

Livre blanc AWS

Chiffrement des données de fichier avec Amazon Elastic File System



Chiffrement des données de fichier avec Amazon Elastic File System: Livre blanc AWS

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et l'habillage commerciaux d'Amazon ne peuvent pas être utilisés en connexion avec un produit ou un service qui n'est pas celui d'Amazon, d'une manière susceptible de causer de la confusion chez les clients ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon sont la propriété de leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Résumé et introduction	1
Résumé	1
Introduction	1
Concepts de base et terminologie	3
Chiffrement de données au repos	5
Gestion de clés	5
Création d'un système de fichiers chiffrés	8
Création d'un système de fichiers chiffrés à l'aide de l'AWS Management Console	9
Création d'un système de fichiers chiffrés à l'aide de l'AWS CLI	16
Application du chiffrement des données au repos	17
Création d'une politique IAM exigeant que tous les systèmes de fichiers EFS soient chiffrés	18
Détection des systèmes de fichiers non chiffrés	20
Chiffrement des données en transit	21
Configuration du chiffrement des données en transit	24
Utilisation du chiffrement des données en transit	28
Conclusion	30
Ressources	31
Historique du document et participants	32
Historique du document	32
Participants	32

Chiffrement des données de fichier avec Amazon Elastic File System

Date de publication : 22 février 2021 ([Historique du document et participants](#))

Résumé

La sécurité est une priorité pour AWS et nous donnons à nos clients les outils nécessaires pour faire de la sécurité une priorité dans leur entreprise. Les réglementations gouvernementales et les politiques de conformité de l'industrie ou de l'entreprise peuvent exiger que les données de différentes classifications soient sécurisées à l'aide de politiques de chiffrement, d'algorithmes cryptographiques et d'une gestion appropriée des clés. Ce livre blanc présente les bonnes pratiques pour le chiffrement d'Amazon Elastic File System (Amazon EFS).


Introduction

[Amazon Elastic File System](#) (Amazon EFS) fournit des systèmes de fichiers partagés simples, évolutifs, hautement disponibles et hautement durables dans le cloud. Les systèmes de fichiers que vous créez à l'aide d'Amazon EFS sont élastiques, ce qui leur permet de croître et de se réduire automatiquement à mesure que vous ajoutez et supprimez des données. Leur taille peut atteindre des pétaoctets, en répartissant les données sur un nombre illimité de serveurs de stockage dans plusieurs zones de disponibilité (AZ).

Les données stockées dans ces systèmes de fichiers peuvent être chiffrées au repos et en transit à l'aide d'Amazon EFS. Pour le chiffrement des données au repos, vous pouvez créer des systèmes de fichiers chiffrés via l'AWS Management Console ou AWS Command Line Interface (AWS CLI). Vous pouvez également créer des systèmes de fichiers chiffrés par programmation via l'API Amazon EFS ou l'un des kits SDK AWS.

Pour le chiffrement des données au repos, Amazon EFS s'intègre à [AWS Key Management Service](#) (AWS KMS) pour la gestion des clés. Vous pouvez également activer le chiffrement des données en transit en montant le système de fichiers et en transférant tout le trafic NFS via un protocole TLS (Transport Layer Security).

Ce livre blanc présente les bonnes pratiques de chiffrement pour Amazon EFS. Il explique comment activer le chiffrement des données en transit au niveau de la couche de connexion client et comment créer un système de fichiers chiffrés dans l'AWS Management Console et dans l'AWS CLI.

 Note

L'utilisation des API et des kits SDK pour créer un système de fichiers chiffrés n'entre pas dans le cadre de ce document. Pour de plus amples informations sur la façon de le faire, consultez [API Amazon EFS](#) dans le Guide de l'utilisateur Amazon EFS ou la [documentation des kits SDK](#).

Concepts de base et terminologie

Cette section définit les concepts et la terminologie référencés dans ce livre blanc.

- Amazon Elastic File System (Amazon EFS) : service hautement disponible et hautement durable qui fournit un stockage de fichiers partagés simple, évolutif et dans AWS Cloud. Amazon EFS fournit une interface et une sémantique de système de fichiers standard. Vous pouvez stocker une quantité pratiquement illimitée de données sur un nombre illimité de serveurs de stockage dans plusieurs zones de disponibilité.
- [AWS Identity and Access Management \(IAM\)](#) : service qui vous permet de contrôler en toute sécurité l'accès précis aux API de service AWS. Les politiques sont créées et utilisées pour limiter l'accès à des utilisateurs, des groupes et des rôles individuels. Vous pouvez gérer vos clés AWS KMS via la console IAM.
- AWS KMS : service géré qui facilite la création et le contrôle des clés principales client (CMK), les clés de chiffrement utilisées pour chiffrer vos données. Les clés CMK AWS KMS sont protégées par des modules de sécurité matériels (HSM) qui sont validés par le programme de validation des modules cryptographiques FIPS 140-2 sauf dans les régions Chine (Pékin) et Chine (Ningxia). AWS KMS est intégré à d'autres services AWS qui chiffrent vos données. Il est également entièrement intégré à AWS CloudTrail pour fournir des journaux des appels d'API effectués par AWS KMS en votre nom, ce qui peut être utile pour répondre aux exigences de conformité ou réglementaires applicables à votre organisation.
- Clé principale client (CMK) : représente le sommet de votre hiérarchie de clés. Elle contient des éléments de clé pour chiffrer et déchiffrer les données. AWS KMS peut générer ces éléments de clé, ou vous pouvez les générer puis les importer dans AWS KMS. Les clés CMK sont spécifiques à un compte AWS et à une région AWS et peuvent être gérées par le client ou par AWS.
- Clé CMK gérée par AWS : clé CMK générée par AWS en votre nom. Une clé CMK gérée par AWS est créée lorsque vous activez le chiffrement pour une ressource d'un service AWS intégré. Les politiques de clé CMK gérées par AWS sont gérées par AWS et vous ne pouvez pas les modifier. La création ou le stockage de clés CMK gérées par AWS sont gratuits.
- Clé CMK gérée par le client : clé CMK que vous créez à l'aide d'AWS Management Console, de l'API AWS, d'AWS CLI ou des kits SDK. Vous pouvez utiliser une clé CMK gérée par le client lorsque vous avez besoin d'un contrôle plus détaillé sur la clé CMK.
- Politique de clé KMS : politique de ressources qui contrôle l'accès à une clé CMK gérée par le client. Les clients définissent ces autorisations à l'aide de la politique de clé ou d'une combinaison

de politiques IAM et de politique de clé. Pour de plus amples informations, consultez [Aperçu de la gestion de l'accès](#) dans le Guide du développeur AWS KMS.

- Clés de données : clés cryptographiques générées par AWS KMS pour chiffrer les données en dehors d'AWS KMS. AWS KMS permet aux entités autorisées (utilisateurs ou services) d'obtenir des clés de données protégées par une clé CMK.
- Protocole TLS (Transport Layer Security) : successeur du protocole SSL (Secure Sockets Layer, couche de sockets sécurisés), TLS est un protocole cryptographique essentiel au chiffrement des informations échangées sur un réseau.
- Assistant de montage EFS : agent client Linux (`amazon-efs-utils`) utilisé pour simplifier le montage des systèmes de fichiers EFS. Il peut être utilisé pour configurer, gérer et acheminer tout le trafic NFS via un tunnel TLS.

Pour de plus amples informations sur les concepts de base et la terminologie, consultez [Concepts d'AWS Key Management Service](#) dans le Guide du développeur AWS KMS.

Chiffrement de données au repos

AWS fournit les outils nécessaires pour vous permettre de créer un système de fichiers chiffrés qui chiffre toutes vos données et métadonnées au repos à l'aide d'un algorithme de chiffrement standard AES-256. Un système de fichiers chiffrés est conçu pour gérer le chiffrement et le déchiffrement automatiquement et de manière transparente, afin que vous n'ayez pas à modifier vos applications. Si votre organisation est soumise à des politiques d'entreprise ou réglementaires qui exigent le chiffrement des données et des métadonnées au repos, nous vous recommandons de créer un système de fichiers chiffrés.

Rubriques

- [Gestion de clés](#)
- [Création d'un système de fichiers chiffrés](#)
- [Application du chiffrement des données au repos](#)
- [Création d'une politique IAM exigeant que tous les systèmes de fichiers EFS soient chiffrés](#)
- [Détection des systèmes de fichiers non chiffrés](#)

Gestion de clés

Amazon EFS est intégré à AWS KMS, qui gère les clés de chiffrement des systèmes de fichiers chiffrés. AWS KMS prend également en charge le chiffrement par d'autres services AWS tels qu'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. Pour chiffrer le contenu du système de fichiers, Amazon EFS utilise l'algorithme Advanced Encryption Standard avec le mode XTS et une clé 256 bits (XTS-AES-256).

Il faut répondre à trois questions importantes lorsque l'on considère comment sécuriser les données au repos en adoptant une politique de chiffrement. Ces questions s'appliquent également aux données stockées dans des services gérés et non gérés tels qu'Amazon EBS.

Où sont stockées les clés ?

AWS KMS stocke vos clés principales dans un stockage hautement durable dans un format chiffré afin de garantir qu'elles peuvent être récupérées en cas de besoin.

Où sont utilisées les clés ?

L'utilisation d'un système de fichiers Amazon EFS chiffrés est transparente pour les clients qui montent le système de fichiers. Toutes les opérations cryptographiques ont lieu au sein du service EFS, car les données sont chiffrées avant d'être écrites sur le disque et déchiffrées après qu'un client a émis une demande de lecture.

Qui peut utiliser les clés ?

Les politiques de clé AWS KMS contrôlent l'accès aux clés de chiffrement.

Nous vous recommandons de les associer à des politiques IAM pour fournir une autre couche de contrôle. Chaque clé possède une politique de clé. Si la clé est une clé CMK gérée par AWS, AWS gère la politique de clé. Si la clé est une clé CMK gérée par le client, vous gérez la politique de clé. Ces politiques de clé constituent le principal moyen de contrôler l'accès aux clés CMK. Elles définissent les autorisations qui régissent l'utilisation et la gestion des clés.

Lorsque vous créez un système de fichiers chiffrés à l'aide d'Amazon EFS, vous accordez à Amazon EFS l'accès pour utiliser la clé CMK en votre nom. Les appels qu'Amazon EFS effectue à AWS KMS en votre nom apparaissent dans vos journaux CloudTrail comme s'ils provenaient de votre compte AWS. La capture d'écran suivante montre l'exemple d'événement CloudTrail pour un appel KMS Decrypt effectué par Amazon EFS.

```
Event record Info Copy

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2020-12-21T18:00:45Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": {
    "encryptionContext": {
      "aws:elasticfilesystem:filesystem:id": "fs-d7743722"
    },
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
  },
  "responseElements": null,
  "requestID": "e522cb61-72f1-45f4-9e3c-4d6d4cacia46",
  "eventID": "1c2ebc27-3b67-4902-be53-3e8a8d95a1b1",
  "readOnly": true,
  "resources": [
    {
      "accountId": "123456789012",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-east-1:123456789012:key/7f9500cb-d28f-454f-9cb6-1aa38f252b9f"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "sharedEventID": "8b366c91-1da8-42e5-8a37-393f3e5f9f0b"
}
```

Journal CloudTrail pour KMS Decrypt

Pour de plus amples informations sur AWS KMS et sur la façon de gérer l'accès aux clés de chiffrement, consultez [Gestion de l'accès aux clés CMK AWS KMS](#) dans le Guide du développeur AWS KMS.

Pour de plus amples informations sur la façon dont AWS KMS gère le chiffrement, consultez le livre blanc [Détails cryptographiques AWS KMS](#).

Pour de plus amples informations sur la création d'un utilisateur et d'un groupe IAM administrateur, consultez [Création de votre premier utilisateur et groupe administrateur IAM](#) dans le Guide de l'utilisateur IAM.

Création d'un système de fichiers chiffrés

Vous pouvez créer un système de fichiers chiffrés à l'aide de l'AWS Management Console, de l'AWS CLI, de l'API Amazon EFS ou des kits SDK AWS. Vous ne pouvez activer le chiffrement d'un système de fichiers que lorsque vous le créez.

Amazon EFS s'intègre à AWS KMS pour la gestion des clés et utilise une clé CMK pour chiffrer le système de fichiers. Les métadonnées du système de fichiers, telles que les noms de fichiers, les noms de répertoires et le contenu des répertoires, sont chiffrées et déchiffrées à l'aide d'une clé CMK gérée par AWS.

Le contenu de vos fichiers, ou données de fichiers, est chiffré et déchiffré à l'aide d'une clé CMK de votre choix. Il existe trois types de clé CMK :

- Une clé CMK gérée par AWS pour Amazon EFS
- Une clé CMK gérée par le client à partir de votre compte AWS
- Une clé CMK gérée par le client à partir d'un autre compte AWS

Votre organisation peut être soumise à des politiques d'entreprise ou réglementaires qui nécessitent un contrôle total en termes de création, de rotation, de suppression ainsi que le contrôle d'accès et la politique d'utilisation des clés CMK. Si c'est le cas, nous vous recommandons d'utiliser une clé CMK gérée par le client. Dans d'autres scénarios, vous pouvez utiliser une clé CMK gérée par AWS.

Tous les utilisateurs disposent d'une clé CMK gérée par AWS pour Amazon EFS, dont l'alias est `aws/elasticfilesystem`. AWS gère la politique de clé de cette clé CMK et vous ne pouvez pas la modifier. La création et le stockage des clés CMK gérées par AWS sont gratuits.

Si vous décidez d'utiliser une clé CMK gérée par le client pour chiffrer votre système de fichiers, sélectionnez l'alias de clé de la clé CMK gérée par le client que vous possédez. Vous pouvez également saisir l'Amazon Resource Name (ARN) d'une clé CMK gérée par le client détenue par un autre compte. Avec une clé CMK gérée par le client dont vous êtes propriétaire, vous contrôlez quels utilisateurs et services peuvent utiliser la clé par le biais de politiques de clé et d'octroi de clés.

Vous pouvez également contrôler la durée de vie et la rotation de ces clés en choisissant quand désactiver, réactiver, supprimer ou révoquer l'accès à celles-ci. Pour de plus amples informations sur la gestion de l'accès aux clés d'autres comptes AWS, consultez [Modification d'une politique de clé](#) dans le Guide du développeur AWS KMS.

Pour de plus amples informations sur la façon de gérer les clés CMK gérées par le client, consultez [Clés principales client](#) (CMK) dans le Guide du développeur AWS KMS.

Les sections suivantes expliquent comment créer un système de fichiers chiffrés à l'aide de l'AWS Management Console et de l'AWS CLI.

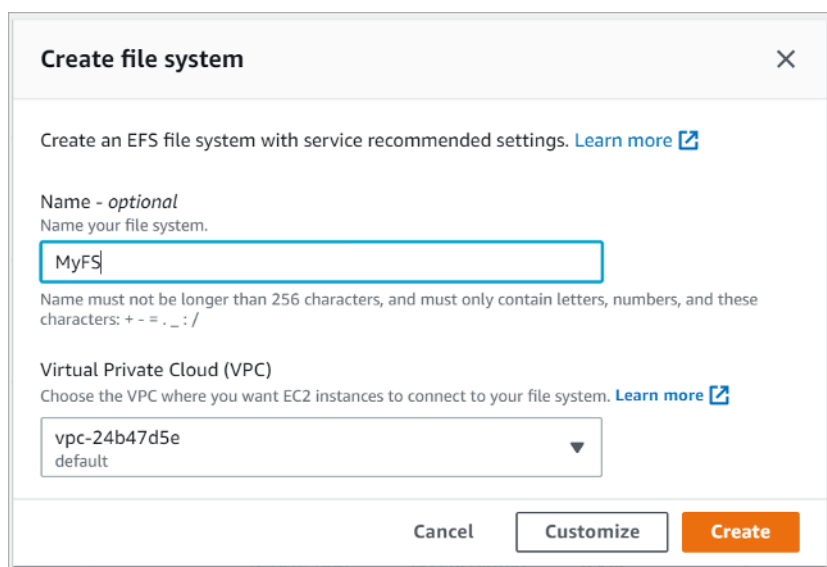
Création d'un système de fichiers chiffrés à l'aide de l'AWS Management Console

Suivez la procédure ci-après pour créer un système de fichiers Amazon EFS chiffrés à l'aide de l'AWS Management Console.

Étape 1. Configurer les paramètres du système de fichiers

Dans cette étape, vous configurez les paramètres généraux du système de fichiers, y compris la gestion du cycle de vie, les modes Performances et Débit, et le chiffrement des données au repos.

1. Connectez-vous à l'AWS Management Console et ouvrez la [console Amazon EFS](#).
2. Choisissez Créer un système de fichiers pour ouvrir la boîte de dialogue Créer un système de fichiers. Pour de plus amples informations sur la création d'un système de fichiers à l'aide des paramètres recommandés qui incluent l'activation du chiffrement par défaut, consultez [Créer votre système de fichiers Amazon EFS](#).



Create file system [X]

Create an EFS file system with service recommended settings. [Learn more](#)

Name - *optional*
Name your file system.

Name must not be longer than 256 characters, and must only contain letters, numbers, and these characters: + - = . _ : /

Virtual Private Cloud (VPC)
Choose the VPC where you want EC2 instances to connect to your file system. [Learn more](#)

Cancel Customize Create

Créer un système de fichiers EFS

3. (Facultatif) Sélectionnez Personnaliser pour créer un système de fichiers personnalisé au lieu de créer un système de fichiers à l'aide des paramètres recommandés par le service.

La page Paramètres du système de fichiers s'affiche.

File system settings

General

Name - *optional*
Name your file system.
MyFS
Name must not be longer than 256 characters, and must only contain letters, numbers, and these characters: + - = . _ : /

Automatic backups
Automatically backup your file system data with AWS Backup using recommended settings. Additional pricing applies. [Learn more](#)

Enable automatic backups

Lifecycle management
Automatically save money as access patterns change by moving files into the EFS Infrequent Access storage class. [Learn more](#)

30 days since last access

Performance mode
Set your file system's performance mode based on IOPS required. [Learn more](#)

General Purpose
Ideal for latency-sensitive use cases, like web serving environments and content management systems

Max I/O
Scale to higher levels of aggregate throughput and operations per second

Throughput mode
Set how your file system's throughput limits are determined. [Learn more](#)

Bursting
Throughput scales with file system size

Provisioned
Throughput fixed at specified amount

Provisioned Throughput (MiB/s)
80
Valid range is 1-1024 MiB/s
Throughput bill can be up to \$480.00/month.

Maximum Read Throughput (MiB/s)
240

Encryption
Choose to enable encryption of your file system's data at rest. Uses the AWS KMS service key (aws/elasticfilesystem) by default. [Learn more](#)

Enable encryption of data at rest

▼ **Customize encryption settings**

KMS key
Choose or input a KMS key ID or ARN to use instead of the AWS KMS service key. [Learn more](#)

🔍 Choose an AWS KMS key or enter an ARN

Create an AWS KMS key

Créer un système de fichiers EFS : paramètres généraux

4. Pour les paramètres généraux, saisissez ce qui suit.

- (Facultatif) Saisissez un Nom pour le système de fichiers.
- Les sauvegardes automatiques sont activées par défaut. Vous pouvez désactiver les sauvegardes automatiques en désactivant la case à cocher. Pour de plus amples informations, consultez [Utilisation d'AWS Backup avec Amazon EFS](#).

- Choisissez une politique de gestion du cycle de vie. La fonction de gestion du cycle de vie Amazon EFS gère automatiquement et de manière économique le stockage de fichiers de vos systèmes de fichiers. Lorsque cette fonction est activée, la gestion du cycle de vie migre les fichiers qui n'ont pas été consultés pendant une période de définie vers la classe de stockage Infrequent Access (IA). Vous définissez cette période à l'aide d'une politique de cycle de vie. Si vous ne souhaitez pas que la gestion du cycle de vie soit activée, choisissez Aucun. Pour de plus amples informations, consultez [Gestion du cycle de vie EFS](#) dans le Guide de l'utilisateur Amazon EFS.
 - Choisissez un mode de performance, soit le mode par défaut Polyvalent ou I/O max. Pour de plus amples informations, consultez [Modes de performance](#) dans le Guide de l'utilisateur Amazon EFS.
 - Choisissez un mode de débit, soit le mode par défaut Transmission en rafales soit Alloué.
 - Si vous avez sélectionné Alloué, le champ Débit alloué (Mio/s) s'affiche. Entrez le débit à allouer pour le système de fichiers. Une fois que vous avez saisi le débit, la console affiche une estimation du coût mensuel en regard du champ. Pour de plus amples informations, consultez [Modes de débit](#) dans le Guide de l'utilisateur Amazon EFS.
 - Dans le champ Chiffrement, le chiffrement des données au repos est activé par défaut. Il utilise votre clé de service EFS AWS Key Management Service (AWS KMS) (`aws/elasticfilesystem`) par défaut. Pour choisir une autre clé KMS à utiliser pour le chiffrement, développez Personnaliser les paramètres de chiffrement et choisissez une clé dans la liste. Vous pouvez également saisir un ID de clé KMS ou un Amazon Resource Name (ARN) pour la clé KMS que vous souhaitez utiliser.
- Si vous devez créer une nouvelle clé, choisissez Création d'une clé AWS KMS pour lancer la console AWS KMS et créer une nouvelle clé.
5. (Facultatif) Choisissez Ajouter une identification pour ajouter des paires clé-valeur à votre système de fichiers.
 6. Choisissez Suivant pour passer à l'étape Accès réseau de la procédure de configuration.

Étape 2. Configurer l'accès réseau

Au cours de cette étape, vous configurez les paramètres réseau du système de fichiers, y compris le Virtual Private Cloud (VPC) et les cibles de montage. Pour chaque cible de montage, définissez la zone de disponibilité, le sous-réseau, l'adresse IP et les groupes de sécurité.

Amazon EFS > File systems > Create

Step 1
File system settings

Step 2
Network access

Step 3 - optional
File system policy

Step 4
Review and create

Network access

Network

Virtual Private Cloud (VPC)
Choose the VPC where you want EC2 instances to connect to your file system. [Learn more](#)

vpc-24b47d5e
default

Mount targets

A mount target provides an NFSv4 endpoint at which you can mount an Amazon EFS file system. We recommend creating one mount target per Availability Zone. [Learn more](#)

Availability zone	Subnet ID	IP address	Security groups	
us-east-1a	subnet-751...	Automatic	Choose secu... sg-1004395a default	Remove
us-east-1b	subnet-16fd...	Automatic	Choose secu... sg-1004395a default	Remove
us-east-1c	subnet-43b...	Automatic	Choose secu... sg-1004395a default	Remove
us-east-1d	subnet-57e...	Automatic	Choose secu... sg-1004395a default	Remove
us-east-1e	subnet-907...	Automatic	Choose secu... sg-1004395a default	Remove
us-east-1f	subnet-6ef0...	Automatic	Choose secu... sg-1004395a default	Remove

Add mount target

You can only create one mount target per Availability Zone.

Cancel Previous **Next**

Créer un système de fichiers EFS : accès au réseau

1. Choisissez le Virtual Private Cloud (VPC) dans lequel vous souhaitez que les instances EC2 se connectent à votre système de fichiers. Pour de plus amples informations, consultez [Gestion de l'accessibilité réseau du système de fichiers](#) du Guide de l'utilisateur Amazon EFS.
 - Zone de disponibilité : par défaut, une cible de montage est configurée dans chaque zone de disponibilité d'une région AWS. Si vous ne voulez pas de cible de montage dans une zone de disponibilité particulière, choisissez Supprimer pour supprimer la cible de montage de cette

zone. Créez une cible de montage dans chaque zone de disponibilité à partir de laquelle vous prévoyez d'accéder à votre système de fichiers. Cette opération n'engendre aucun coût.

- **ID de sous-réseau** : choisissez un des sous-réseaux disponibles dans une zone de disponibilité. Le sous-réseau par défaut est présélectionné. Une bonne pratique consiste à s'assurer que le sous-réseau choisi est public ou privé en fonction de vos exigences de sécurité.
- **Adresse IP** : par défaut, Amazon EFS choisit automatiquement l'adresse IP parmi les adresses disponibles dans le sous-réseau. Vous pouvez également saisir une adresse IP spécifique qui se trouve dans le sous-réseau. Bien que les cibles de montage possèdent une seule adresse IP, ce sont des ressources réseau redondantes et hautement disponibles.
- **Groupes de sécurité** : vous pouvez spécifier un ou plusieurs groupes de sécurité pour la cible de montage. Une bonne pratique consiste à s'assurer que le groupe de sécurité est uniquement utilisé à des fins de montage EFS (port NFS 2049) et que les règles de trafic entrant autorisent uniquement le port 2049 d'une autre plage de blocs d'adresse CIDR VPC ou utilisent le groupe de sécurité comme source pour les ressources qui ont besoin d'accéder à EFS. Pour de plus amples informations, consultez [Utilisation de groupes de sécurité pour les instances Amazon EC2 Instances et les cibles de montage](#) du Guide de l'utilisateur Amazon EFS.

Pour ajouter un autre groupe de sécurité, ou pour modifier le groupe de sécurité, sélectionnez Choisir des groupes de sécurité et ajoutez un autre groupe de sécurité dans la liste. Si vous ne souhaitez pas utiliser le groupe de sécurité par défaut, vous pouvez le supprimer. Pour de plus amples informations, consultez [Création de groupes de sécurité](#) dans le Guide de l'utilisateur Amazon EFS.

2. Choisissez Ajouter une cible de montage pour créer une cible de montage pour une zone de disponibilité qui n'en possède pas. Si une cible de montage est configurée pour chaque zone de disponibilité, ce choix n'est pas disponible.
3. Choisissez Suivant pour continuer. La page Politique de système de fichiers s'affiche.

Étape 3. Créer une politique de système de fichiers

Dans cette étape, vous créez une politique de système de fichiers pour contrôler l'accès du client NFS au système de fichiers. Une politique de système de fichiers EFS est une politique de ressource IAM que vous utilisez pour contrôler l'accès du client NFS au système de fichiers. Pour de plus amples informations, consultez [Utilisation d'IAM pour contrôler l'accès NFS à Amazon EFS](#) dans le Guide de l'utilisateur Amazon EFS.

Créer un système de fichiers EFS : politique de système de fichiers

1. Dans Options de politique, nous vous recommandons de choisir les options de politique préconfigurées disponibles suivantes :
 - Empêcher l'accès racine par défaut
 - Appliquer l'accès en lecture seule par défaut
 - Appliquer le chiffrement en transit pour tous les clients
2. Utilisez Accorder des autorisations supplémentaires pour accorder des autorisations de système de fichiers à d'autres principaux IAM, y compris un autre compte AWS. Choisissez Ajouter, puis saisissez l'ARN de principal de l'entité à laquelle vous accordez des autorisations, puis choisissez les autorisations à accorder.
3. Utilisez l'éditeur de politique pour personnaliser une politique préconfigurée ou pour créer votre propre politique. Lorsque vous choisissez l'une des politiques préconfigurées, la définition de politique JSON apparaît dans l'éditeur de politique.
4. Choisissez Suivant pour continuer. La page Vérifier et créer s'affiche.

Étape 4. Vérifier et créer

Dans cette étape, vous passez en revue les paramètres du système de fichiers, apportez des modifications, puis créez le système de fichiers.

Step 1
File system settings

Step 2
Network access

Step 3 - optional
File system policy

Step 4
Review and create

Review and create

Step 1: File system settings Edit

Field	Value	Is editable?
Name	MyFS	Yes
Performance mode	General Purpose	No
Throughput mode	Provisioned (60 MiB/s)	Yes
Encrypted	Yes	No
KMS Key ID	-	No
Lifecycle policy	AFTER_30_DAYS	Yes
Automatic backups	Yes	Yes
VPC ID	vpc-24b47d5e	Yes

Tags

Tag key	Tag value
EFS-Budget-tag	509

Step 2: Network access Edit

Availability zone	Subnet	IP address	Security groups
us-east-1a	subnet-751c533f	-	sg-1004395a
us-east-1b	subnet-16fd454a	-	sg-1004395a

Step 3: File system policy Edit

File system policy

```

1- {
2-   "Version": "2012-10-17",
3-   "Id": "efs-policy-wizard-e0d80035-a7ac-448d-b2f1-95e76150bace",
4-   "Statement": [
5-     {
6-       "Sid": "efs-statement-763f07ab-0dc4-4d44-a0b5-2e65edc3cc0c",
7-       "Effect": "Allow",
8-       "Principal": {
9-         "AWS": "*"
10-      },
11-      "Action": [
12-        "elasticfilesystem:ClientMount"
13-      ]
14-    },
15-    {
16-       "Sid": "efs-statement-73905941-2fec-4096-840f-3ba69c82c9be",
17-       "Effect": "Deny",
18-       "Principal": {
19-         "AWS": "*"
20-      },
21-       "Action": "*",
22-       "Condition": {
23-         "Bool": {
24-           "aws:SecureTransport": "false"
25-         }
26-       }
27-    }
28-  ]
29- }
```

Cancel Previous Create

Créer un système de fichiers EFS : vérifier et créer

1. Passez en revue chacun des groupes de configuration du système de fichiers. À ce stade, vous pouvez apporter des modifications à chaque groupe en choisissant Modifier.
2. Choisissez Créer pour créer votre système de fichiers et revenir à la page Systèmes de fichiers.
3. La page Systèmes de fichiers affiche le système de fichiers et les détails de sa configuration, comme indiqué dans l'image suivante.

MyFS (fs-6ef8b3ed) [Delete] [Attach]

General [Edit]

Performance mode	Automatic backups
General Purpose	✔ Enabled
Throughput mode	Encrypted
Provisioned (60 MiB/s)	16cddf9a-2e02-42df-ad44-9b2328602f45 (aws/elasticfilesystem)
Lifecycle policy	File system state
AFTER_30_DAYS	✔ Available

Metered size

Total size	
6 KiB	
Size in EFS Standard	
6 KiB (100%)	Size in EFS IA
Size in EFS Infrequent Access (IA)	
0 Bytes (0%)	

Systèmes de fichiers

Création d'un système de fichiers chiffrés à l'aide de l'AWS CLI

Lorsque vous utilisez l'AWS CLI pour créer un système de fichiers chiffrés, vous pouvez utiliser des paramètres supplémentaires pour définir le statut du chiffrement et la clé CMK gérée par le client. Veillez à utiliser la dernière version de l'AWS CLI. Pour de plus amples informations sur la façon de mettre à niveau votre AWS CLI, consultez [Installation, mise à jour et désinstallation de l'AWS CLI](#) dans le Guide de l'utilisateur de l'interface de ligne de commande.

Dans l'opération `CreateFileSystem`, le paramètre `--encrypted` est un booléen et est requis pour créer des systèmes de fichiers chiffrés. `--kms-key-id` est requis uniquement lorsque vous utilisez une clé CMK gérée par le client et que vous incluez l'alias ou l'ARN de la clé. N'incluez pas ce paramètre si vous utilisez la clé CMK gérée par AWS.

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

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

Pour de plus amples informations sur la création de systèmes de fichiers Amazon EFS à l'aide de l'AWS Management Console, de l'AWS CLI, des kits SDK AWS ou de l'API Amazon EFS, consultez [Qu'est-ce qu'Amazon Elastic File System](#) dans le Guide de l'utilisateur Amazon EFS.

Application du chiffrement des données au repos

Le chiffrement a un effet minime sur la latence et le débit des I/O. Le chiffrement et le déchiffrement sont transparents pour les utilisateurs, les applications et les services. Toutes les données et métadonnées sont chiffrées par Amazon EFS en votre nom avant d'être écrites sur le disque et déchiffrées avant d'être lues par les clients. Il n'est pas nécessaire de modifier les outils, les applications ou les services du client pour accéder à un système de fichiers chiffrés.

Votre organisation peut exiger le chiffrement de toutes les données qui répondent à une classification spécifique ou qui sont associées à une application, une charge de travail ou un environnement spécifique. Vous pouvez utiliser des politiques basées sur l'identité [AWS Identity and Access Management \(IAM\)](#) pour appliquer le chiffrement des données au repos pour les ressources de votre système de fichiers Amazon EFS. En utilisant une clé de condition IAM, vous pouvez empêcher les utilisateurs de créer des systèmes de fichiers EFS non chiffrés.

Par exemple, une politique IAM qui autorise explicitement les utilisateurs à créer uniquement des systèmes de fichiers EFS chiffrés utilise la combinaison suivante d'effet, d'action et de condition :

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

L'exemple suivant illustre une politique basée sur l'identité IAM qui autorise les principaux à créer uniquement des systèmes de fichiers chiffrés.

```
{  
  "Version": "2012-10-17",
```

```
“Statement”: [  
  {  
    “Sid”: “VisualEditor0”,  
    “Effect”: “Allow”,  
    “Action”: “elasticfilesystem:CreateFileSystem”,  
    “Condition”: {  
      “Bool”: {  
        “elasticfilesystem:Encrypted”: “true”  
      }  
    },  
    “Resource”: “*”  
  }  
]
```

L'attribut `Resource` défini sur `*` signifie que la politique IAM s'applique à toutes les ressources EFS créées. Vous pouvez ajouter des attributs conditionnels supplémentaires basés sur des identifications afin de les appliquer uniquement pour un sous-ensemble de ressources EFS nécessitant une classification des données.

Vous pouvez également appliquer la création de systèmes de fichiers Amazon EFS chiffrés au niveau d'AWS Organizations en utilisant des stratégies de contrôle des services pour tous les comptes AWS ou unités d'organisation de votre organisation. Pour de plus amples informations sur les stratégies de contrôle des services dans AWS Organizations, consultez [Stratégies de contrôle des services](#) dans le Guide de l'utilisateur AWS Organizations.

Création d'une politique IAM exigeant que tous les systèmes de fichiers EFS soient chiffrés

Vous pouvez créer une politique basée sur l'identité IAM qui autorise les utilisateurs à créer uniquement des systèmes de fichiers Amazon EFS chiffrés à l'aide de la console, de l'AWS CLI ou de l'API. La procédure suivante explique comment créer une telle politique à l'aide de la console IAM, puis appliquer la politique à un utilisateur de votre compte.

Pour créer une politique IAM afin d'appliquer des systèmes de fichiers EFS chiffrés :

1. Connectez-vous à l'AWS Management Console et ouvrez la [console IAM](#).
2. Dans le panneau de navigation, sous Gestion de l'accès, choisissez Politiques.
3. Choisissez Créer une politique pour ouvrir la page Créer une politique.

4. Dans l'onglet Éditeur visuel, saisissez les informations suivantes.
 - Pour Service, choisissez EFS.
 - Pour Actions, saisissez `create` dans le champ de recherche, puis choisissez `CreateFileSystem`.
 - Pour Conditions de demande, cliquez sur le lien Ajouter une condition, recherchez `elasticfilesystem:Encrypted` pour Clé de condition, `Bool` pour Opérateur et `true` pour Valeur.
5. Fournissez un nom et une description pour la politique. Vérifiez le résumé de la politique, y compris la condition de demande chiffrée.
6. Choisissez Créer une politique pour créer la politique.

Pour appliquer la politique à un utilisateur de votre compte :

1. Dans la console IAM, sous Gestion des accès, choisissez Utilisateurs.
2. Sélectionnez l'utilisateur auquel vous souhaitez appliquer la politique.
3. Choisissez Ajouter des autorisations pour afficher la page Ajouter des autorisations.
4. Choisissez Joindre directement les politiques existantes.
5. Saisissez le nom de la politique EFS que vous avez créée au cours de la procédure précédente.
6. Sélectionnez et développez la politique. Choisissez ensuite `{JSON}` pour vérifier le contenu de la politique. Elle doit ressembler à la politique JSON.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "elasticfilesystem:CreateFileSystem",
      "Condition": {
        "Bool": {
          "elasticfilesystem:Encrypted": "true"
        }
      },
      "Resource": "*"
    }
  ]
}
```

Détection des systèmes de fichiers non chiffrés

Votre organisation peut avoir besoin d'identifier les ressources Amazon EFS qui ne sont pas chiffrées. Vous pouvez détecter les systèmes de fichiers non chiffrés à l'aide des règles gérées par AWS Config. AWS Config fournit des règles gérées par AWS. Il s'agit de règles personnalisables et prédéfinies utilisées par AWS Config pour évaluer la conformité des ressources AWS de votre compte avec les bonnes pratiques courantes et identifier les ressources qui ne respectent pas les règles comme NON_CONFORMES.

Vous pouvez utiliser la règle gérée par AWS Config `efs-encrypted-check` pour vérifier si Amazon Elastic File System (Amazon EFS) est configuré pour chiffrer les données des fichiers à l'aide d'AWS Key Management Service (AWS KMS). Pour de plus amples informations sur la configuration et l'activation des règles gérées par AWS, consultez [Utilisation des règles gérées par AWS Config](#).

Chiffrement des données en transit

Vous pouvez monter un système de fichiers de telle sorte que tout le trafic NFS soit chiffré en transit à l'aide du protocole TLS (Transport Layer Security) 1.2 avec un cipher AES-256 conforme aux normes de l'industrie. TLS est un ensemble de protocoles cryptographiques standard utilisés pour chiffrer les informations échangées sur le réseau. AES-256 est un cipher de chiffrement 256 bits utilisé pour la transmission de données dans TLS. Nous vous recommandons de configurer le chiffrement en transit sur chaque client accédant au système de fichiers.

Vous pouvez utiliser des politiques IAM pour appliquer le chiffrement en transit pour l'accès du client NFS à Amazon EFS. Lorsqu'un client se connecte à un système de fichiers, Amazon EFS évalue la politique de ressources IAM du système de fichiers (appelée « politique de système de fichiers ») ainsi que les politiques IAM basées sur l'identité afin de déterminer les autorisations d'accès au système de fichiers appropriées à accorder. Vous pouvez utiliser la clé de condition `aws:SecureTransport` dans la politique de ressources du système de fichiers pour obliger les clients NFS à utiliser TLS lors de la connexion à un système de fichiers EFS.

Note

Vous devez utiliser l'assistant de montage EFS pour monter vos systèmes de fichiers Amazon EFS afin d'utiliser l'autorisation IAM pour contrôler l'accès par les clients NFS. Pour de plus amples informations, consultez [Montage avec l'autorisation IAM](#) dans le Guide de l'utilisateur Amazon EFS.

L'exemple de politique de système de fichiers EFS suivant applique le chiffrement en transit et présente les caractéristiques suivantes :

- Le effect est `allow`.
- Le mandataire est défini sur `*` pour toutes les entités IAM.
- L'action est définie sur `ClientMount`, `ClientWrite` et `ClientRootAccess`.
- La condition d'octroi des autorisations est définie sur `SecureTransport`. Seuls les clients NFS utilisant TLS pour se connecter au système de fichiers peuvent y accéder.

```
{  
  "Version": "2012-10-17",
```



```
    "Id": "ExamplePolicy01",
    "Statement": [
      {
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Principal": {
          "AWS": "*"
        },
        "Action": [
          "elasticfilesystem:ClientRootAccess",
          "elasticfilesystem:ClientMount",
          "elasticfilesystem:ClientWrite"
        ],
        "Condition": {
          "Bool": {
            "aws:SecureTransport": "true"
          }
        }
      }
    ]
  }
}
```

Vous pouvez créer une politique de système de fichiers à l'aide de la console Amazon EFS ou de l'AWS CLI.

Pour créer une politique de système de fichiers à l'aide de la console EFS :

1. Ouvrez la [console Amazon EFS](#).
2. Choisissez Systèmes de fichiers.
3. Sur la page Systèmes de fichiers, choisissez le système de fichiers pour lequel vous souhaitez créer une politique de système de fichiers. La page de détails de ce système de fichiers s'affiche.
4. Choisissez Politique de système de fichiers, puis Modifier. La page Politique du système de fichiers s'affiche.

File system policy

Policy options

Select one or more of these common policy options, or create a custom policy using the editor. [Learn more](#)

- Prevent root access by default*
- Enforce read-only access by default*
- Prevent anonymous access
- Enforce in-transit encryption for all clients

* Identity-based policies can override these default permissions.

► [Grant additional permissions](#)

Policy editor {JSON}

Clear

```
1 {
2   "Version": "2012-10-17",
3   "Id": "efs-policy-wizard-0c7665fa-5293-4f5c-97eb-2e42299b4597",
4   "Statement": [
5     {
6       "Sid": "efs-statement-78c057ae-6438-4a40-992e-2e96efe3307f",
7       "Effect": "Allow",
8       "Principal": {
9         "AWS": "*"
10      },
11      "Action": [
12        "elasticfilesystem:ClientMount"
13      ],
14      "Condition": {
15        "Bool": {
16          "elasticfilesystem:AccessedViaMountTarget": "true"
17        }
18      }
19    },
20    {
21      "Sid": "efs-statement-4c8a90fd-610e-4c4f-925d-e9bd1513efed",
22      "Effect": "Deny",
23      "Principal": {
24        "AWS": "*"
25      },
26      "Action": "*",
27      "Condition": {
28        "Bool": {
29          "aws:SecureTransport": "false"
30        }
31      }
32    }
33  ]
34 }
```

Manual changes will prevent the use of the policy options on the left until the editor is cleared.

Cancel **Save**

Créer une politique de système de fichiers

- Dans Options de politique, nous vous recommandons de choisir les options de politique préconfigurées disponibles suivantes :
 - Empêcher l'accès racine par défaut
 - Appliquer l'accès en lecture seule par défaut
 - Appliquer le chiffrement en transit pour tous les clients

Si vous choisissez une politique préconfigurée, l'objet JSON de politique s'affiche dans le panneau Éditeur de politique.

- Utilisez [Accorder des autorisations supplémentaires](#) pour accorder des autorisations de système de fichiers à d'autres principaux IAM, y compris un autre compte AWS. Choisissez [Ajouter](#), puis saisissez l'ARN de principal de l'entité à laquelle vous accordez des autorisations, puis choisissez les autorisations à accorder.

7. Utilisez l'éditeur de politique pour personnaliser une politique préconfigurée ou pour créer votre propre politique. Lorsque vous utilisez l'éditeur, les options de stratégie préconfigurées deviennent indisponibles. Pour annuler vos modifications de politique, choisissez Effacer.

Lorsque vous effacez l'éditeur, les stratégies préconfigurées redeviennent disponibles.

8. Après avoir terminé la modification ou la création de la politique, choisissez Enregistrer.

La page de détails du système de fichiers s'affiche et présente la politique dans Politique de système de fichiers.

Vous pouvez également créer une politique de système de fichiers par programmation en utilisant directement AWS CloudFormation, les kits SDK AWS ou l'API Amazon EFS. Pour de plus amples informations sur la création de politiques de système de fichiers, consultez [Création de politiques de système de fichiers](#) dans le Guide de l'utilisateur Amazon EFS.

Configuration du chiffrement des données en transit

Pour configurer le chiffrement des données en transit, nous vous recommandons de télécharger l'assistant de montage EFS sur chaque client. L'assistant de montage EFS est un utilitaire open source fourni par AWS pour simplifier l'utilisation d'EFS, y compris la configuration du chiffrement des données en transit. L'assistant de montage utilise les options de montage recommandées par EFS par défaut.

L'assistant de montage EFS est pris en charge sur les distributions Linux suivantes :

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

Pour configurer le chiffrement des données en transit :

1. Installez l'assistant de montage EFS :
 - Pour Amazon Linux, utilisez cette commande :

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

- Pour les autres distributions Linux, téléchargez depuis GitHub et installez.

Le package `amazon-efs-utils` installe automatiquement les dépendances suivantes : client NFS (`nfs-utils`), relais réseau (`stunnel`), OpenSSL et Python.

2. Montez le système de fichiers :

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

- `mount -t efs` appelle l'assistant de montage EFS.
- L'utilisation du nom DNS du système de fichiers ou de l'adresse IP d'une cible de montage n'est pas prise en charge lors du montage à l'aide de l'assistant de montage EFS, utilisez plutôt l'ID du système de fichiers.
- L'assistant de montage EFS utilise les options de montage recommandées par AWS par défaut. Il n'est pas recommandé de remplacer ces options de montage par défaut, mais nous offrons la flexibilité nécessaire pour le faire lorsque l'occasion se présente. Nous vous recommandons de tester minutieusement les remplacements d'options de montage afin de comprendre l'impact de ces modifications sur l'accès et les performances du système de fichiers.
- Le tableau suivant représente les options de montage par défaut utilisées par l'assistant de montage EFS.

Option	Description			
<code>nfsvers=4.1</code>	Version du protocole NFS			
<code>rsize=1048576</code>	Nombre maximal d'octets de données que le client NFS peut recevoir			

Option	Description			
	pour chaque demande READ du réseau			
wsiz=1048576	Nombre maximal d'octets de données que le client NFS peut envoyer pour chaque demande WRITE du réseau			
hard	Comportement de récupération du client NFS après qu'une demande NFS a expiré, de sorte que les demandes NFS sont relancées indéfiniment jusqu'à ce que le serveur réponde			

Option	Description			
timeo=600	Valeur de délai d'expiration que le client NFS utilise pour attendre une réponse avant de relancer une demande NFS en décisecon des			
retrans=2	Nombre de fois que le client NFS essaie une demande avant de tenter une action de récupération			
noresvport	Indique au client NFS d'utiliser un nouveau port source TCP lorsqu'une connexion réseau est rétablie			

- Ajoutez la ligne suivante à `/etc/fstab` pour remonter automatiquement votre système de fichiers après tout redémarrage du système.

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

Utilisation du chiffrement des données en transit

Si votre organisation est soumise à des politiques d'entreprise ou réglementaires qui exigent le chiffrement des données en transit, nous vous recommandons d'utiliser le chiffrement des données en transit sur chaque client accédant au système de fichiers. Le chiffrement et le déchiffrement sont configurés au niveau de la connexion et ajoutent une couche de sécurité supplémentaire.

Le montage du système de fichiers à l'aide de l'assistant de montage EFS permet de configurer et de maintenir un tunnel TLS 1.2 entre le client et Amazon EFS, et d'acheminer tout le trafic NFS sur ce tunnel chiffré. Le certificat utilisé pour établir la connexion TLS chiffrée est signé par l'autorité de certification Amazon (CA) et approuvé par la plupart des distributions Linux modernes. L'assistant de montage EFS génère également un processus de surveillance pour contrôler tous les tunnels sécurisés vers chaque système de fichiers et s'assurer qu'ils sont en cours d'exécution.

Après avoir utilisé l'assistant de montage EFS pour établir des connexions chiffrées à Amazon EFS, aucune autre saisie ou configuration de l'utilisateur n'est requise. Le chiffrement est transparent pour les connexions utilisateur et les applications accédant au système de fichiers.

Après avoir monté et établi une connexion chiffrée à un système de fichiers EFS à l'aide de l'assistant de montage EFS, la sortie d'une commande de montage indique que le système de fichiers est monté et qu'un tunnel chiffré a été établi en utilisant l'hôte local (127.0.0.1) comme relais réseau. Consultez l'exemple de sortie suivant.

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

Pour mapper un `efs-mount-point` à un système de fichiers EFS, effectuez une requête sur le fichier `mount.log` dans `/var/log/amazon/efs` et recherchez la dernière opération de montage réussie. La simple commande `grep` suivante permet de le faire.

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

La sortie de cette commande `grep` renvoie le nom DNS du système de fichiers EFS monté. Consultez l'exemple de sortie ci-dessous.

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


Conclusion

Les données du système de fichiers Amazon EFS peuvent être chiffrées au repos et en transit. Vous pouvez chiffrer les données au repos à l'aide de clés CMK que vous pouvez contrôler et gérer à l'aide d'AWS KMS. Pour créer un système de fichiers chiffrés, il suffit de cocher une case dans l'assistant de création de système de fichiers Amazon EFS dans l'AWS Management Console ou d'ajouter un seul paramètre à l'opération `CreateFileSystem` dans l'AWS CLI, les kits SDK AWS ou l'API Amazon EFS.

Vous pouvez appliquer le chiffrement au repos et en transit à l'aide des politiques basées sur l'identité et des politiques de système de fichiers AWS IAM pour renforcer davantage vos exigences de sécurité et vous aider à répondre à vos besoins de conformité. L'utilisation d'un système de fichiers chiffrés est également transparente pour les services, les applications et les utilisateurs, avec un impact minimal sur les performances du système de fichiers. Vous pouvez chiffrer les données en transit à l'aide de l'assistant de montage EFS pour établir un tunnel TLS chiffré sur chaque client, en chiffrant tout le trafic NFS entre le client et le système de fichiers EFS monté. L'application du chiffrement des données Amazon EFS au repos à l'aide de politiques d'identité IAM et en transit à l'aide de politiques de système de fichiers EFS est disponible sans coût supplémentaire.

Ressources

- [Livre blanc Détails cryptographiques AWS KMS](#)
- [Guide de l'utilisateur Amazon EFS](#)

Historique du document et participants

Historique du document

Pour être informé des mises à jour de ce livre blanc, abonnez-vous au flux RSS.

update-history-change	update-history-description	update-history-date
Mises à jour mineures	Mise en page ajustée	30 avril 2021
Livre blanc mis à jour	Ajout de l'application du chiffrement au repos et en transit à l'aide d'IAM	22 février 2021
Livre blanc mis à jour	Ajout du chiffrement des données en transit	1 avril 2018
Publication initiale	Chiffrer les données au repos avec Amazon EFS Encrypted File Systems publié	1 septembre 2017

Note

Pour vous abonner aux mises à jour RSS, vous devez activer un plug-in RSS pour le navigateur que vous utilisez.

Participants

Ont participé à la préparation du présent document :

- Darryl S. Osborne, spécialiste du stockage, architecte de solutions, AWS
- Joseph Travaglini, Senior Product Manager, Amazon EFS
- Peter Buonora, architecte de solutions principal, AWS

- Siva Rajamani, architecte de solutions senior, AWS