Whitepaper AWS

Crittografia dei dati dei file con Amazon Elastic File System

Crittografia dei dati dei file con Amazon Elastic File System: Whitepaper AWS

Table of Contents

Crittografia dei dati dei file con Amazon Elastic File System

Data di pubblicazione: 22 febbraio 2021 (Cronologia del documento e collaboratori)

Riassunto

La sicurezza è l'aspetto più importante per AWS e offriamo ai nostri clienti gli strumenti per gestire la sicurezza come l'aspetto più importante nella propria azienda. Le normative governative e le policy di conformità del settore o dell'azienda possono richiedere la protezione di dati di diversi livelli di classificazione utilizzando policy di crittografia e algoritmi crittografici e una corretta gestione delle chiavi. Questo documento descrive le best practice per la crittografia di Amazon Elastic File System (Amazon EFS).

Introduzione

Amazon Elastic File System (Amazon EFS) offre file system condivisi in cloud semplici, scalabili, a disponibilità elevata ed estremamente durevoli. I file system creati utilizzando Amazon EFS sono elastici, consentendo loro di crescere e ridursi automaticamente man mano che si aggiungono e rimuovono dati. Possono raggiungere dimensioni misurabili in petabyte, distribuendo i dati su un numero illimitato di server di archiviazione in più zone di disponibilità (AZ).

I dati archiviati in questi file system possono essere soggetti a crittografia dei dati a riposo e in transito utilizzando Amazon EFS. Per la crittografia dei dati a riposo, è possibile creare file system crittografati tramite Console di gestione AWS o AWS Command Line Interface (AWS CLI). In alternativa è possibile creare file system crittografati a livello programmatico tramite l'API di Amazon EFS o uno degli SDK AWS.

Per la crittografia dei dati a riposo, Amazon EFS si integra con AWS Key Management Service (AWS KMS) per la gestione delle chiavi. È inoltre possibile abilitare la crittografia dei dati in transito montando il file system e trasferendo tutto il traffico NFS su Transport Layer Security (TLS).

Questo documento illustra le best practice di crittografia per Amazon EFS. Descrive come abilitare la crittografia dei dati in transito a livello di connessione client e come creare un file system crittografato nella Console di gestione AWS e nell'AWS CLI.

> **Note**
>
> L'utilizzo delle API e degli SDK per creare un file system crittografato non rientra nell'ambito di questo documento. Per ulteriori informazioni su come eseguire questa operazione, consultare la sezione API di Amazon EFS nella Guida per l'utente di Amazon EFS o nella documentazione del SDK.

Concetti di base e terminologia

Questa sezione definisce i concetti e la terminologia a cui fa riferimento questo whitepaper.

- Amazon Elastic File System (Amazon EFS): un servizio altamente disponibile ed estremamente durevole che fornisce un servizio di archiviazione di file condiviso semplice e scalabile in AWS Cloud. Amazon EFS fornisce un'interfaccia e semantica standard da file system. È possibile archiviare una quantità praticamente illimitata di dati su un numero illimitato di server di archiviazione in molteplici zone di disponibilità.
- AWS Identity and Access Management (IAM): un servizio che consente di controllare in modo sicuro l'accesso granulare alle API dei servizi AWS. Le policy vengono create e utilizzate per limitare l'accesso a singoli utenti, gruppi e ruoli. Tramite la console IAM è possibile gestire le chiavi AWS KMS.
- AWS KMS : un servizio gestito che semplifica la creazione e il controllo delle chiavi master del cliente (CMK), le chiavi crittografiche utilizzate per la crittografia dei dati. Le CMK di AWS KMS sono protette da moduli di sicurezza hardware (HSM) che sono convalidati dal FIPS 140-2 Cryptographic Module Validation Program tranne nelle regioni Cina (Pechino) e Cina (Ningxia). AWS KMS è integrato con altri servizi AWS che crittografano i dati. È inoltre completamente integrato con AWS CloudTrail per fornire i log delle chiamate API effettuate da AWS KMS per conto dell'utente, che possono essere utili per soddisfare i requisiti di conformità o normativi applicabili alla sua organizzazione.
- Chiave master del cliente (CMK): rappresenta l'apice della gerarchia delle chiavi. Contiene la chiave materiale per crittografare e decrittografare i dati. Questa chiave materiale può essere generata da AWS KMS oppure è possibile generarla e importarla in AWS KMS. Le CMK sono specifiche di un account AWS e di una regione AWS e possono essere gestite dall'utente o da AWS.
- CMK gestita da AWS: una CMK generata da AWS per conto dell'utente. Una CMK gestita da AWS viene creata quando si abilita la crittografia per una risorsa di un servizio AWS integrato. Le policy della chiave CMK gestite da AWS sono gestite da AWS e non è possibile modificarle. Non sono previsti costi per la creazione o l'archiviazione di CMK gestite da AWS.
- CMK gestita dall'utente: una CMK creata utilizzando la console di gestione AWS o l'API AWS, l'AWS CLI o gli SDK. È possibile utilizzare una CMK gestita dall'utente quando è necessario un controllo più granulare sulla CMK.
- Policy della chiave KMS: una policy basata sulla risorsa che controlla l'accesso a una CMK gestita dall'utente. I clienti definiscono queste autorizzazioni utilizzando la policy della chiave

o una combinazione di policy IAM e policy della chiave. Per ulteriori informazioni, consultare la Panoramica della gestione dell'accesso nella Guida per gli sviluppatori di AWS KMS.

- Chiavi dati: chiavi crittografiche generate da AWS KMS per crittografare i dati al di fuori di AWS KMS. AWS KMS consente alle entità autorizzate (utenti o servizi) di ottenere chiavi di dati protette da una CMK.
- Transport Layer Security (TLS): Il successore di Secure Sockets Layer (SSL), TLS è un protocollo crittografico essenziale per crittografare le informazioni che vengono scambiate su una rete.
- Assistente per il montaggio di EFS : Un agente client Linux (`amazon-efs-utils`) utilizzato per semplificare il montaggio dei file system EFS. Può essere utilizzato per impostare, mantenere e instradare tutto il traffico NFS su un tunnel TLS.

Per ulteriori informazioni sui concetti di base e sulla terminologia, consultare Concetti di AWS Key Management Service nella Guida per gli sviluppatori di AWS KMS.

Crittografia dei dati inattivi

AWS fornisce gli strumenti per creare un file system crittografato che crittografa tutti i dati e i metadati inattivi utilizzando un algoritmo di crittografia AES-256 standard del settore. Un file system crittografato è progettato per gestire la crittografia e la decrittografia in modo automatico e trasparente, in modo da non dover modificare le applicazioni. Se la propria organizzazione è soggetta a policy aziendali o normative che richiedono la crittografia dei dati e dei metadati inattivi, consigliamo di creare un file system crittografato.

Argomenti

Gestione delle chiavi

Amazon EFS è integrato con AWS KMS, che gestisce le chiavi di crittografia per i file system crittografati. AWS KMS supporta anche la crittografia da parte di altri servizi AWS come 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, ecc. Per crittografare i contenuti del file system, Amazon EFS utilizza l'algoritmo Advanced Encryption Standard con modalità XTS e una chiave a 256 bit (XTS-AES-256).

Ci sono tre domande importanti a cui rispondere quando si valuta la modalità di protezione dei dati a riposo adottando qualsiasi policy di crittografia. Queste domande sono valide anche per i dati archiviati in servizi gestiti e non gestiti come Amazon EBS.

Dove sono conservate le chiavi?

AWS KMS archivia le chiavi master in un sistema di archiviazione estremamente durevole e in un formato crittografato per garantire che possano essere recuperate quando necessario.

Dove vengono utilizzate le chiavi?

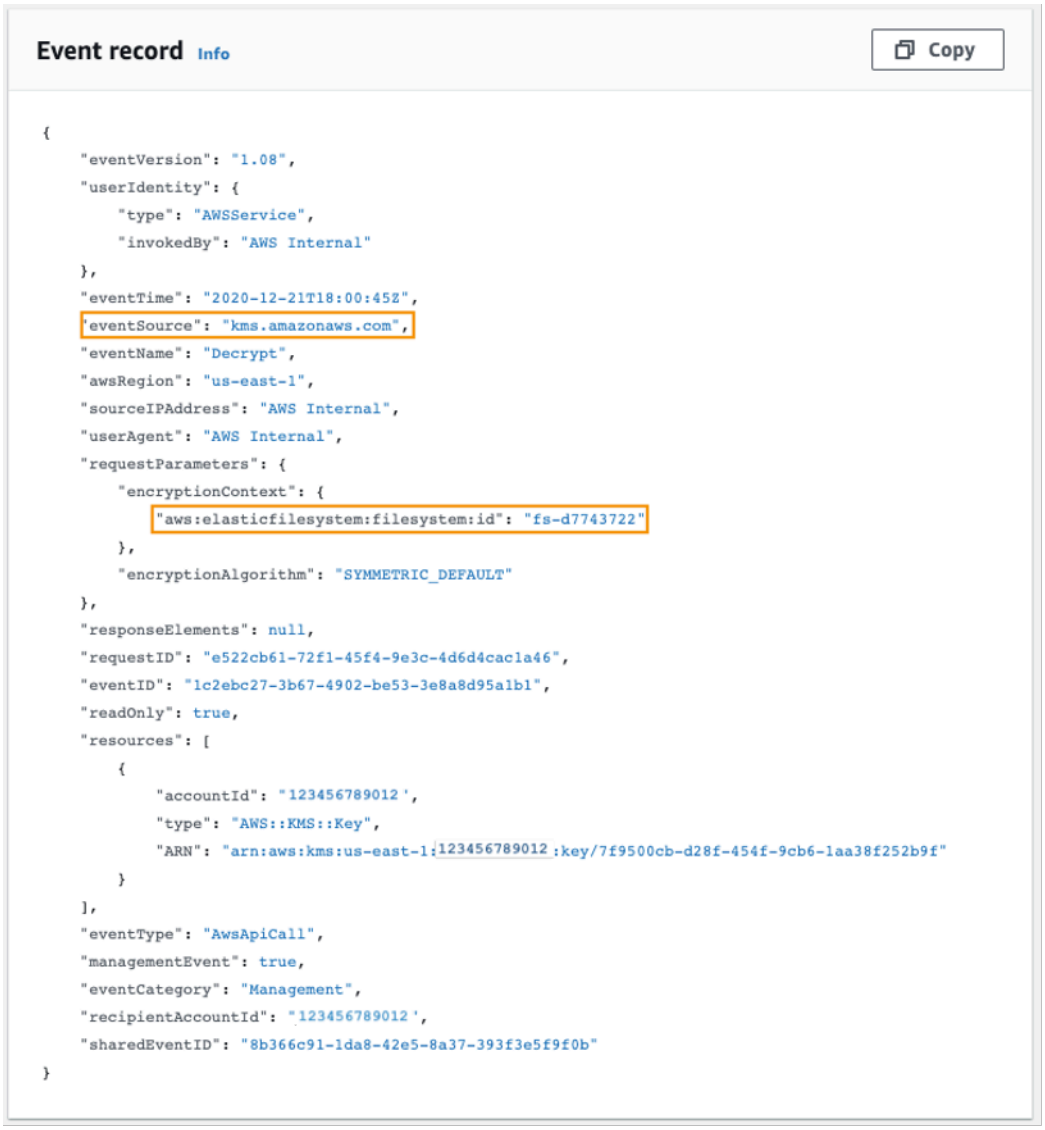
L'uso di un file system Amazon EFS crittografato è trasparente per i client che montano il file system. Tutte le operazioni crittografiche avvengono all'interno del servizio EFS, poiché i dati vengono crittografati prima di essere scritti su disco e decrittografati dopo che un client invia una richiesta di lettura.

Chi può usare le chiavi?

Le policy sulle chiavi di AWS KMS controllano l'accesso alle chiavi di crittografia.

Consigliamo di combinarle con le policy IAM per garantire un ulteriore livello di controllo. Ogni chiave è associata a una policy della chiave. Se la chiave è una CMK gestita da AWS, AWS gestisce la policy della chiave. Se la chiave è una CMK gestita dal cliente, è quest'ultimo che si prende carico della gestione della policy della chiave. Le policy delle chiavi sono lo strumento principale per controllare l'accesso alle CMK. Definiscono le autorizzazioni che regolano l'uso e la gestione delle chiavi.

Quando si crea un file system crittografato utilizzando Amazon EFS, si concede ad Amazon EFS l'accesso affinché possa utilizzare la CMK per conto dell'utente. Le chiamate che Amazon EFS effettua ad AWS KMS per conto dell'utente appaiono nei log di CloudTrail come se provenissero dal suo account AWS. La seguente schermata mostra l'evento CloudTrail di esempio per una chiamata di decrittografia KMS effettuata da Amazon EFS.



Registro di CloudTrail per KMS Decrypt

Per ulteriori informazioni su AWS KMS e su come gestire l'accesso alle chiavi di crittografia, consultare Gestione dell'accesso alle CMK di AWS KMS nella Guida per gli sviluppatori di AWS KMS.

Per ulteriori informazioni su come AWS KMS gestisce la crittografia, consultare il whitepaper Dettagli sulla crittografia di AWS KMS.

Per ulteriori informazioni su come creare un utente e un gruppo di amministratori IAM, consultare Creazione del primo utente e del primo gruppo di amministratori IAM nella Guida per l'utente di IAM.

Creazione di un file system crittografato

È possibile creare un file system crittografato utilizzando la Console di gestione AWS, l'AWS CLI, l'API di Amazon EFS o gli SDK AWS. È possibile abilitare la crittografia per un file system solo al momento della sua creazione.

Amazon EFS si integra con AWS KMS per la gestione delle chiavi e utilizza una CMK per crittografare il file system. I metadati del file system, come nomi di file, nomi di directory e contenuti delle directory, vengono crittografati e decrittografati utilizzando una CMK gestita da AWS.

Il contenuto dei file, o dati dei file, viene crittografato e decrittografato utilizzando una CMK a scelta dell'utente. La CMK può essere di uno dei tre seguenti tipi:

- Una CMK gestita da AWS per Amazon EFS
- Una CMK gestita dal cliente dal suo account AWS
- Una CMK gestita dal cliente da un altro account AWS

La propria organizzazione potrebbe essere soggetta a policy aziendali o normative che richiedono il controllo completo in termini di creazione, rotazione, eliminazione, nonché il controllo degli accessi e la policy di utilizzo per le CMK. In tal caso, consigliamo di utilizzare una CMK gestita dal cliente. In altri scenari è possibile utilizzare una CMK gestita da AWS.

Tutti gli utenti dispongono di una CMK gestita da AWS per Amazon EFS, il cui alias è `aws/elasticfilesystem`. AWS gestisce la policy della chiave di questa CMK e non è possibile modificarla. Non ci sono costi per la creazione e l'archiviazione di CMK gestite da AWS.

Se si decide di utilizzare una CMK gestita dal cliente per crittografare il file system, selezionare l'alias della chiave della CMK gestita dal cliente di cui si è proprietari. In alternativa, è possibile inserire l'Amazon Resource Name (ARN) di una CMK gestita dal cliente di proprietà di un altro account. Con una CMK gestita dal cliente di proprietà, è possibile controllare quali utenti e servizi possono utilizzare la chiave attraverso policy della chiave e autorizzazioni sulla chiave.

È anche possibile controllare la durata e la rotazione di queste chiavi scegliendo quando disabilitare, riattivare, eliminare o revocare l'accesso. Per informazioni sulla gestione dell'accesso alle chiavi in altri account AWS, consultare Modifica della policy della chiave nella Guida per gli sviluppatori di AWS KMS.

Per ulteriori informazioni su come gestire le CMK gestite dai clienti, consultare Chiavi master del cliente (CMK) nella Guida per gli sviluppatori di AWS KMS.

Nelle sezioni seguenti viene illustrato come creare un file system crittografato utilizzando la Console di gestione AWS e l'AWS CLI.

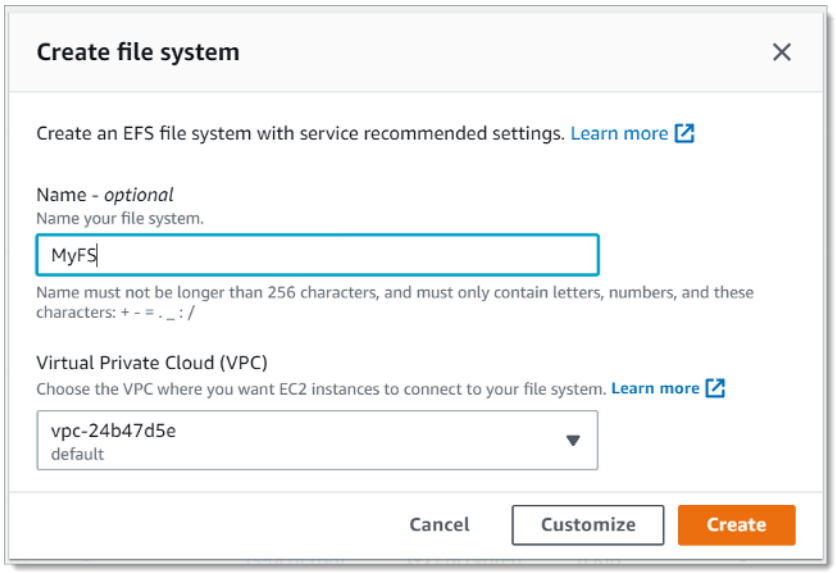
Creazione di un file system crittografato utilizzando la Console di gestione AWS

Utilizzare la seguente procedura per creare un file system Amazon EFS crittografato utilizzando la Console di gestione AWS.

Fase 1. Configurazione delle impostazioni del file system

In questa fase si configurano le impostazioni generali del file system, incluse la gestione del ciclo di vita, le modalità Prestazioni e Throughput e la crittografia dei dati a riposo.

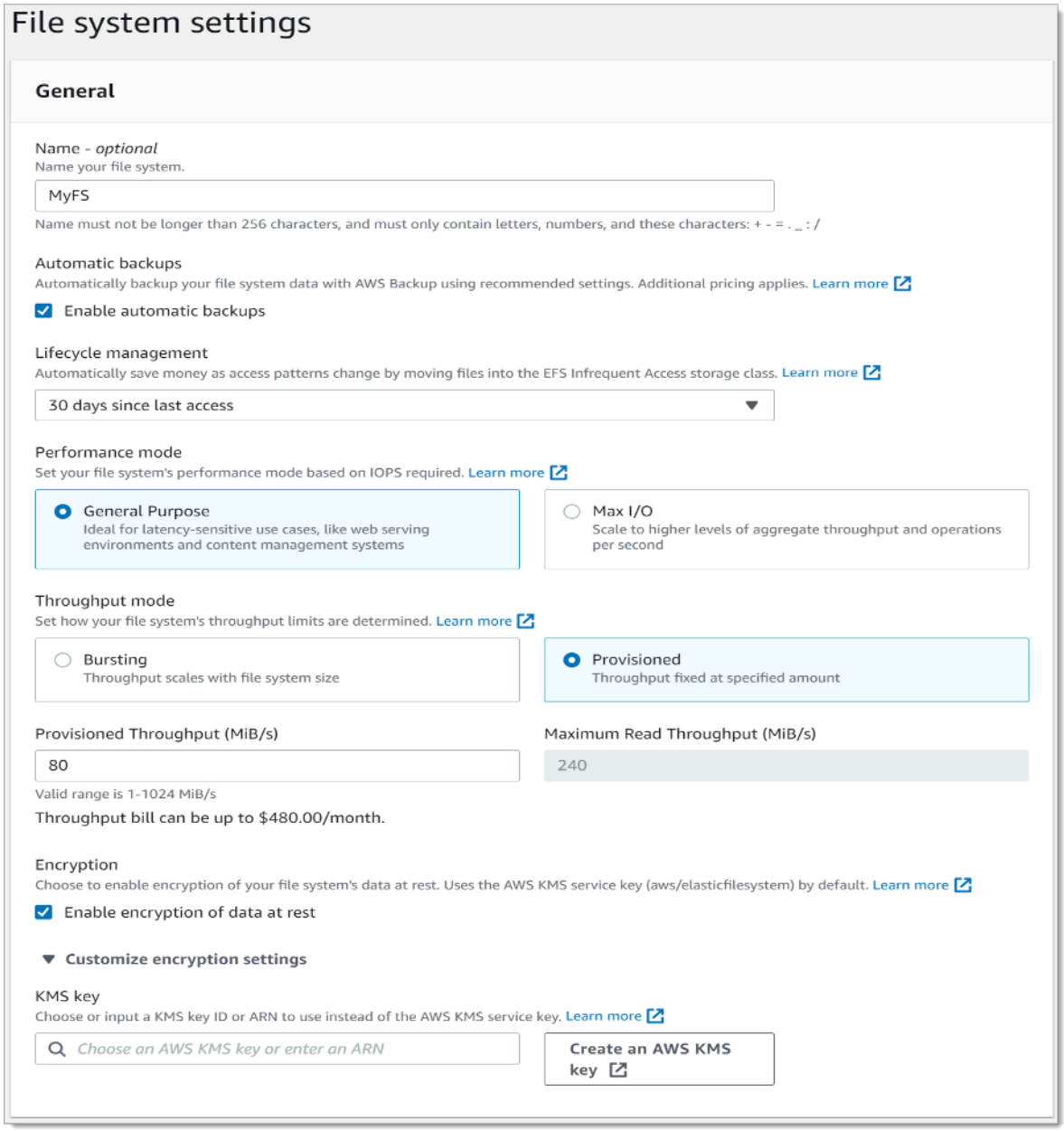
1. Accedere alla Console di gestione AWS e aprire la console di Amazon EFS.
2. Scegliere Create file system (Crea file system) per aprire la finestra di dialogo Create file system (Crea file system). Per ulteriori informazioni sulla creazione di un file system utilizzando le impostazioni consigliate che includono l'abilitazione della crittografia di default, consultare Create Your Amazon EFS File System (Creare il file system Amazon EFS).



Creazione del file system EFS

3. (Facoltativo) Scegliere Customize (Personalizza) per creare un file system personalizzato anziché creare un file system utilizzando le impostazioni consigliate dal servizio.

   Viene visualizzata la pagina Impostazioni file system.



Creazione del file system EFS: impostazioni generali

4. Nelle impostazioni General (Generali), inserire i dettagli seguenti.
   - (Facoltativo) Inserire un Name (Nome) per il file system.
   - I Automatic backups (Backup automatici) sono attivati di default. È possibile disattivare i backup automatici deselezionando la casella di controllo. Per ulteriori informazioni, consultare Utilizzo di AWS Backup con Amazon EFS.
   - Scegliere una policy di Gestione del ciclo di vita. La gestione del ciclo di vita di Amazon EFS gestisce automaticamente l'archiviazione di file a costi contenuti per i file system. Quando

abilitata, la gestione del ciclo di vita consente di migrare nella classe di archiviazione Infrequent Access (IA) i file che non sono stati utilizzati per un determinato periodo di tempo, definito utilizzando una policy del ciclo di vita. Se non si desidera abilitare la gestione del ciclo di vita, scegliere None (Nessuno). Per maggiori informazioni, consultare Gestione del ciclo di vita di EFS nella Guida per l'utente di Amazon EFS.

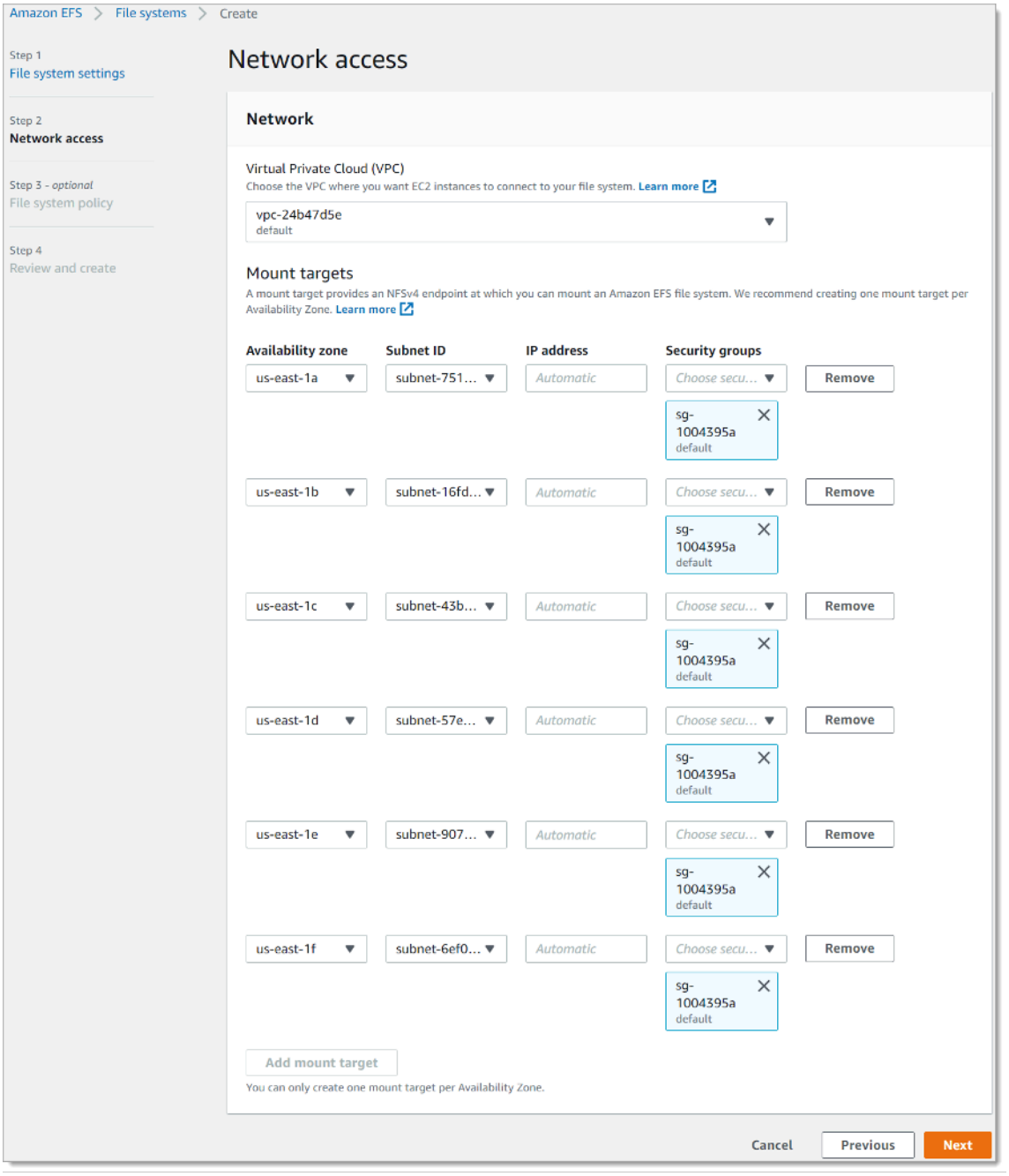
- Scegliere un Performance mode (Modalità prestazioni), ovvero la modalità General Purpose mode (Scopo generico) di default o Max I/O (I/O massimo). Per maggiori informazioni, consultare modalità Prestazioni nella Guida per l'utente di Amazon EFS.
- Scegliere un Throughput mode (modalità Throughput), ovvero la Bursting mode (Modalità ottimizzazione) di default o il Provisioned mode (Modalità Provisioned).
- Se è stato selezionato Provisioned viene visualizzato il campo Provisioned Throughput (Throughput provisionato) (MiB/s). Immettere la quantità di velocità effettiva di cui eseguire il provisioning per il file system. Dopo aver immesso la velocità effettiva, la console visualizza una stima del costo mensile accanto al campo. Per ulteriori informazioni, consultare le modalità Throughput nella Guida degli utenti di Amazon EFS.
- Relativamente al campo Encryption (Crittografia), la crittografia dei dati a riposo è abilitata di default. Utilizzare la chiave di servizio EFS (`aws/elasticfilesystem`) di AWS Key Management Service (AWS KMS) di default. Per scegliere una chiave KMS diversa da utilizzare per la crittografia, espandere le impostazioni di Personalizzazione della crittografia e scegliere una chiave dall'elenco. In alternativa, inserire un ID chiave di KMS o l'Amazon Resource Name (ARN) della chiave KMS che si desidera utilizzare.

  Se è necessario creare una nuova chiave, scegliere Create an AWS KMS key (Crea una chiave AWS KMS) per avviare la console di AWS KMS e creare una nuova chiave.

5. (Facoltativo) Scegliere Add tag (Aggiungi tag) per aggiungere coppie chiave-valore al file system.
6. Scegliere Next (Successivo) per proseguire alla fase Network Access (Accesso alla rete) nel processo di configurazione.

Fase 2. Configurazione dell'accesso di rete

In questa fase si configurano le impostazioni di rete del file system, inclusi il Virtual Private Cloud (VPC) e le destinazioni di montaggio. Per ogni destinazione di montaggio, impostare la zona di disponibilità, la sottorete, l'indirizzo IP e i gruppi di sicurezza.



Creazione di file system EFS: accesso alla rete

1. Scegliere il Virtual Private Cloud (VPC) in cui si desidera che le istanze EC2 si connettano al file system. Per ulteriori informazioni, consultare Gestione dell'accessibilità alla rete del file system nella Guida per l'utente di Amazon EFS.
   - Zona di disponibilità: di default, in ogni zona di disponibilità in una regione AWS è configurata una destinazione di montaggio. Se non si desidera una destinazione di montaggio in una determinata zona di disponibilità, scegliere Remove (Rimuovi) per eliminare la destinazione di

montaggio per tale zona. Creare una destinazione di montaggio in ogni zona di disponibilità da cui si prevede di accedere al file system. Tale operazione è gratuita.

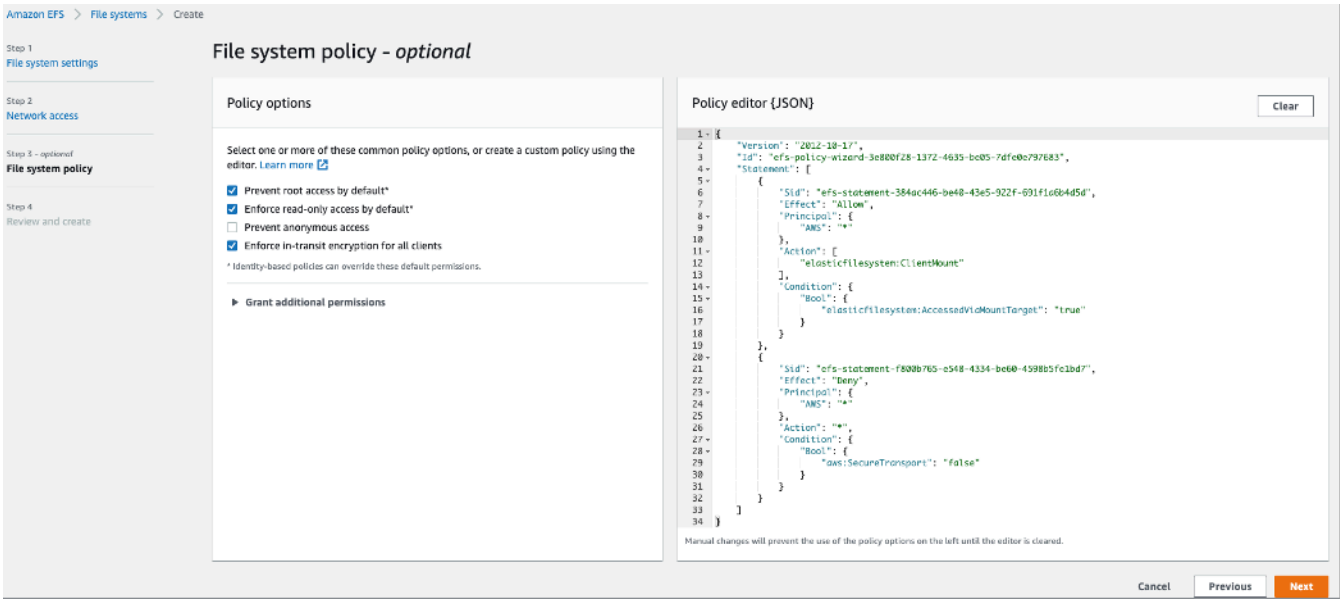
- ID sottorete: scegliere tra le sottoreti disponibili in una zona di disponibilità. La sottorete di default è preselezionata. Come best practice, assicurarsi che la sottorete scelta sia pubblica o privata in base ai requisiti di sicurezza.
- Indirizzo IP: di default, Amazon EFS seleziona automaticamente l'indirizzo IP tra gli indirizzi disponibili nella sottorete. In alternativa, è possibile inserire un indirizzo IP specifico disponibile nella sottorete. Sebbene le destinazioni di montaggio abbiano un unico indirizzo IP, si tratta di risorse di rete ridondanti e altamente disponibili.
- Gruppi di sicurezza: è possibile specificare uno o più gruppi di sicurezza per la destinazione di montaggio. Come best practice, assicurarsi che il gruppo di sicurezza venga utilizzato solo per scopi di montaggio EFS (porta NFS 2049) e che le regole in ingresso permettano solo la porta 2049 da un altro intervallo di blocchi CIDR VPC o utilizzare il gruppo di sicurezza come origine per le risorse che devono accedere a EFS. Per ulteriori informazioni, consultare la sezione Utilizzo dei gruppi di sicurezza per le istanze e le destinazioni di montaggio Amazon EC2 della Guida per l'utente di Amazon EFS.

  Per aggiungere un altro gruppo di sicurezza o per modificare il gruppo di sicurezza, selezionare Choose security groups (Scegliere gruppi di sicurezza) e aggiungere un altro gruppo di sicurezza dall'elenco. Se non si desidera utilizzare il gruppo di sicurezza di default, è possibile eliminarlo. Per ulteriori informazioni, consultare Creazione di gruppi di sicurezza nella Guida per l'utente di Amazon EFS.

2. Scegliere Add mount target (Aggiungere destinazione di montaggio) per creare una destinazione di montaggio per una zona di disponibilità che non ne includa una. Se una destinazione di montaggio è configurata per ciascuna zona di disponibilità, questa scelta non è disponibile.
3. Scegliere Next (Successivo) per continuare. Viene visualizzata la pagina File system policy (Policy del file system).

Fase 3. Creazione di una policy per il file system

In questa fase è possibile creare una policy del file system per controllare l'accesso dei client NFS al file system. Una policy del file system EFS è una policy IAM basata sulle risorse utilizzata per controllare l'accesso dei client NFS al file system. Per maggiori informazioni, consultare Utilizzo di IAM per controllare l’accesso NFS ad Amazon EFS nella Guida per l'utente di Amazon EFS.

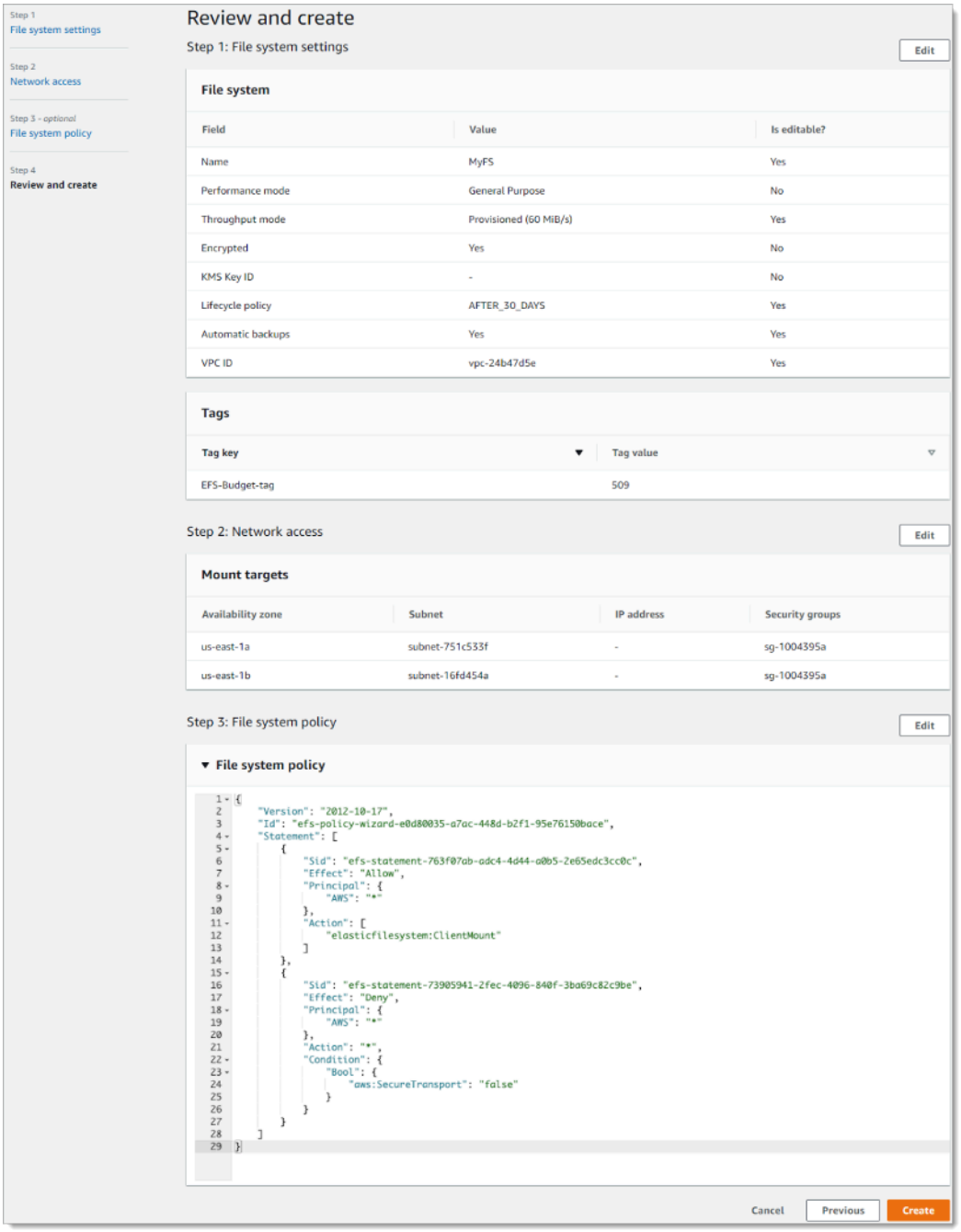


Creazione di file system EFS: policy del file system

1. Nelle Policy options (Opzioni della policy), si consiglia di scegliere le seguenti opzioni per le policy preconfigurati disponibili:
   - Impedisci l'accesso root per impostazione predefinita
   - Applica l'accesso in sola lettura per impostazione predefinita
   - Applica la crittografia in transito per tutti i client
2. Utilizzare Grant additional permissions (Concedi autorizzazioni aggiuntive) per concedere le autorizzazioni sul file system a entità IAM aggiuntive, incluso un altro account AWS. Scegliere Add (Aggiungi), quindi inserire l'ARN principale dell'entità a cui si stanno concedendo le autorizzazioni e poi scegliere le Permissions (Autorizzazioni) da concedere.
3. Utilizzare il Policy editor (Editor delle policy) per personalizzare una policy preconfigurata o per creare policy personalizzate. Quando si sceglie una delle policy preconfigurate, la definizione delle policy JSON viene visualizzata nell'editor delle policy.
4. Scegliere Next (Successivo) per continuare. Viene visualizzata la pagina Review and create (Rivedi e crea).

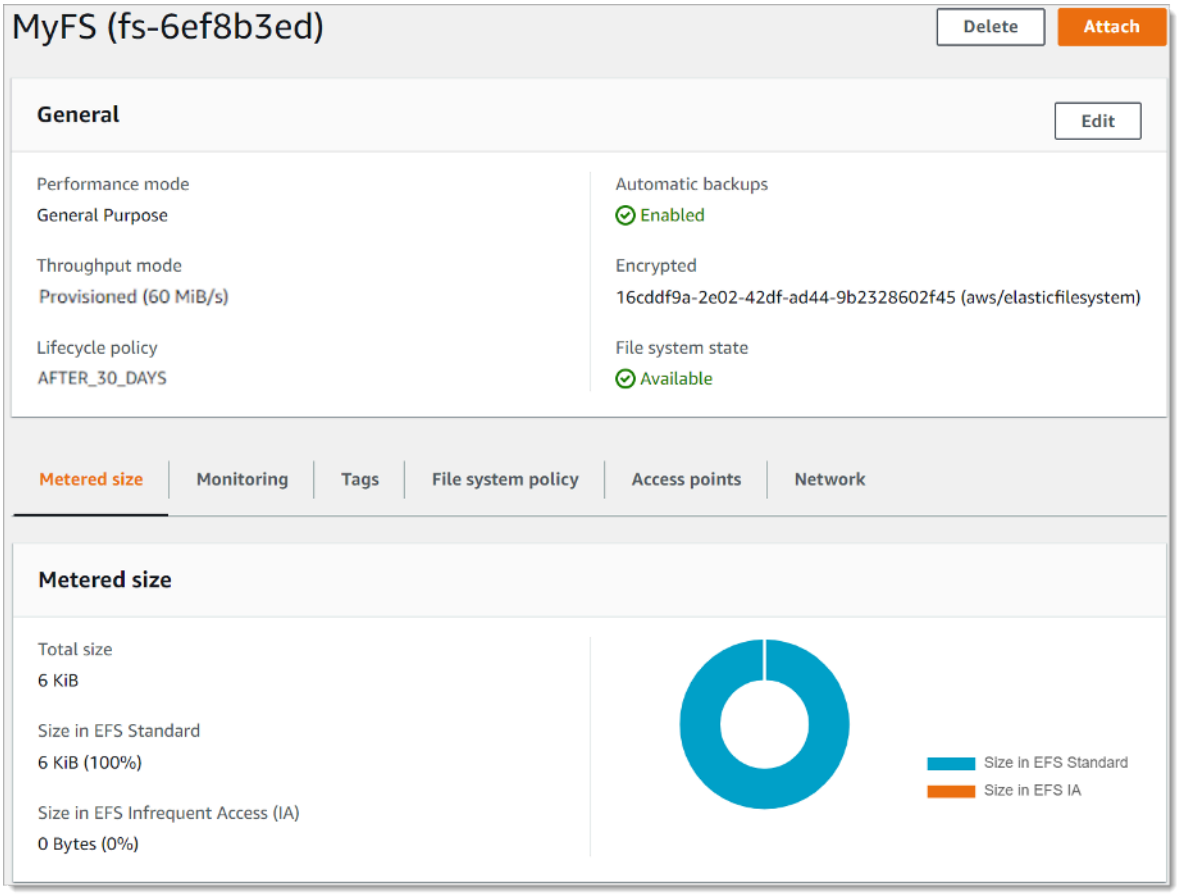
Fase 4. Revisione e creazione

In questa fase si esaminano le impostazioni del file system, si apportano eventuali modifiche e quindi si crea il file system.



Creazione di file system EFS: revisione e creazione

1. Esaminare ciascuno dei gruppi di configurazione del file system. È possibile apportare modifiche a ciascun gruppo in questo momento scegliendo Edit (Modifica).
2. Scegliere Create (Crea) per creare il file system e tornare alla pagina File system.
3. La pagina File system visualizza il file system e i relativi dettagli di configurazione, come illustrato di seguito.



File System

Creazione di un file system crittografato utilizzando l'AWS CLI

Quando si utilizza l'AWS CLI per creare un file system crittografato, è possibile utilizzare parametri aggiuntivi per impostare lo stato della crittografia e la CMK gestita dal cliente. Assicurarsi di disporre della versione più recente dell'AWS CLI. Per informazioni su come aggiornare l'AWS CLI, consultare Installazione, aggiornamento e disinstallazione di AWS CLI nella Guida per l'utente dell'Interfaccia a riga di comando di AWS.

Nell'operazione `CreateFileSystem`, il parametro `--encrypted` è un valore booleano ed è obbligatorio per la creazione di file system crittografati. L'indicazione di `--kms-key-id` è obbligatoria solo quando si utilizza una CMK gestita dal cliente e si include l'alias o l'ARN della chiave. Non includere questo parametro se si utilizza la CMK gestita da AWS.

```
$ aws efs create-file-system \
```

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

Per ulteriori informazioni sulla creazione di file system Amazon EFS utilizzando la Console di gestione AWS, l'AWS CLI, gli SDK AWS o l'API Amazon EFS, consultare Cos'è Amazon Elastic File System nella Guida per l'utente di Amazon EFS.

Applicazione della crittografia dei dati a riposo

La crittografia ha un effetto minimo sulla latenza e sul throughput di I/O. La crittografia e la decrittografia sono trasparenti per utenti, applicazioni e servizi. Tutti i dati e i metadati vengono crittografati da Amazon EFS per conto del cliente prima di essere scritti su disco e decrittografati prima di essere letti dai client. Non è necessario modificare gli strumenti, le applicazioni o i servizi client per accedere a un file system crittografato.

Un'organizzazione potrebbe richiedere la crittografia di tutti i dati che soddisfano una determinata classificazione o sono associati a una determinata applicazione, carico di lavoro o ambiente. È possibile utilizzare policy basate sull'identità di AWS Identity and Access Management (IAM) per imporre la crittografia dei dati a riposo per le risorse del file system Amazon EFS. Utilizzando una chiave di condizione IAM, è possibile impedire agli utenti di creare file system EFS non crittografati.

Ad esempio, una policy IAM che consente esplicitamente agli utenti di creare solo file system EFS crittografati utilizza la seguente combinazione di effetti, operazioni e condizioni:

- Il valore del campo `Effect` è `Allow`.
- Il valore del campo `Action` è `elasticfilesystem:CreateFileSystem`.
- Il valore del campo `Condition elasticfilesystem:Encrypted` è `true`.

L'esempio seguente illustra una policy basata sull'identità IAM che autorizza le entità alla sola creazione di file system crittografati.

```
{
  “Version”: “2012-10-17”,
  “Statement”: [
    {
```

```
      “Sid”: “VisualEditior0”,
      “Effect”: “Allow”,
      “Action”: “elasticfilesystem:CreateFileSystem”,
      “Condition”: {
        “Bool”: {
          “elasticfilesystem:Encrypted”: “true”
        }
      },
      “Resource”: “*”
    }
}
```

L'attributo `Resource` impostato su `*` indica che la policy IAM si applica a tutte le risorse EFS create. È possibile aggiungere attributi condizionali aggiuntivi basati su tag per applicarli solo a un sottoinsieme di risorse EFS con esigenze di riservatezza dei dati.

È anche possibile imporre la creazione di file system Amazon EFS crittografati a livello di AWS Organizations utilizzando policy di controllo dei servizi per tutti gli account AWS o le unità organizzative dell'organizzazione. Per ulteriori informazioni sulle policy di controllo dei servizi in AWS Organizations, consultare Policy di controllo dei servizi nella Guida per gli utenti di AWS Organizations.

Creazione di una policy IAM che richiede la crittografia di tutti i file system EFS

È possibile creare una policy basata sull'identità IAM che autorizzi gli utenti a creare solo file system Amazon EFS crittografati utilizzando la console, l'AWS CLI o l'API. La procedura seguente descrive la creazione di tale policy utilizzando la console IAM e quindi la sua applicazione a un utente nel proprio account.

Per creare una policy IAM per imporre la creazione di file system EFS crittografati:

1. Accedere alla Console di gestione AWS e aprire la console IAM.
2. Nel pannello di navigazione, sotto Access management (Gestione accessi), scegliere Policies (Policy).
3. Scegliere Create policy (Crea policy) per visualizzare la pagina Crea policy.
4. Nella scheda Visual Editor, inserire le seguenti informazioni.

    - Alla voce Service (Servizio) scegliere EFS.

- Alla voce Actions (Operazioni), inserire `create` nel campo di ricerca e quindi scegliere Create File System (Crea File System).
- Alla voce Request conditions (Condizioni della richiesta), fare clic sul collegamento Add condition (Aggiungi condizione), cercare `elasticfilesystem:Encrypted` nel campo Condition Key (Chiave della condizione), `Bool` nel campo Operator (Operatore) e `true` nel campo Value (Valore).

5. Indicare un Nome e una Descrizione per la policy. Verificare il riepilogo della policy, inclusa la condizione della richiesta Encrypted (Crittografato).
6. Scegliere Create policy (Crea policy) per creare la policy.

Per applicare la policy a un utente nel proprio account:

1. Nella console IAM, in Access management (Gestione accessi), scegliere Users (Utenti).
2. Selezionare l'utente a cui si desidera applicare la policy.
3. Scegliere Add permissions (Aggiungi autorizzazioni) per visualizzare la pagina Aggiungi autorizzazioni.
4. Scegliere Attach existing policies directly (Collega direttamente le policy esistenti).
5. Inserire il nome della policy EFS creata nella procedura precedente.
6. Selezionare ed espandere la policy. Quindi scegliere {}JSON per verificare il contenuto della policy. Dovrebbe essere simile alla seguente policy JSON.

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

Rilevamento di file system non crittografati

La propria organizzazione potrebbe avere l'obbligo di identificare le risorse Amazon EFS che non sono crittografate. È possibile rilevare file system non crittografati utilizzando le Regole gestite di AWS Config. AWS Config fornisce AWS Managed Rules, regole predefinite e personalizzabili che AWS Config utilizza per valutare se le risorse AWS rispettano le best practice comuni e contrassegnare le risorse che non rispettano le regole come NON_COMPLIANT.

È possibile utilizzare la regola AWS Managed Config `efs-encrypted-check` per verificare se Amazon Elastic File System (Amazon EFS) è configurato per crittografare i dati dei file utilizzando AWS Key Management Service (AWS KMS). Per ulteriori informazioni sulla configurazione e l'attivazione di AWS Managed Rules, consultare Utilizzare le Regole gestite di AWS Config.

Crittografia dei dati in transito

È possibile montare un file system in modo che tutto il traffico NFS sia crittografato in transito utilizzando Transport Layer Security 1.2 (TLS) con crittografia AES-256 standard del settore. TLS è un insieme di protocolli crittografici standard del settore utilizzati per crittografare le informazioni scambiate sulla rete. AES-256 è un codice di crittografia a 256 bit utilizzato per la trasmissione dei dati in TLS. Consigliamo di impostare la crittografia in transito su ogni client che accede al file system.

È possibile utilizzare le policy IAM per applicare la crittografia in transito per l'accesso dei client NFS ad Amazon EFS. Quando un client si connette a un file system, Amazon EFS valuta la policy IAM basata sulle risorse del file system, chiamata policy del file system, insieme alle eventuali policy IAM basate sull'identità per determinare le autorizzazioni di accesso al file system appropriate da concedere. Nella policy basata sulle risorse del file system è possibile utilizzare la chiave di condizione di `aws:SecureTransport` per imporre ai client NFS di utilizzare TLS durante la connessione a un file system EFS.

> **Note**
>
> Per montare i file system Amazon EFS è necessario utilizzare l'assistente per il montaggio di EFS al fine di utilizzare l'autorizzazione IAM per controllare l'accesso da parte dei client NFS. Per maggiori informazioni, consultare Montaggio con autorizzazione IAM nella Guida per l'utente di Amazon EFS.

Il seguente esempio di policy del file system EFS applica la crittografia in transito e presenta le seguenti caratteristiche:

- Il valore del campo `effect` è `allow`.
- L'entità è impostata su * per tutte le entità IAM.
- L'operazione è impostata su `ClientMount`, `ClientWrite`, `ClientRootAccess`.
- La condizione per la concessione delle autorizzazioni è impostata su `SecureTransport`. L'accesso è consentito solo ai client NFS che utilizzano TLS per connettersi al file system.

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

È possibile creare una policy del file system utilizzando la console Amazon EFS o l'AWS CLI.

Per creare una policy del file system utilizzando la console EFS:

1. Aprire la console di Amazon EFS.
2. Scegliere File system.
3. Nella pagina File system, scegliere il file system per cui si desidera modificare o creare una policy del file system. Viene visualizzata la pagina dei dettagli del file system.
4. Scegliere File system policy (Policy del file system), quindi scegliere Edit (Modifica). Viene visualizzata la pagina Policy del file system.

Creare policy del file system

5. Alla voce Policy options (Opzioni della policy), si consiglia di scegliere le seguenti opzioni preconfigurate della policy disponibili:

   - Impedisci l'accesso root per impostazione predefinita
   - Applica l'accesso in sola lettura per impostazione predefinita
   - Applica la crittografia in transito per tutti i client

   Se si sceglie una policy preconfigurata, l'oggetto JSON policy viene visualizzato nel pannello Policy editor (Editor della policy).

6. Utilizzare Grant additional permissions (Concedi autorizzazioni aggiuntive) per concedere le autorizzazioni sul file system a entità IAM aggiuntive, incluso un altro account AWS. Scegliere Add (Aggiungi), quindi inserire l'ARN principale dell'entità a cui si stanno concedendo le autorizzazioni e poi scegliere le Permissions (Autorizzazioni) da concedere.

7. Utilizzare il Policy editor (Editor delle policy) per personalizzare una policy preconfigurata o per creare policy personalizzate. Quando si utilizza l'editor, le opzioni delle policy preconfigurate diventano non disponibili. Per annullare le modifiche alle policy, scegliere Clear (Cancella).

   Quando si deseleziona l'editor, le policy preconfigurate diventano nuovamente disponibili.

8. Dopo aver completato la modifica o la creazione della policy, scegliere Save (Salva).

   Viene visualizzata la pagina dei dettagli del file system, che mostra la policy in File system policy (Policy del file system).

   Inoltre, è possibile creare una policy del file system a livello di codice utilizzando AWS CloudFormation, i SDK di AWS oppure direttamente l'API di Amazon EFS. Per ulteriori informazioni sulla creazione di policy per i file system, consultare Creazioni di policy del file system nella Guida per l'utente di Amazon EFS.

Impostazione della crittografia dei dati in transito

Per impostare la crittografia dei dati in transito, si consiglia di scaricare l'Assistente per il montaggio di EFS su ogni client. L'Assistente per il montaggio è un'utilità open source fornita da AWS per semplificare l'utilizzo di EFS, inclusa l'impostazione della crittografia dei dati in transito. L'Assistente per il montaggio utilizza di default le opzioni di montaggio consigliate da EFS.

L'Assistente per il montaggio di EFS è supportato nelle seguenti distribuzioni Linux:

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

Per configurare la crittografia dei dati in transito:

1. Installare l'Assistente per il montaggio di EFS:
   - Per Amazon Linux, usare il seguente comando:

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

- Per altre distribuzioni Linux, scaricare da GitHub e installare.

  Il pacchetto amazon-efs-utils installa automaticamente le seguenti dipendenze: client NFS (nfs-utils), Network relay (stunnel), OpenSSL e Python.

2. Montare il file system:

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

- `mount -t efs` richiama l'Assistente per il montaggio di EFS.
- Il montaggio utilizzando l'Assistente per il montaggio di EFS non supporta l'utilizzo del nome DNS del file system o dell'indirizzo IP di una destinazione di montaggio, utilizzare invece l'id del file system.
- L'Assistente per il montaggio di EFS utilizza di default le opzioni di montaggio consigliate da AWS. Non è consigliabile sovrascrivere queste opzioni di montaggio di default, ma viene garantita la flessibilità necessaria per farlo qualora fosse necessario. Consigliamo di testare a fondo le eventuali alternative delle opzioni di montaggio per capire come queste modifiche influiscono sull'accesso e sulle prestazioni del file system.
- La tabella seguente rappresenta le opzioni di montaggio di default utilizzate dall'Assistente per il montaggio di EFS.

Opzione	Descrizione
nfsvers=4.1	La versione del protocollo NFS
rsize=1048576	Il numero massimo di byte di dati che il client NFS è in grado di ricevere per

Opzione	Descrizione
	ogni richiesta READ di rete.
wsize=1048576	Il numero massimo di byte di dati che il client NFS è in grado di inviare per ogni richiesta WRITE di rete.
hard	Il comportamento di ripristino del client NFS dopo il timeout di una richiesta NFS, in modo che la richiesta NFS venga ritentata a tempo indeterminato fino alla risposta del server.
timeo=600	Il valore di timeout utilizzato dal client NFS in attesa di una risposta prima di ripetere la richiesta NFS in decimi di secondo

Opzione	Descrizione
retrans=2	Il numero di volte che il client NFS ritenta una richiesta prima di eseguire un'ulteriore operazione di ripristino.
noresvport	Indica al client NFS di utilizzare una nuova porta sorgente TCP quando viene ristabilita una connessione di rete

- Aggiungere la seguente riga a `/etc/fstab` per rimontare automaticamente il file system dopo ogni riavvio del sistema.

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

Utilizzo della crittografia dei dati in transito

Se la propria organizzazione è soggetta a policy aziendali o normative che richiedono la crittografia dei dati in transito, consigliamo di utilizzare la crittografia dei dati in transito su ogni client che accede al file system. Crittografia e decrittografia sono configurate a livello di connessione e aggiungono un ulteriore livello di sicurezza.

Il montaggio del file system utilizzando l'Assistente per il montaggio di EFS configura e mantiene un tunnel TLS 1.2 tra il client e Amazon EFS e instrada tutto il traffico NFS su questo tunnel crittografato.

Il certificato utilizzato per stabilire la connessione TLS crittografata è firmato dalla Amazon Certificate Authority (CA) e considerato affidabile dalla maggior parte delle distribuzioni Linux moderne. L'Assistente per il montaggio di EFS genera anche un processo watchdog per monitorare tutti i tunnel sicuri su ciascun file system e garantisce che siano in esecuzione.

Dopo aver utilizzato l'Assistente per il montaggio di EFS per stabilire connessioni crittografate ad Amazon EFS, non sono richiesti ulteriori input o configurazioni da parte dell'utente. La crittografia è trasparente per le connessioni degli utenti e le applicazioni che accedono al file system.

Dopo aver montato e stabilito una connessione crittografata a un file system EFS utilizzando l'Assistente per il montaggio di EFS, l'output di un comando mount mostra che il file system è montato e che è stato creato un tunnel crittografato utilizzando localhost (127.0.0.1) come relay di rete. Vedere il seguente output di esempio.

```
     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
```

Per mappare un `efs-mount-point` su un file system EFS, interrogare il file mount.log in `/var/log/amazon/efs` e trovare l'ultima operazione di montaggio eseguita correttamente. Questo può essere fatto usando il seguente semplice comando grep.

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

L'output di questo comando grep restituirà il nome DNS del file system EFS montato. Vedere qui di seguito un output di esempio.

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

Conclusioni

I dati del file system di Amazon EFS possono essere soggetti a crittografia dei dati a riposo e crittografia dei dati in transito. È possibile crittografare i dati a riposo utilizzando CMK controllabili e gestibili utilizzando AWS KMS. Creare un file system crittografato è semplice: basta selezionare una casella di controllo nella procedura guidata di creazione del file system di Amazon EFS nella Console di gestione AWS o aggiungere un singolo parametro all'operazione `CreateFileSystem` nell'AWS CLI, negli SDK AWS o nell'API di Amazon EFS.

È possibile applicare la crittografia dei dati a riposo e in transito utilizzando le policy basate sull'identità di AWS IAM e le policy del file system per rafforzare ulteriormente i requisiti di sicurezza e contribuire a soddisfare le esigenze di conformità. L'uso di un file system crittografato è inoltre trasparente per servizi, applicazioni e utenti, con un effetto minimo sulle sue prestazioni. È possibile crittografare i dati in transito utilizzando l'assistente per il montaggio di EFS per stabilire un tunnel TLS crittografato su ciascun client, in grado di crittografare tutto il traffico NFS tra il client e il file system EFS montato. L'applicazione della crittografia dei dati a riposo di Amazon EFS tramite l'utilizzo delle policy di identità IAM e dei dati in transito utilizzando le policy del file system EFS è disponibile senza costi aggiuntivi.

Risorse

- Whitepaper sui dettagli della crittografia di AWS KMS
- Guida per l'utente di Amazon EFS

Cronologia del documento e collaboratori

Cronologia dei documenti

Per ricevere una notifica sugli aggiornamenti di questo whitepaper, iscriviti al feed RSS.

update-history-change	update-history-description	update-history-date
Aggiornamenti minori	Layout di pagina modificato	30 aprile 2021
Whitepaper aggiornato	Aggiunta dell'applicazione della crittografia dei dati a riposo e in transito tramite IAM	22 febbraio 2021
Whitepaper aggiornato	Aggiunta della crittografia dei dati in transito	1 Aprile 2018
Pubblicazione iniziale	Crittografia dei dati a riposo con i file system crittografati di Amazon EFS	1 settembre 2017

> **Note**
>
> Nota: per iscriversi e ricevere gli aggiornamenti RSS, è necessario disporre di un plug-in RSS abilitato per il browser in uso.

Collaboratori

I collaboratori di questo documento includono:

- Darryl S. Osborne, Storage Specialist Solutions Architect, AWS
- Joseph Travaglini, Senior Product Manager, Amazon EFS
- Peter Buonora, Principal Solutions Architect, AWS
- Siva Rajamani, Senior Solutions Architect, AWS