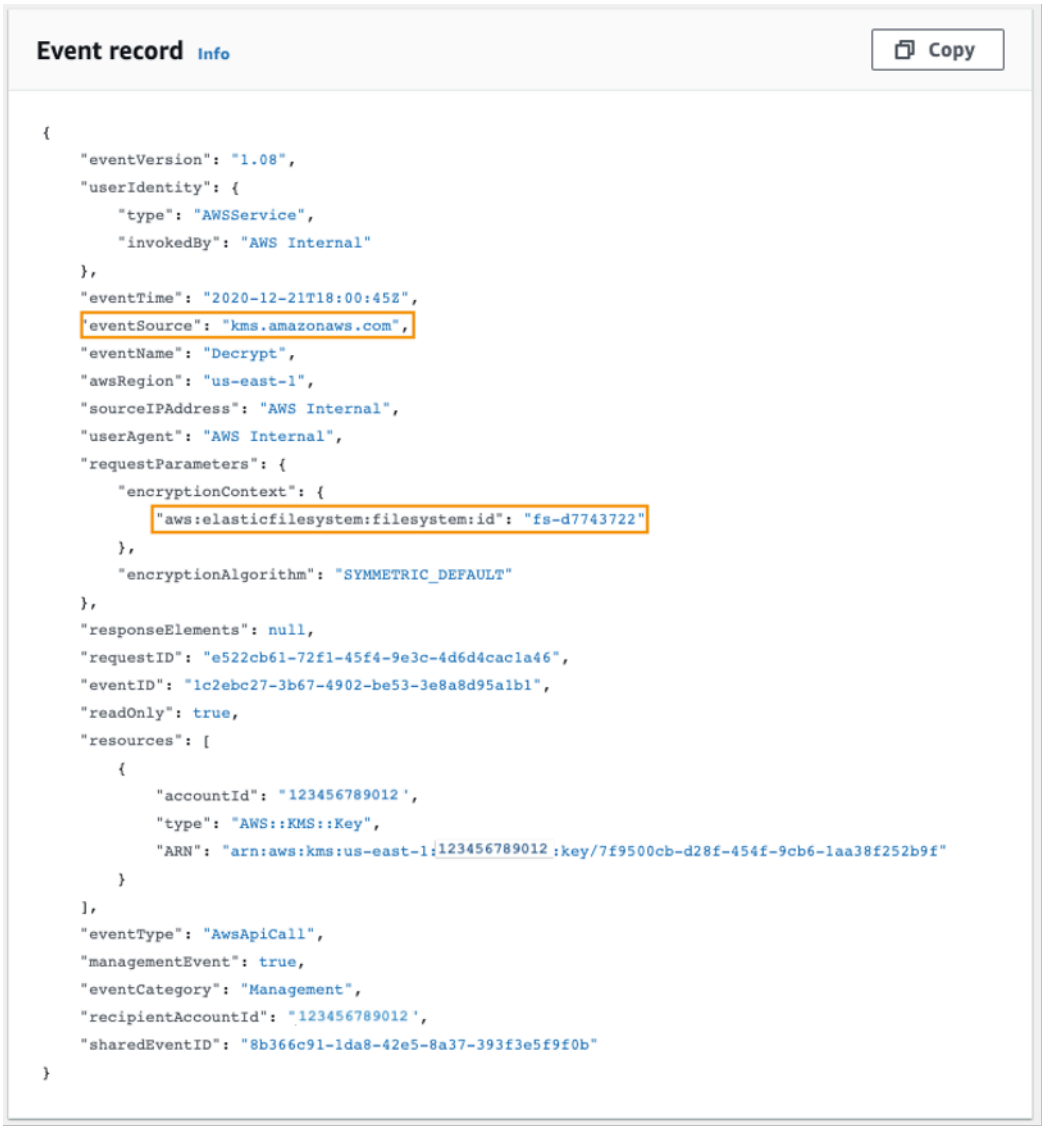
Penggunaan sistem file Amazon EFS terenkripsi akan terlihat untuk klien yang memasang sistem file. Semua operasi kriptografi terjadi dalam layanan EFS, karena data dienkripsi sebelum ditulis ke disk dan didekripsi setelah klien mengeluarkan permintaan baca.

Siapa yang bisa menggunakan kunci?

Kebijakan kunci AWS KMS mengontrol akses ke kunci enkripsi.

Kami sarankan Anda menggabungkannya dengan kebijakan IAM untuk menyediakan lapisan kontrol lain. Setiap kunci memiliki kebijakan kunci. Jika kuncinya adalah CMK yang dikelola AWS, AWS yang akan mengelola kebijakan kunci. Jika kuncinya adalah CMK yang dikelola pelanggan, Anda yang akan mengelola kebijakan kunci. Kebijakan kunci ini adalah cara utama untuk mengontrol akses ke CMK. Kebijakan ini mendefinisikan izin yang mengatur penggunaan dan pengelolaan kunci.

Saat Anda membuat sistem file terenkripsi menggunakan Amazon EFS, Anda memberikan akses ke Amazon EFS untuk menggunakan CMK atas nama Anda. Panggilan yang dibuat Amazon EFS ke AWS KMS atas nama Anda muncul di log CloudTrail Anda seolah-olah berasal dari akun AWS Anda. Cuplikan layar berikut menunjukkan contoh peristiwa CloudTrail untuk panggilan KMS Decrypt yang dibuat oleh Amazon EFS.



Log CloudTrail untuk KMS Decrypt

Untuk informasi selengkapnya tentang AWS KMS dan cara mengelola akses ke kunci enkripsi, lihat Mengelola Akses ke AWS KMS CMK dalam Panduan Developer AWS KMS.

Untuk informasi selengkapnya tentang cara AWS KMS mengelola kriptografi, lihat laporan resmi Detail Kriptografi AWS KMS.

Untuk informasi selengkapnya tentang cara membuat pengguna dan grup IAM administrator, lihat Membuat Pengguna dan Grup Admin IAM Pertama Anda dalam Panduan Pengguna IAM.

Membuat Sistem File Terenkripsi

Anda dapat membuat sistem file terenkripsi menggunakan Konsol Manajemen AWS, AWS CLI, Amazon EFS API, atau SDK AWS. Anda hanya dapat mengaktifkan enkripsi untuk sistem file saat Anda membuatnya.

Amazon EFS terintegrasi dengan AWS KMS untuk manajemen kunci dan menggunakan CMK untuk mengenkripsi sistem file. Metadata sistem file, seperti nama file, nama direktori, dan konten direktori, dienkripsi dan didekripsi menggunakan CMK yang dikelola AWS.

Konten file Anda, atau data file, dienkripsi dan didekripsi menggunakan CMK yang Anda pilih. CMK bisa berupa salah satu dari tiga jenis berikut:

- CMK yang dikelola AWS untuk Amazon EFS
- CMK yang dikelola pelanggan dari akun AWS Anda
- CMK yang dikelola pelanggan dari akun AWS yang berbeda

Organisasi Anda mungkin tunduk pada kebijakan korporasi atau peraturan yang mewajibkan kontrol penuh dalam hal pembuatan, rotasi, penghapusan, serta kontrol akses dan kebijakan penggunaan untuk CMK. Jika demikian, kami sarankan Anda menggunakan CMK yang dikelola pelanggan. Dalam skenario lain, Anda dapat menggunakan CMK yang dikelola AWS.

Semua pengguna memiliki CMK yang dikelola AWS untuk Amazon EFS, yang aliasnya adalah `aws/elasticfilesystem`. AWS mengelola kebijakan kunci CMK ini dan Anda tidak dapat mengubahnya. Tidak ada biaya untuk membuat dan menyimpan CMK yang dikelola AWS.

Jika Anda memutuskan untuk menggunakan CMK yang dikelola pelanggan untuk mengenkripsi sistem file Anda, pilih alias kunci CMK yang dikelola pelanggan yang Anda miliki. Atau, Anda dapat memasukkan Amazon Resource Name (ARN) dari CMK yang dikelola pelanggan yang dimiliki oleh akun yang berbeda. Dengan CMK yang dikelola pelanggan yang Anda miliki, Anda mengontrol pengguna dan layanan mana yang dapat menggunakan kunci ini melalui kebijakan kunci dan pemberian kunci.

Anda juga mengontrol masa aktif dan rotasi kunci ini dengan memilih kapan harus menonaktifkan, mengaktifkan kembali, menghapus, atau mencabut akses ke kunci tersebut. Untuk informasi tentang mengelola akses ke kunci di akun AWS lainnya, lihat Mengubah kebijakan kunci dalam Panduan Developer AWS KMS.

Untuk informasi selengkapnya tentang cara mengelola CMK yang dikelola pelanggan, lihat Kunci utama pelanggan (CMK) dalam Panduan Developer AWS KMS.

Bagian berikut membahas cara membuat sistem file terenkripsi menggunakan Konsol Manajemen AWS dan menggunakan AWS CLI.

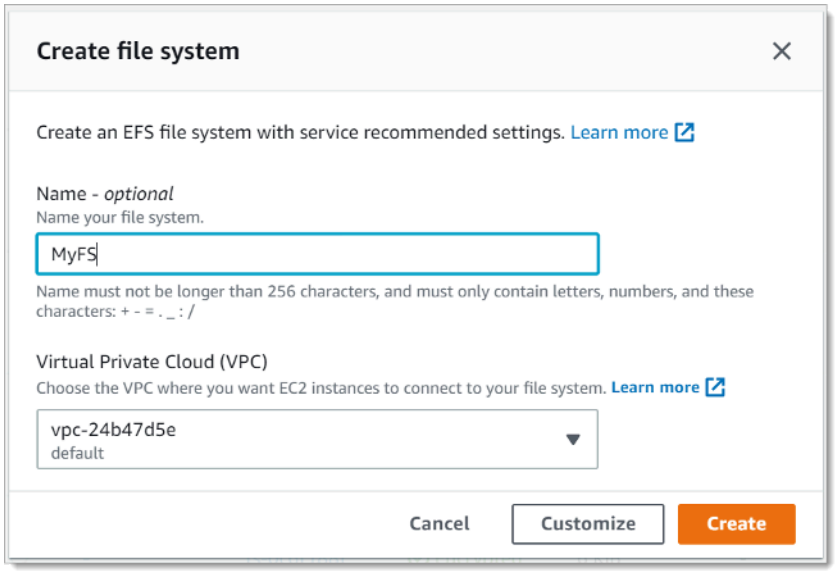
Membuat Sistem File Terenkripsi Menggunakan Konsol Manajemen AWS

Gunakan prosedur berikut untuk membuat sistem file Amazon EFS terenkripsi menggunakan Konsol Manajemen AWS.

Langkah 1. Konfigurasikan Pengaturan Sistem File

Pada langkah ini, Anda mengonfigurasi pengaturan sistem file umum, termasuk manajemen Siklus Hidup, mode Performa dan Throughput, serta enkripsi data at rest.

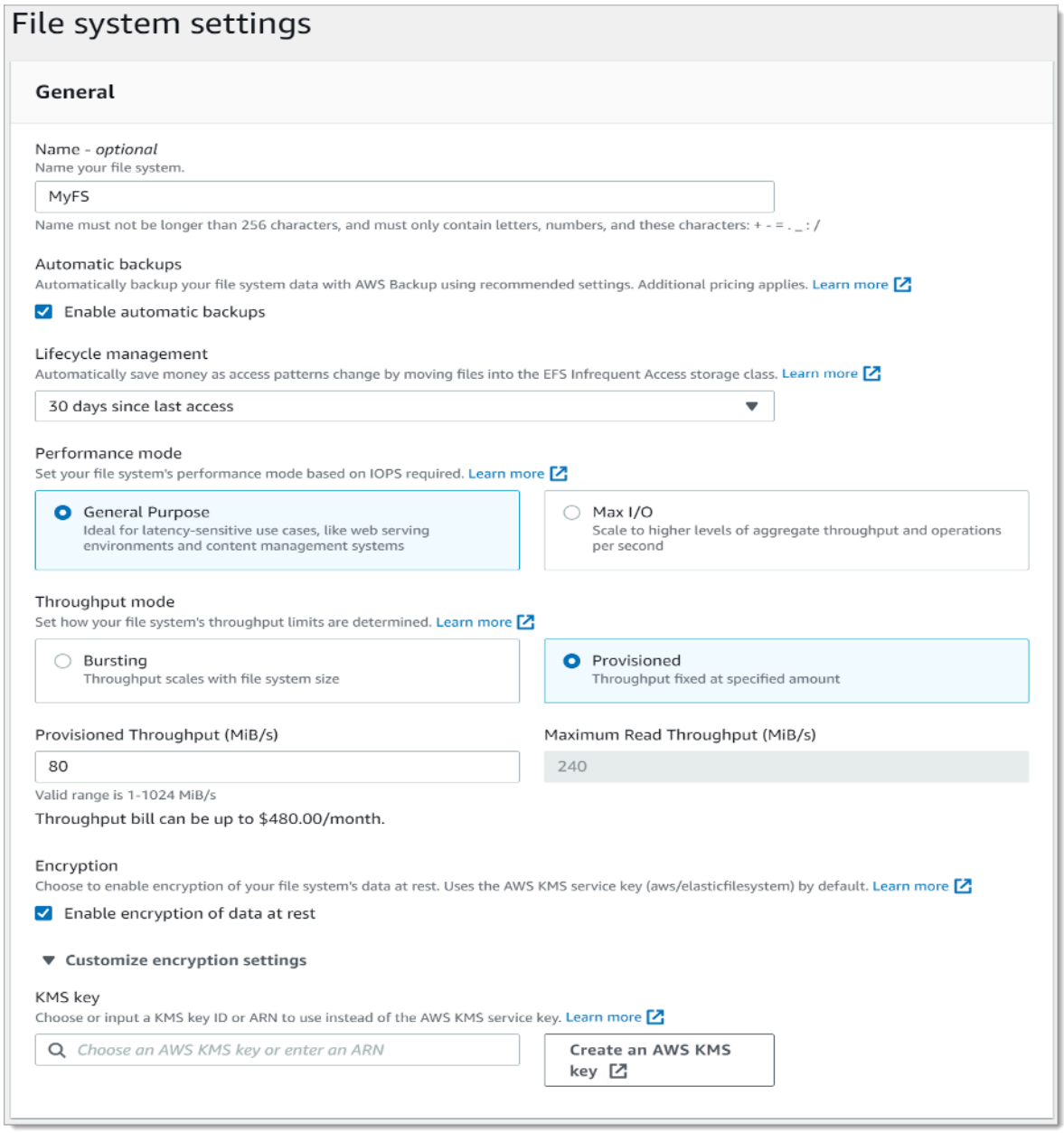
1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon EFS.
2. Pilih Create file system (Buat sistem file) untuk membuka kotak dialog Create file system (Buat sistem file). Untuk informasi selengkapnya tentang membuat sistem file menggunakan pengaturan yang disarankan yang mencakup mengaktifkan enkripsi secara default, lihat Membuat Sistem File Amazon EFS Anda.



Buat Sistem File EFS

3. (Opsional) Pilih Customize (Sesuaikan) untuk membuat sistem file yang disesuaikan alih-alih membuat sistem file menggunakan pengaturan yang direkomendasikan layanan.

Halaman Pengaturan sistem file muncul.



Buat sistem file EFS: pengaturan umum

4. Untuk pengaturan General (Umum), masukkan detail berikut.
   - (Opsional) Masukkan Name (Nama) untuk sistem file.
   - Automatic backups (Pencadangan otomatis) diaktifkan secara default. Anda dapat menonaktifkan pencadangan otomatis dengan mengosongkan kotak centang. Untuk informasi selengkapnya, lihat Menggunakan AWS Backup dengan Amazon EFS.

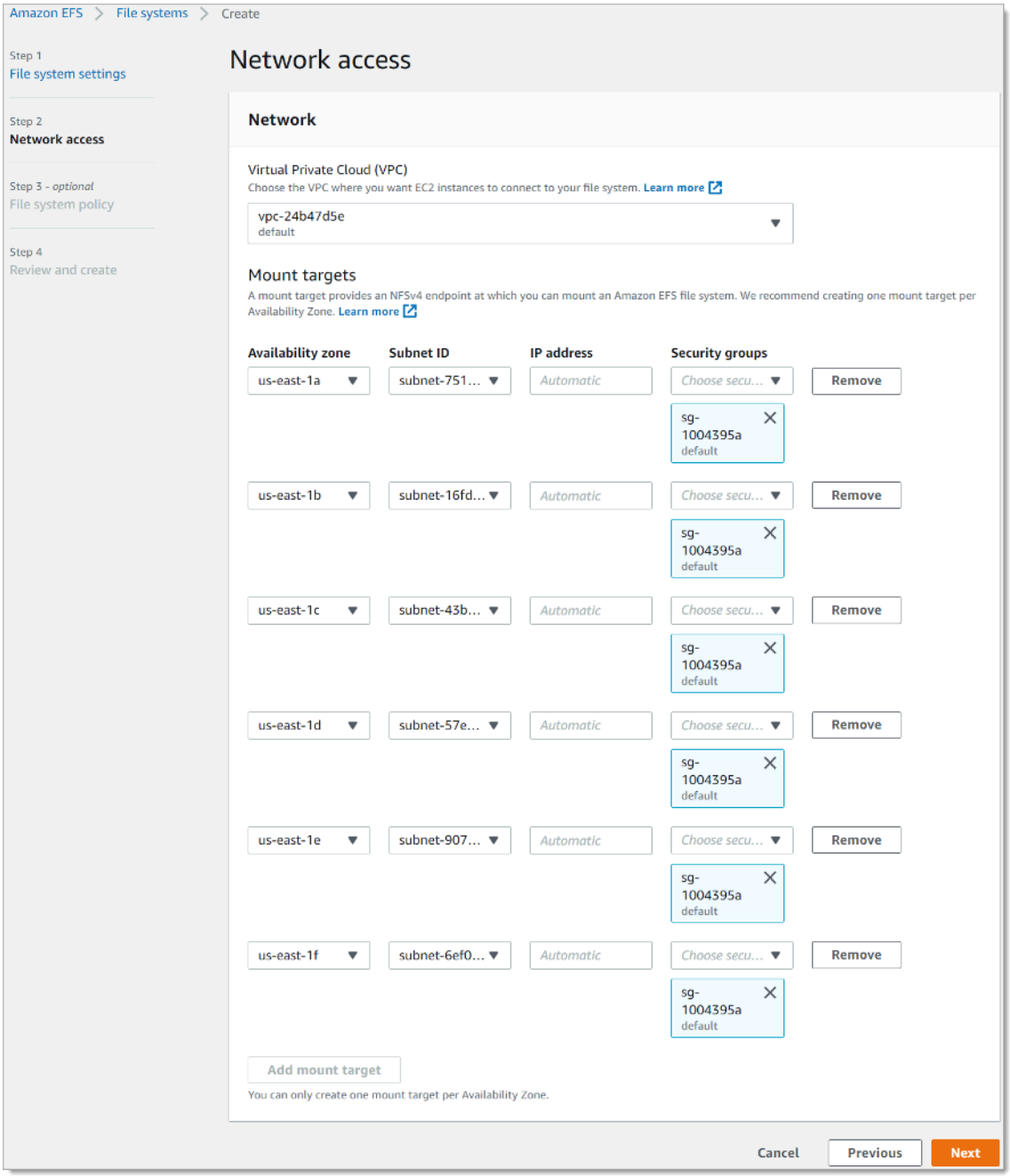
- Pilih kebijakan Lifecycle management (Manajemen siklus hidup). Manajemen siklus hidup Amazon EFS secara otomatis mengelola penyimpanan file hemat biaya untuk sistem file Anda. Ketika diaktifkan, manajemen siklus hidup memigrasikan file yang belum diakses selama periode yang ditetapkan ke kelas penyimpanan Infrequent Access (IA). Anda menentukan periode tersebut dengan menggunakan kebijakan siklus hidup. Jika Anda tidak ingin manajemen siklus hidup diaktifkan, pilih None (Tidak ada). Untuk informasi selengkapnya, lihat Manajemen siklus hidup EFS dalam Panduan Pengguna Amazon EFS.
- Pilih sebuah Performance mode (Mode Performa), yaitu General Purpose mode (Mode Tujuan Umum) default atau Max I/O (I/O maks.). Untuk informasi selengkapnya, lihat Mode Performa dalam Panduan Pengguna Amazon EFS.
- Pilih sebuah Throughput mode (Mode throughput), yaitu Bursting mode (Mode puncak) default atau Provisioned mode (Mode disediakan).
- Jika Anda memilih Provisioned (Disediakan), bidang Throughput Provisioned (MiB/s) (Throughput Disediakan (MiB/dtk)) akan ditampilkan. Masukkan jumlah throughput yang disediakan untuk sistem file. Setelah Anda memasukkan throughput, konsol menampilkan perkiraan biaya bulanan di samping bidang tersebut. Untuk informasi selengkapnya, lihat Mode Throughput dalam Panduan Pengguna Amazon EFS.
- Untuk Encryption (Enkripsi), enkripsi data at rest diaktifkan secara default. Enkripsi ini menggunakan kunci layanan EFS AWS Key Management Service (AWS KMS) (`aws/elasticfilesystem`) secara default. Untuk memilih kunci KMS yang berbeda untuk digunakan dalam enkripsi, perluas bagian “Customize encryption settings” (Sesuaikan pengaturan enkripsi) dan pilih kunci dari daftar. Atau, masukkan ID kunci KMS atau Amazon Resource Name (ARN) untuk kunci KMS yang ingin Anda gunakan.

  Jika Anda perlu membuat kunci baru, pilih Create an AWS KMS key (Buat kunci AWS KMS) untuk meluncurkan konsol AWS KMS dan membuat kunci baru.

5. (Opsional) Pilih Add tag (Tambahkan tag) untuk menambahkan pasangan kunci-nilai ke sistem file Anda.
6. Pilih Next (Berikutnya) untuk melanjutkan ke langkah Network Access (Akses Jaringan) dalam proses konfigurasi.

Langkah 2. Konfigurasikan Akses Jaringan

Pada langkah ini, Anda mengonfigurasi pengaturan jaringan sistem file-nya, termasuk Virtual Private Cloud (VPC) dan target pemasangan. Untuk setiap target pemasangan, atur Zona Ketersediaan, subnet, alamat IP, dan grup keamanan.



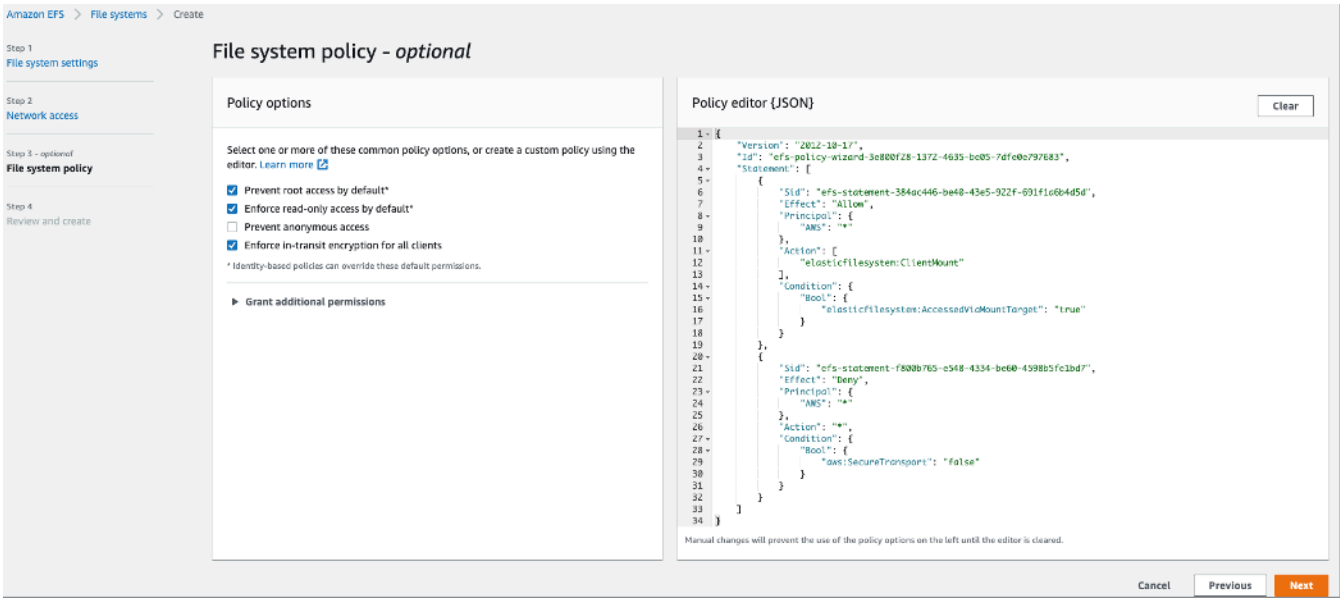
Buat sistem file EFS: Akses jaringan

1. Pilih Virtual Private Cloud (VPC) tempat Anda ingin instans EC2 terhubung ke sistem file Anda. Untuk informasi selengkapnya, lihat Mengelola aksesibilitas jaringan sistem file dalam Panduan Pengguna Amazon EFS.
   - Zona ketersediaan – Secara default, target pemasangan dikonfigurasi di setiap Zona Ketersediaan di Wilayah AWS. Jika Anda tidak menginginkan target pemasangan di Zona Ketersediaan tertentu, pilih Remove (Hapus) untuk menghapus target pemasangan untuk zona tersebut. Buat target pemasangan di setiap Zona Ketersediaan yang Anda rencanakan untuk mengakses sistem file Anda. Tidak ada biaya untuk melakukannya.
   - Subnet ID (ID Subnet) – Pilih dari subnet yang tersedia di Zona Ketersediaan. Subnet default telah dipilih sebelumnya. Sebagai praktik terbaik, pastikan subnet yang dipilih bersifat publik atau privat berdasarkan persyaratan keamanan Anda.
   - IP Address (Alamat IP) – Secara default, Amazon EFS memilih alamat IP secara otomatis dari alamat yang tersedia di subnet. Atau, Anda dapat memasukkan alamat IP tertentu yang ada di subnet. Meskipun target pemasangan memiliki alamat IP tunggal, target pemasangan ini adalah sumber daya jaringan yang redundan dan berketersediaan tinggi.
   - Security groups (Grup keamanan) – Anda dapat menentukan satu atau beberapa grup keamanan untuk target pemasangan. Sebagai praktik terbaik, pastikan grup keamanan hanya digunakan untuk tujuan pemasangan EFS (NFS Port 2049) dan aturan masuk hanya mengizinkan port 2049 dari rentang blok CIDR VPC lainnya atau menggunakan Grup Keamanan sebagai sumber untuk sumber daya yang perlu mengakses EFS. Untuk informasi selengkapnya, lihat Menggunakan Grup Keamanan untuk Instans dan Target Pemasangan Amazon EC2 dalam Panduan Pengguna Amazon EFS.

     Untuk menambahkan grup keamanan lain, atau untuk mengubah grup keamanan, pilih Choose security groups (Pilih grup keamanan) dan tambahkan grup keamanan lain dari daftar. Jika Anda tidak ingin menggunakan grup keamanan default, Anda dapat menghapusnya. Untuk informasi selengkapnya, lihat Membuat grup keamanan dalam Panduan Pengguna Amazon EFS.
2. Pilih Add mount target (Tambahkan target pemasangan) untuk membuat target pemasangan untuk Zona Ketersediaan yang tidak memilikinya. Jika target pemasangan dikonfigurasi untuk setiap Zona Ketersediaan, pilihan ini tidak tersedia.
3. Pilih Next (Berikutnya) untuk melanjutkan. Halaman File system policy (Kebijakan sistem file) ditampilkan.

Langkah 3. Buat Kebijakan Sistem File

Pada langkah ini, Anda membuat kebijakan sistem file untuk mengontrol akses klien NFS ke sistem file. Kebijakan sistem file EFS adalah kebijakan sumber daya IAM yang Anda gunakan untuk mengontrol akses klien NFS ke sistem file. Untuk informasi selengkapnya, lihat Menggunakan IAM untuk Mengontrol Akses NFS ke Amazon EFS dalam Panduan Pengguna Amazon EFS.



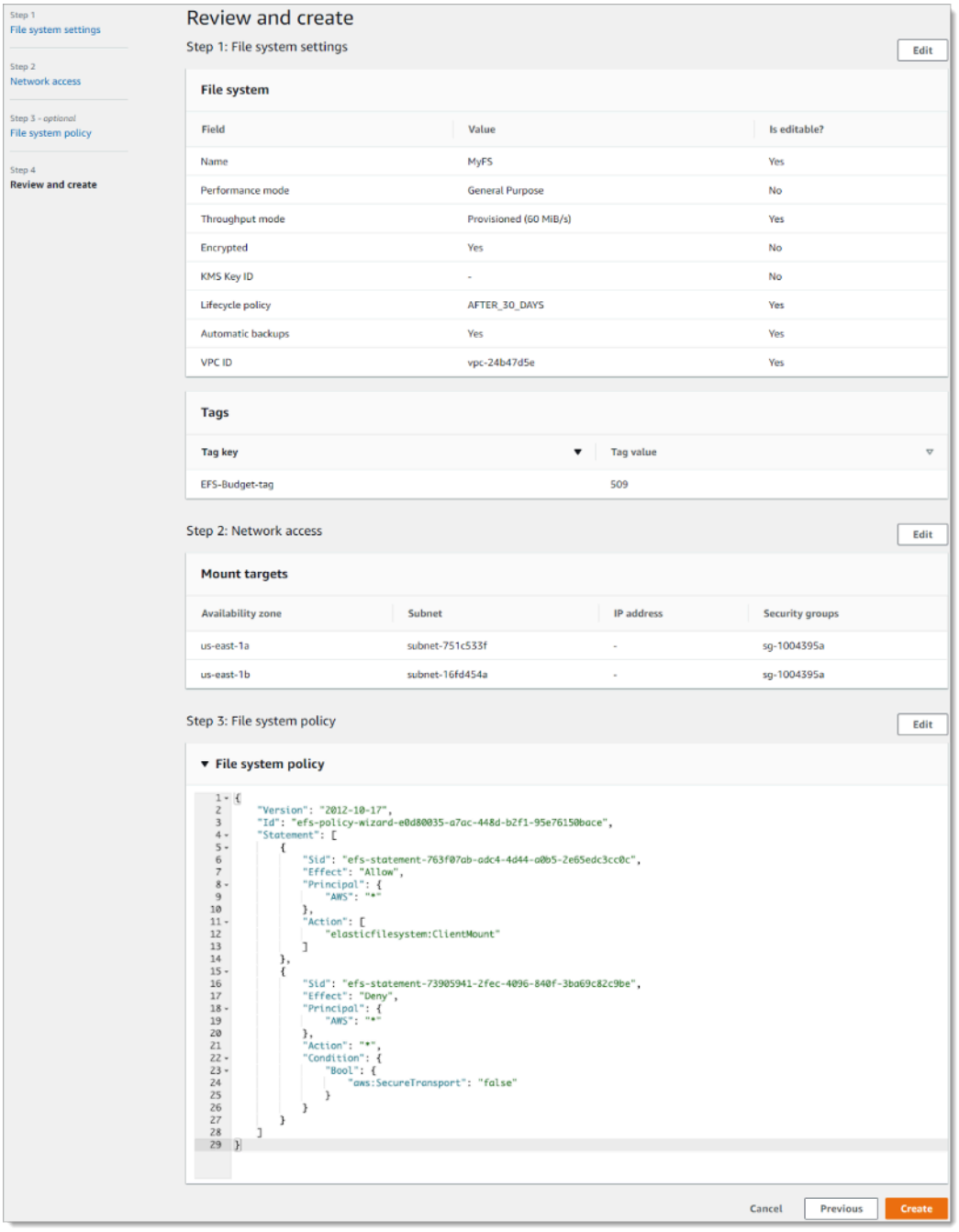
Buat sistem file EFS: Kebijakan sistem file

1. Dalam Policy options (Opsi kebijakan), kami menyarankan Anda memilih opsi kebijakan yang telah dikonfigurasikan sebelumnya sebagai berikut:
   - Cegah akses root secara default
   - Berlakukan akses hanya-baca secara default
   - Berlakukan enkripsi saat in transit untuk semua klien
2. Gunakan Grant additional permissions (Berikan izin tambahan) untuk memberikan izin sistem file kepada principal IAM tambahan, termasuk akun AWS lainnya. Pilih Add (Tambahkan), lalu masukkan ARN Principal dari entitas yang Anda beri izin, lalu pilih Permissions (Izin) yang akan diberikan.
3. Gunakan Kebijakan editor untuk menyesuaikan kebijakan yang telah dikonfigurasi sebelumnya atau untuk membuat kebijakan Anda sendiri berdasarkan kebutuhan Anda. Jika Anda memilih salah satu kebijakan yang telah dikonfigurasi sebelumnya, definisi kebijakan JSON akan muncul di editor kebijakan.

4. Pilih Next (Berikutnya) untuk melanjutkan. Halaman Review and create (Tinjau dan buat) akan muncul.

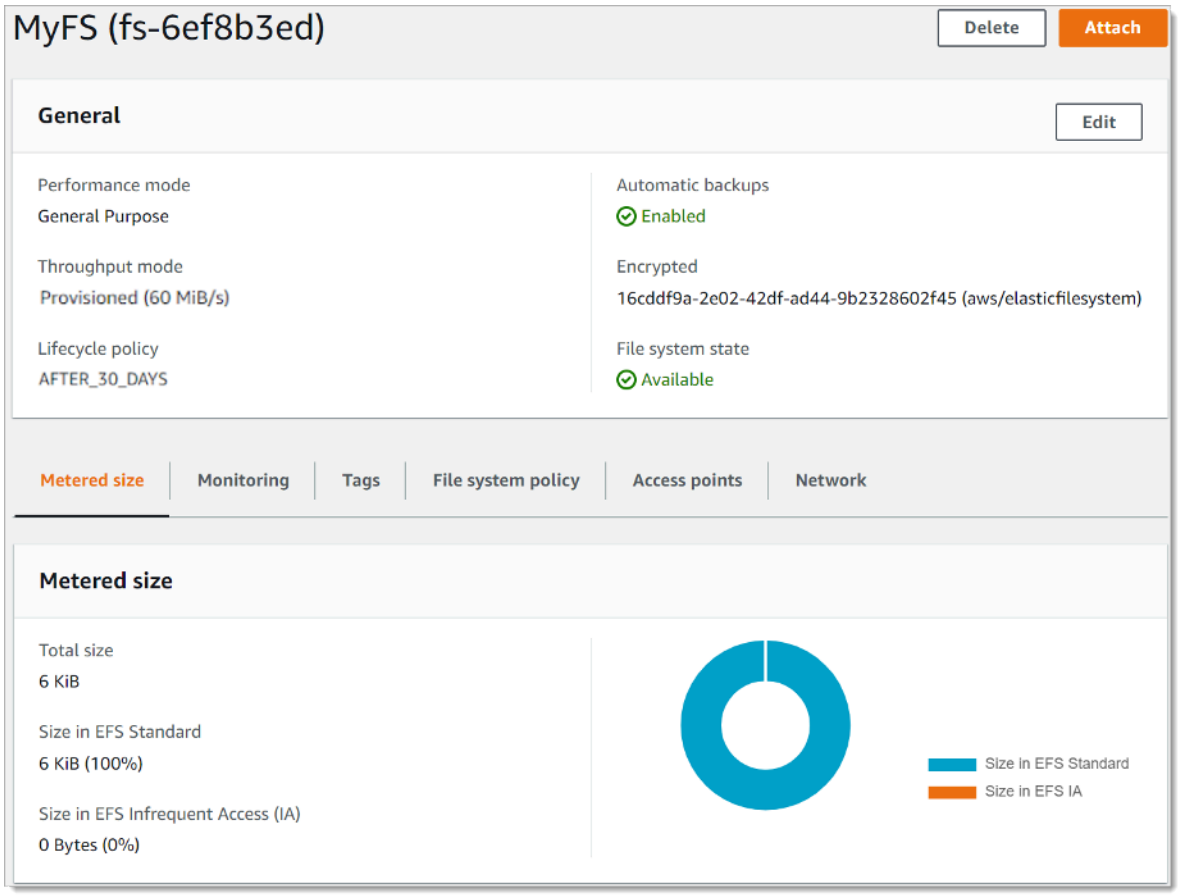
Langkah 4. Tinjau dan Buat

Pada langkah ini, Anda meninjau pengaturan sistem file, membuat modifikasi, kemudian membuat sistem file.



Buat sistem file EFS: Tinjau dan buat

1. Tinjau setiap grup konfigurasi sistem file. Anda dapat membuat perubahan pada setiap grup saat ini dengan memilih “Edit”.
2. Pilih “Create” (Buat) untuk membuat sistem file Anda dan kembali ke halaman Sistem file.
3. Halaman Sistem file menampilkan sistem file dan detail konfigurasinya, seperti yang ditunjukkan pada gambar berikut.



Sistem File

Membuat Sistem File Terenkripsi Menggunakan AWS CLI

Ketika Anda menggunakan AWS CLI untuk membuat sistem file terenkripsi, Anda dapat menggunakan parameter tambahan untuk mengatur status enkripsi dan CMK yang dikelola pelanggan. Pastikan Anda menggunakan AWS CLI versi terbaru. Untuk informasi tentang cara melakukan upgrade AWS CLI Anda, lihat Menginstal, Memperbarui, dan Menghapus Instalan AWS CLI dalam Panduan Pengguna Antarmuka Command Line AWS.

Dalam operasi `CreateFileSystem`, parameter `--encrypted` adalah Boolean dan diperlukan untuk membuat sistem file terenkripsi. `--kms-key-id` diperlukan hanya ketika Anda menggunakan CMK yang dikelola pelanggan dan Anda menyertakan alias atau ARN kunci. Jangan sertakan parameter ini jika Anda menggunakan CMK yang dikelola AWS.

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

Untuk informasi selengkapnya tentang membuat sistem file Amazon EFS menggunakan Konsol Manajemen AWS, AWS CLI, SDK AWS, atau API Amazon EFS, lihat Apa itu Amazon Elastic File System dalam Panduan Pengguna Amazon EFS.

Memberlakukan Enkripsi Data at Rest

Enkripsi memiliki efek minimal pada latensi dan throughput I/O. Enkripsi dan dekripsi akan terlihat untuk pengguna, aplikasi, dan layanan. Semua data dan metadata dienkripsi oleh Amazon EFS atas nama Anda sebelum ditulis ke disk dan didekripsi sebelum dibaca oleh klien. Anda tidak perlu mengubah alat klien, aplikasi, atau layanan untuk mengakses sistem file terenkripsi.

Organisasi Anda mungkin mewajibkan enkripsi terhadap semua data yang memenuhi klasifikasi tertentu atau terkait dengan aplikasi, beban kerja, atau lingkungan tertentu. Anda dapat menggunakan kebijakan berbasis identitas AWS Identity and Access Management (IAM) untuk memberlakukan enkripsi data at rest untuk sumber daya sistem file Amazon EFS Anda. Dengan menggunakan kunci kondisi IAM, Anda dapat mencegah pengguna membuat sistem file EFS yang tidak dienkripsi.

Misalnya, kebijakan IAM yang secara eksplisit memungkinkan pengguna untuk membuat hanya sistem file EFS terenkripsi akan menggunakan kombinasi efek, tindakan, dan kondisi berikut:

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

Contoh berikut menggambarkan kebijakan berbasis identitas IAM yang mengotorisasi principal untuk membuat hanya sistem file terenkripsi.

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

Atribut `Resource` yang diatur ke * berarti bahwa kebijakan IAM berlaku untuk semua sumber daya EFS yang dibuat. Anda dapat menambahkan atribut kondisional tambahan berdasarkan tag guna memberlakukannya hanya untuk subset sumber daya EFS dengan kebutuhan klasifikasi data.

Anda juga dapat menerapkan pembuatan sistem file Amazon EFS terenkripsi di tingkat AWS Organizations dengan menggunakan kebijakan kontrol layanan untuk semua Akun AWS atau OU di organisasi Anda. Untuk informasi selengkapnya tentang kebijakan kontrol layanan di AWS Organizations, lihat Kebijakan kontrol layanan dalam Panduan Pengguna AWS Organizations.

Membuat Kebijakan IAM yang Mewajibkan Semua Sistem File EFS Dienkripsi

Anda dapat membuat kebijakan berbasis identitas IAM yang mengizinkan pengguna untuk membuat hanya sistem file Amazon EFS terenkripsi menggunakan konsol, AWS CLI, atau API. Prosedur berikut menjelaskan cara membuat kebijakan tersebut menggunakan konsol IAM, dan kemudian menerapkan kebijakan tersebut ke pengguna di akun Anda.

Untuk membuat kebijakan IAM untuk memberlakukan sistem file EFS terenkripsi:

1. Masuk ke Konsol Manajemen AWS dan buka konsol IAM.
2. Di panel navigasi, di bagian Access Management (Manajemen Akses), pilih Policies (Kebijakan).

3. Pilih Create policy (Buat kebijakan) untuk menampilkan halaman Buat kebijakan.
4. Di tab Visual Editor (Editor Visual), masukkan informasi berikut.
   - Untuk Service (Layanan), pilih EFS.
   - Untuk Actions (Tindakan), masukkan `create` di bidang pencarian, lalu pilih CreateFileSystem.
   - Untuk Request conditions (Kondisi permintaan), klik tautan Add condition (Tambahkan kondisi), cari `elasticfilesystem:Encrypted` Condition Key (Kunci Kondisi), `Bool` untuk Operator dan `true` Value (Nilai).
5. Isi Name (Nama) dan Description (Deskripsi) untuk kebijakan tersebut. Periksa ringkasan kebijakan tersebut, termasuk kondisi permintaan Encrypted (Terenkripsi).
6. Pilih Create policy (Buat kebijakan) untuk membuat kebijakan.

Untuk menerapkan kebijakan tersebut ke pengguna di akun Anda:

1. Di konsol IAM, di bagian Access management (Manajemen akses), pilih Users (Pengguna).
2. Pilih pengguna yang akan menerima kebijakan tersebut.
3. Pilih Add permissions (Tambahkan izin) untuk menampilkan halaman Tambahkan izin.
4. Pilih Attach existing policies directly (Lampirkan kebijakan yang ada secara langsung).
5. Masukkan nama kebijakan EFS yang Anda buat dalam prosedur sebelumnya.
6. Pilih dan luaskan kebijakan ini. Kemudian pilih {}JSON untuk memeriksa isi kebijakan. Ini seharusnya terlihat seperti kebijakan JSON berikut.

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

Mendeteksi Sistem File yang Tidak Terenkripsi

Organisasi Anda mungkin memiliki persyaratan untuk mengidentifikasi sumber daya Amazon EFS yang tidak dienkripsi. Anda dapat mendeteksi sistem file yang tidak terenkripsi dengan menggunakan Aturan Terkelola AWS Config. AWS Config menyediakan Aturan Terkelola AWS, yang merupakan aturan yang telah ditentukan sebelumnya dan dapat disesuaikan yang digunakan AWS Config untuk mengevaluasi apakah sumber daya AWS Anda mematuhi praktik terbaik umum dan melaporkan sumber daya yang melanggar aturan sebagai NON_COMPLIANT.

Anda dapat menggunakan aturan Config yang Dikelola AWS, yaitu `efs-encrypted-check`, untuk memeriksa apakah Amazon Elastic File System (Amazon EFS) dikonfigurasi untuk mengenkripsi data file menggunakan AWS Key Management Service (AWS KMS). Untuk informasi selengkapnya tentang menyiapkan dan mengaktifkan Aturan yang Dikelola AWS, lihat Menggunakan Aturan yang Dikelola AWS Config.

Enkripsi Data in Transit

Anda dapat memasang sistem file sehingga semua lalu lintas NFS dienkripsi saat in transit menggunakan Keamanan Lapisan Pengangkutan (TLS) 1.2 dengan cipher AES-256 standar industri. TLS adalah serangkaian protokol kriptografi standar industri yang digunakan untuk mengenkripsi informasi yang dipertukarkan melalui jaringan. AES-256 adalah cipher enkripsi 256-bit yang digunakan untuk transmisi data di TLS. Sebaiknya siapkan enkripsi saat in transit pada setiap klien yang mengakses sistem file.

Anda dapat menggunakan kebijakan IAM untuk menerapkan enkripsi saat in transit untuk akses klien NFS ke Amazon EFS. Ketika klien terhubung ke sistem file, Amazon EFS akan mengevaluasi kebijakan sumber daya IAM untuk sistem file, yang disebut kebijakan sistem file, bersama dengan kebijakan IAM berbasis identitas apa pun, untuk menentukan izin akses sistem file yang sesuai untuk diberikan. Anda dapat menggunakan Kunci Kondisi `aws:SecureTransport` dalam kebijakan sumber daya sistem file untuk mendorong klien NFS untuk menggunakan TLS saat terhubung ke sistem file EFS.

> **Note**
>
> Anda harus menggunakan EFS mount helper untuk memasang sistem file Amazon EFS Anda agar menggunakan otorisasi IAM untuk mengontrol akses oleh klien NFS. Untuk informasi selengkapnya, lihat Pemasangan dengan otorisasi IAM dalam Panduan Pengguna Amazon EFS.

Contoh kebijakan sistem file EFS berikut memberlakukan enkripsi saat in transit dan memiliki karakteristik berikut:

- `effect` adalah `allow`.
- Principal diatur ke * untuk semua entitas IAM.
- Tindakan diatur ke `ClientMount`, `ClientWrite`, `ClientRootAccess`.
- Kondisi pemberian izin diatur ke `SecureTransport`. Hanya klien NFS yang menggunakan TLS untuk terhubung ke sistem file yang akan diberikan akses.

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

Anda dapat membuat kebijakan sistem file menggunakan konsol Amazon EFS atau menggunakan AWS CLI.

Untuk membuat kebijakan sistem file menggunakan konsol EFS:

1. Buka konsol Amazon EFS.
2. Pilih File Systems (Sistem File).
3. Pada halaman Sistem file, pilih sistem file yang ingin diedit atau dibuatkan kebijakan sistem file-nya. Halaman detail untuk sistem file tersebut ditampilkan.
4. Pilih File system policy (Kebijakan sistem file), lalu pilih Edit. Halaman Kebijakan sistem file muncul.

Buat kebijakan sistem file

5. Dalam Policy options (Opsi kebijakan), kami menyarankan Anda memilih opsi kebijakan yang telah dikonfigurasikan sebelumnya sebagai berikut:

   - Cegah akses root secara default
   - Berlakukan akses hanya-baca secara default
   - Berlakukan enkripsi saat in transit untuk semua klien

   Jika Anda memilih kebijakan yang telah dikonfigurasi sebelumnya, objek JSON kebijakan akan ditampilkan di panel Policy editor (Editor kebijakan).

6. Gunakan Grant additional permissions (Berikan izin tambahan) untuk memberikan izin sistem file kepada principal IAM tambahan, termasuk akun AWS lainnya. Pilih Add (Tambahkan), lalu masukkan ARN Principal dari entitas yang Anda beri izin, lalu pilih Permissions (Izin) yang akan diberikan.

7. Gunakan Kebijakan editor untuk menyesuaikan kebijakan yang telah dikonfigurasi sebelumnya atau untuk membuat kebijakan Anda sendiri berdasarkan kebutuhan Anda. Saat Anda menggunakan editor, opsi kebijakan yang telah dikonfigurasi sebelumnya menjadi tidak tersedia. Untuk membatalkan perubahan kebijakan, pilih Clear (Kosongkan).

   Ketika Anda mengosongkan editor, kebijakan yang telah dikonfigurasikan sebelumnya akan tersedia lagi.
8. Setelah Anda selesai mengedit atau membuat kebijakan, pilih Save (Simpan).

   Halaman detail untuk sistem file ditampilkan, yang menunjukkan kebijakan dalam File system policy (Kebijakan sistem file).

   Anda juga dapat membuat kebijakan sistem file secara terprogram menggunakan AWS CloudFormation, SDK AWS, atau API Amazon EFS secara langsung. Untuk informasi selengkapnya tentang membuat kebijakan sistem file, lihat Membuat kebijakan sistem file dalam Panduan Pengguna Amazon EFS.

Menyiapkan Enkripsi Data in Transit

Untuk menyiapkan enkripsi data in transit, kami sarankan Anda mengunduh EFS mount helper pada setiap klien. EFS mount helper adalah utilitas sumber terbuka yang disediakan AWS untuk menyederhanakan penggunaan EFS, termasuk menyiapkan enkripsi data in transit. EFS mount helper menggunakan opsi pemasangan yang direkomendasikan EFS secara default.

EFS mount helper didukung pada distribusi Linux berikut:

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

Untuk menyiapkan enkripsi data in transit:

1. Instal EFS mount helper:

- Untuk Amazon Linux, gunakan perintah ini:

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

- Untuk distribusi Linux lainnya, unduh dari GitHub dan instal.

  Paket amazon-efs-utils secara otomatis menginstal dependensi berikut: NFS client (nfs-utils), Network relay (stunnel), OpenSSL, dan Python.

2. Pasang sistem file:

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

- `mount -t efs` memanggil EFS mount helper.
- Menggunakan nama DNS dari sistem file atau alamat IP dari target pemasangan tidak didukung ketika pemasangan menggunakan EFS mount helper, jadi gunakan ID sistem file sebagai gantinya.
- EFS mount helper menggunakan opsi pemasangan yang direkomendasikan AWS secara default. Mengganti opsi pemasangan default ini tidak disarankan tetapi kami memberikan fleksibilitas untuk melakukannya ketika terdapat kesempatan yang sesuai. Kami menyarankan untuk menguji secara menyeluruh setiap penggantian opsi pemasangan sehingga Anda memahami bagaimana perubahan ini memengaruhi akses dan performa sistem file.
- Tabel berikut menunjukkan opsi pemasangan default yang digunakan oleh EFS helper mount.

Opsi	Deskripsi
nfsvers=4.1	Versi protokol NFS
rsize=1048576	Jumlah maksimum bita data yang dapat diterima klien NFS untuk setiap

Opsi	Deskripsi
	permintaan READ jaringan)
wsize=1048576	Jumlah maksimum bita data yang dapat dikirim klien NFS untuk setiap permintaan WRITE jaringan
hard	Perilaku pemulihan klien NFS setelah waktu permintaan NFS habis, sehingga permintaan NFS dicoba ulang tanpa batas waktu sampai server membalas

Opsi	Deskripsi
timeo=600	Nilai batas waktu yang digunakan klien NFS untuk menunggu respons sebelum mencoba ulang permintaan NFS dalam Desidetik
retrans=2	Frekuensi klien NFS mencoba kembali permintaa n sebelum mencoba tindakan pemulihan lebih lanjut
noresvport	Memberi tahu klien NFS untuk menggunakan port sumber TCP baru ketika koneksi jaringan dibuat kembali

- Tambahkan baris berikut ke `/etc/fstab` untuk secara otomatis memasang ulang sistem file Anda setelah sistem dimulai ulang.

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

Menggunakan Enkripsi Data in Transit

Jika organisasi Anda tunduk pada kebijakan korporasi atau peraturan yang mengharuskan enkripsi data in transit, sebaiknya gunakan enkripsi data in transit pada setiap klien yang mengakses sistem file. Enkripsi dan dekripsi dikonfigurasi pada tingkat koneksi dan menambahkan lapisan keamanan lainnya.

Memasang sistem file menggunakan EFS mount helper akan menyiapkan dan mempertahankan terowongan TLS 1.2 antara klien dan Amazon EFS, serta merutekan semua lalu lintas NFS melalui terowongan terenkripsi ini. Sertifikat yang digunakan untuk membuat koneksi TLS terenkripsi ditandatangani oleh Amazon Certificate Authority (CA) dan dipercaya oleh sebagian besar distribusi Linux modern. EFS mount helper juga menghasilkan proses watchdog guna memantau semua terowongan aman untuk setiap sistem file dan memastikan sistem file ini berjalan.

Setelah menggunakan EFS mount helper untuk membuat koneksi terenkripsi ke Amazon EFS, tidak diperlukan input atau konfigurasi pengguna lain. Enkripsi akan terlihat untuk koneksi pengguna dan aplikasi yang mengakses sistem file.

Setelah berhasil memasang dan membuat koneksi terenkripsi ke sistem file EFS menggunakan EFS mount helper, output dari perintah pasang menunjukkan sistem file dipasang dan terowongan yang terenkripsi telah dibuat menggunakan localhost (127.0.0.1) sebagai relai jaringan. Lihat contoh output berikut.

```
     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
```

Untuk memetakan `efs-mount-point` ke sistem file EFS, lakukan kueri file mount.log dalam `/var/log/amazon/efs` dan temukan operasi pemasangan yang terakhir berhasil. Hal ini dapat dilakukan dengan menggunakan perintah grep sederhana berikut.

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

Output dari perintah grep ini akan mengembalikan nama DNS dari sistem file EFS yang dipasang. Lihat contoh output di bawah ini.

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

Kesimpulan

Data sistem file Amazon EFS dapat dienkripsi saat at rest dan in transit. Anda dapat mengenkripsi data at rest dengan menggunakan CMK yang dapat Anda kontrol dan kelola menggunakan AWS KMS. Membuat sistem file terenkripsi semudah memilih kotak centang di wizard pembuatan sistem file Amazon EFS di Konsol Manajemen AWS, atau menambahkan parameter tunggal ke operasi `CreateFileSystem` di AWS CLI, SDK AWS, atau Amazon EFS API.

Anda dapat menerapkan enkripsi saat at rest dan dalam transit menggunakan kebijakan berbasis identitas AWS IAM dan kebijakan sistem file untuk lebih memperkuat persyaratan keamanan Anda dan membantu memenuhi kebutuhan kepatuhan Anda. Penggunaan sistem file terenkripsi juga akan terlihat untuk layanan, aplikasi, dan pengguna, dengan efek minimal pada performa sistem file. Anda dapat mengenkripsi data in transit dengan menggunakan EFS mount helper untuk membuat terowongan TLS terenkripsi pada setiap klien, dengan mengenkripsi semua lalu lintas NFS antara klien dan sistem file EFS yang terpasang. Penerapan enkripsi data Amazon EFS saat at rest menggunakan kebijakan identitas IAM dan saat in transit menggunakan kebijakan sistem file EFS tersedia untuk Anda tanpa biaya tambahan.

Sumber daya

- Laporan Resmi Detail Kriptografi AWS KMS
- Panduan Pengguna Amazon EFS

Riwayat Dokumen dan Kontributor

Riwayat Dokumen

Untuk mendapatkan notifikasi tentang pembaruan laporan resmi ini, sebaiknya berlangganan umpan RSS.

perubahan-riwayat-pembaruan	deskripsi-riwayat-pembaruan	tanggal-riwayat-pembaruan
Pembaruan kecil	Menyesuaikan tata letak halaman	30 April 2021
Laporan resmi diperbarui	Menambahkan penegakan enkripsi saat at rest dan saat in transit menggunakan IAM	22 Februari 2021
Laporan resmi diperbarui	Menambahkan enkripsi data in transit	1 April 2018
Publikasi awal	Enkripsi Data at Rest dengan Sistem File Terenkripsi Amazon EFS dipublikasikan	1 September 2017

> **Note**
>
> Untuk berlangganan pembaruan RSS, Anda harus mengaktifkan plugin RSS untuk browser yang Anda gunakan.

Kontributor

Kontributor dokumen ini meliputi:

- Darryl S. Osborne, Arsitek Solusi Spesialis Penyimpanan (Storage Specialist Solutions Architect), AWS
- Joseph Travaglini, Manajer Produk Senior (Senior Product Manager), Amazon EFS

- Peter Buonora, Arsitek Solusi Utama (Principal Solutions Architect), AWS
- Siva Rajamani, Arsitek Solusi Senior (Senior Solutions Architect), AWS