aws

Guide de l'utilisateur ONTAP

FSx pour ONTAP

FSx pour ONTAP: Guide de l'utilisateur ONTAP

Table of Contents

Qu'est-ce qu'Amazon FSx for NetApp ONTAP ?

Amazon FSx for NetApp ONTAP est un service entièrement géré qui fournit un stockage de fichiers hautement fiable, évolutif, performant et riche en fonctionnalités, basé sur NetApp le célèbre système de fichiers ONTAP. FSx for ONTAP combine les fonctionnalités, les performances, les capacités et les opérations d'API habituelles des systèmes de NetApp fichiers avec l'agilité, l'évolutivité et la simplicité d'un système entièrement géré. Service AWS

FSx for ONTAP fournit un stockage de fichiers partagé riche en fonctionnalités, rapide et flexible, largement accessible à partir d'instances de calcul Linux, Windows et macOS exécutées sur site ou sur site. AWS FSx for ONTAP propose un stockage sur disque SSD (Solid State Drive) à hautes performances avec des latences inférieures à la milliseconde. Avec FSx for ONTAP, vous pouvez atteindre les niveaux de performance des SSD adaptés à votre charge de travail tout en ne payant pour le stockage SSD que pour une petite partie de vos données.

La gestion de vos données avec FSx for ONTAP est plus simple car vous pouvez créer un instantané, cloner et répliquer vos fichiers en un seul clic. En outre, FSx for ONTAP hiérarchise automatiquement vos données vers un stockage élastique à moindre coût, ce qui vous évite d'avoir à provisionner ou à gérer des capacités.

FSx for ONTAP fournit également un stockage hautement disponible et durable avec des sauvegardes entièrement gérées et un support pour la reprise après sinistre entre régions. Pour faciliter la protection et la sécurisation de vos données, FSx for ONTAP prend en charge les applications antivirus et de sécurité des données les plus populaires.

Pour les clients qui utilisent NetApp ONTAP sur site, FSx for ONTAP est une solution idéale pour migrer, sauvegarder ou transférer en rafale vos applications basées sur des fichiers depuis le local vers le site AWS sans qu'il soit nécessaire de modifier le code de votre application ou la façon dont vous gérez vos données.

En tant que service entièrement géré, FSx for ONTAP facilite le lancement et le dimensionnement d'un stockage de fichiers partagé fiable, performant et sécurisé dans le cloud. Avec FSx for ONTAP, vous n'avez plus à vous soucier de :

- Configuration et provisionnement de serveurs de fichiers et de volumes de stockage
- Réplication des données
- Installation de logiciels de serveur de fichiers et application de correctifs

- Détection et résolution des défaillances matérielles
- Gestion du basculement et du retour en arrière
- Exécution manuelle de sauvegardes

FSx for ONTAP fournit également une intégration riche avec d'autres AWS services, tels que AWS Identity and Access Management (IAM), Amazon WorkSpaces, AWS Key Management Service (AWS KMS) et. AWS CloudTrail

Rubriques

Caractéristiques de FSx for ONTAP

Avec FSx for ONTAP, vous bénéficiez d'une solution de stockage de fichiers entièrement gérée avec :

- Support pour les ensembles de données de plusieurs pétaoctets dans un espace de noms unique
- Jusqu'à des dizaines de gigaoctets par seconde (Gbit/s) de débit par système de fichiers
- Accès multiprotocole aux données à l'aide des protocoles NFS (Network File System), SMB (Server Message Block) et iSCSI (Internet Small Computer Systems Interface)
- Options de déploiement multi-AZ et mono-AZ hautement disponibles et durables
- Hiérarchisation automatique des données qui réduit les coûts de stockage en transférant automatiquement les données rarement consultées vers un niveau de stockage moins coûteux en fonction de vos modèles d'accès
- Compression, déduplication et compactage des données pour réduire votre consommation de stockage
- Support pour NetApp la fonctionnalité SnapMirror de réplication
- Support pour les solutions NetApp de mise en cache sur site : NetApp Global File Cache et FlexCache

- Support pour l'accès et la gestion à l'aide d' NetApp outils natifs AWS ou d'opérations d'API
  - AWS Management Console, AWS Command Line Interface (AWS CLI) et SDK
  - NetApp CLI ONTAP, API REST et BlueXP
- Support pour les fonctionnalités de protection et de sécurité des données suivantes :
  - Chiffrement des données du système de fichiers et des sauvegardes au repos à l'aide de AWS KMS keys
  - Chiffrement des données en transit à l'aide des clés de session Kerberos SMB
  - Analyse antivirus à la demande
  - Authentification et autorisation à l'aide de Microsoft Active Directory
  - Audit d'accès aux fichiers
  - NetAppSnapLockFonctionnalité WORM avec prise en charge des volumes Compliance et Enterprise

Sécurité et protection des données

Amazon FSx fournit plusieurs niveaux de sécurité et de conformité pour faciliter la protection de vos données. Il chiffre automatiquement les données inactives dans les systèmes de fichiers et les sauvegardes à l'aide de clés que vous gérez dans AWS Key Management Service (AWS KMS). Vous pouvez également chiffrer les données en transit à l'aide de Kerberos pour les clients NFS et SMB.

Amazon FSx a été évalué comme étant conforme aux normes suivantes :

- Organisation internationale de normalisation (ISO)
- Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)
- Certifications de contrôle des systèmes et des organisations (SOC)
- Loi de 1996 sur la portabilité et la responsabilité de l'assurance maladie (HIPAA)

Pour plus d’informations, consultez Protection des données dans Amazon FSx pour ONTAP NetApp .

Amazon FSx fournit également les niveaux de contrôle d'accès suivants :

- Au niveau du système de fichiers, Amazon FSx fournit un contrôle d'accès en utilisant les groupes de sécurité Amazon Virtual Private Cloud (Amazon VPC).
- Au niveau de l'API, Amazon FSx fournit un contrôle d'accès en utilisant des politiques d'accès AWS Identity and Access Management (IAM).

- Pour fournir un contrôle d'accès au niveau des fichiers et des dossiers, Amazon FSx prend en charge les autorisations Unix, les listes de contrôle d'accès (ACL) NFS et les ACL NTFS. Lorsque vous associez Amazon FSx à un Active Directory, les utilisateurs qui accèdent à des systèmes de fichiers peuvent s'authentifier à l'aide de leurs informations d'identification Active Directory.

Afin que vous puissiez voir les actions entreprises par les utilisateurs sur vos ressources Amazon FSx, Amazon FSx s'intègre AWS CloudTrail pour surveiller et consigner vos appels d'API Amazon FSx. Pour plus d’informations, consultez Enregistrement de FSx pour les appels d'API ONTAP avecAWS CloudTrail.

En outre, Amazon FSx protège vos données grâce à des sauvegardes de systèmes de fichiers extrêmement durables. Amazon FSx effectue des sauvegardes quotidiennes automatiques, et vous pouvez effectuer des sauvegardes supplémentaires à tout moment. Pour plus d’informations, consultez Protection de vos données.

Tarification de FSx for ONTAP

Les systèmes de fichiers vous sont facturés selon les catégories suivantes :

- Capacité de stockage SSD (par gigaoctet par mois ou Go par mois)
- Nombre d'IOPS sur SSD que vous provisionnez au-dessus de trois IOPS/Go (par IOPS par mois)
- Capacité de débit (par mégaoctets par seconde [Mb/s] -mois)
- Consommation de stockage du pool de capacité (par Go par mois)
- Demandes de pool de capacités (par lecture et écriture)
- Consommation de stockage de sauvegarde (par Go par mois)

Pour plus d'informations sur la tarification et les frais associés au service, consultez Amazon FSx pour la tarification NetApp ONTAP.

Forums FSx pour ONTAP

Si vous rencontrez des problèmes lors de l'utilisation d'Amazon FSx, utilisez les forums de discussion FSx for ONTAP pour obtenir des réponses.

Utilisez-vous Amazon FSx pour la première fois ?

Si vous utilisez Amazon FSx pour la première fois, nous vous recommandons de lire les sections suivantes dans l'ordre :

1. Si vous êtes nouveau dans le AWS domaine, Configuration de FSx pour ONTAP voir pour configurer un Compte AWS.
2. Si vous êtes prêt à créer votre premier système de fichiers Amazon FSx, suivez les instructions figurant dans. Commencer à utiliser Amazon FSx pour ONTAP NetApp
3. Pour plus d'informations sur les performances, consultez Amazon FSx pour NetApp les performances d'ONTAP.
4. Pour plus d'informations sur la sécurité d'Amazon FSx, consultez. Sécurité dans Amazon FSx pour ONTAP NetApp
5. Pour plus d'informations sur l'API Amazon FSx, consultez le manuel Amazon FSx API Reference.

Comment fonctionne Amazon FSx pour NetApp ONTAP

Cette rubrique présente les principales fonctionnalités d'Amazon FSx pour les systèmes de fichiers NetApp ONTAP et leur fonctionnement, avec des liens vers des sections contenant des descriptions détaillées, des détails d'implémentation importants et step-by-step des procédures de configuration.

Rubriques

Systèmes de fichiers FSx pour ONTAP

Un système de fichiers est la principale ressource FSx pour ONTAP, à l'instar d'un cluster ONTAP sur site. NetApp Vous spécifiez la capacité de stockage et le débit du disque SSD (Solid State Drive) pour votre système de fichiers, puis vous choisissez un Amazon Virtual Private Cloud (VPC) dans lequel votre système de fichiers est créé. Pour plus d'informations, consultez Gestion de FSx pour les systèmes de fichiers ONTAP.

Votre système de fichiers peut comporter une à 12 paires de haute disponibilité (HA) en fonction de sa configuration. Une paire HA est composée de deux serveurs de fichiers dans une configuration active en veille. Les systèmes de fichiers dotés d'une seule paire HA sont appelés systèmes de fichiers scale-up. Les systèmes de fichiers comportant plusieurs paires HA sont appelés systèmes de fichiers scale-out. Pour plus d'informations, consultez Paires à haute disponibilité (HA).

Machines virtuelles de stockage

Une machine virtuelle de stockage (SVM) est un serveur de fichiers isolé doté de ses propres points de terminaison administratifs et d'accès aux données pour administrer et accéder aux données. Lorsque vous accédez aux données de votre système de fichiers FSx for ONTAP, vos clients et

postes de travail interagissent avec une SVM en utilisant l'adresse IP du point de terminaison de la SVM. Pour plus d'informations, consultez Gestion des SVM.

Vous pouvez associer des SVM à un répertoire Microsoft Active Directory pour l'authentification et l'autorisation d'accès aux fichiers. Pour plus d'informations, consultez Utilisation de Microsoft Active Directory dans FSx pour ONTAP.

Volumes

Les volumes FSx for ONTAP sont des ressources virtuelles que vous utilisez pour organiser et regrouper vos données. Les volumes sont des conteneurs logiques hébergés sur des SVM et les données qui y sont stockées consomment de la capacité de stockage physique de votre système de fichiers.

Lorsque vous créez un volume, vous définissez sa taille, qui détermine la quantité de données physiques que vous pouvez y stocker, quel que soit le niveau de stockage sur lequel les données sont stockées. Vous définissez également le type de volume, soit RW (lecture-écriture) soit DP (protection des données). Un volume DP est en lecture seule et peut être utilisé comme destination dans une relation NetApp SnapMirror or SnapVault .

Les volumes FSx for ONTAP sont dotés d'un provisionnement léger, ce qui signifie qu'ils ne consomment de la capacité de stockage que pour les données qui y sont stockées. Dans le cas de volumes à provisionnement léger, la capacité de stockage n'est pas réservée à l'avance. Au lieu de cela, le stockage est alloué de manière dynamique, selon les besoins. L'espace libre est libéré dans le système de fichiers lorsque les données du volume ou du LUN sont supprimées. Par exemple, vous pouvez créer trois volumes de 10 TiB sur un système de fichiers configuré avec une capacité de stockage libre de 10 TiB, à condition que la quantité totale de données stockées dans les trois volumes ne dépasse à aucun moment 10 TiB. La quantité de données physiquement stockées sur un volume est prise en compte dans votre consommation globale de capacité de stockage. Pour plus d'informations, consultez Gestion de FSx pour les volumes ONTAP.

Niveaux de stockage

Un système de fichiers FSx for ONTAP comporte deux niveaux de stockage : le stockage principal et le stockage par pool de capacité. Le stockage principal est un stockage SSD haute performance, évolutif et provisionné spécialement conçu pour la partie active de votre ensemble de données. Le stockage en pool de capacité est un niveau de stockage entièrement élastique qui peut atteindre des pétaoctets et dont les coûts sont optimisés pour les données rarement consultées. Les données que

vous écrivez sur vos volumes consomment de la capacité sur vos niveaux de stockage. Pour plus d'informations, consultez niveaux de stockage FSx pour ONTAP.

Mise à niveau des données

La hiérarchisation des données est le processus par lequel Amazon FSx NetApp for ONTAP déplace automatiquement les données entre le SSD et les niveaux de stockage du pool de capacité. Chaque volume dispose d'une politique de hiérarchisation qui contrôle si les données sont déplacées vers le niveau de capacité lorsqu'elles deviennent inactives (froides). La période de refroidissement de la politique de hiérarchisation d'un volume détermine le moment où les données deviennent inactives (froides). Pour plus d'informations, consultez Hiérarchisation des données de volume.

Efficacité du stockage

Amazon FSx for NetApp ONTAP prend en charge les fonctionnalités d'efficacité du stockage au niveau des blocs d'ONTAP (compactage, compression et déduplication) afin de réduire la capacité de stockage consommée par vos données. Les fonctionnalités d'efficacité du stockage peuvent réduire l'encombrement de vos données dans le stockage SSD, le stockage en pool de capacité et les sauvegardes. Les économies de capacité de stockage typiques pour les charges de travail de partage de fichiers à usage général sans pour autant sacrifier les performances sont de 65 % grâce à la compression, à la déduplication et au compactage, à la fois sur les niveaux de stockage SSD et sur le pool de capacité. Pour plus d'informations, consultez FSx pour l'efficacité du stockage ONTAP.

Accès aux données stockées sur les systèmes de fichiers FSx for ONTAP

Vous pouvez accéder à vos données sur les volumes FSx for ONTAP à partir de plusieurs clients Linux, Windows ou macOS simultanément via les protocoles NFS (v3, v4, v4.1, v4.2) et SMB. Vous pouvez également accéder aux données à l'aide du protocole iSCSI (bloc). Pour plus d'informations, consultez Accès aux données .

Gestion des ressources FSx pour ONTAP

Il existe plusieurs manières d'interagir avec votre système de fichiers FSx for ONTAP et de gérer ses ressources. Vous pouvez gérer vos ressources FSx for ONTAP à l'aide des deux outils de gestion AWS et d' NetApp ONTAP :

- AWS outils de gestion
  - Le AWS Management Console
  - Le AWS Command Line Interface (AWS CLI)
  - L'API et les kits de développement logiciel Amazon FSx
  - AWS CloudFormation
- NetApp outils de gestion :
  - NetApp Blue XP
  - La NetApp CLI ONTAP
  - L'API REST NetApp ONTAP

Pour plus d'informations, voir Administration des ressources.

Configuration de FSx pour ONTAP

Avant d'utiliser Amazon FSx pour la première fois, effectuez les tâches suivantes :

1. Inscrivez-vous pour un Compte AWS
2. Création d'un utilisateur doté d'un accès administratif

Rubriques

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique en matière de sécurité consiste à attribuer un accès administratif à un utilisateur et à n'utiliser que l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Une fois que vous vous êtes inscrit à un utilisateur administratif Compte AWS, que vous Utilisateur racine d'un compte AWS l'avez sécurisé AWS IAM Identity Center, que vous l'avez activé et que vous en avez créé un, afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, consultez la section Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

   Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.
2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, consultez la section Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

Étape suivante

Pour commencer à utiliser FSx for ONTAP, consultez Commencer à utiliser Amazon FSx pour ONTAP NetApp les instructions pour créer vos ressources Amazon FSx.

Commencer à utiliser Amazon FSx pour ONTAP NetApp

Découvrez comment commencer à utiliser Amazon FSx pour NetApp ONTAP. Cet exercice de mise en route comprend les étapes suivantes.

Rubriques

Étape 1 : créer un système de fichiers Amazon FSx pour NetApp ONTAP

La console Amazon FSx propose deux options pour créer un système de fichiers : une option de création rapide et une option de création standard. Pour créer rapidement et facilement un système de fichiers Amazon FSx for NetApp ONTAP avec la configuration recommandée par le service, utilisez l'option de création rapide.

L'option de création rapide crée un système de fichiers composé d'une seule paire haute disponibilité (HA), d'une seule machine virtuelle de stockage (SVM) et d'un seul volume. L'option de création rapide configure ce système de fichiers pour autoriser l'accès aux données à partir d'instances Linux via le protocole NFS (Network File System). Une fois votre système de fichiers créé, vous pouvez créer des SVM et des volumes supplémentaires selon vos besoins, y compris une SVM jointe à un Active Directory pour permettre aux clients Windows et macOS d'y accéder via le protocole SMB (Server Message Block).

Pour plus d'informations sur l'utilisation de l'option de création standard pour créer un système de fichiers avec une configuration personnalisée, et sur l'utilisation de l'API AWS CLI and, consultezCréation de FSx pour les systèmes de fichiers ONTAP.

Pour créer votre système de fichiers .

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans Sur le tableau de bord, choisissez Create file system (Créer un système de fichiers) pour ouvrir l'assistant de création de système de fichiers.

3. Sur la page Sélectionner le type de système de fichiers, choisissez Amazon FSx pour NetApp ONTAP, puis Next. La page Créer un système de fichiers ONTAP apparaît.
4. Pour Méthode de création, choisissez Création rapide.
5. Dans la section Configuration rapide, pour Nom du système de fichiers - facultatif, entrez le nom de votre système de fichiers. Il est plus facile de trouver et de gérer vos systèmes de fichiers lorsque vous les nommez. Vous pouvez utiliser un maximum de 256 lettres Unicode, espaces blancs et chiffres, plus les caractères spéciaux suivants : + - (tiret) =. _ (soulignement) :/
6. Pour le type de déploiement, choisissez Multi-AZ ou Single-AZ.

   - Les systèmes de fichiers multi-AZ répliquent vos données et prennent en charge le basculement entre plusieurs zones de disponibilité au même endroit. Région AWS
   - Les systèmes de fichiers mono-AZ répliquent vos données et offrent un basculement automatique au sein d'une seule zone de disponibilité.

   Pour plus d'informations, consultez Disponibilité et durabilité.
7. Pour la capacité de stockage SSD, spécifiez la capacité de stockage de votre système de fichiers, en gibioctets (GiB). Entrez un nombre entier compris entre 1 024 et 196 608. Si vous avez besoin d'une plus grande capacité de stockage SSD, vous pouvez utiliser la création standard. Pour plus d'informations, consultez Pour créer un système de fichiers (console).

   Vous pouvez augmenter la capacité de stockage selon vos besoins à tout moment après avoir créé le système de fichiers. Pour plus d'informations, consultez Gestion de la capacité de stockage.
8. Pour ce qui est de la capacité de débit, Amazon FSx fournit automatiquement une capacité de débit recommandée en fonction de votre stockage SSD. Vous pouvez également choisir le débit de votre système de fichiers (jusqu'à 4 096 Mo/s). Si vous avez besoin d'une plus grande capacité de débit, vous pouvez utiliser Standard Create.
9. Pour Virtual Private Cloud (VPC), choisissez l'Amazon VPC que vous souhaitez associer à votre système de fichiers.
10. Pour l'efficacité du stockage, choisissez Activé pour activer les fonctionnalités d'efficacité du stockage ONTAP (compression, déduplication et compactage) ou Désactivé pour les désactiver.
11. (Multi-AZ uniquement) La plage d'adresses IP du point de terminaison indique la plage d'adresses IP dans laquelle sont créés les points de terminaison permettant d'accéder à votre système de fichiers.

Choisissez une option de création rapide pour la plage d'adresses IP du point de terminaison :

- Plage d'adresses IP non allouée depuis votre VPC — Choisissez cette option pour qu'Amazon FSx utilise les 64 dernières adresses IP de la plage d'adresses CIDR principale du VPC comme plage d'adresses IP de point de terminaison pour le système de fichiers. Notez que cette plage est partagée entre plusieurs systèmes de fichiers si vous sélectionnez cette option plusieurs fois.

  > **Note**
  >
  > - Chaque système de fichiers que vous créez consomme deux adresses IP de cette plage : une pour le cluster et une pour la première SVM. Les première et dernière adresses IP sont également réservées. Pour chaque SVM supplémentaire, le système de fichiers consomme une autre adresse IP. Par exemple, un système de fichiers hébergeant 10 SVM utilise 11 adresses IP. Les systèmes de fichiers supplémentaires fonctionnent de la même manière. Ils consomment les deux adresses IP initiales, plus une pour chaque SVM supplémentaire. Le nombre maximum de systèmes de fichiers utilisant la même plage d'adresses IP, dotés chacun d'une seule SVM, est de 31.
  > - Cette option est grisée si l'une des 64 dernières adresses IP de la plage CIDR principale d'un VPC est utilisée par un sous-réseau.

- Plage d'adresses IP flottantes en dehors de votre VPC — Choisissez cette option pour qu'Amazon FSx utilise une plage d'adresses 198.19.x.0/24 qui n'est pas déjà utilisée par d'autres systèmes de fichiers dotés du même VPC et des mêmes tables de routage.

Vous pouvez également spécifier votre propre plage d'adresses IP dans l'option de création standard.

12. Choisissez Next, puis passez en revue la configuration du système de fichiers sur la page Créer un système de fichiers ONTAP. Notez les paramètres du système de fichiers que vous pouvez modifier une fois le système de fichiers créé.
13. Choisissez Create file system (Créer un système de fichiers).

La création rapide crée un système de fichiers avec une SVM (nommée`fsx`) et un volume (nommé`vol1`). Le volume possède un chemin de jonction `/vol1` et une politique de hiérarchisation

du pool de capacités automatique (qui hiérarchise automatiquement toutes les données non consultées depuis 31 jours vers un stockage de pool de capacité à moindre coût). La politique de capture d'écran par défaut est attribuée au volume par défaut. Les données du système de fichiers sont chiffrées au repos à l'aide de votre AWS KMS clé de gestion de service par défaut.

Étape 2 : Montage de votre système de fichiers à partir d'une instance Linux Amazon EC2

Vous pouvez monter votre système de fichiers à partir d'une instance Amazon Elastic Compute Cloud (Amazon EC2). Cette procédure utilise une instance exécutant Amazon Linux 2.

Pour monter votre système de fichiers depuis Amazon EC2

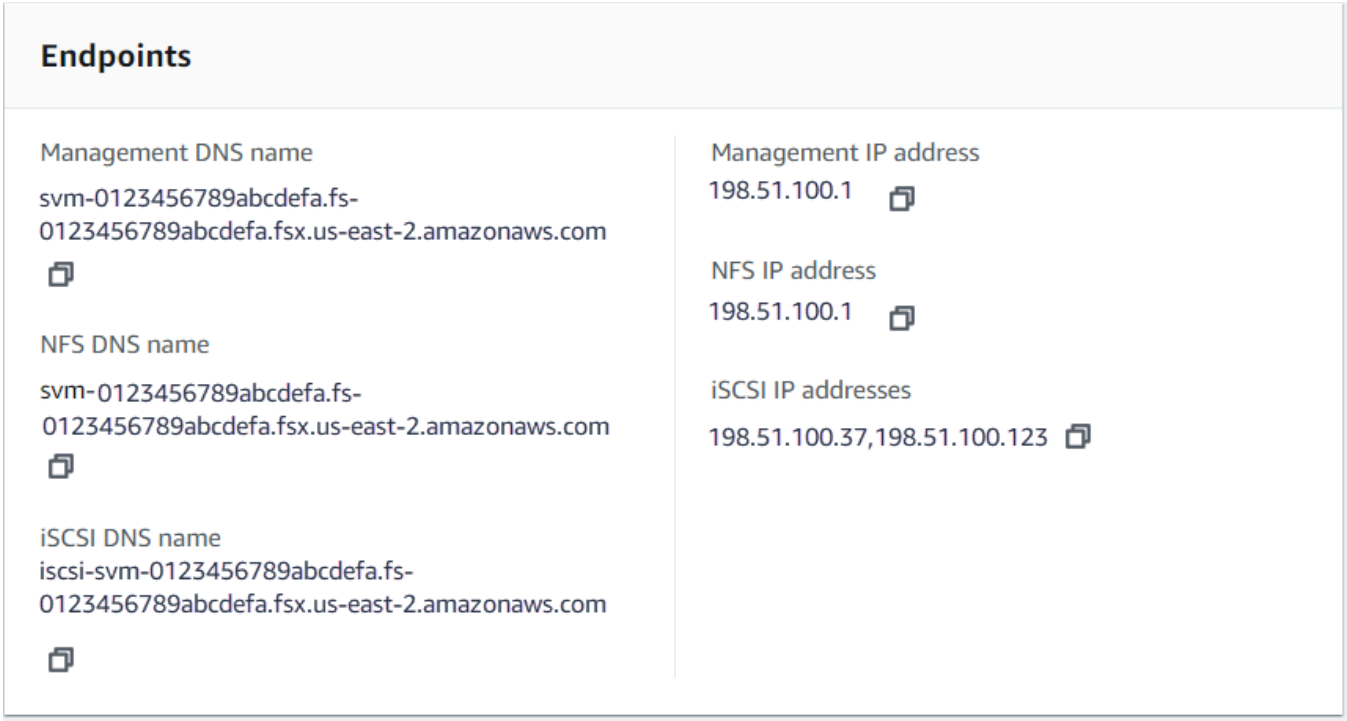
1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Créez ou sélectionnez une instance Amazon EC2 exécutant Amazon Linux 2 située dans le même cloud privé virtuel (VPC) que votre système de fichiers. Pour plus d'informations sur le lancement d'une instance, consultez Étape 1 : Lancer une instance dans le guide de l'utilisateur Amazon EC2.
3. Connectez-vous à votre instance Linux Amazon EC2. Pour plus d'informations, consultez Connect to your Linux instance dans le guide de l'utilisateur Amazon EC2.
4. Ouvrez un terminal sur votre instance Amazon EC2 à l'aide de Secure Shell (SSH) et connectez-vous avec les informations d'identification appropriées.
5. Créez un répertoire sur votre instance Amazon EC2 à utiliser comme point de montage du volume à l'aide de la commande suivante. Dans l'exemple suivant, remplacez *mount-point* par vos propres informations.

   ```
   $ sudo mkdir /mount-point
   ```

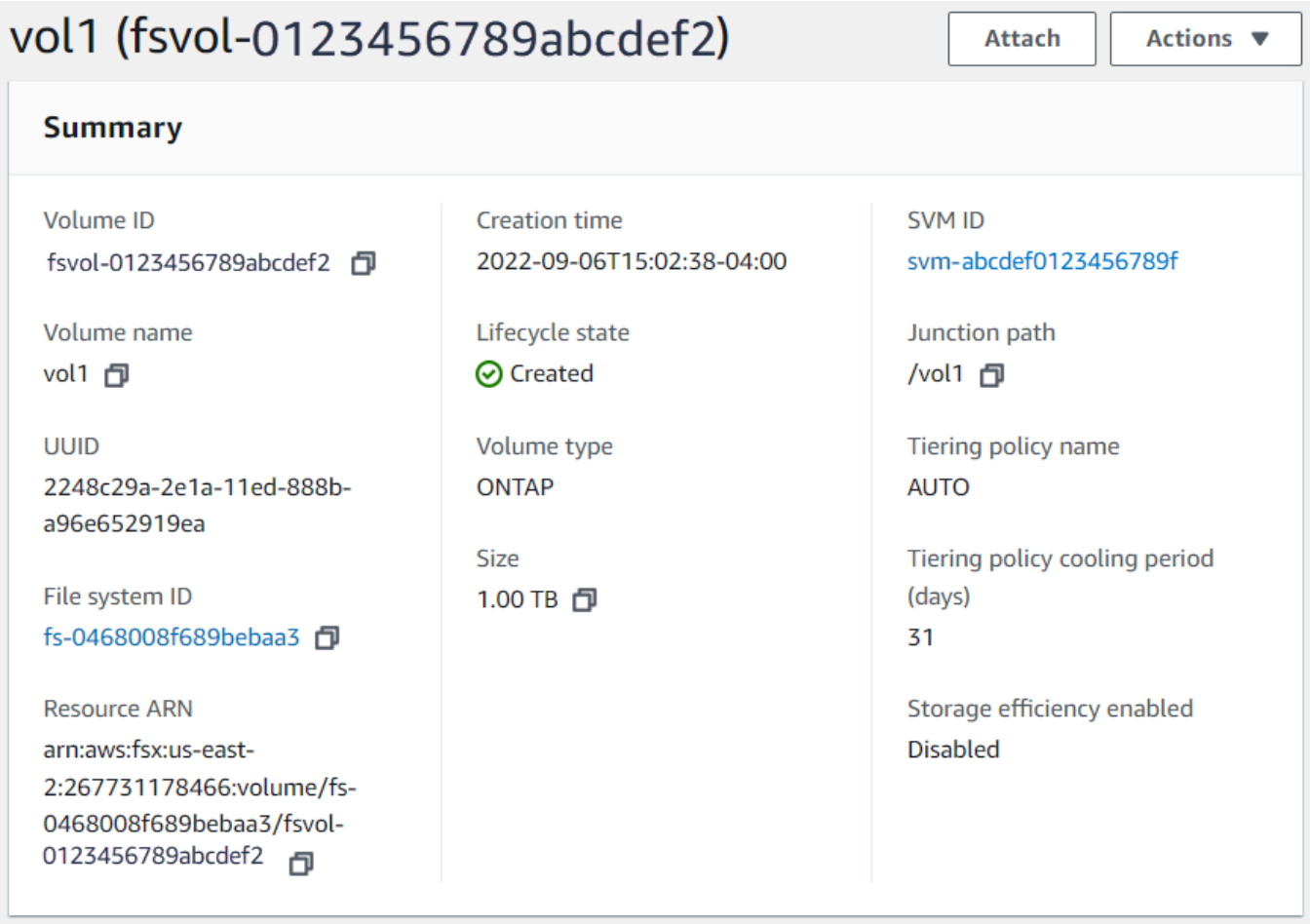
6. Montez votre système de fichiers Amazon FSx for NetApp ONTAP dans le répertoire que vous avez créé. Utilisez une `mount` commande similaire à l'exemple ci-dessous. Dans l'exemple suivant, remplacez les valeurs d'espace réservé suivantes par vos propres informations.

   - *nfs_version*— La version NFS que vous utilisez ; FSx for ONTAP prend en charge les versions 3, 4.0, 4.1 et 4.2.
   - *nfs-dns-name*— Le nom DNS NFS de la machine virtuelle de stockage (SVM) sur laquelle se trouve le volume que vous montez. Vous pouvez trouver le nom DNS NFS dans la console Amazon FSx en choisissant Storage virtual machines, puis en choisissant la SVM sur

laquelle se trouve le volume que vous montez. Le nom DNS NFS se trouve dans le panneau Endpoints, illustré dans l'image suivante.



- *`volume-junction-path`*— Le chemin de jonction du volume que vous montez. Vous pouvez trouver le chemin de jonction d'un volume dans la console Amazon FSx dans le panneau Résumé de la page des détails du volume, illustré dans l'image suivante.



- *mount-point*— Le nom du répertoire que vous avez créé sur votre instance EC2 pour le point de montage du volume.

```
sudo mount -t nfs -o nfsvers=nfs_version nfs-dns-name:/volume-junction-path /mount-point
```

La commande suivante utilise des exemples de valeurs.

```
sudo mount -t nfs -o nfsvers=4.1 svm-abcdef1234567890c.fs-012345abcdef6789b.fsx.us-east-2.amazonaws.com:/vol1 /fsxN
```

Si vous rencontrez des problèmes avec votre instance Amazon EC2 (tels que l'expiration du délai de connexion), consultez la section Résolution des problèmes liés aux instances EC2 dans le guide de l'utilisateur Amazon EC2.

Étape 3 : Nettoyer les ressources

Une fois cet exercice terminé, vous devez suivre ces étapes pour nettoyer vos ressources et protéger vos Compte AWS.

Pour nettoyer des ressources

1. Sur la console Amazon EC2, mettez fin à votre instance. Pour plus d'informations, consultez la section Résiliation de votre instance dans le guide de l'utilisateur Amazon EC2.
2. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
3. Sur la console Amazon FSx, supprimez tous vos volumes FSx for ONTAP qui ne sont pas des volumes racine de votre SVM. Pour plus d'informations, consultez Suppression d'un volume.
4. Supprimez toutes vos SVM FSx for ONTAP. Pour plus d'informations, consultez Supprimer une machine virtuelle de stockage (SVM).
5. Sur la console Amazon FSx, supprimez votre système de fichiers. Lorsque vous supprimez un système de fichiers, toutes les sauvegardes automatiques sont automatiquement supprimées. Cependant, vous devez toujours supprimer les sauvegardes créées manuellement. Les étapes suivantes décrivent ce processus.

    a. Dans le tableau de bord de la console, choisissez le nom du système de fichiers que vous avez créé pour cet exercice.

    b. Dans Actions, choisissez Supprimer le système de fichiers.

    c. Dans la boîte de dialogue Supprimer le système de fichiers, entrez l'ID du système de fichiers que vous souhaitez supprimer dans le champ ID du système de fichiers.

    d. Choisissez Supprimer le système de fichiers.

    e. Lorsqu'Amazon FSx supprime le système de fichiers, son statut dans le tableau de bord devient DELETING. Une fois le système de fichiers supprimé, il n'apparaît plus dans le tableau de bord. Toutes les sauvegardes automatiques sont supprimées en même temps que le système de fichiers.

    f. Vous pouvez désormais supprimer toutes les sauvegardes créées manuellement pour votre système de fichiers. Dans la barre de navigation de gauche, sélectionnez Sauvegardes.

    g. Dans le tableau de bord, choisissez les sauvegardes qui ont le même ID de système de fichiers que le système de fichiers que vous avez supprimé, puis choisissez Supprimer la sauvegarde. Assurez-vous de conserver la sauvegarde finale, si vous en avez créé une.

h. La boîte de dialogue Supprimer les sauvegardes s'ouvre. Gardez la case à cocher sélectionnée pour les ID des sauvegardes que vous souhaitez supprimer, puis choisissez Supprimer les sauvegardes.

Votre système de fichiers Amazon FSx et toutes les sauvegardes automatiques associées sont désormais supprimés, de même que toutes les sauvegardes manuelles que vous avez choisi de supprimer.

Accès aux données

Vous pouvez accéder à vos systèmes de fichiers Amazon FSx à l'aide de divers clients et méthodes pris en charge, dans les environnements locaux AWS Cloud et sur site.

Chaque SVM possède quatre points de terminaison qui sont utilisés pour accéder aux données ou pour gérer la SVM à l'aide de la NetApp CLI ONTAP ou de l'API REST :

- `Nfs`— Pour la connexion à l'aide du protocole NFS (Network File System)
- `Smb`— Pour la connexion via le protocole SMB (Service Message Block) (si votre SVM est jointe à un Active Directory ou si vous utilisez un groupe de travail.)
- `Iscsi`— Pour la connexion à l'aide du protocole iSCSI (Internet Small Computer Systems Interface) (pour les systèmes de fichiers évolutifs uniquement).
- `Management`— Pour gérer les SVM à l'aide de la NetApp CLI ou de l'API ONTAP, ou de BlueXP NetApp

Rubriques

Clients pris en charge

Les systèmes de fichiers FSx for ONTAP permettent d'accéder aux données à partir d'une grande variété d'instances de calcul et de systèmes d'exploitation. Pour ce faire, il prend en charge l'accès via le protocole NFS (Network File System) (v3, v4.0, v4.1 et v4.2), toutes les versions du protocole Server Message Block (SMB) (y compris 2.0, 3.0 et 3.1.1) et le protocole Internet Small Computer Systems Interface (iSCSI).

> **Important**
>
> Amazon FSx ne prend pas en charge l'accès aux systèmes de fichiers depuis l'Internet public. Amazon FSx détache automatiquement toute adresse IP élastique qui est une adresse IP publique accessible depuis Internet, qui est attachée à l'interface réseau élastique d'un système de fichiers.

Les instances de AWS calcul suivantes sont prises en charge pour une utilisation avec FSx for ONTAP :

- Instances Amazon Elastic Compute Cloud (Amazon EC2) exécutant Linux avec support NFS ou SMB, Microsoft Windows et macOS. Pour plus d'informations, consultez Volumes de montage.
- Conteneurs Docker Amazon Elastic Container Service (Amazon ECS) sur les instances Windows et Linux Amazon EC2. Pour plus d'informations, consultez Utilisation d'Amazon Elastic Container Service avec FSx pour ONTAP.
- Amazon Elastic Kubernetes Service — Pour en savoir plus, consultez le pilote Amazon FSx pour NetApp ONTAP CSI dans le guide de l'utilisateur Amazon EKS.
- Red Hat OpenShift Service on AWS (ROSA) — Pour en savoir plus, consultez Qu'est-ce que Red Hat OpenShift Service on AWS ? dans le Guide de l' AWS utilisateur de Red Hat OpenShift Service on.
- WorkSpaces Instances Amazon. Pour plus d'informations, consultez Utilisation d'Amazon WorkSpaces avec FSx pour ONTAP.
- Instances Amazon AppStream 2.0.
- AWS Lambda — Pour plus d'informations, consultez le billet de AWS blog Enabling SMB access for server-less workloads with Amazon FSx.
- Machines virtuelles (VM) exécutées dans VMware Cloud sur AWS des environnements. Pour plus d'informations, consultez Configurer Amazon FSx pour NetApp ONTAP en tant que stockage externe et Guide de déploiement de VMware Cloud on with AWS Amazon FSx for ONTAP. NetApp

Une fois montés, les systèmes de fichiers FSx for ONTAP apparaissent sous forme de répertoire local ou de lettre de lecteur sur NFS et SMB, fournissant un stockage de fichiers réseau partagé et entièrement géré auquel des milliers de clients peuvent accéder simultanément. Les LUN iSCSI sont accessibles sous forme de blocs lorsqu'ils sont montés sur iSCSI.

Accès aux données depuis l'intérieur AWS

Chaque système de fichiers Amazon FSx est associé à un Virtual Private Cloud (VPC). Vous pouvez accéder à votre système de fichiers FSx for ONTAP depuis n'importe où dans le VPC du système de fichiers, quelle que soit la zone de disponibilité. Vous pouvez également accéder à votre système de fichiers depuis d'autres VPC appartenant à AWS des comptes différents ou Régions AWS. Outre les exigences décrites dans les sections suivantes pour accéder aux ressources FSx for ONTAP, vous devez également vous assurer que le groupe de sécurité VPC de votre système de fichiers est configuré de manière à ce que le trafic de données et de gestion puisse circuler entre votre système de fichiers et les clients. Pour plus d'informations sur la configuration des groupes de sécurité dotés des ports requis, consultezGroupes de sécurité Amazon VPC.

Rubriques

Accès aux données depuis le même VPC

Lorsque vous créez votre système de fichiers Amazon FSx for NetApp ONTAP, vous sélectionnez le VPC Amazon dans lequel il se trouve. Toutes les SVM et tous les volumes associés au système de fichiers Amazon FSx NetApp for ONTAP se trouvent également dans le même VPC. Lors du montage d'un volume, si le système de fichiers et le client qui monte le volume se trouvent dans le même VPC Compte AWS, vous pouvez utiliser le nom DNS et la jonction de volume ou le partage SMB de la SVM, selon le client. Pour plus d’informations, consultez Volumes de montage.

Vous pouvez obtenir des performances optimales si le client et le volume se trouvent dans la même zone de disponibilité que le sous-réseau du système de fichiers, ou dans le sous-réseau préféré pour les systèmes de fichiers multi-AZ. Pour identifier le sous-réseau ou le sous-réseau préféré d'un système de fichiers, dans la console Amazon FSx, sélectionnez Systèmes de fichiers, puis choisissez le système de fichiers ONTAP dont vous montez le volume. Le sous-réseau ou le sous-réseau préféré (Multi-AZ) s'affiche dans le panneau Sous-réseau ou Sous-réseau préféré.

Accès aux données depuis l'extérieur du VPC de déploiement

Cette section décrit comment accéder aux points de terminaison d'un système de fichiers FSx for ONTAP depuis des AWS emplacements situés en dehors du VPC de déploiement du système de fichiers.

Accès aux points de terminaison de gestion NFS, SMB et ONTAP sur les systèmes de fichiers multi-AZ

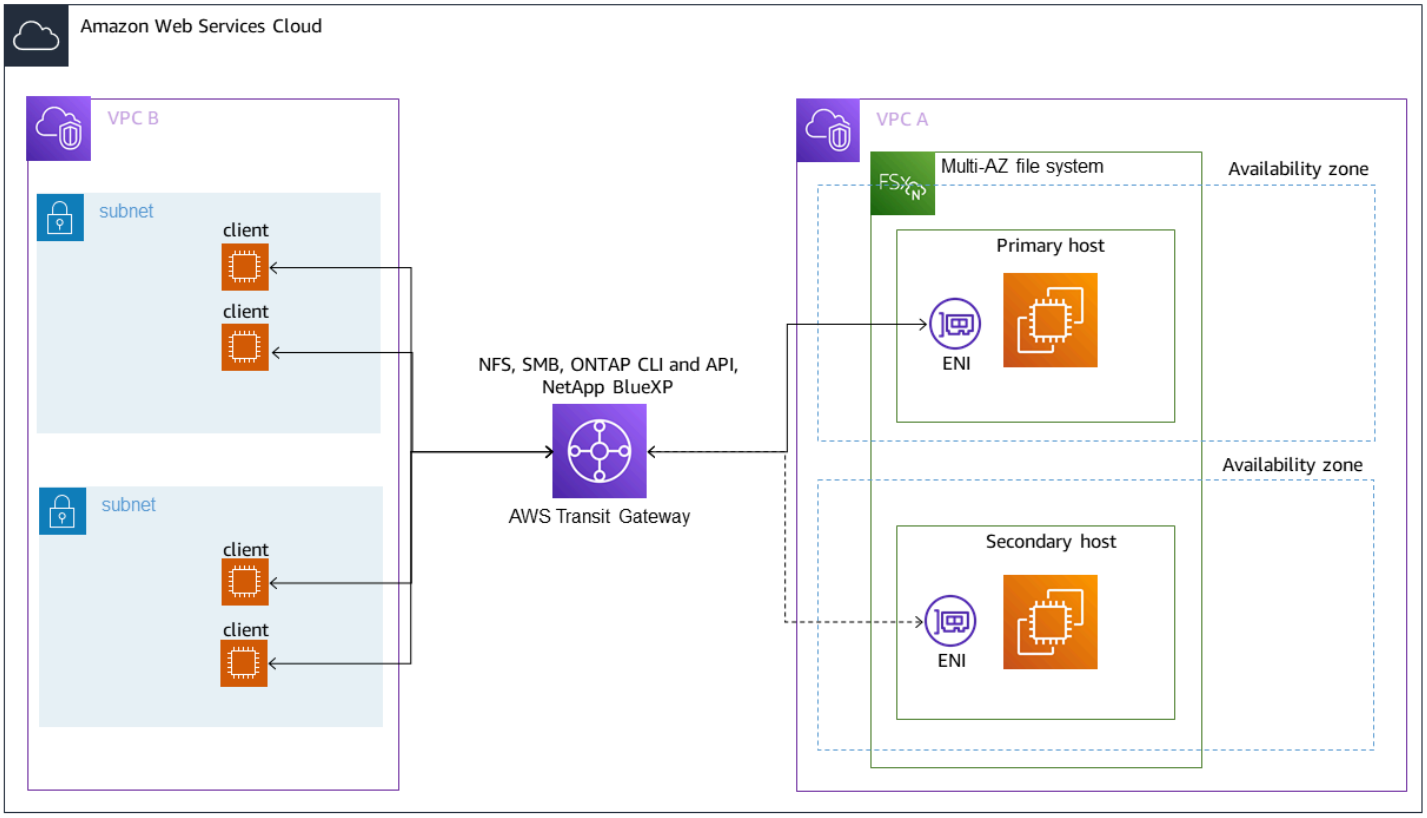
Les points de terminaison de gestion NFS, SMB et ONTAP sur Amazon FSx NetApp pour les systèmes de fichiers ONTAP Multi-AZ utilisent des adresses IP flottantes afin que les clients connectés puissent effectuer une transition fluide entre les serveurs de fichiers préférés et de secours lors d'un événement de basculement. Pour plus d'informations sur les basculements, consultez Processus de basculement pour FSx for ONTAP.

Ces adresses IP flottantes sont créées dans les tables de routage VPC que vous associez à votre système de fichiers et font partie des systèmes de fichiers que vous pouvez spécifier lors de `EndpointIpAddressRange` la création. `EndpointIpAddressRange`Utilise les plages d'adresses suivantes, en fonction de la manière dont le système de fichiers est créé :

- Les systèmes de fichiers multi-AZ créés à l'aide de la console Amazon FSx utilisent par défaut les 64 dernières adresses IP de la plage CIDR principale du VPC pour le système de fichiers. `EndpointIpAddressRange`
- Les systèmes de fichiers multi-AZ créés à l'aide de l'API AWS CLI ou Amazon FSx utilisent par défaut une plage d'adresses IP comprise dans `198.19.0.0/16` le bloc d'`EndpointIpAddressRange`adresses.

Ne AWS Transit Gatewayprend en charge que le routage vers des adresses IP flottantes, également connu sous le nom de peering transitif. Peering VPC, et AWS VPN ne prenez pas en charge AWS Direct Connect le peering transitif. Par conséquent, vous devez utiliser Transit Gateway pour accéder à ces interfaces depuis des réseaux extérieurs au VPC de votre système de fichiers.

Le schéma suivant illustre l'utilisation de Transit Gateway pour l'accès NFS, SMB ou de gestion à un système de fichiers multi-AZ situé dans un VPC différent de celui des clients qui y accèdent.



> **Note**
>
> Assurez-vous que toutes les tables de routage que vous utilisez sont associées à votre système de fichiers multi-AZ. Cela permet d'éviter toute indisponibilité lors d'un basculement. Pour plus d'informations sur l'association de vos tables de routage Amazon VPC à votre système de fichiers, consultez. Mettre à jour un système de fichiers

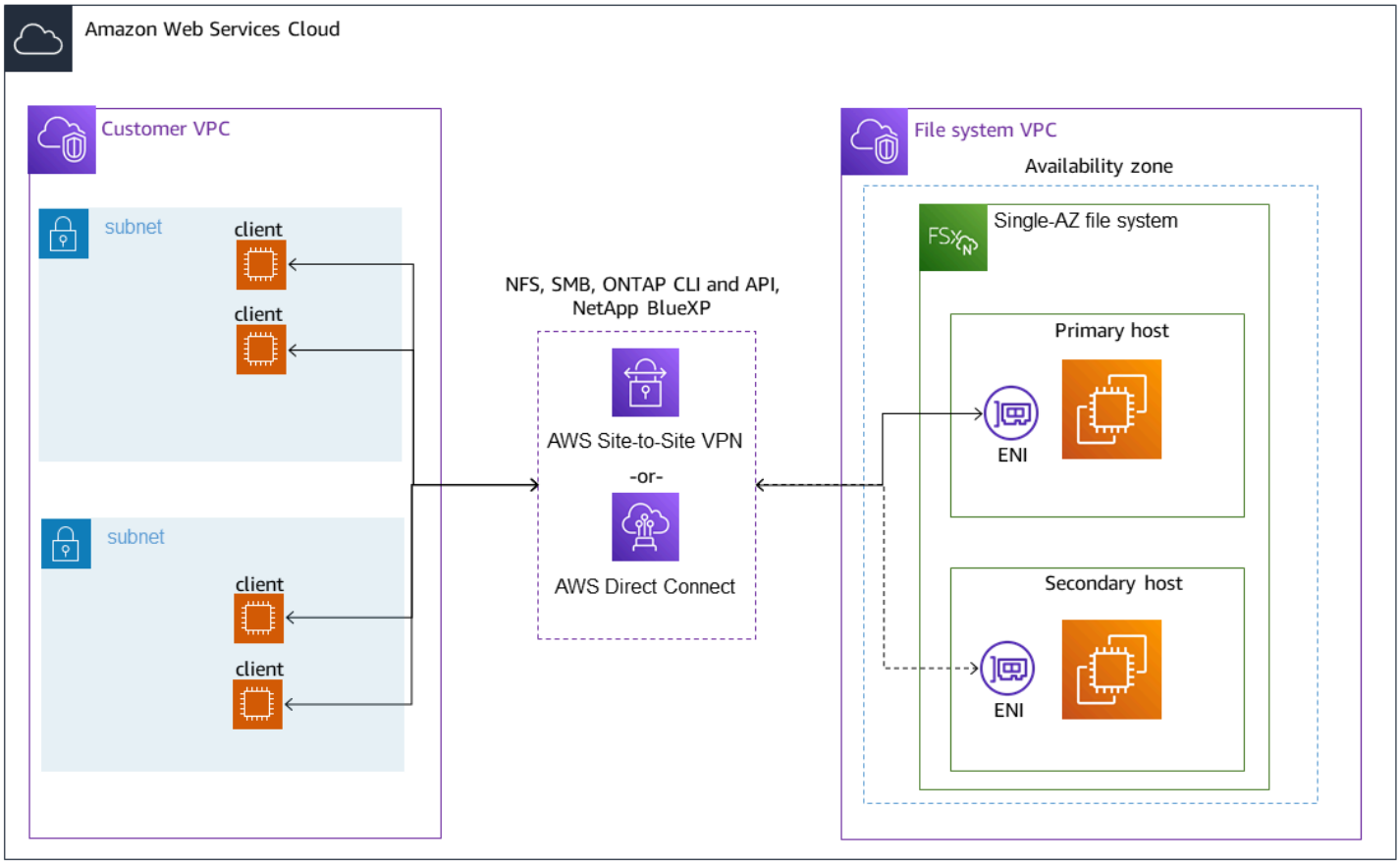
Pour savoir dans quels cas vous devez utiliser Transit Gateway pour accéder à votre système de fichiers FSx for ONTAP, consultez. Quand est-ce que Transit Gateway est requis ?

Accès à NFS, SMB ou à la CLI et à l'API ONTAP pour les systèmes de fichiers mono-AZ

Les points de terminaison utilisés pour accéder à FSx pour les systèmes de fichiers ONTAP mono-AZ via NFS ou SMB, et pour administrer les systèmes de fichiers à l'aide de la CLI ONTAP ou de l'API REST, sont des adresses IP secondaires sur l'ENI du serveur de fichiers actif. Les adresses IP secondaires se situent dans la plage CIDR du VPC, de sorte que les clients peuvent accéder aux

données et aux ports de gestion à l'aide de l'appairage VPC, ou sans en avoir besoin. AWS Direct Connect AWS VPN AWS Transit Gateway

Le schéma suivant illustre l'utilisation AWS VPN ou AWS Direct Connect pour l'accès NFS, SMB ou de gestion à un système de fichiers mono-AZ situé dans un VPC différent de celui des clients qui y accèdent.



Quand est-ce que Transit Gateway est requis ?

La nécessité ou non de Transit Gateway pour vos systèmes de fichiers multi-AZ dépend de la méthode que vous utilisez pour accéder aux données de votre système de fichiers. Les systèmes de fichiers mono-AZ ne nécessitent pas Transit Gateway. Le tableau suivant décrit à quel moment vous devrez utiliser pour accéder AWS Transit Gateway aux systèmes de fichiers multi-AZ.

Accès aux données	Nécessite Transit Gateway ?
Accès à FSx via NFS, SMB ou l' NetApp API REST ONTAP, CLI ou BlueEXP	Uniquement si :

Accès aux données	Nécessite Transit Gateway ?
	• Accès depuis un réseau pair (sur site, par exemple), et • Vous n'accédez pas à FSx via une instance NetApp FlexCache ou une instance de Global File Cache
Accès aux données via iSCSI	Non
Joindre une SVM à un Active Directory	Non
SnapMirror	Non
FlexCache Mise en cache	Non
Cache de fichiers global	Non

Configuration du routage à l'aide de AWS Transit Gateway

Si vous disposez d'un système de fichiers multi-AZ `EndpointIPAddressRange` dont un se situe en dehors de la plage d'adresses CIDR de votre VPC, vous devez configurer un routage supplémentaire pour accéder à votre système de fichiers AWS Transit Gateway à partir de réseaux pairs ou sur site.

Important

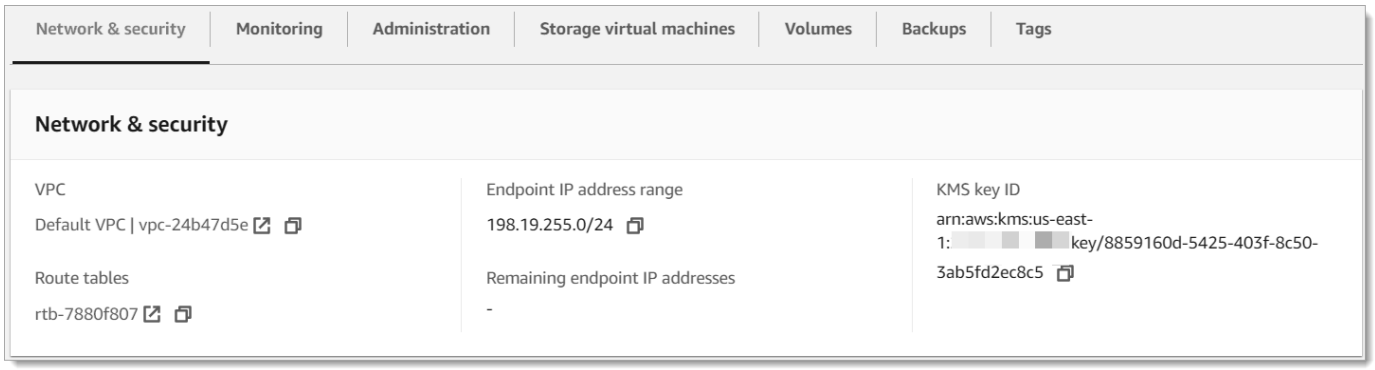
Pour accéder à un système de fichiers multi-AZ à l'aide d'un Transit Gateway, chacune des pièces jointes du Transit Gateway doit être créée dans un sous-réseau dont la table de routage est associée à votre système de fichiers.

Note

Aucune configuration supplémentaire de Transit Gateway n'est requise pour les systèmes de fichiers mono-AZ ou multi-AZ `EndpointIPAddressRange` dont l'adresse IP se situe dans la plage d'adresses IP de votre VPC.

Pour configurer le routage à l'aide de AWS Transit Gateway

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Choisissez le système de fichiers FSx for ONTAP pour lequel vous configurez l'accès depuis un réseau pair.
3. Dans Réseau et sécurité, copiez la plage d'adresses IP du point de terminaison.



4. Ajoutez une route à Transit Gateway qui achemine le trafic destiné à cette plage d'adresses IP vers le VPC de votre système de fichiers. Pour plus d'informations, consultez Utiliser les passerelles de transit dans les passerelles de transit Amazon VPC.
5. Vérifiez que vous pouvez accéder à votre système de fichiers FSx for ONTAP depuis le réseau pair.

Pour ajouter la table de routage à votre système de fichiers, consultezMettre à jour un système de fichiers.

> **Note**
>
> Les enregistrements DNS pour les points de terminaison de gestion, NFS et SMB ne peuvent être résolus qu'au sein du même VPC que le système de fichiers. Pour monter un volume ou vous connecter à un port de gestion depuis un autre réseau, vous devez utiliser l'adresse IP du point de terminaison. Ces adresses IP ne changent pas au fil du temps.

Accès aux points de terminaison iSCSI ou inter-clusters en dehors du VPC de déploiement

Vous pouvez utiliser le peering VPC ou accéder AWS Transit Gateway aux points de terminaison iSCSI ou inter-clusters de votre système de fichiers depuis l'extérieur du VPC de déploiement du

système de fichiers. Vous pouvez utiliser le peering VPC pour acheminer le trafic iSCSI et inter-clusters entre les VPC. Une connexion d'appairage VPC est une connexion réseau entre deux VPC, utilisée pour acheminer le trafic entre eux à l'aide d'adresses IPv4 privées. Vous pouvez utiliser le peering VPC pour connecter des VPC au sein d'un même Région AWS VPC ou entre différents. Régions AWS Pour plus d'informations sur le peering VPC, voir Qu'est-ce que le peering VPC ? dans le guide de peering Amazon VPC.

Accès aux données sur site

Vous pouvez accéder à vos systèmes de fichiers FSx for ONTAP sur site en utilisant AWS VPNet AWS Direct Connect; des instructions de cas d'utilisation plus spécifiques sont disponibles dans les sections suivantes. Outre les exigences répertoriées ci-dessous pour accéder aux différentes ressources FSx for ONTAP sur site, vous devez également vous assurer que le groupe de sécurité VPC de votre système de fichiers autorise le flux de données entre votre système de fichiers et les clients ; pour obtenir la liste des ports requis, consultez les groupes de sécurité Amazon VPC.

Accès aux points de terminaison NFS, SMB, ONTAP CLI ou REST API depuis le site

Cette section décrit comment accéder aux ports de gestion NFS, SMB et ONTAP sur les systèmes de fichiers FSx for ONTAP à partir de réseaux locaux.

Accès aux systèmes de fichiers multi-AZ

Amazon FSx nécessite que vous utilisiez ou configuriez le NetApp Global File Cache à distance AWS Transit Gateway ou que vous accédiez NetApp FlexCache à des systèmes de fichiers multi-AZ à partir d'un réseau sur site. Afin de prendre en charge le basculement entre les zones d'accès pour les systèmes de fichiers multi-AZ, Amazon FSx utilise des adresses IP flottantes pour les interfaces utilisées pour les points de terminaison de gestion NFS, SMB et ONTAP. Étant donné que les points de terminaison NFS, SMB et de gestion utilisent des adresses IP flottantes, vous devez les utiliser AWS Transit Gatewayconjointement avec AWS Direct Connect ou AWS VPN pour accéder à ces interfaces depuis un réseau sur site. Les adresses IP flottantes utilisées pour ces interfaces se situent dans les limites `EndpointIpAddressRange` que vous avez spécifiées lors de la création de votre système de fichiers multi-AZ. Si vous créez votre système de fichiers à partir de la console Amazon FSx, Amazon FSx choisit par défaut les 64 dernières adresses IP de la plage d'adresses CIDR principale du VPC à utiliser comme plage d'adresses IP de point de terminaison pour le système de fichiers. Si vous créez votre système de fichiers à partir de l'API Amazon FSx AWS CLI ou de

l'API Amazon FSx, Amazon FSx choisit par défaut une plage d'adresses IP comprise dans cette plage d'adresses IP. `198.19.0.0/16` Les adresses IP flottantes sont utilisées pour permettre une transition fluide de vos clients vers le système de fichiers de secours au cas où un basculement serait nécessaire. Pour plus d'informations, consultez Processus de basculement pour FSx for ONTAP.

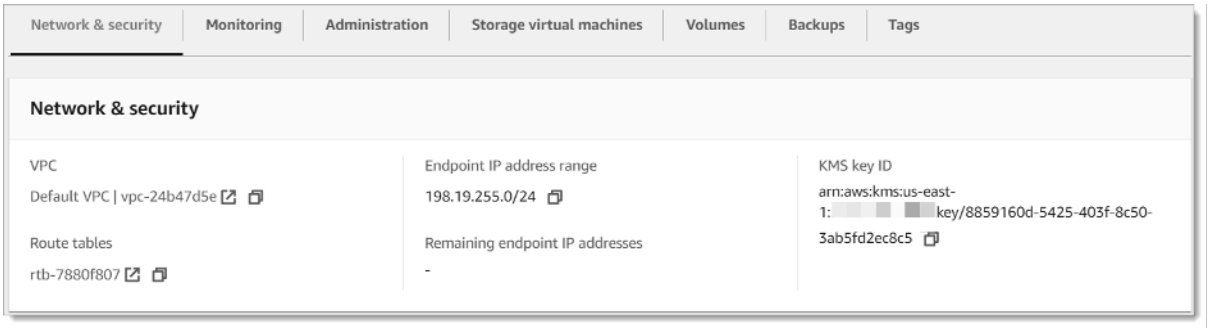
> **Important**
>
> Pour accéder à un système de fichiers multi-AZ à l'aide d'un Transit Gateway, chacune des pièces jointes du Transit Gateway doit être créée dans un sous-réseau dont la table de routage est associée à votre système de fichiers.

AWS Transit Gateway Pour configurer l'accès depuis l'extérieur de votre VPC

Si vous disposez d'un système de fichiers multi-AZ `EndpointIPAddressRange` dont un se situe en dehors de la plage d'adresses CIDR de votre VPC, vous devez configurer un routage supplémentaire pour accéder à votre système de fichiers AWS Transit Gateway à partir de réseaux pairs ou sur site.

> **Note**
>
> Aucune configuration supplémentaire de Transit Gateway n'est requise pour les systèmes de fichiers mono-AZ ou multi-AZ `EndpointIPAddressRange` dont l'adresse IP se situe dans la plage d'adresses IP de votre VPC.

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Choisissez le système de fichiers FSx for ONTAP pour lequel vous configurez l'accès depuis un réseau pair.
3. Dans Réseau et sécurité, copiez la plage d'adresses IP du point de terminaison.



4. Ajoutez une route au Transit Gateway qui achemine le trafic destiné à cette plage d'adresses IP vers le VPC de votre système de fichiers. Pour plus d'informations, consultez la section Travailler avec les passerelles de transit dans le guide de l'utilisateur d'Amazon VPC Transit Gateway.
5. Vérifiez que vous pouvez accéder à votre système de fichiers FSx for ONTAP depuis le réseau pair.

> **Important**
>
> Pour accéder à un système de fichiers multi-AZ à l'aide d'un Transit Gateway, chacune des pièces jointes du Transit Gateway doit être créée dans un sous-réseau dont la table de routage est associée à votre système de fichiers.

Pour ajouter une table de routage à votre système de fichiers, consultezMettre à jour un système de fichiers.

Accès aux systèmes de fichiers mono-AZ

L'utilisation pour accéder AWS Transit Gateway aux données depuis un réseau sur site n'existe pas pour les systèmes de fichiers mono-AZ. Les systèmes de fichiers mono-AZ sont déployés dans un sous-réseau unique, et aucune adresse IP flottante n'est requise pour assurer le basculement entre les nœuds. Au lieu de cela, les adresses IP auxquelles vous accédez sur les systèmes de fichiers mono-AZ sont implémentées en tant qu'adresses IP secondaires dans la plage d'adresses CIDR VPC du système de fichiers, ce qui vous permet d'accéder à vos données depuis un autre réseau sans en avoir besoin. AWS Transit Gateway

Accès aux points de terminaison inter-clusters sur site

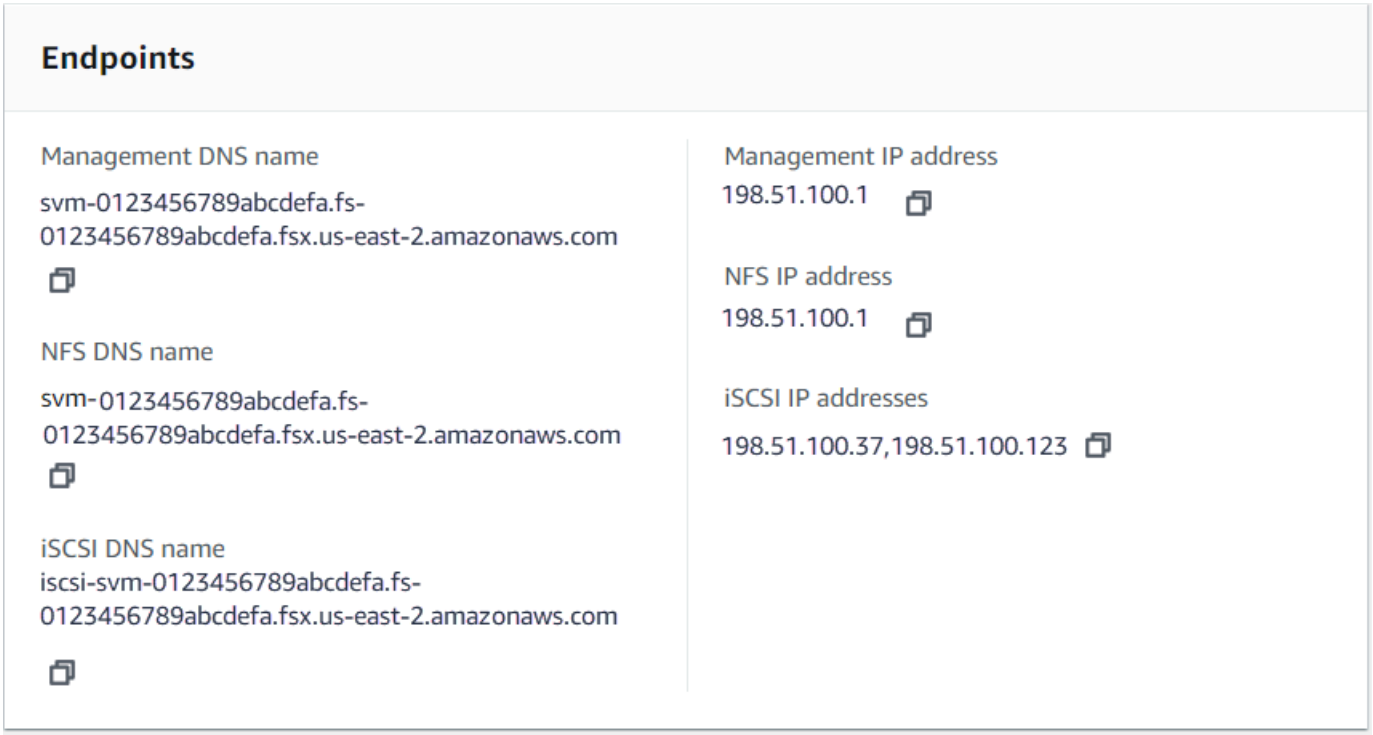
Les points de terminaison inter-clusters de FSx for ONTAP sont dédiés au trafic de réplication entre les systèmes de fichiers NetApp ONTAP, y compris entre les déploiements sur site et FSx for ONTAP. NetApp Le trafic de réplication inclut SnapMirror FlexCache, et FlexClone les relations entre les machines virtuelles de stockage (SVM) et les volumes de différents systèmes de fichiers, ainsi que le cache NetApp global de fichiers. Les points de terminaison inter-clusters sont également utilisés pour le trafic Active Directory.

Étant donné que les points de terminaison inter-clusters d'un système de fichiers utilisent des adresses IP situées dans la plage CIDR du VPC que vous fournissez lorsque vous créez votre

système de fichiers FSx for ONTAP, vous n'êtes pas obligé d'utiliser un Transit Gateway pour acheminer le trafic inter-clusters entre le système sur site et le. AWS Cloud Toutefois, les clients sur site doivent toujours utiliser AWS VPN ou AWS Direct Connect établir une connexion sécurisée avec votre VPC.

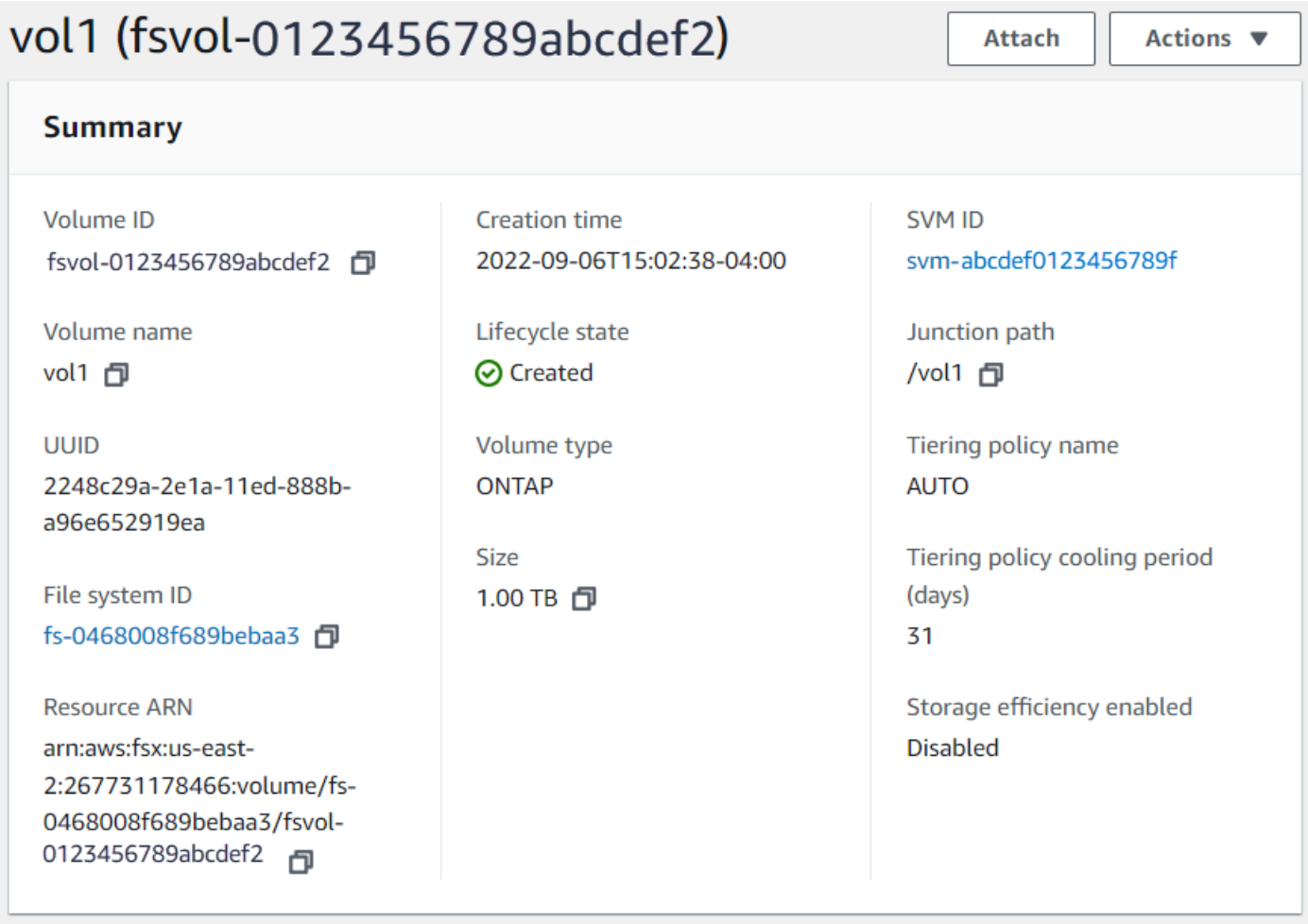
Volumes de montage

Vous accédez aux données dans FSx for ONTAP en montant un volume sur votre client. Les commandes de cette section utilisent le nom DNS ou l'adresse IP de la SVM dans laquelle le volume a été créé pour monter ou attacher un volume. Vous pouvez trouver le nom DNS et l'adresse IP de la SVM dans la console Amazon FSx en choisissant ONTAP > Machines virtuelles de stockage, ou sur l'onglet Machine virtuelle de stockage sur la page de détails du système de fichiers du système de fichiers, illustrée dans l'image suivante.



Vous pouvez également les trouver dans la réponse de l'opération d'DescribeStorageVirtualMachinesAPI.

Vous pouvez trouver le chemin de jonction d'un volume dans la console Amazon FSx dans le panneau Résumé de la page de détails du volume, illustré dans l'image suivante.



Rubriques

- Montage sur des clients Linux
- Montage sur les clients Microsoft Windows
- Montage sur des clients macOS

Montage sur des clients Linux

Nous recommandons que le style de sécurité des volumes SVM auxquels vous attachez des clients Linux soit défini sur `UNIX` ou`mixed`. Pour plus d'informations, consultez Gestion de FSx pour les volumes ONTAP.

> **Note**
>
> Par défaut, les montages FSx pour ONTAP NFS sont des montages. `hard` Pour garantir un basculement fluide en cas de basculement, nous vous recommandons d'utiliser l'option de `hard` montage par défaut.

Pour monter un volume ONTAP sur un client Linux

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Créez ou sélectionnez une instance Amazon EC2 exécutant Amazon Linux 2 qui se trouve dans le même VPC que le système de fichiers.

   Pour plus d'informations sur le lancement d'une instance Linux EC2, consultez Étape 1 : Lancer une instance dans le guide de l'utilisateur Amazon EC2.
3. Connectez-vous à votre instance Linux Amazon EC2. Pour plus d'informations, consultez Connect to your Linux instance dans le guide de l'utilisateur Amazon EC2.
4. Ouvrez un terminal sur votre instance EC2 à l'aide de Secure Shell (SSH) et connectez-vous avec les informations d'identification appropriées.
5. Créez un répertoire sur l'instance EC2 pour monter le volume de la SVM comme suit :

   ```
   sudo mkdir /fsx
   ```
6. Montez le volume dans le répertoire que vous venez de créer à l'aide de la commande suivante :

   ```
   sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
   ```

   L'exemple suivant utilise des exemples de valeurs.

   ```
   sudo mount -t nfs svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
   east-1.amazonaws.com:/vol1 /fsx
   ```

   Vous pouvez également utiliser l'adresse IP de la SVM au lieu de son nom DNS. Nous recommandons d'utiliser le nom DNS pour monter les clients sur des systèmes de fichiers évolutifs, car cela permet de garantir que vos clients sont équilibrés entre les paires de haute disponibilité (HA) de votre système de fichiers.

```
sudo mount -t nfs 198.51.100.1:/vol1 /fsx
```

> **Note**
>
> Pour les systèmes de fichiers scale-out, le protocole parallel NFS (pNFS) est activé par défaut et est utilisé par défaut pour tous les clients qui montent des volumes avec NFS v4.1 ou version ultérieure.

Utilisation de /etc/fstab pour le montage automatique lors du redémarrage de l'instance

Pour remonter automatiquement votre volume FSx for ONTAP lorsqu'une instance Linux Amazon EC2 redémarre, utilisez le fichier. `/etc/fstab` Le fichier `/etc/fstab` contient des informations sur les systèmes de fichiers. La commande`mount -a`, qui s'exécute au démarrage de l'instance, monte les systèmes de fichiers répertoriés dans`/etc/fstab`.

> **Note**
>
> Les systèmes de fichiers FSx for ONTAP ne prennent pas en charge le montage automatique à l'aide d'instances `/etc/fstab` Mac Amazon EC2.

> **Note**
>
> Avant de mettre à jour le `/etc/fstab` fichier de votre instance EC2, assurez-vous que vous avez déjà créé votre système de fichiers FSx for ONTAP. Pour plus d'informations, consultez Création de FSx pour les systèmes de fichiers ONTAP.

Pour mettre à jour le fichier /etc/fstab sur votre instance EC2

1. Connectez-vous à votre instance EC2 :

   - Pour vous connecter à votre instance à partir d'un ordinateur exécutant macOS ou Linux, spécifiez le fichier .pem dans votre commande SSH. Pour ce faire, utilisez l'option `-i` et le chemin d'accès à votre clé privée.

- Pour vous connecter à votre instance depuis un ordinateur exécutant Windows, vous pouvez utiliser MindTerm PuTTY. Pour utiliser PuTTY, installez-le et convertissez le fichier .pem en fichier .ppk.

Pour plus d'informations, consultez les rubriques suivantes dans le guide de l'utilisateur Amazon EC2 :

- Connexion à votre instance Linux à l'aide de SSH
- Connexion à votre instance Linux à partir de Windows à l'aide de PuTTY

2. Créez un répertoire local qui sera utilisé pour monter le volume de la SVM.

```
sudo mkdir /fsx
```

3. Ouvrez le `/etc/fstab` fichier dans l'éditeur de votre choix.
4. Ajoutez la ligne suivante dans le fichier `/etc/fstab`. Insérez un caractère de tabulation entre chaque paramètre. Il doit apparaître sous la forme d'une seule ligne sans sauts de ligne.

```
svm-dns-name:volume-junction-path /fsx nfs nfsvers=version,defaults 0 0
```

Vous pouvez également utiliser l'adresse IP de la SVM du volume. Les trois derniers paramètres indiquent les options NFS (que nous avons définies par défaut), le vidage du système de fichiers et la vérification du système de fichiers (elles ne sont généralement pas utilisées, nous les avons donc définies sur 0).

5. Enregistrez les Modifications dans le fichier.
6. Montez maintenant le partage de fichiers à l'aide de la commande suivante. Au prochain démarrage du système, le dossier sera automatiquement monté.

```
sudo mount /fsx
sudo mount svm-dns-name:volume-junction-path
```

Votre instance EC2 est désormais configurée pour monter le volume ONTAP à chaque redémarrage.

Montage sur les clients Microsoft Windows

Cette section décrit comment accéder aux données de votre système de fichiers FSx for ONTAP avec des clients exécutant le système d'exploitation Microsoft Windows. Passez en revue les exigences suivantes, quel que soit le type de client que vous utilisez.

Cette procédure suppose que le client et le système de fichiers se trouvent dans le même VPC et. Compte AWS Si le client est situé sur site ou dans un autre VPC Compte AWS, Région AWS cette procédure suppose également que vous avez AWS Transit Gateway configuré ou utilisé une connexion réseau dédiée ou un tunnel privé sécurisé AWS Direct Connect utilisant. AWS Virtual Private Network Pour plus d'informations, consultez Accès aux données depuis l'extérieur du VPC de déploiement.

Nous vous recommandons d'associer des volumes à vos clients Windows à l'aide du protocole SMB.

Prérequis

Pour accéder à un volume de stockage ONTAP à l'aide d'un client Microsoft Windows, vous devez remplir les conditions suivantes :

- La SVM du volume que vous attachez doit être jointe à l'Active Directory de votre organisation, ou vous devez utiliser un groupe de travail. Pour plus d'informations sur l'association de votre SVM à un Active Directory, consultezGestion de FSx pour les machines virtuelles de stockage ONTAP. Pour plus d'informations sur l'utilisation des groupes de travail, consultez la section Configuration d'un serveur SMB dans un groupe de travail dans le NetApp Centre de documentation.
- Le volume que vous êtes en train de joindre possède un paramètre de style de sécurité égal à `NTFS` ou`mixed`. Pour plus d'informations, consultez Gestion de FSx pour les volumes ONTAP.

Pour attacher un volume ONTAP à un client Windows à l'aide de SMB et d'Active Directory

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Créez ou sélectionnez une instance Amazon EC2 exécutant Microsoft Windows qui se trouve dans le même VPC que le système de fichiers et jointe au même répertoire Microsoft Active Directory que la SVM du volume.

   Pour plus d'informations sur le lancement d'une instance, consultez Étape 1 : Lancer une instance dans le guide de l'utilisateur Amazon EC2.

Pour plus d'informations sur l'association d'une SVM à un Active Directory, consultezGestion de FSx pour les machines virtuelles de stockage ONTAP.

3. Connectez-vous à votre instance Windows Amazon EC2. Pour plus d'informations, consultez la section Connexion à votre instance Windows dans le guide de l'utilisateur Amazon EC2.
4. Ouvrir une invite de commande.
5. Exécutez la commande suivante. Remplacez les éléments suivants :

   - `Z:`Remplacez-la par n'importe quelle lettre de lecteur disponible.
   - `DNS_NAME`Remplacez-le par le nom DNS ou l'adresse IP du point de terminaison SMB de la SVM du volume.
   - `SHARE_NAME`Remplacez-le par le nom d'un partage SMB. `C$`est le partage SMB par défaut situé à la racine de l'espace de noms de la SVM, mais vous ne devez pas le monter car cela expose le stockage au volume racine et peut entraîner des interruptions de sécurité et de service. Vous devez fournir un nom de partage SMB à monter au lieu de`C$`. Pour plus d'informations sur la création de partages SMB, consultezGestion des actions des PME.

   ```
   net use Z: \\DNS_NAME\SHARE_NAME
   ```

   L'exemple suivant utilise des exemples de valeurs.

   ```
   net use Z: \\corp.example.com\group_share
   ```

   Vous pouvez également utiliser l'adresse IP de la SVM au lieu de son nom DNS. Nous recommandons d'utiliser le nom DNS pour monter les clients sur des systèmes de fichiers évolutifs, car cela permet de garantir que vos clients sont équilibrés entre les paires de haute disponibilité (HA) de votre système de fichiers.

   ```
   net use Z: \\198.51.100.5\group_share
   ```

Montage sur des clients macOS

Cette section décrit comment accéder aux données de votre système de fichiers FSx for ONTAP avec des clients exécutant le système d'exploitation macOS. Passez en revue les exigences suivantes, quel que soit le type de client que vous utilisez.

Cette procédure suppose que le client et le système de fichiers se trouvent dans le même VPC et. Compte AWS Si le client est situé sur site ou dans un autre VPC Compte AWS , Région AWS ou si vous avez AWS Transit Gateway configuré une connexion réseau dédiée à l'aide ou un tunnel privé et sécurisé à AWS Direct Connect l'aide de. AWS Virtual Private Network Pour plus d'informations, consultez Accès aux données depuis l'extérieur du VPC de déploiement.

Nous vous recommandons d'associer des volumes à vos clients Mac à l'aide du protocole SMB.

Pour monter un volume ONTAP sur un client macOS à l'aide de SMB

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Créez ou sélectionnez une instance Mac Amazon EC2 exécutant le macOS qui se trouve dans le même VPC que le système de fichiers.

   Pour plus d'informations sur le lancement d'une instance, consultez Étape 1 : Lancer une instance dans le guide de l'utilisateur Amazon EC2.
3. Connectez-vous à votre instance Mac Amazon EC2. Pour plus d'informations, consultez Connect to your Linux instance dans le guide de l'utilisateur Amazon EC2.
4. Ouvrez un terminal sur votre instance EC2 à l'aide de Secure Shell (SSH) et connectez-vous avec les informations d'identification appropriées.
5. Créez un répertoire sur l'instance EC2 pour monter le volume comme suit :

   ```
   sudo mkdir /fsx
   ```
6. Montez le volume à l'aide de la commande suivante.

   ```
   sudo mount -t smbfs filesystem-dns-name:/smb-share-name mount-point
   ```

   L'exemple suivant utilise des exemples de valeurs.

   ```
   sudo mount -t smbfs svm-01234567890abcde2.fs-01234567890abcde5.fsx.us-
   east-1.amazonaws.com:/C$ /fsx
   ```

   Vous pouvez également utiliser l'adresse IP de la SVM au lieu de son nom DNS. Nous recommandons d'utiliser le nom DNS pour monter les clients sur des systèmes de fichiers évolutifs, car cela permet de garantir que vos clients sont équilibrés entre les paires de haute disponibilité (HA) de votre système de fichiers.

```
sudo mount -t smbfs 198.51.100.10:/C$ /fsx
```

`C$`est le partage SMB par défaut que vous pouvez monter pour voir la racine de l'espace de noms de la SVM. Si vous avez créé des partages SMB (Server Message Block) dans votre SVM, indiquez les noms des partages SMB au lieu de. `C$` Pour plus d'informations sur la création de partages SMB, consultezGestion des actions des PME.

Pour monter un volume ONTAP sur un client macOS à l'aide de NFS

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Créez ou sélectionnez une instance Amazon EC2 exécutant Amazon Linux 2 qui se trouve dans le même VPC que le système de fichiers.

   Pour plus d'informations sur le lancement d'une instance Linux EC2, consultez Étape 1 : Lancer une instance dans le guide de l'utilisateur Amazon EC2.
3. Connectez-vous à votre instance Linux Amazon EC2. Pour plus d'informations, consultez Connect to your Linux instance dans le guide de l'utilisateur Amazon EC2.
4. Montez votre volume FSx for ONTAP sur l'instance Linux EC2 en utilisant un script de données utilisateur lors du lancement de l'instance ou en exécutant les commandes suivantes :

   ```
   sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /mount-point
   ```

   L'exemple suivant utilise des exemples de valeurs.

   ```
   sudo mount -t nfs -o nfsvers=4.1
    svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /
   fsxontap
   ```

   Vous pouvez également utiliser l'adresse IP de la SVM au lieu de son nom DNS. Nous recommandons d'utiliser le nom DNS pour monter les clients sur des systèmes de fichiers évolutifs, car cela permet de garantir que vos clients sont équilibrés entre les paires HA de votre système de fichiers.

   ```
   sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
   ```

5. Montez le volume dans le répertoire que vous venez de créer à l'aide de la commande suivante.

```
sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
```

L'exemple suivant utilise des exemples de valeurs.

```
sudo mount -t nfs svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
east-1.amazonaws.com:/vol1 /fsx
```

Vous pouvez également utiliser l'adresse IP de la SVM au lieu de son nom DNS. Nous recommandons d'utiliser le nom DNS pour monter les clients sur des systèmes de fichiers évolutifs, car cela permet de garantir que vos clients sont équilibrés entre les paires de haute disponibilité (HA) de votre système de fichiers.

```
sudo mount -t nfs 198.51.100.1:/vol1 /fsx
```

Montage de LUN iSCSI

Amazon FSx for NetApp ONTAP fournit une prise en charge du stockage par blocs partagé via le protocole iSCSI (Internet Small Computer Systems Interface). Vous pouvez activer le stockage iSCSI en provisionnant des LUN (numéro d'unité logique) et en les mappant à des groupes d'initiateurs (igroups), exposant ainsi le stockage par blocs à vos hôtes Linux et Windows.

> **Note**
>
> Le protocole iSCSI n'est pas pris en charge pour les systèmes de fichiers FSx for ONTAP scale-out, qui sont des systèmes de fichiers dotés de plusieurs paires de serveurs de fichiers à haute disponibilité (HA).

Rubriques

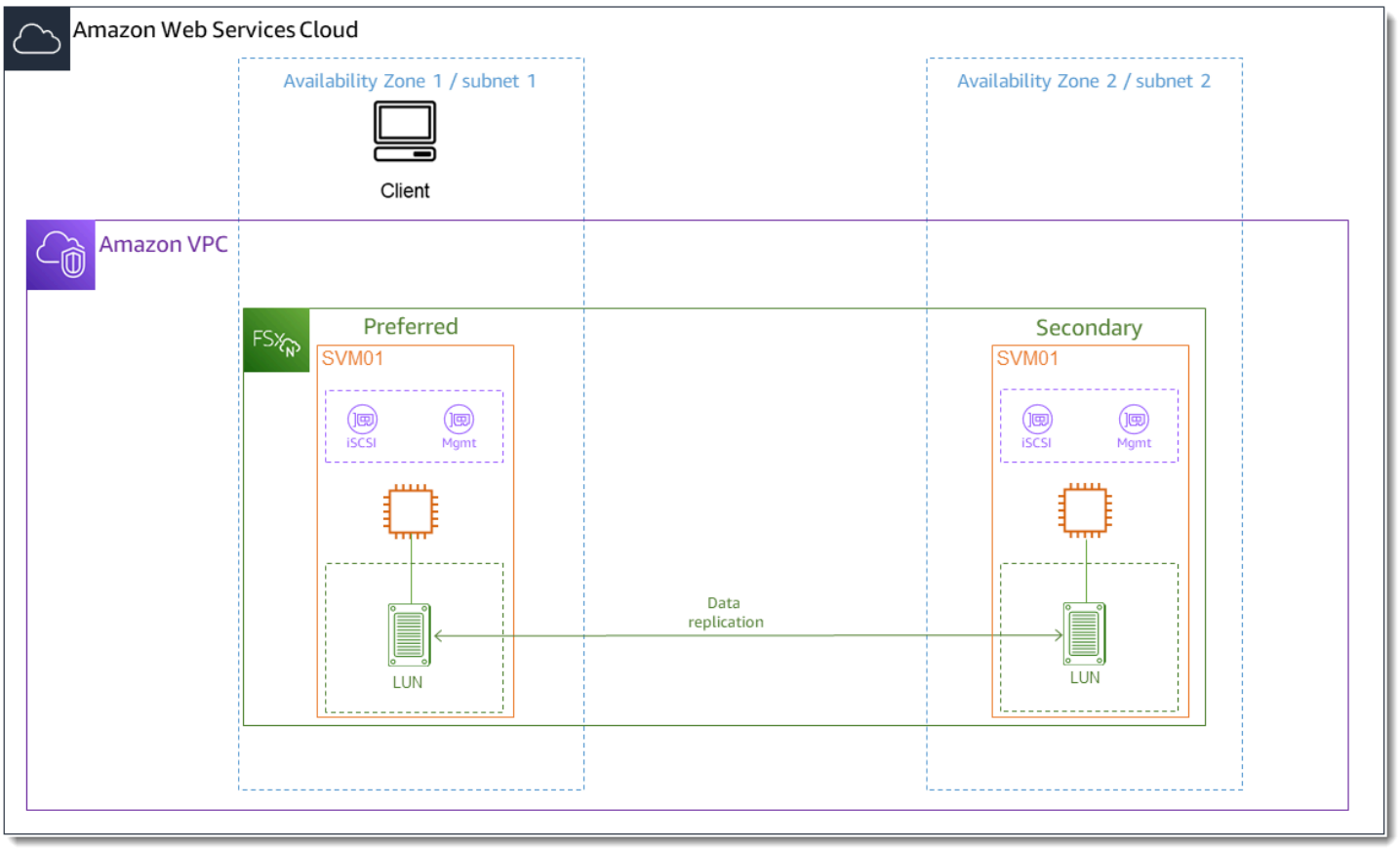
Montage de LUN iSCSI sur un client Linux

Les exemples présentés dans ces procédures utilisent la configuration suivante :

- Le LUN iSCSI qui est monté sur l'hôte Linux est déjà créé. Pour plus d'informations, consultez Création d'un LUN iSCSI.
- L'hôte Linux qui monte le LUN iSCSI est une instance Amazon EC2 exécutant l'Amazon Machine Image (AMI) Amazon Linux 2. Il possède des groupes de sécurité VPC configurés pour autoriser le trafic entrant et sortant, comme décrit dans. Contrôle d'accès au système de fichiers avec Amazon VPC
- L'hôte Linux et le système de fichiers FSx for ONTAP sont situés dans le même VPC et. Compte AWS Si l'hôte est situé dans un autre VPC, vous pouvez utiliser le peering VPC ou accorder AWS Transit Gateway à d'autres VPC l'accès aux points de terminaison iSCSI du volume. Pour plus d'informations, consultez Accès aux données depuis l'extérieur du VPC de déploiement.

  Si vous utilisez une instance EC2 exécutant une autre AMI Linux, certains utilitaires installés sur l'hôte peuvent être préinstallés et vous pouvez utiliser différentes commandes pour installer les packages requis. Outre l'installation des packages, les commandes utilisées dans cette section sont valides pour les autres AMI Linux EC2.

  Nous recommandons que l'instance EC2 se trouve dans la même zone de disponibilité que le sous-réseau préféré de votre système de fichiers, comme illustré dans le graphique suivant.



Rubriques

- Installation et configuration de l'iSCSI sur le client Linux
- Configuration de l'iSCSI sur le système de fichiers FSx pour ONTAP
- Montez un LUN iSCSI sur votre client Linux

Installation et configuration de l'iSCSI sur le client Linux

Pour installer le client iSCSI

1. Confirmez-le `iscsi-initiator-utils` et `device-mapper-multipath` ils sont installés sur votre appareil Linux. Connectez-vous à votre instance Linux à l'aide d'un client SSH. Pour plus d'informations, consultez Se connecter à votre instance Linux à l'aide de SSH.
2. Installez `multipath` et le client iSCSI à l'aide de la commande suivante. L'installation `multipath` est nécessaire si vous souhaitez basculer automatiquement entre vos serveurs de fichiers.

```
~$ sudo yum install -y device-mapper-multipath iscsi-initiator-utils
```

3. Pour accélérer la réponse en cas de basculement automatique entre les serveurs de fichiers lors de l'utilisation`multipath`, définissez la valeur du délai d'expiration de remplacement dans le `/etc/iscsi/iscsid.conf` fichier sur une valeur égale à `5` au lieu d'utiliser la valeur par défaut de`120`.

```
~$ sudo sed -i 's/node.session.timeo.replacement_timeout = .*/
node.session.timeo.replacement_timeout = 5/' /etc/iscsi/iscsid.conf; sudo cat /etc/
iscsi/iscsid.conf | grep node.session.timeo.replacement_timeout
```

4. Démarrez le service iSCSI.

```
~$ sudo service iscsid start
```

Notez qu'en fonction de votre version de Linux, vous devrez peut-être utiliser cette commande à la place :

```
~$ sudo systemctl start iscsid
```

5. Vérifiez que le service est en cours d'exécution à l'aide de la commande suivante.

```
~$ sudo systemctl status iscsid.service
```

Le système répond avec le résultat suivant :

```
iscsid.service - Open-iSCSI
    Loaded: loaded (/usr/lib/systemd/system/iscsid.service; disabled; vendor
 preset: disabled)
    Active: active (running) since Fri 2021-09-02 00:00:00 UTC; 1min ago
    Docs: man:iscsid(8)
    man:iscsiadm(8)
    Process: 14658 ExecStart=/usr/sbin/iscsid (code=exited, status=0/SUCCESS)
    Main PID: 14660 (iscsid)
    CGroup: /system.slice/iscsid.service
    ##14659 /usr/sbin/iscsid
    ##14660 /usr/sbin/iscsid
```

Pour configurer iSCSI sur votre client Linux

1. Pour permettre à vos clients de basculer automatiquement entre vos serveurs de fichiers, vous devez configurer le multipath. Utilisez la commande suivante :

   ```
   ~$ sudo mpathconf --enable --with_multipathd y
   ```

2. Déterminez le nom de l'initiateur de votre hôte Linux à l'aide de la commande suivante. L'emplacement du nom de l'initiateur dépend de votre utilitaire iSCSI. Si vous utilisez`iscsi-initiator-utils`, le nom de l'initiateur se trouve dans le fichier`/etc/iscsi/initiatorname.iscsi`.

   ```
   ~$ sudo cat /etc/iscsi/initiatorname.iscsi
   ```

   Le système répond avec le nom de l'initiateur.

   ```
   InitiatorName=iqn.1994-05.com.redhat:abcdef12345
   ```

Configuration de l'iSCSI sur le système de fichiers FSx pour ONTAP

1. Connectez-vous à la CLI NetApp ONTAP sur le système de fichiers FSx for ONTAP sur lequel vous avez créé le LUN iSCSI à l'aide de la commande suivante. Pour plus d'informations, consultez Utilisation de la CLI NetApp ONTAP.

   ```
   ~$ ssh fsxadmin@your_management_endpoint_ip
   ```

2. Créez le groupe d'initiateurs (`igroup`) à l'aide de la NetApp commande ONTAP lun igroup createCLI. Un groupe d'initiateurs est mappé aux LUN iSCSI et contrôle quels initiateurs (clients) ont accès aux LUN. `host_initiator_name`Remplacez-le par le nom de l'initiateur de votre hôte Linux que vous avez récupéré lors de la procédure précédente.

   ```
   ::> lun igroup create -vserver svm_name -igroup igroup_name -
   initiator host_initiator_name -protocol iscsi -ostype linux
   ```

   Si vous souhaitez que les LUN mappés à cet igroup soient accessibles à plusieurs hôtes, vous pouvez spécifier plusieurs noms d'initiateurs séparés par une virgule. Pour plus d'informations, consultez lun igroup create dans le centre de documentation NetApp ONTAP.

3. Vérifiez qu'il `igroup` existe à l'aide de la lun igroup showcommande :

```
::> lun igroup show
```

Le système répond avec le résultat suivant :

```
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
svm_name  igroup_name  iscsi    linux    iqn.1994-05.com.redhat:abcdef12345
```

4. Cette étape suppose que vous avez déjà créé un LUN iSCSI. Si ce n'est pas le cas, consultez step-by-step les instructions Création d'un LUN iSCSI pour le faire.

Créez un mappage entre le LUN que vous avez créé et l'igroup que vous avez créé, en utilisant le lun mapping create, en spécifiant les attributs suivants :

- *svm_name*— Nom de la machine virtuelle de stockage fournissant la cible iSCSI. L'hôte utilise cette valeur pour atteindre le LUN.
- *vol_name*— Nom du volume hébergeant le LUN.
- *lun_name*— Le nom que vous avez attribué au LUN.
- *igroup_name*— Nom du groupe d'initiateurs.
- *lun_id*— L'entier de l'ID de LUN est spécifique au mappage, et non au LUN lui-même. Ceci est utilisé par les initiateurs de l'igroup car le numéro d'unité logique utilise cette valeur pour l'initiateur lors de l'accès au stockage.

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -
igroup igroup_name -lun-id lun_id
```

5. Utilisez la `lun show -path`commande pour confirmer que le LUN est créé, en ligne et mappé.

```
::> lun show -path /vol/vol_name/lun_name -fields state,mapped,serial-hex
```

Le système répond avec le résultat suivant :

```
 Vserver    Path                            serial-hex              state    mapped
 --------- ------------------------------- ----------------------- -------
 --------
```

```
 svm_name  /vol/vol_name/lun_name          6c5742314e5d52766e796150 online   mapped
```

Enregistrez la `serial_hex` valeur (dans cet exemple, elle l'est`6c5742314e5d52766e796150`), vous l'utiliserez ultérieurement pour créer un nom convivial pour le périphérique de blocage.

6. Utilisez la `network interface show -vserver`commande pour récupérer les adresses des `iscsi_2` interfaces `iscsi_1` et de la SVM dans laquelle vous avez créé votre LUN iSCSI.

```
::> network interface show -vserver svm_name
```

Le système répond avec le résultat suivant :

```
            Logical               Status     Network            Current
        Current Is
Vserver     Interface             Admin/Oper Address/Mask       Node
        Port    Home
----------- ----------            ---------- ------------------ -------------
        ------- ----
svm_name
            iscsi_1               up/up      172.31.0.143/20
 FSxId0123456789abcdef8-01  e0e     true
            iscsi_2               up/up      172.31.21.81/20
 FSxId0123456789abcdef8-02  e0e     true
            nfs_smb_management_1
                                  up/up      198.19.250.177/20
 FSxId0123456789abcdef8-01  e0e     true
3 entries were displayed.
```

Dans cet exemple, l'adresse IP de `iscsi_1` is `172.31.0.143` et `iscsi_2` is`172.31.21.81`.

Montez un LUN iSCSI sur votre client Linux

1. *Sur votre client Linux, utilisez la commande suivante pour découvrir les nœuds iSCSI cibles à l'aide de l'adresse IP iscsi_1 iSCSI_1_IP.*

```
~$ sudo iscsiadm --mode discovery --op update --type sendtargets --
portal iscsi_1_IP
```

```
172.31.0.143:3260,1029
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
```

```
172.31.21.81:3260,1028
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
```

Dans cet exemple, `iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3` correspond au `target_initiator` LUN iSCSI dans la zone de disponibilité préférée.

2. (Facultatif) Vous pouvez établir des sessions supplémentaires avec le`target_initiator`. Amazon EC2 a une limite de bande passante de 5 Go/s (~625 Mo/s) pour le trafic à flux unique, mais vous pouvez créer plusieurs sessions pour augmenter le débit de votre système de fichiers à partir d'un seul client. Pour plus d'informations, consultez la bande passante du réseau des instances Amazon EC2 dans le guide de l'utilisateur Amazon Elastic Compute Cloud pour les instances Linux.

   La commande suivante établit 8 sessions par initiateur et par nœud ONTAP dans chaque zone de disponibilité, permettant au client de générer jusqu'à 40 Gbit/s (5 000 Mo/s) de débit agrégé vers le LUN iSCSI.

   ```
   ~$ sudo iscsiadm --mode node -T target_initiator --op update -n
    node.session.nr_sessions -v 8
   ```

3. Connectez-vous aux initiateurs cibles. Vos LUN iSCSI sont présentés sous forme de disques disponibles.

   ```
   ~$ sudo iscsiadm --mode node -T target_initiator --login
   ```

   ```
   Logging in to [iface: default, target:
    iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:
    172.31.14.66,3260] (multiple)
   Login to [iface: default, target:
    iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:
    172.31.14.66,3260] successful.
   ```

   Le résultat ci-dessus est tronqué ; vous devriez voir une `Logging in` et une `Login successful` réponse pour chaque session sur chaque serveur de fichiers. Dans le cas de 4 sessions par nœud, il y aura 8 `Logging in` et 8 `Login successful` réponses.

4. Utilisez la commande suivante pour vérifier que les sessions iSCSI ont `dm-multipath` été identifiées et fusionnées en affichant un seul LUN avec plusieurs politiques. Il doit y avoir un nombre égal d'appareils répertoriés comme `active` et ceux répertoriés commeenabled.

```
~$ sudo multipath -ll
```

Dans la sortie, le nom du disque est formaté sous la formedm-xyz, où xyz est un entier. S'il n'existe aucun autre disque à chemins multiples, cette valeur estdm-0.

```
3600a09806c5742314e5d52766e79614f dm-xyz NETAPP  ,LUN C-Mode
size=10G features='4 queue_if_no_path pg_init_retries 50 retain_attached_hw_handle'
 hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- 0:0:0:1 sda     8:0   active ready running
| |- 1:0:0:1 sdc     8:32  active ready running
| |- 3:0:0:1 sdg     8:96  active ready running
| `- 4:0:0:1 sdh     8:112 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 2:0:0:1 sdb     8:16  active ready running
  |- 7:0:0:1 sdf     8:80  active ready running
  |- 6:0:0:1 sde     8:64  active ready running
  `- 5:0:0:1 sdd     8:48  active ready running
```

Votre périphérique de blocage est désormais connecté à votre client Linux. Il est situé sous le chemin/dev/*dm-xyz*. Vous ne devez pas utiliser ce chemin à des fins administratives ; utilisez plutôt le lien symbolique situé sous le chemin/dev/mapper/*wwid*, où se *wwid* trouve un identifiant unique pour votre LUN qui est cohérent sur tous les appareils. À l'étape suivante, vous allez donner un nom convivial au *wwid* afin de le distinguer des autres disques à chemins multiples.

Pour attribuer un nom convivial à votre appareil de blocage

1. Pour attribuer un nom convivial à votre appareil, créez un alias dans le /etc/multipath.conf fichier. Pour ce faire, ajoutez l'entrée suivante au fichier à l'aide de votre éditeur de texte préféré, en remplaçant les espaces réservés suivants :

   - Remplacez serial_hex par la valeur que vous avez enregistrée dans la Configuration de l'iSCSI sur le système de fichiers FSx pour ONTAP procédure.
   - Ajoutez le préfixe 3600a0980 à la serial_hex valeur comme indiqué dans l'exemple. Il s'agit d'un préambule unique pour la distribution NetApp ONTAP utilisée par Amazon FSx for ONTAP. NetApp

- `device_name`Remplacez-le par le nom convivial que vous souhaitez utiliser pour votre appareil.

```
multipaths {
    multipath {
        wwid 3600a0980serial_hex
        alias device_name
    }
}
```

Vous pouvez également copier et enregistrer le script suivant dans un fichier bash, tel que`multipath_alias.sh`. Vous pouvez exécuter le script avec les privilèges sudo, en le remplaçant *`serial_hex`* (sans le préfixe 3600a0980) par votre numéro de série respectif et *`device_name`* le nom convivial souhaité. Ce script recherche une `multipaths` section non commentée du `/etc/multipath.conf` fichier. S'il en existe une, elle ajoute une `multipath` entrée à cette section ; sinon, elle créera une nouvelle `multipaths` section avec une `multipath` entrée pour votre appareil bloqué.

```
#!/bin/bash
SN=serial_hex
ALIAS=device_name
CONF=/etc/multipath.conf
grep -q '^multipaths {' $CONF
UNCOMMENTED=$?
if [ $UNCOMMENTED -eq 0 ]
then
        sed -i '/^multipaths {/a\\tmultipath {\n\t\twwid 3600a0980'"${SN}"'\n\t
\talias '"${ALIAS}"'\n\t}\n' $CONF
else
        printf "multipaths {\n\tmultipath {\n\t\twwid 3600a0980$SN\n\t\talias
 $ALIAS\n\t}\n}" >> $CONF
fi
```

2. Redémarrez le `multipathd` service pour que les modifications `/etc/multipathd.conf` prennent effet.

```
~$ systemctl restart multipathd.service
```

Pour partitionner le LUN

L'étape suivante consiste à formater et partitionner votre LUN à l'aide `fdisk` de.

1. Utilisez la commande suivante pour vérifier que le chemin d'accès à votre `device_name`

```
~$ ls /dev/mapper/device_name
```

```
/dev/device_name
```

2. Partitionnez le disque en utilisant`fdisk`. Vous allez entrer une invite interactive. Entrez les options dans l'ordre indiqué. Notez que la `Last sector` valeur varie en fonction de la taille de votre LUN iSCSI (10 Go dans cet exemple). Vous pouvez créer plusieurs partitions en utilisant une valeur inférieure au dernier secteur (`20971519`dans cet exemple).

```
~$ sudo fdisk /dev/mapper/device_name
```

L'invite `fsdisk` interactive démarre.

```
Welcome to fdisk (util-linux 2.30.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x66595cb0.

Command (m for help): n
Partition type
   p primary (0 primary, 0 extended, 4 free)
   e extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048): 2048
Last sector, +sectors or +size{K,M,G,T,P} (2048-20971519, default
 20971519): 20971519

Created a new partition 1 of type 'Linux' and of size 512 B.
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
```

```
Syncing disks.
```

Une fois que vous w êtes entrée, votre nouvelle `/dev/mapper/`*`partition_name`* partition est disponible. <device_name><partition_number>Le *`partition_name a le format`*. 1a été utilisé comme numéro de partition utilisé dans la `fdisk` commande de l'étape précédente.

3. Créez votre système de fichiers en utilisant `/dev/mapper/`*`partition_name`* comme chemin.

```
~$ sudo mkfs.ext4 /dev/mapper/partition_name
```

Le système répond avec le résultat suivant :

```
mke2fs 1.42.9 (28-Dec-2013)
Discarding device blocks: done
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=16 blocks
655360 inodes, 2621184 blocks
131059 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
80 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
     32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632
Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

Pour monter le LUN sur le client Linux

1. Créez un répertoire *`directory_path`* comme point de montage pour votre système de fichiers.

```
~$ sudo mkdir /directory_path/mount_point
```

2. Montez le système de fichiers à l'aide de la commande suivante.

```
~$ sudo mount -t ext4 /dev/mapper/partition_name /directory_path/mount_point
```

3. (Facultatif) Vous pouvez transférer la propriété du répertoire de montage à votre utilisateur. Remplacez *username* par votre nom d'utilisateur.

```
~$ sudo chown username:username /directory_path/mount_point
```

4. (Facultatif) Vérifiez que vous pouvez lire et écrire des données dans le système de fichiers.

```
~$ echo "Hello world!" > /directory_path/mount_point/HelloWorld.txt
~$ cat directory_path/HelloWorld.txt
Hello world!
```

Vous avez créé et monté avec succès un LUN iSCSI sur votre client Linux.

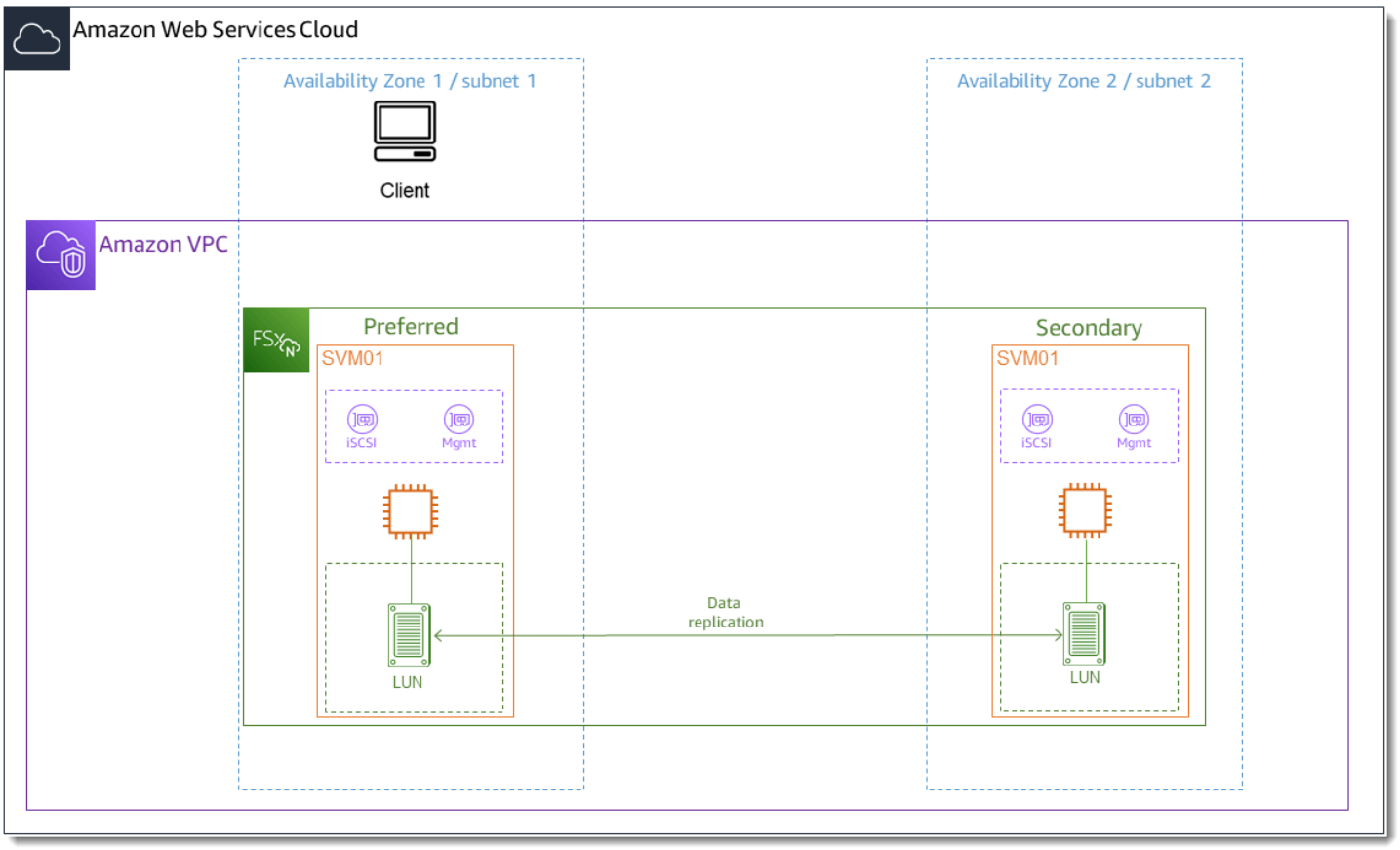
Montage de LUN iSCSI sur un client Windows

Les exemples présentés dans ces procédures utilisent la configuration suivante :

- Le LUN iSCSI qui est monté sur un hôte Windows est déjà créé. Pour plus d'informations, consultez Création d'un LUN iSCSI.
- L'hôte Microsoft Windows qui monte le LUN iSCSI est une instance Amazon EC2 exécutant une Amazon Machine Image (AMI) Microsoft Windows Server 2019. Il possède des groupes de sécurité VPC configurés pour autoriser le trafic entrant et sortant, comme décrit dans. Contrôle d'accès au système de fichiers avec Amazon VPC

  Il se peut que vous utilisiez une autre AMI Microsoft Windows dans votre configuration.
- Le client et le système de fichiers se trouvent dans le même VPC et. Compte AWS Si le client se trouve dans un autre VPC, vous pouvez utiliser le peering VPC ou accorder AWS Transit Gateway à d'autres VPC l'accès aux points de terminaison iSCSI. Pour plus d'informations, consultez Accès aux données depuis l'extérieur du VPC de déploiement.

  Nous recommandons que l'instance EC2 se trouve dans la même zone de disponibilité que le sous-réseau préféré de votre système de fichiers, comme illustré dans le graphique suivant.



Rubriques

- Configuration de l'iSCSI sur le client Windows
- Configuration de l'iSCSI sur le système de fichiers FSx pour ONTAP
- Monter un LUN iSCSI sur le client Windows
- Validation de votre configuration iSCSI

Configuration de l'iSCSI sur le client Windows

1. Utilisez Windows Remote Desktop pour vous connecter au client Windows sur lequel vous souhaitez monter le LUN iSCSI. Pour plus d'informations, consultez Connect to your Windows instance using RDP dans le manuel Amazon Elastic Compute Cloud User Guide.
2. Ouvrez une fenêtre PowerShell en tant qu'administrateur. Utilisez les commandes suivantes pour activer iSCSI sur votre instance Windows et configurer le service iSCSI pour qu'il démarre automatiquement.

```
PS C:\> Start-Service MSiSCSI
```

```
PS C:\> Set-Service -Name msiscsi -StartupType Automatic
```

3. Récupérez le nom de l'initiateur de votre instance Windows. Vous utiliserez cette valeur pour configurer iSCSI sur votre système de fichiers FSx for ONTAP à l'aide de la CLI ONTAP. NetApp

   ```
   PS C:\> (Get-InitiatorPort).NodeAddress
   ```

   Le système répond par le port initiateur :

   ```
   iqn.1991-05.com.microsoft:ec2amaz-abc123d
   ```

4. Pour permettre à vos clients de basculer automatiquement entre vos serveurs de fichiers, vous devez installer `Multipath-IO` (MPIO) sur votre instance Windows. Utilisez la commande suivante :

   ```
   PS C:\> Install-WindowsFeature Multipath-IO
   ```

5. Redémarrez votre instance Windows une fois l'`Multipath-IO`installation terminée. Gardez votre instance Windows ouverte pour effectuer les étapes de montage du LUN iSCSI dans la section suivante.

Configuration de l'iSCSI sur le système de fichiers FSx pour ONTAP

1. Connectez-vous à la CLI NetApp ONTAP sur le système de fichiers FSx for ONTAP sur lequel vous avez créé le LUN iSCSI à l'aide de la commande suivante. Pour plus d'informations, consultez Utilisation de la CLI NetApp ONTAP.

   ```
   ~$ ssh fsxadmin@your_management_endpoint_ip
   ```

2. À l'aide de la CLI NetApp ONTAP lun igroup create, créez le groupe d'initiateurs, ou. `igroup` Un groupe d'initiateurs est mappé aux LUN iSCSI et contrôle quels initiateurs (clients) ont accès aux LUN. `host_initiator_name`Remplacez-le par le nom de l'initiateur de votre hôte Windows que vous avez récupéré lors de la procédure précédente.

   ```
   ::> lun igroup create -vserver svm_name -igroup igroup_name -
   initiator host_initiator_name -protocol iscsi -ostype windows
   ```

Si vous souhaitez que les LUN mappés à celui-ci soient `igroup` accessibles à plusieurs hôtes, vous pouvez spécifier plusieurs noms d'initiateurs séparés par des virgules. Pour plus d'informations, consultez `lun igroup create`le centre de documentation NetApp ONTAP.

3. Vérifiez que le `igroup` a été créé avec succès à l'aide de la commande suivante :

```
::> lun igroup show
```

Le système répond avec le résultat suivant :

```
Vserver    Igroup        Protocol OS Type  Initiators
---------  ------------  -------- -------- ------------------------------------
svm_name   igroup_name   iscsi    windows  iqn.1994-05.com.windows:abcdef12345
```

Une fois `igroup` créé, vous êtes prêt à créer des LUN et à les mapper au`igroup`.

4. Cette étape suppose que vous avez déjà créé un LUN iSCSI. Si ce n'est pas le cas, consultez step-by-step les instructions Création d'un LUN iSCSI pour le faire.

Créez un mappage de LUN entre le LUN et votre nouveau. `igroup`

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -
igroup igroup_name -lun-id lun_id
```

5. Vérifiez que le LUN est créé, en ligne et mappé à l'aide de la commande suivante :

```
::> lun show -path /vol/vol_name/lun_name
Vserver     Path                            State   Mapped   Type     Size
---------   ------------------------------- ------- -------- -------- --------
svm_name    /vol/vol_name/lun_name          online  mapped   windows  10GB
```

Vous êtes maintenant prêt à ajouter la cible iSCSI sur votre instance Windows.

6. Récupérez les adresses IP des `iscsi_2` interfaces `iscsi_1` et de votre SVM à l'aide de la commande suivante :

```
::> network interface show -vserver svm_name
```

```
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
```

```
----------- ---------- ---------- ------------------ ------------- ------- ----
svm_name
            iscsi_1    up/up      172.31.0.143/20    FSxId0123456789abcdef8-01
                                                                   e0e     true
            iscsi_2    up/up      172.31.21.81/20    FSxId0123456789abcdef8-02
                                                                   e0e     true
            nfs_smb_management_1
                       up/up      198.19.250.177/20  FSxId0123456789abcdef8-01
                                                                   e0e     true
3 entries were displayed.
```

Dans cet exemple, l'adresse IP de `iscsi_1` is `172.31.0.143` et `iscsi_2` is`172.31.21.81`.

Monter un LUN iSCSI sur le client Windows

1. Sur votre instance Windows, ouvrez un PowerShell terminal en tant qu'administrateur.
2. Vous allez créer un `.ps1` script qui effectue les opérations suivantes :

   - Se connecte à chacune des interfaces iSCSI de votre système de fichiers.
   - Ajoute et configure le MPIO pour iSCSI.
   - Établit 8 sessions pour chaque connexion iSCSI, ce qui permet au client de générer jusqu'à 40 Gbit/s (5 000 Mo/s) de débit agrégé vers le LUN iSCSI. Le fait de disposer de 8 sessions garantit qu'un seul client peut exploiter la capacité de débit totale de 4 000 Mo/s pour le plus haut niveau de capacité de débit FSx for ONTAP. Vous pouvez éventuellement augmenter ou diminuer le nombre de sessions (chaque session fournit jusqu'à 625 Mo/s de débit) en modifiant la boucle for du script lors de l'`#Establish iSCSI connection`étape passant d'une borne supérieure `1..8` à une autre. Pour plus d'informations, consultez la bande passante réseau des instances Amazon EC2 dans le guide de l'utilisateur Amazon Elastic Compute Cloud pour les instances Windows.

   Copiez le jeu de commandes suivant dans un fichier pour créer le `.psl` script.

   - Remplacez `iscsi_1` et `iscsi_2` par les adresses IP que vous avez récupérées à l'étape précédente.
   - Remplacez `ec2_ip` par l'adresse IP de votre instance Windows.

```
#iSCSI IP addresses for Preferred and Standby subnets
```

```
$TargetPortalAddresses = @("iscsi_1","iscsi_2")

#iSCSI Initator IP Address (Local node IP address)
$LocaliSCSIAddress = "ec2_ip"

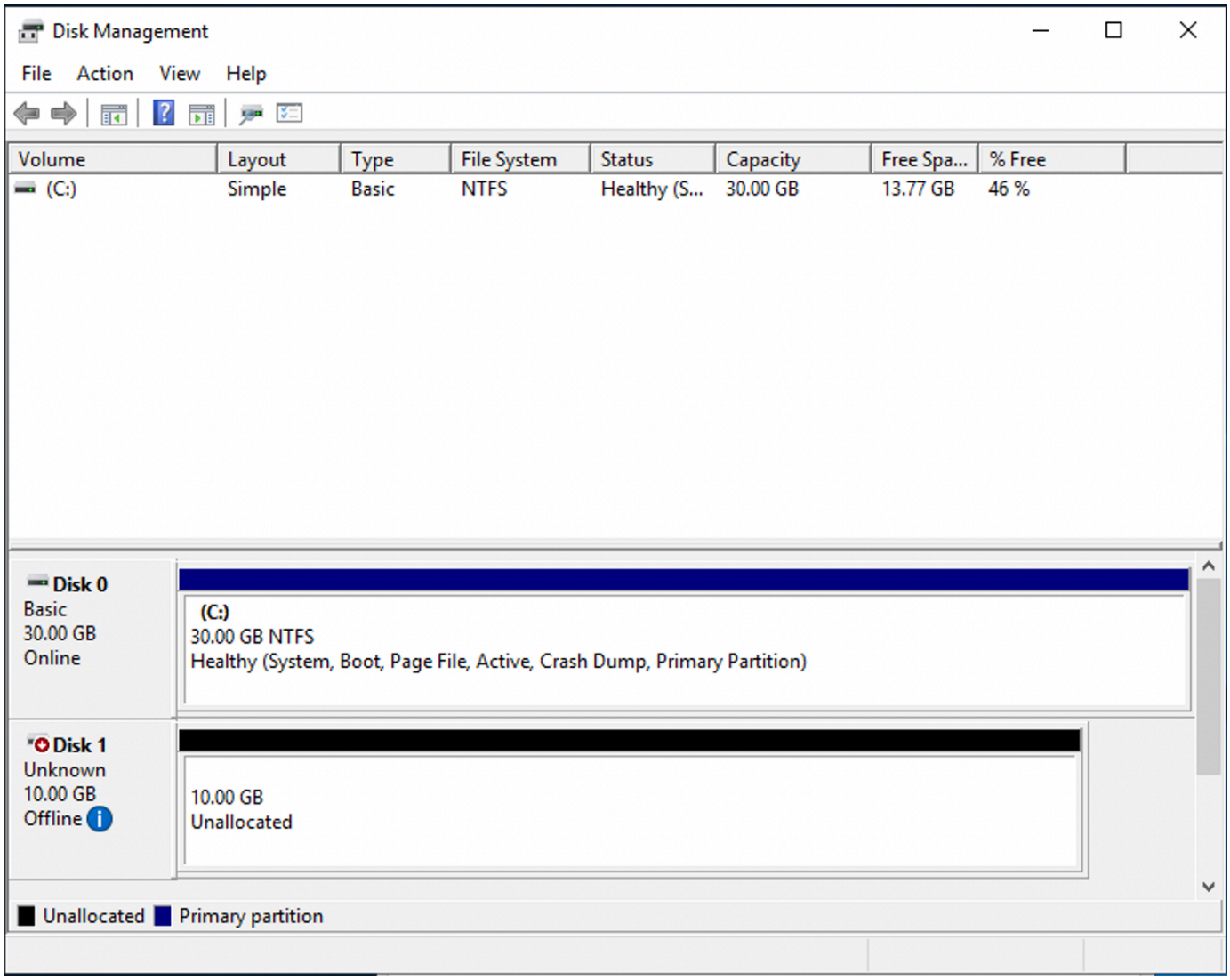
#Connect to FSx for NetApp ONTAP file system
Foreach ($TargetPortalAddress in $TargetPortalAddresses) {
New-IscsiTargetPortal -TargetPortalAddress $TargetPortalAddress -
TargetPortalPortNumber 3260 -InitiatorPortalAddress $LocaliSCSIAddress
}

#Add MPIO support for iSCSI
New-MSDSMSupportedHW -VendorId MSFT2005 -ProductId iSCSIBusType_0x9

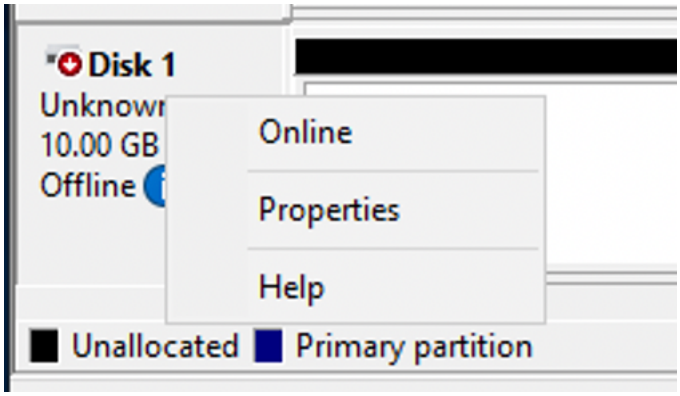
#Establish iSCSI connection
1..8 | %{Foreach($TargetPortalAddress in $TargetPortalAddresses)
{Get-IscsiTarget | Connect-IscsiTarget -IsMultipathEnabled $true -
TargetPortalAddress $TargetPortalAddress -InitiatorPortalAddress $LocaliSCSIAddress
 -IsPersistent $true}}

#Set the MPIO Policy to Round Robin
Set-MSDSMGlobalDefaultLoadBalancePolicy -Policy RR
```

3. Lancez l'application Windows Disk Management. Ouvrez la boîte de dialogue Windows Run, entrez `diskmgmt.msc` et appuyez sur Entrée. L'application de gestion des disques s'ouvre.



4. Localisez le disque non alloué. Il s'agit du LUN iSCSI. Dans l'exemple, le disque 1 est le disque iSCSI. Il est hors ligne.



Mettez le volume en ligne en plaçant le curseur sur le disque 1, cliquez avec le bouton droit de la souris, puis choisissez En ligne.

> **Note**
>
> Vous pouvez modifier la politique du réseau de stockage (SAN) afin que les nouveaux volumes soient automatiquement mis en ligne. Pour plus d'informations, consultez les politiques relatives au SAN dans le Microsoft Windows Server Command Reference.

5. Pour initialiser le disque, placez le curseur sur le disque 1 avec le bouton droit de la souris, puis sélectionnez Initialiser. La boîte de dialogue Initialiser apparaît. Cliquez sur OK pour initialiser le disque.
6. Formatez le disque comme vous le feriez normalement. Une fois le formatage terminé, le lecteur iSCSI apparaît comme un lecteur utilisable sur le client Windows.

Validation de votre configuration iSCSI

Nous avons fourni un script pour vérifier que votre configuration iSCSI est correctement configurée. Le script examine des paramètres tels que le nombre de sessions, la distribution des nœuds et l'état des E/S multivoies (MPIO). La tâche suivante explique comment installer et utiliser le script.

Pour valider votre configuration iSCSI

1. Ouvrez une PowerShell fenêtre Windows.
2. Téléchargez le script à l'aide de la commande suivante.

```
PS C:\> Invoke-WebRequest "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/
samples/CheckiSCSI.zip" -OutFile "CheckiSCSI.zip"
```

3. Décompressez le fichier zip à l'aide de la commande suivante.

```
PS C:\> Expand-Archive -Path ".\CheckiSCSI.zip" -DestinationPath "./"
```

4. Exécutez le script à l'aide de la commande suivante.

```
PS C:\> ./CheckiSCSI.ps1
```

5. Passez en revue le résultat pour comprendre l'état actuel de votre configuration. L'exemple suivant illustre une configuration iSCSI réussie.

```
PS C:\> ./CheckiSCSI.ps1
```

```
This script checks the iSCSI configuration on the local instance.
It will provide information about the number of connected sessions, connected file
 servers, and MPIO status.

MPIO is installed on this server.

Initiator: 'iqn.1991-05.com.microsoft:ec2amaz-d2cebnb'
to Target: 'iqn.1992-08.com.netapp:sn.13266b10e61411ee8bc0c76ad263d613:vs.3'
has 16 total sessions (16 active, 0 non-active)
spread across 2 node(s).
MPIO: Yes
```

Utilisation de FSx for ONTAP avec d'autres services AWS

Outre Amazon EC2, vous pouvez utiliser d'autres AWS services avec vos volumes pour accéder à vos données.

Rubriques

- Utilisation d'Amazon WorkSpaces avec FSx pour ONTAP
- Utilisation d'Amazon Elastic Container Service avec FSx pour ONTAP
- Utilisation de VMware Cloud avec FSx pour ONTAP

Utilisation d'Amazon WorkSpaces avec FSx pour ONTAP

FSx for ONTAP peut être utilisé avec Amazon WorkSpaces pour fournir un stockage partagé en réseau (NAS) ou pour stocker des profils d'itinérance pour les comptes Amazon. WorkSpaces Après s'être connecté à un partage de fichiers SMB avec une WorkSpaces instance, l'utilisateur peut créer et modifier des fichiers sur le partage de fichiers.

Les procédures suivantes montrent comment utiliser Amazon FSx avec Amazon WorkSpaces pour fournir un accès cohérent au profil d'itinérance et au dossier de base et pour fournir un dossier d'équipe partagé aux utilisateurs de Windows et Linux. WorkSpaces Si vous utilisez Amazon pour la première fois WorkSpaces, vous pouvez créer votre premier WorkSpaces environnement Amazon en

suivant les instructions de la section Commencer avec la configuration WorkSpaces rapide du guide d' WorkSpaces administration Amazon.

Rubriques

- Fournir un support pour les profils d'itinérance
- Fournir un dossier partagé pour accéder aux fichiers communs

Fournir un support pour les profils d'itinérance

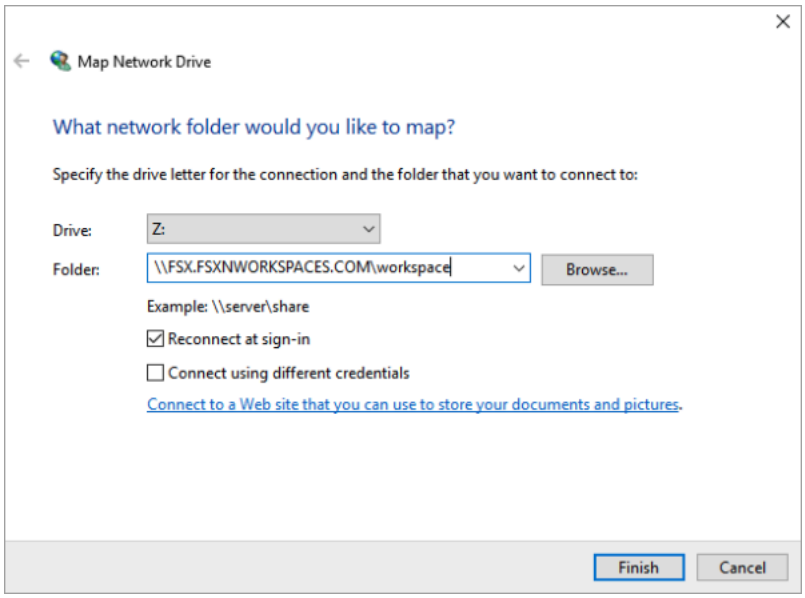
Vous pouvez utiliser Amazon FSx pour fournir une assistance en matière de profil d'itinérance aux utilisateurs de votre organisation. Un utilisateur sera autorisé à accéder uniquement à son profil d'itinérance. Le dossier sera automatiquement connecté à l'aide des politiques de groupe Active Directory. Avec un profil d'itinérance, les données et les paramètres de bureau des utilisateurs sont enregistrés lorsqu'ils se déconnectent d'un partage de fichiers Amazon FSx, ce qui permet de partager des documents et des paramètres entre WorkSpaces différentes instances, et sauvegardés automatiquement à l'aide des sauvegardes automatiques quotidiennes d'Amazon FSx.

Étape 1 : créer un emplacement de dossier de profil pour les utilisateurs du domaine à l'aide d'Amazon FSx

1. Créez un système de fichiers FSx pour ONTAP à l'aide de la console Amazon FSx. Pour en savoir plus, consultez Pour créer un système de fichiers (console).

> **Important**
>
> Chaque système de fichiers FSx for ONTAP possède une plage d'adresses IP de point de terminaison à partir de laquelle les points de terminaison associés au système de fichiers sont créés. Pour les systèmes de fichiers multi-AZ, FSx for ONTAP choisit une plage d'adresses IP non utilisées par défaut comprise entre 198.19.0.0/16 comme plage d'adresses IP de point de terminaison. Cette plage d'adresses IP est également utilisée WorkSpaces pour la gestion de la plage de trafic, comme décrit dans la section Exigences relatives aux adresses IP et WorkSpaces aux ports du guide d' WorkSpaces administration Amazon. Par conséquent, pour accéder à votre système de fichiers Multi-AZ FSx for ONTAP WorkSpaces depuis, vous devez sélectionner une plage d'adresses IP de point de terminaison qui ne chevauche pas 198.19.0.0/16.

2. Si aucune machine virtuelle de stockage (SVM) n'est associée à un Active Directory, créez-en une dès maintenant. Par exemple, vous pouvez configurer une SVM nommée `fsx` et définir le style de sécurité surNTFS. Pour en savoir plus, consultez Pour créer une machine virtuelle de stockage (console).
3. Créez un volume pour votre SVM. Par exemple, vous pouvez créer un volume nommé `fsx-vol` qui hérite du style de sécurité du volume racine de votre SVM. Pour en savoir plus, consultez Pour créer un FlexVol volume (console).
4. Créez un partage SMB sur votre volume. Par exemple, vous pouvez créer un partage appelé `workspace` sur votre volume nomméfsx-vol, dans lequel vous créez un dossier nomméprofiles. Pour en savoir plus, consultez Gestion des actions des PME.
5. Accédez à votre SVM Amazon FSx depuis une instance Amazon EC2 exécutant Windows Server ou depuis un. WorkSpace Pour en savoir plus, consultez Accès aux données .
6. Vous mappez votre partage `Z:\` sur votre WorkSpaces instance Windows :



Étape 2 : lier le partage de fichiers FSx for ONTAP aux comptes d'utilisateurs

1. Sur celui de votre utilisateur de test WorkSpace, choisissez Windows > Système > Paramètres système avancés.
2. Dans Propriétés du système, sélectionnez l'onglet Avancé et appuyez sur le bouton Paramètres dans la section Profils utilisateur. L'utilisateur connecté aura un type de profil de. `Local`
3. Déconnectez l'utilisateur de test du WorkSpace.

4. Configurez l'utilisateur de test pour qu'il dispose d'un profil d'itinérance situé sur votre système de fichiers Amazon FSx. Dans votre administrateur WorkSpaces, ouvrez une PowerShell console et utilisez une commande similaire à l'exemple suivant (qui utilise le `profiles` dossier que vous avez créé précédemment à l'étape 1) :

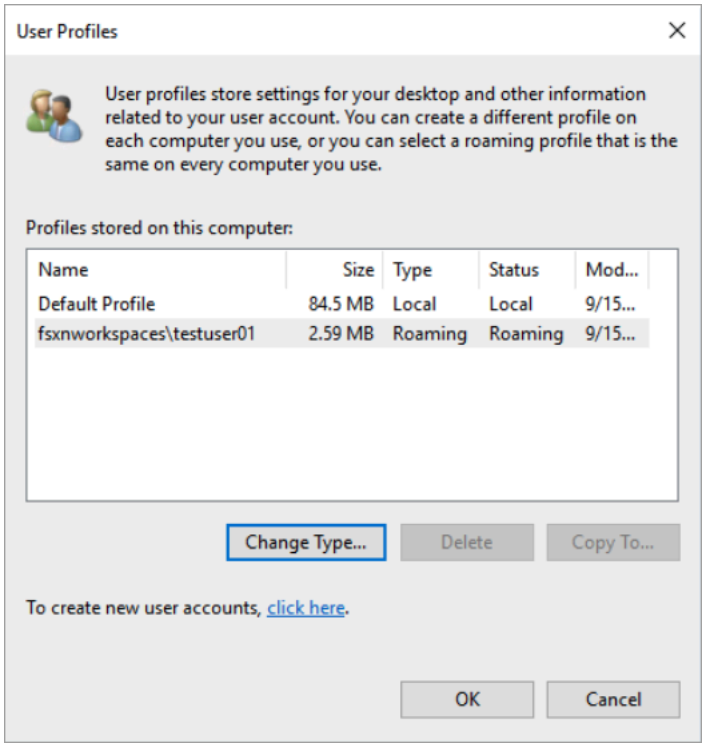
   ```
   Set-ADUser username -ProfilePath \\filesystem-dns-name\sharename\foldername\username
   ```

   Par exemple :

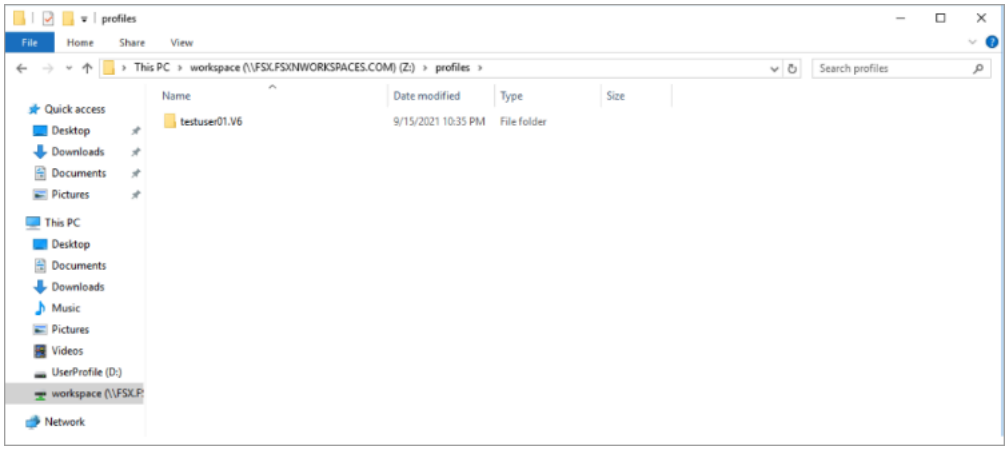
   ```
   Set-ADUser testuser01 -ProfilePath \\fsx.fsxnworkspaces.com\workspace\profiles\testuser01
   ```

5. Connectez-vous à l'utilisateur de test WorkSpace.

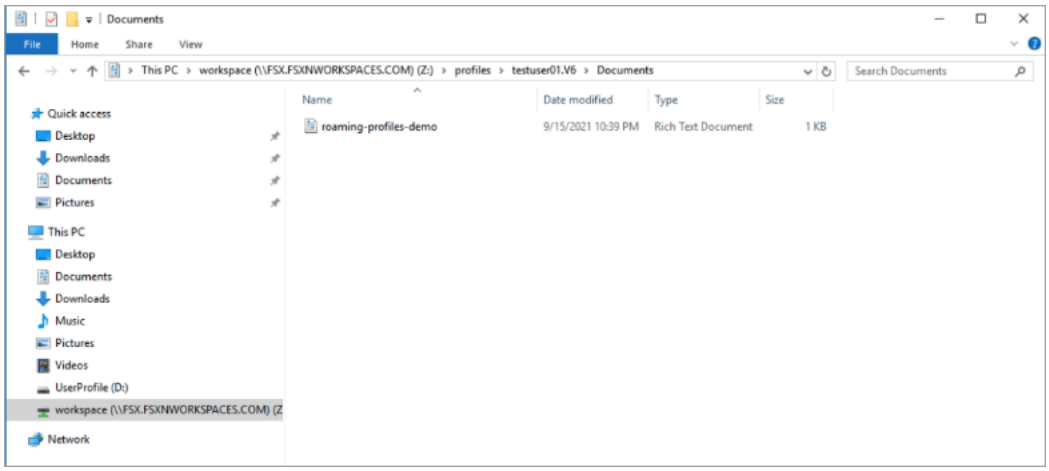
6. Dans Propriétés du système, sélectionnez l'onglet Avancé et appuyez sur le bouton Paramètres dans la section Profils utilisateur. L'utilisateur connecté aura un type de profil de. `Roaming`



7. Parcourez le dossier partagé FSx for ONTAP. Dans le `profiles` dossier, vous verrez un dossier pour l'utilisateur.



8. Création d'un document dans le `Documents` dossier de l'utilisateur de test
9. Déconnectez l'utilisateur de test de son WorkSpace.
10. Si vous vous reconnectez en tant qu'utilisateur test et que vous accédez à sa boutique de profils, vous verrez le document que vous avez créé.



Fournir un dossier partagé pour accéder aux fichiers communs

Vous pouvez utiliser Amazon FSx pour fournir un dossier partagé aux utilisateurs de votre organisation. Un dossier partagé peut être utilisé pour stocker des fichiers utilisés par votre communauté d'utilisateurs, tels que des fichiers de démonstration, des exemples de code et des manuels d'instructions nécessaires à tous les utilisateurs. Généralement, vous avez des lecteurs mappés pour des dossiers partagés ; toutefois, comme les lecteurs mappés utilisent des lettres, le nombre de partages que vous pouvez avoir est limité. Cette procédure crée un dossier partagé Amazon FSx disponible sans lettre de lecteur, ce qui vous donne une plus grande flexibilité dans l'attribution de partages aux équipes.

Pour monter un dossier partagé pour un accès multiplateforme depuis Linux et Windows WorkSpaces

1. Dans la barre des tâches, choisissez Lieux > Connect to Server.

   a. Pour Serveur, entrez *`file-system-dns-name`*.

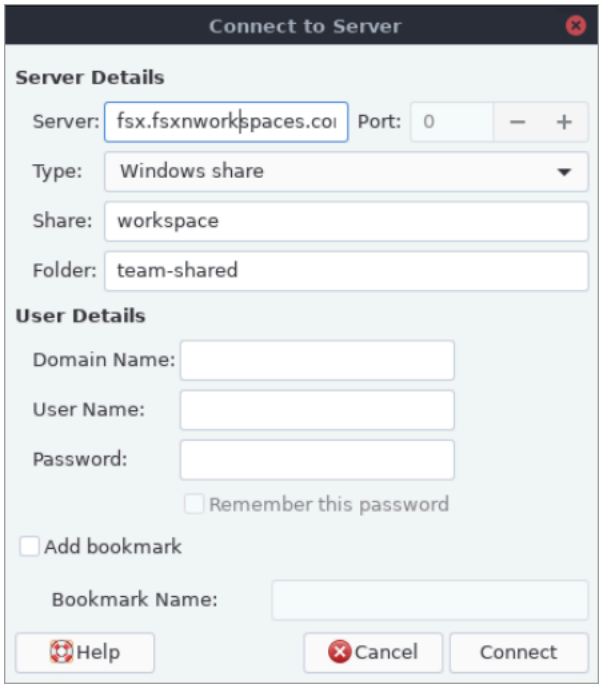
   b. Réglez Type sur`Windows share`.

   c. Définissez Share sur le nom du partage SMB, tel que`workspace`.

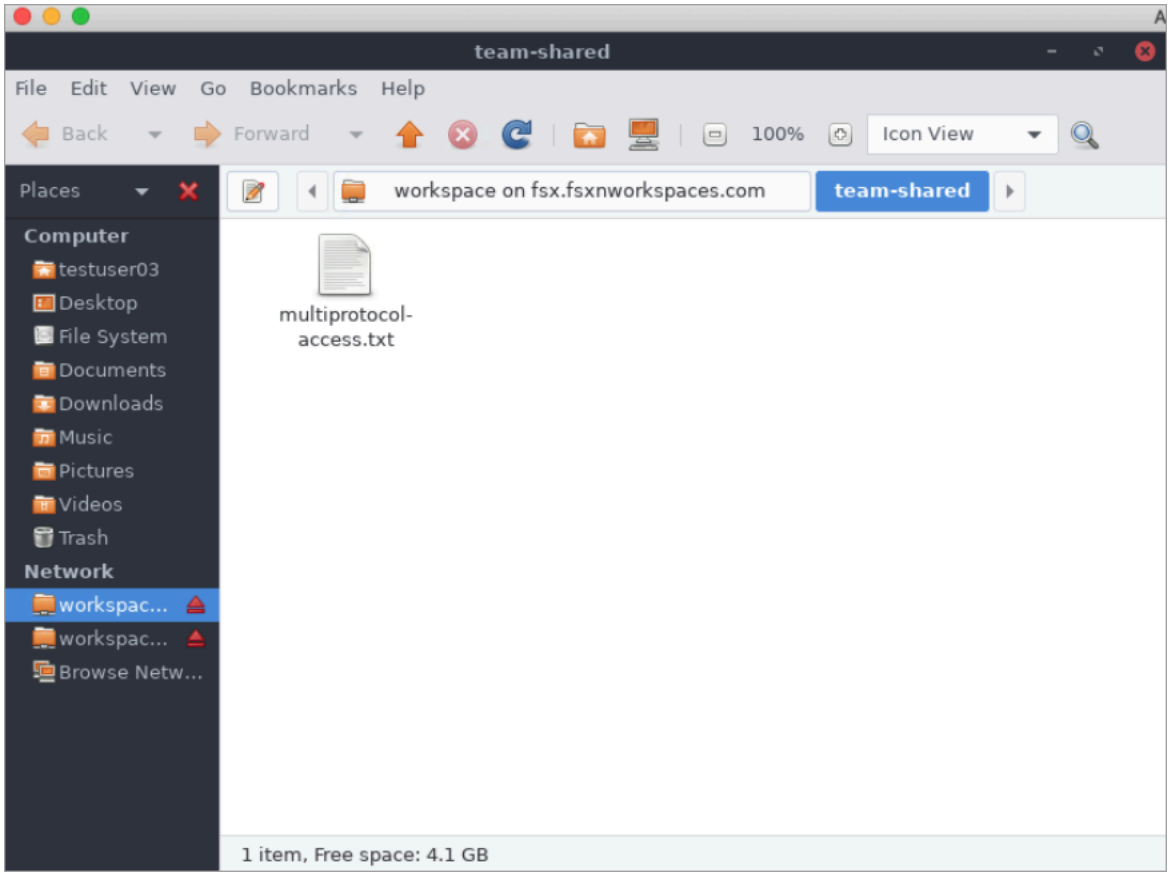
   d. Vous pouvez laisser le dossier tel quel / ou le définir comme dossier, tel qu'un dossier nommé`team-shared`.

   e. Pour un système Linux WorkSpace, vous n'avez pas besoin de saisir vos informations d'utilisateur si votre système Linux WorkSpace appartient au même domaine que le partage Amazon FSx.

   f. Choisissez Se connecter.



2. Une fois la connexion établie, vous pouvez voir le dossier partagé (nommé `team-shared` dans cet exemple) dans le partage SMB nommé`workspace`.



Utilisation d'Amazon Elastic Container Service avec FSx pour ONTAP

Vous pouvez accéder à vos systèmes de fichiers Amazon FSx for NetApp ONTAP depuis un conteneur Docker Amazon Elastic Container Service (Amazon ECS) sur une instance Amazon EC2 Linux ou Windows.

Montage sur un conteneur Linux Amazon ECS

1. Créez un cluster ECS à l'aide du modèle de cluster EC2 Linux + Networking pour vos conteneurs Linux. Pour plus d'informations, consultez la section Création d'un cluster dans le manuel Amazon Elastic Container Service Developer Guide.
2. Créez un répertoire sur l'instance EC2 pour monter le volume de la SVM comme suit :

```
sudo mkdir /fsxontap
```

3. Montez votre volume FSx for ONTAP sur l'instance Linux EC2 en utilisant un script de données utilisateur lors du lancement de l'instance ou en exécutant les commandes suivantes :

```
sudo mount -t nfs svm-ip-address:/vol1 /fsxontap
```

4. Montez le volume à l'aide de la commande suivante :

```
sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /
fsxontap
```

L'exemple suivant utilise des exemples de valeurs.

```
sudo mount -t nfs -o nfsvers=4.1
 svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /
fsxontap
```

Vous pouvez également utiliser l'adresse IP de la SVM au lieu de son nom DNS.

```
sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
```

5. Lorsque vous créez vos définitions de tâches Amazon ECS, ajoutez les propriétés de `mountPoints` conteneur `volumes` et les propriétés de conteneur suivantes dans la définition de conteneur JSON. Remplacez-le `sourcePath` par le point de montage et le répertoire de votre système de fichiers FSx for ONTAP.

```
{
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
```

```
}
```

Montage sur un conteneur Windows Amazon ECS

1. Créez un cluster ECS à l'aide du modèle de cluster réseau EC2 Windows + pour vos conteneurs Windows. Pour plus d'informations, consultez la section Création d'un cluster dans le manuel Amazon Elastic Container Service Developer Guide.
2. Ajoutez une instance Windows EC2 jointe à un domaine au cluster Windows ECS et mappez un partage SMB.

   Lancez une instance Windows EC2 optimisée pour ECS jointe à votre domaine Active Directory et initialisez l'agent ECS en exécutant la commande suivante.

   ```
   PS C:\Users\user> Initialize-ECSAgent -Cluster windows-fsx-cluster -
   EnableTaskIAMRole
   ```

   Vous pouvez également transmettre les informations d'un script au champ de texte des données utilisateur comme suit.

   ```
   <powershell>
   Initialize-ECSAgent -Cluster windows-fsx-cluster -EnableTaskIAMRole
   </powershell>
   ```

3. Créez un mappage global SMB sur l'instance EC2 afin de pouvoir mapper votre partage SMB à un lecteur. Remplacez les valeurs situées sous le nom netbios ou DNS pour votre système de fichiers FSx et le nom de partage. Le volume NFS vol1 qui a été monté sur l'instance Linux EC2 est configuré en tant que partage CIFS fsxontap sur le système de fichiers FSx.

   ```
   vserver cifs share show -vserver svm08 -share-name fsxontap


                                   Vserver: svm08
                                     Share: fsxontap
                   CIFS Server NetBIOS Name: FSX0NTAPDEMO
                                     Path: /vol1
                            Share Properties: oplocks
                                              browsable
                                              changenotify
                                              show-previous-versions
   ```

```
                          Symlink Properties: symlinks
                    File Mode Creation Mask: -
                Directory Mode Creation Mask: -
                               Share Comment: -
                                   Share ACL: Everyone / Full Control
            File Attribute Cache Lifetime: -
                             Volume Name: vol1
                            Offline Files: manual
            Vscan File-Operations Profile: standard
        Maximum Tree Connections on Share: 4294967295
               UNIX Group for File Create: -
```

4. Créez le mappage global SMB sur l'instance EC2 à l'aide de la commande suivante :

```
New-SmbGlobalMapping -RemotePath \\fsxontapdemo.fsxontap.com\fsxontap -LocalPath Z:
```

5. Lorsque vous créez vos définitions de tâches Amazon ECS, ajoutez les propriétés de `mountPoints` conteneur `volumes` et les propriétés de conteneur suivantes dans la définition de conteneur JSON. Remplacez-le `sourcePath` par le point de montage et le répertoire de votre système de fichiers FSx for ONTAP.

```
{
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
}
```

Utilisation de VMware Cloud avec FSx pour ONTAP

Vous pouvez utiliser FSx for ONTAP comme banque de données externe pour VMware Cloud sur des centres de données AWS définis par logiciel (SDDC). Pour plus d'informations, consultez Configurer Amazon FSx pour NetApp ONTAP en tant que stockage externe et Guide de déploiement de VMware Cloud on with AWS Amazon FSx for ONTAP. NetApp

Disponibilité et durabilité

Amazon FSx for NetApp ONTAP utilise deux types de déploiement, mono-AZ et multi-AZ, qui offrent différents niveaux de disponibilité et de durabilité. Cette rubrique décrit les fonctionnalités de disponibilité et de durabilité de chaque type de déploiement afin de vous aider à choisir celui qui convient le mieux à vos charges de travail. Pour plus d'informations sur le SLA (Service Level Agreement) de disponibilité du service, consultez l'accord de niveau de service Amazon FSx.

Rubriques

Choix d'un type de déploiement de système de fichiers

Les fonctionnalités de disponibilité et de durabilité des types de déploiement de systèmes de fichiers mono-AZ et multi-AZ sont décrites dans les sections suivantes.

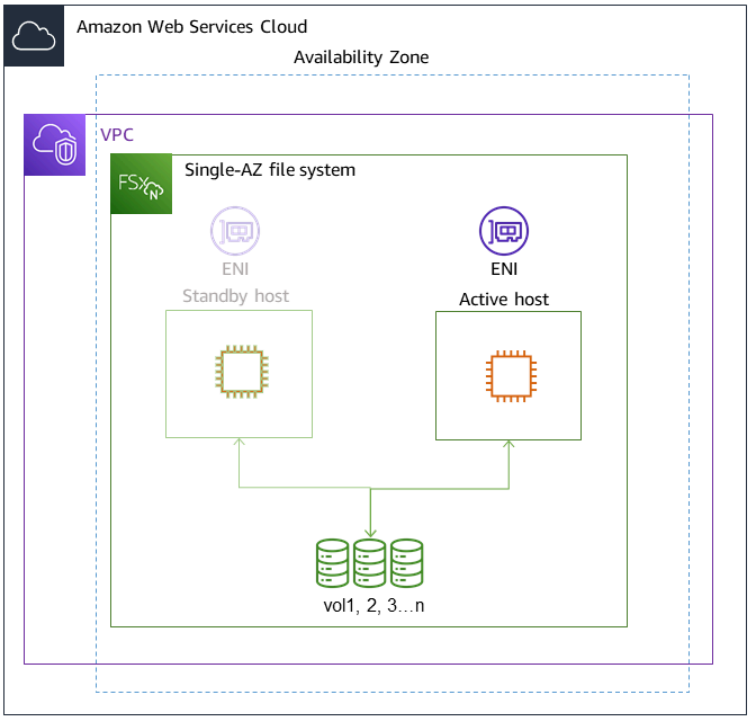
Type de déploiement mono-AZ

Lorsque vous créez un système de fichiers mono-AZ, Amazon FSx approvisionne automatiquement une à douze paires de serveurs de fichiers dans une configuration en veille active, les serveurs de fichiers actifs et de secours de chaque paire étant situés dans des domaines de défaillance distincts au sein d'une seule zone de disponibilité du. Région AWS Lors de la maintenance planifiée du système de fichiers ou d'une interruption de service imprévue d'un serveur de fichiers actif, Amazon FSx bascule automatiquement et indépendamment cette paire de haute disponibilité (HA) sur le serveur de fichiers de secours, généralement en quelques secondes. Lors d'un basculement, vous continuez à avoir accès à vos données sans intervention manuelle.

Pour garantir une haute disponibilité, Amazon FSx surveille en permanence les défaillances matérielles et remplace automatiquement les composants de l'infrastructure en cas de panne. Pour garantir une durabilité élevée, Amazon FSx réplique automatiquement vos données au sein d'une zone de disponibilité afin de les protéger contre les défaillances des composants. En outre, vous avez la possibilité de configurer des sauvegardes quotidiennes automatiques des données de votre système de fichiers. Ces sauvegardes sont stockées dans plusieurs zones de disponibilité afin de garantir la résilience multi-AZ de toutes les données de sauvegarde.

Les systèmes de fichiers mono-AZ sont conçus pour les cas d'utilisation qui ne nécessitent pas le modèle de résilience des données d'un système de fichiers multi-AZ. Ils fournissent une solution optimisée en termes de coûts pour les cas d'utilisation tels que les environnements de développement et de test, ou le stockage de copies secondaires de données déjà stockées sur site ou dans un autre Régions AWS, en ne répliquant les données que dans une seule zone de disponibilité.

Le schéma suivant illustre l'architecture d'un système de fichiers mono-AZ FSx for ONTAP.

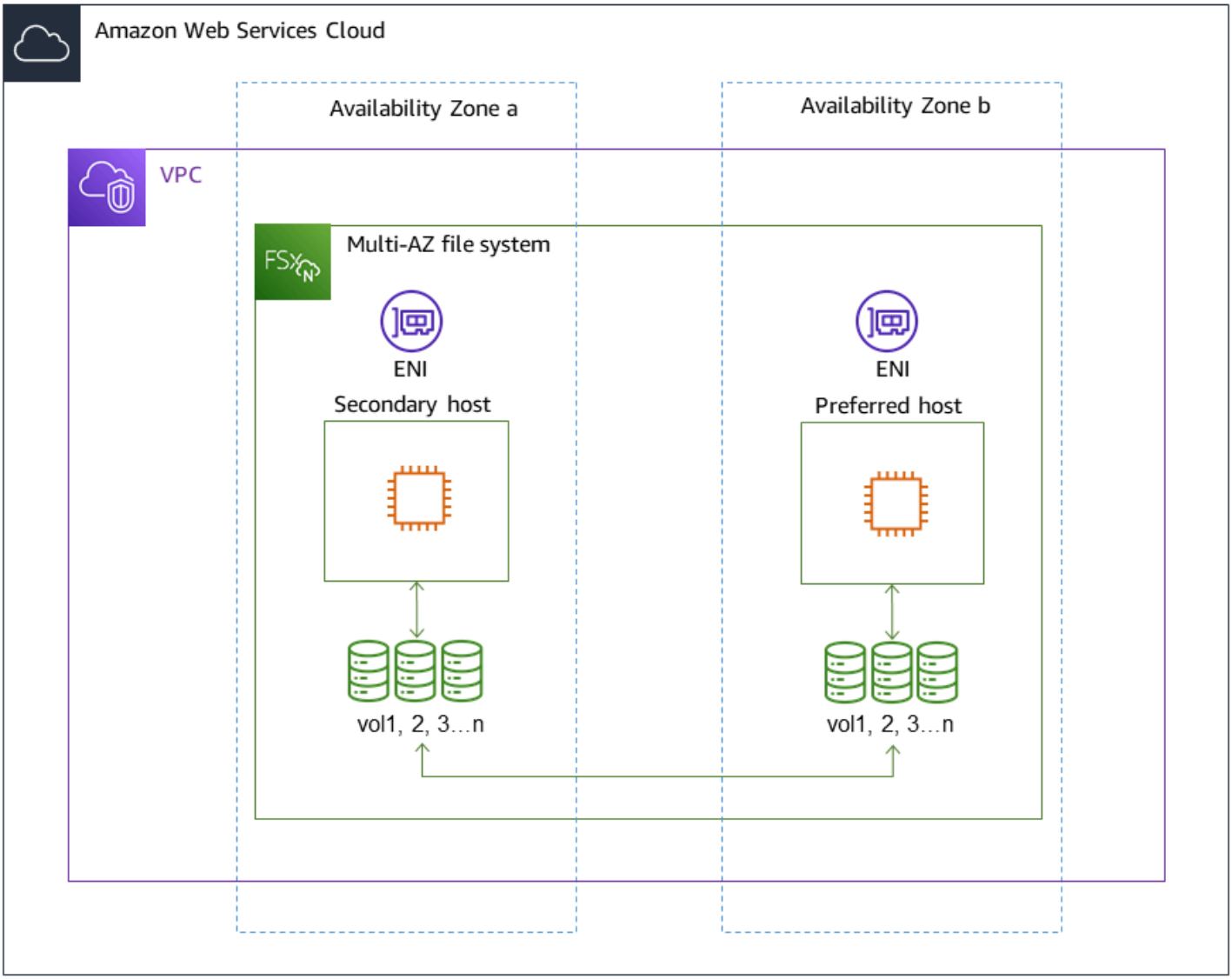


Type de déploiement multi-AZ

Les systèmes de fichiers multi-AZ prennent en charge toutes les fonctionnalités de disponibilité et de durabilité des systèmes de fichiers mono-AZ. En outre, ils sont conçus pour garantir la disponibilité continue des données, même lorsqu'une zone de disponibilité n'est pas disponible. Les déploiements multi-AZ comportent une seule paire de serveurs de fichiers HA, le serveur de fichiers de secours étant déployé dans une zone de disponibilité différente de celle du serveur de fichiers actif dans la même zone. Région AWS Toutes les modifications apportées à votre système de fichiers sont répliquées de manière synchrone entre les zones de disponibilité vers le mode veille.

Les systèmes de fichiers multi-AZ sont conçus pour des cas d'utilisation tels que les charges de travail de production critiques qui nécessitent une haute disponibilité des données de fichiers ONTAP

partagées et un stockage avec réplication intégrée entre les zones de disponibilité. Le schéma suivant illustre l'architecture d'un système de fichiers FSx for ONTAP Multi-AZ.



Processus de basculement pour FSx for ONTAP

Les systèmes de fichiers mono-AZ et multi-AZ basculent automatiquement sur une paire HA donnée du serveur de fichiers préféré ou actif vers le serveur de fichiers de secours si l'une des conditions suivantes se produit :

- Le serveur de fichiers préféré ou actif devient indisponible
- La capacité de débit du système de fichiers est modifiée
- Le serveur de fichiers préféré ou actif fait l'objet d'une maintenance planifiée

- Une panne de zone de disponibilité se produit (systèmes de fichiers multi-AZ uniquement)

> **Note**
>
> Pour les systèmes de fichiers évolutifs, le comportement de basculement de chaque paire HA est indépendant. Si le serveur de fichiers préféré pour une paire HA n'est pas disponible, seule cette paire HA basculera vers son serveur de fichiers de secours.

En cas de basculement d'un serveur de fichiers à un autre, le nouveau serveur de fichiers actif commence automatiquement à traiter toutes les demandes de lecture et d'écriture du système de fichiers adressées à cette paire HA. Pour les systèmes de fichiers multi-AZ, lorsque le serveur de fichiers préféré est entièrement restauré et devient disponible, Amazon FSx y revient automatiquement, le failback s'effectuant généralement en moins de 60 secondes. Pour les systèmes de fichiers mono-AZ et multi-AZ, un basculement s'effectue généralement en moins de 60 secondes entre la détection de la panne sur le serveur de fichiers actif et le passage du serveur de fichiers de secours à l'état actif. Étant donné que l'adresse IP du point de terminaison que les clients utilisent pour accéder aux données via NFS ou SMB reste la même, les basculements sont transparents pour les applications Linux, Windows et macOS, qui reprennent les opérations du système de fichiers sans intervention manuelle.

Pour garantir la transparence des basculements pour les clients connectés à vos systèmes de fichiers FSx for ONTAP mono-AZ ou multi-AZ, voir. Accès aux données depuis l'intérieur AWS

Test du basculement sur un système de fichiers

Vous pouvez tester le basculement sur votre système de fichiers évolutif en modifiant sa capacité de débit. Lorsque vous modifiez la capacité de débit de votre système de fichiers, Amazon FSx change les serveurs de fichiers du système de fichiers en série. Les systèmes de fichiers basculent automatiquement vers le serveur secondaire tandis qu'Amazon FSx remplace d'abord le serveur de fichiers préféré. Une fois mis à jour, le système de fichiers revient automatiquement sur le nouveau serveur principal et Amazon FSx remplace le serveur de fichiers secondaire.

Vous pouvez suivre la progression de la demande de mise à jour de la capacité de débit dans la console Amazon FSx, la CLI et l'API. Pour plus d'informations sur la modification de la capacité de débit de votre système de fichiers et le suivi de la progression de la demande, consultezGestion de la capacité de débit.

Ressources du réseau

Cette section décrit les ressources réseau consommées par les systèmes de fichiers mono-AZ et multi-AZ.

Sous-réseaux

Lorsque vous créez un système de fichiers mono-AZ, vous spécifiez un sous-réseau unique pour le système de fichiers. Le sous-réseau que vous choisissez définit la zone de disponibilité dans laquelle le système de fichiers est créé. Lorsque vous créez un système de fichiers multi-AZ, vous spécifiez deux sous-réseaux, l'un pour le serveur de fichiers préféré et l'autre pour le serveur de fichiers de secours. Les deux sous-réseaux que vous choisissez doivent se trouver dans des zones de disponibilité différentes au sein de la même Région AWS zone. Pour plus d'informations sur Amazon VPC, consultez Qu'est-ce qu'Amazon VPC ? dans le guide de l'utilisateur d'Amazon Virtual Private Cloud.

> **Note**
>
> Quel que soit le sous-réseau que vous spécifiez, vous pouvez accéder à votre système de fichiers depuis n'importe quel sous-réseau au sein du VPC du système de fichiers.

Interfaces réseau élastiques pour systèmes de fichiers

Pour les systèmes de fichiers mono-AZ, Amazon FSx fournit deux interfaces réseau élastiques (ENI) dans le sous-réseau que vous associez à votre système de fichiers. Pour les systèmes de fichiers multi-AZ, Amazon FSx fournit également deux ENI, un dans chacun des sous-réseaux que vous associez à votre système de fichiers. Les clients communiquent avec votre système de fichiers Amazon FSx via l'interface Elastic Network. Les interfaces réseau sont considérées comme relevant du périmètre de service d'Amazon FSx, même si elles font partie du VPC de votre compte. Les systèmes de fichiers multi-AZ utilisent des adresses IP (Internet Protocol) flottantes afin que les clients connectés puissent effectuer une transition fluide entre le serveur de fichiers préféré et le serveur de secours lors d'un incident de basculement.

Warning

- Vous ne devez ni modifier ni supprimer les interfaces réseau élastiques associées à votre système de fichiers. La modification ou la suppression de l'interface réseau peut entraîner une perte permanente de connexion entre votre VPC et votre système de fichiers.
- Les interfaces réseau élastiques associées à votre système de fichiers créeront automatiquement des itinéraires et les ajouteront à vos tables de routage VPC et de sous-réseau par défaut. La modification ou la suppression de ces routes peut entraîner une perte de connectivité temporaire ou permanente pour les clients de votre système de fichiers.

Le tableau suivant récapitule les ressources du sous-réseau, de l'interface Elastic Network et des adresses IP pour chacun des types de déploiement du système de fichiers FSx for ONTAP :

	Mono-AZ (mise à l'échelle)	Mono-AZ (scale-out)	Multi-AZ (mise à l'échelle)
Nombre de sous-réseaux	1	1	2
Nombre d'interfaces réseau élastiques	2	2 par paire HA	2
Nombre d'adresses IP par ENI	1 + le nombre de SVM dans le système de fichiers	Nombre de paires HA + nombre de paires HA multiplié par le nombre de SVM dans le système de fichiers	1 + le nombre de SVM dans le système de fichiers
Nombre de routes	N/A	N/A	1 + le nombre de SVM dans

	Mono-AZ (mise à l'échelle)	Mono-AZ (scale-out)	Multi-AZ (mise à l'échelle)
de table de routage VPC			le système de fichiers

Une fois qu'un système de fichiers ou une SVM est créé, ses adresses IP ne changent pas tant que le système de fichiers n'est pas supprimé.

> **Important**
>
> Amazon FSx ne prend pas en charge l'accès aux systèmes de fichiers depuis l'Internet public ou leur exposition à celui-ci. Amazon FSx détache automatiquement toute adresse IP élastique qui est une adresse IP publique accessible depuis Internet, qui est attachée à l'interface réseau élastique d'un système de fichiers.

Gestion de la capacité de stockage

Amazon FSx for NetApp ONTAP fournit un certain nombre de fonctionnalités liées au stockage que vous pouvez utiliser pour gérer la capacité de stockage de votre système de fichiers.

Rubriques

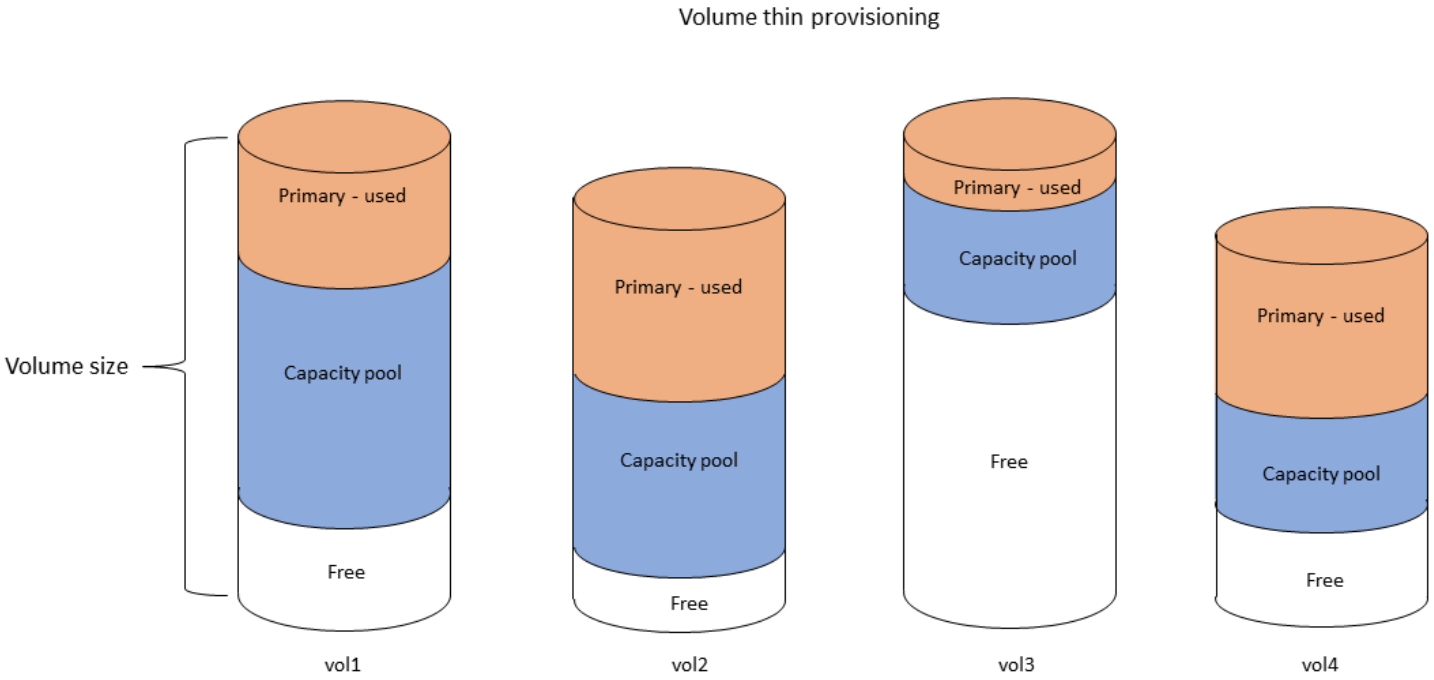
niveaux de stockage FSx pour ONTAP

Les niveaux de stockage sont les supports de stockage physiques d'un système de fichiers Amazon FSx for NetApp ONTAP. FSx for ONTAP propose les niveaux de stockage suivants :

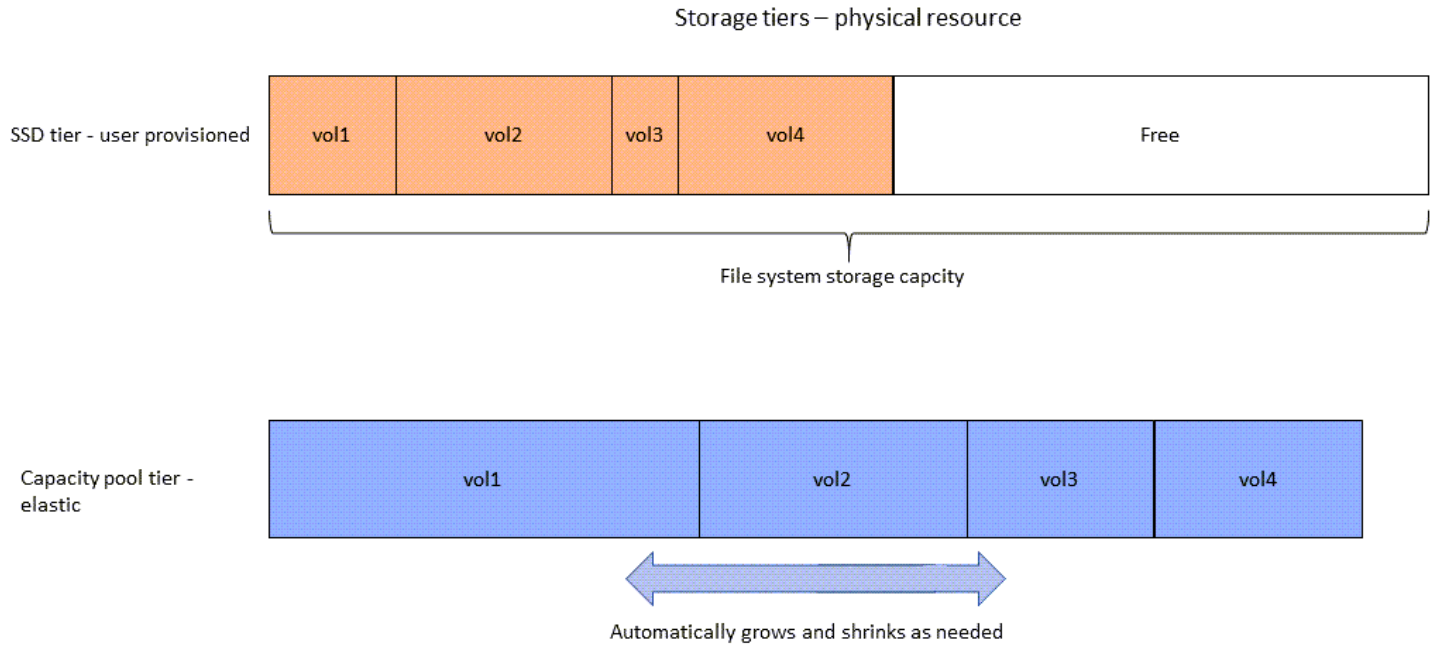
- Niveau SSD : stockage sur disque SSD (SSD) hautes performances, fourni par l'utilisateur, spécialement conçu pour la partie active de votre ensemble de données.
- Niveau du pool de capacité : stockage entièrement élastique qui s'adapte automatiquement à une taille de plusieurs pétaoctets et est optimisé en termes de coûts pour vos données rarement consultées.

Un volume FSx for ONTAP est une ressource virtuelle qui, comme les dossiers, ne consomme pas de capacité de stockage. Les données que vous stockez, et qui consomment de l'espace de stockage physique, se trouvent dans des volumes. Lorsque vous créez un volume, vous spécifiez sa taille, que vous pouvez modifier après sa création. Les volumes FSx for ONTAP sont dotés d'un provisionnement léger et le stockage du système de fichiers n'est pas réservé à l'avance. Au lieu de cela, le stockage SSD et le stockage en pool de capacité sont alloués dynamiquement, selon les besoins. Une politique de hiérarchisation, que vous configurez au niveau du volume, détermine si et quand les données stockées dans le niveau SSD passent au niveau du pool de capacités.

Le schéma suivant illustre un exemple de données réparties sur plusieurs volumes FSx pour ONTAP dans un système de fichiers.



Le schéma suivant montre comment la capacité de stockage physique du système de fichiers est consommée par les données des quatre volumes du schéma précédent.



Vous pouvez réduire vos coûts de stockage en choisissant la politique de hiérarchisation qui répond le mieux aux exigences de chaque volume de votre système de fichiers. Pour plus d'informations, consultez Hiérarchisation des données de volume.

Choisir la bonne quantité de stockage SSD pour le système de fichiers

Lorsque vous choisissez la capacité de stockage SSD pour votre système de fichiers FSx for ONTAP, vous devez garder à l'esprit les éléments suivants qui ont un impact sur la quantité de stockage SSD disponible pour le stockage de vos données :

- Capacité de stockage réservée à la surcharge logicielle NetApp ONTAP.
- Métadonnées des fichiers
- Données récemment écrites
- Les fichiers que vous avez l'intention de stocker sur un disque SSD, qu'il s'agisse de données n'ayant pas atteint la période de refroidissement ou de données que vous avez récemment lues et qui ont été récupérées sur le SSD.

Comment est utilisé le stockage SSD

Le stockage SSD de votre système de fichiers est utilisé à la NetApp fois pour le logiciel ONTAP (surcharge), les métadonnées des fichiers et vos données.

NetApp Frais généraux liés au logiciel ONTAP

À l'instar des autres systèmes de fichiers NetApp ONTAP, jusqu'à 16 % de la capacité de stockage SSD d'un système de fichiers est réservée aux frais généraux d'ONTAP, ce qui signifie qu'il n'est pas disponible pour le stockage de vos fichiers. Les frais généraux de l'ONTAP sont répartis comme suit :

- 11 % sont réservés au logiciel NetApp ONTAP. Pour les systèmes de fichiers dont la capacité de stockage SSD est supérieure à 30 tebioctets (TiB), 6 % sont réservés.
- 5 % sont réservés aux instantanés agrégés, qui sont nécessaires pour synchroniser les données entre les deux serveurs de fichiers d'un système de fichiers.

Métadonnées des fichiers

Les métadonnées des fichiers consomment généralement 3 à 7 % de la capacité de stockage utilisée par les fichiers. Ce pourcentage dépend de la taille moyenne des fichiers (une taille moyenne de fichier inférieure nécessite davantage de métadonnées) et des économies d'efficacité du stockage

réalisées sur vos fichiers. Notez que les métadonnées des fichiers ne bénéficient pas des économies d'efficacité du stockage. Vous pouvez utiliser les directives suivantes pour estimer la quantité de stockage SSD utilisée pour les métadonnées sur votre système de fichiers.

Taille de fichier moyenne	Taille des métadonnées en pourcentage des données du fichier
4 Ko	7 %
8 Ko	3,5 %
32 Ko ou plus	1 à 3 %

Lorsque vous évaluez la capacité de stockage SSD dont vous avez besoin pour les métadonnées des fichiers que vous prévoyez de stocker au niveau du pool de capacité, nous vous recommandons d'utiliser un ratio prudent de 1 Go de stockage SSD pour 10 Go de données que vous prévoyez de stocker au niveau du pool de capacité.

Données de fichiers stockées sur votre niveau SSD

Outre votre ensemble de données actif et toutes les métadonnées des fichiers, toutes les données écrites dans votre système de fichiers sont initialement écrites sur le niveau SSD avant d'être transférées vers le stockage en pool de capacité. Cela est vrai quelle que soit la politique de hiérarchisation du volume, à l'exception du transfert de données SnapMirror vers un volume configuré avec une politique de hiérarchisation de toutes les données.

Les lectures aléatoires provenant du niveau du pool de capacités sont mises en cache dans le niveau SSD, tant que le niveau SSD est inférieur à 90 % d'utilisation. Pour plus d’informations, consultez Hiérarchisation des données de volume.

Utilisation recommandée de la capacité SSD

Nous vous recommandons de ne pas dépasser 80 % d'utilisation du niveau de stockage de votre SSD sur une base continue. Pour les systèmes de fichiers évolutifs, nous vous recommandons également de ne pas dépasser 80 % d'utilisation continue des agrégats de votre système de fichiers. Ces recommandations sont conformes à NetApp la recommandation concernant l'ONTAP. Étant donné que le niveau SSD de votre système de fichiers est également utilisé pour effectuer des écritures et des lectures aléatoires depuis le niveau du pool de capacité, toute modification soudaine

des modèles d'accès peut rapidement entraîner une augmentation de l'utilisation de votre niveau SSD.

À 90 % d'utilisation du SSD, les données lues depuis le niveau du pool de capacités ne sont plus mises en cache sur le niveau SSD, de sorte que la capacité restante du SSD est préservée pour toute nouvelle donnée écrite dans le système de fichiers. Cela entraîne la lecture répétée des mêmes données depuis le niveau du pool de capacité à être lues depuis le stockage du pool de capacité au lieu d'être mises en cache et lues depuis le niveau SSD, ce qui peut avoir un impact sur la capacité de débit de votre système de fichiers.

Toutes les fonctionnalités de hiérarchisation s'arrêtent lorsque le niveau du SSD atteint ou dépasse 98 % d'utilisation. Pour plus d'informations, consultez Seuils de hiérarchisation.

FSx pour l'efficacité du stockage ONTAP

NetApp ONTAP propose des fonctionnalités d'efficacité du stockage au niveau des blocs, notamment la compression, le compactage et la déduplication, qui peuvent vous faire économiser jusqu'à 65 % de capacité de stockage pour les partages de fichiers généraux, sans pour autant sacrifier les performances.

Amazon FSx for NetApp ONTAP prend également en charge d'autres fonctionnalités ONTAP qui vous permettent d'économiser de l'espace, notamment les instantanés, le provisionnement dynamique et les volumes. FlexClone

Les fonctionnalités d'efficacité du stockage ne sont pas activées par défaut. Vous pouvez les activer comme suit :

- Sur le volume racine d'une SVM lorsque vous créez un système de fichiers.
- Lorsque vous créez un nouveau volume.
- Lorsque vous modifiez un volume existant.

Pour connaître le montant des économies de stockage réalisées sur un système de fichiers sur lequel l'efficacité du stockage est activée, voirVisualisation des économies d'efficacité du stockage.

Calcul des économies d'efficacité du stockage

Vous pouvez utiliser les métriques du système de CloudWatch fichiers `LogicalDataStored` et `StorageUsed` FSx for ONTAP pour calculer les économies de stockage réalisées grâce à la compression, à la déduplication, au compactage, aux instantanés et. FlexClones Ces métriques ont

une seule dimension,`FileSystemId`. Pour plus d'informations, consultez Métriques du système de fichiers.

- Pour calculer les économies d'efficacité du stockage en octets, prenez la moyenne `StorageUsed` sur une période donnée et soustrayez-la de la moyenne `LogicalDataStored` sur la même période.
- Pour calculer les économies d'efficacité du stockage en pourcentage de la taille logique totale des données, prenez le chiffre `Average` de `StorageUsed` sur une période donnée et soustrayez-le du chiffre de `LogicalDataStored` sur la `Average` même période. Divisez ensuite la différence par le `Average` nombre de `LogicalDataStored` sur la même période.

Exemple de dimensionnement d'un SSD

Supposons que vous souhaitiez stocker 100 TiB de données pour une application où 80 % des données sont rarement consultées. Dans ce scénario, 80 % (80 To) de vos données sont automatiquement hiérarchisées au niveau du pool de capacité et les 20 % restants (20 To) restent sur un stockage SSD. Sur la base des économies d'efficacité du stockage typiques de 65 % pour les charges de travail de partage de fichiers à usage général, cela équivaut à 7 TiB de données. Pour maintenir un taux d'utilisation des SSD de 80 %, vous avez besoin de 8,75 TiB de capacité de stockage SSD pour les 20 TiB de données activement consultées. La quantité de stockage SSD que vous fournissez doit également tenir compte de la surcharge de stockage du logiciel ONTAP de 16 %, comme indiqué dans le calcul suivant.

```
ssdNeeded = ssdProvisioned * (1 - 0.16)
8.75 TiB / 0.84 = ssdProvisioned
10.42 TiB = ssdProvisioned
```

Dans cet exemple, vous devez donc provisionner au moins 10,42 TiB de stockage SSD. Vous utiliserez également 28 TiB de capacité de stockage en pool pour les 80 TiB restants de données rarement consultées.

Capacité de stockage et IOPS du système de fichiers

Lorsque vous créez un système de fichiers FSx for ONTAP, vous spécifiez la capacité de stockage du niveau SSD. Pour les systèmes de fichiers évolutifs, la capacité de stockage que vous spécifiez est répartie uniformément entre les pools de stockage de chaque paire de haute disponibilité (HA) ; ces pools de stockage sont appelés agrégats.

Pour chaque GiB de stockage SSD que vous fournissez, Amazon FSx fournit automatiquement 3 opérations d'entrée/sortie SSD par seconde (IOPS) pour le système de fichiers, jusqu'à un maximum de 160 000 IOPS SSD par système de fichiers. Pour les systèmes de fichiers évolutifs, les IOPS de vos SSD sont réparties uniformément sur chacun des agrégats de votre système de fichiers. Vous avez la possibilité de spécifier un niveau d'IOPS SSD provisionné supérieur aux 3 IOPS automatiques par GiB. Pour plus d'informations sur le nombre maximal d'IOPS SSD que vous pouvez configurer pour votre système de fichiers FSx for ONTAP, consultez. Impact de la capacité de débit sur les performances

Rubriques

Mise à jour du système de fichiers, du stockage SSD et des IOPS

Lorsque vous avez besoin de stockage supplémentaire pour la partie active de votre ensemble de données, vous pouvez augmenter la capacité de stockage SSD de votre système de fichiers Amazon FSx for NetApp ONTAP. Utilisez la console Amazon FSx, l'API Amazon FSx ou AWS Command Line Interface (AWS CLI) pour augmenter la capacité de stockage SSD. Pour plus d’informations, consultez Modification de la capacité de stockage SSD et des IOPS provisionnées.

Lorsque vous augmentez la capacité de stockage SSD de votre système de fichiers Amazon FSx, la nouvelle capacité est généralement disponible en quelques minutes. La nouvelle capacité de stockage SSD vous sera facturée dès qu'elle sera disponible. Pour plus d'informations sur la tarification, consultez Amazon FSx for NetApp ONTAP Pricing.

Une fois que vous avez augmenté votre capacité de stockage, Amazon FSx exécute un processus d'optimisation du stockage en arrière-plan pour rééquilibrer vos données. Pour la plupart des systèmes de fichiers, l'optimisation du stockage prend quelques heures, avec un impact minimal perceptible sur les performances de votre charge de travail.

Vous pouvez suivre la progression du processus d'optimisation du stockage à tout moment à l'aide de la console, de la CLI et de l'API Amazon FSx. Pour plus d'informations, consultez Surveillance de la capacité de stockage et des mises à jour des IOPS.

Considérations

Voici quelques points importants à prendre en compte lors de la modification de la capacité de stockage SSD et des IOPS provisionnées d'un système de fichiers :

- Augmentation de la capacité de stockage uniquement : vous pouvez uniquement augmenter la capacité de stockage SSD d'un système de fichiers ; vous ne pouvez pas diminuer la capacité de stockage.
- Augmentation minimale de la capacité de stockage — Chaque augmentation de la capacité de stockage SSD doit être d'au moins 10 % de la capacité de stockage SSD actuelle du système de fichiers, jusqu'à la capacité de stockage SSD maximale pour la configuration de votre système de fichiers.
- (Extensibilité externe uniquement) Répartition de la capacité de stockage : la nouvelle capacité de stockage ou IOPS SSD que vous sélectionnez pour votre système de fichiers est répartie uniformément sur chacun des agrégats de votre système de fichiers.
- Intervalle entre les augmentations : après avoir modifié la capacité de stockage SSD, les IOPS provisionnées ou la capacité de débit d'un système de fichiers, vous devez attendre au moins six heures avant de modifier à nouveau l'une de ces configurations sur le même système de fichiers. Cet élément est parfois appelé temps de stabilisation.
- Modes IOPS provisionnés — Pour une modification des IOPS provisionnés, vous devez spécifier l'un des deux modes IOPS :
  - Mode automatique : Amazon FSx adapte automatiquement les IOPS de votre SSD afin de maintenir 3 IOPS par GiB de capacité de stockage SSD, jusqu'au maximum d'IOPS SSD pour la configuration de votre système de fichiers.

    > **Note**
    >
    > Pour plus d'informations sur le nombre maximal d'IOPS SSD que vous pouvez configurer pour votre système de fichiers FSx for ONTAP, consultez. Impact de la capacité de débit sur les performances

  - Mode provisionné par l'utilisateur : vous spécifiez le nombre d'IOPS SSD, qui doit être supérieur ou égal à 3 IOPS par GiB de capacité de stockage SSD. Si vous choisissez de fournir un niveau

d'IOPS supérieur, vous payez pour le nombre moyen d'IOPS fourni en sus de votre tarif mensuel inclus, mesuré en mois d'IOPS.

Pour plus d'informations sur la tarification, consultez Amazon FSx for NetApp ONTAP Pricing.

Quand augmenter la capacité de stockage SSD

Si vous n'avez plus de capacité de stockage SSD disponible, nous vous recommandons d'augmenter la capacité de stockage de votre système de fichiers. Le manque de stockage indique que le niveau de votre SSD est sous-dimensionné pour la partie active de votre ensemble de données.

Pour contrôler la quantité de stockage gratuit disponible sur le système de fichiers, utilisez les métriques au niveau du système de fichiers et `StorageCapacity` `StorageUsed` Amazon CloudWatch . Vous pouvez créer une CloudWatch alarme sur une métrique et être averti lorsqu'elle tombe en dessous d'un seuil spécifique. Pour plus d'informations, consultez Surveillance avec Amazon CloudWatch.

> **Note**
>
> Nous vous recommandons de ne pas dépasser 80 % d'utilisation de la capacité de stockage SSD afin de garantir le bon fonctionnement de la hiérarchisation des données, de la mise à l'échelle du débit et des autres activités de maintenance, ainsi que de la capacité disponible pour des données supplémentaires. Pour les systèmes de fichiers évolutifs, cette recommandation s'applique à la fois à l'utilisation moyenne de tous les agrégats de votre système de fichiers et à chaque agrégat individuel.

Pour plus d'informations sur l'utilisation du stockage SSD d'un système de fichiers et sur la quantité de stockage SSD réservée aux métadonnées des fichiers et aux logiciels d'exploitation, consultezChoisir la bonne quantité de stockage SSD pour le système de fichiers.

Surveillance de l'utilisation du stockage SSD

Vous pouvez surveiller l'utilisation de la capacité de stockage SSD de votre système de fichiers à l'aide AWS de divers NetApp outils. Amazon CloudWatch vous permet de surveiller l'utilisation de la capacité de stockage et de configurer des alarmes pour vous avertir lorsque l'utilisation de la capacité de stockage atteint un seuil personnalisable.

> **Note**
>
> Nous vous recommandons de ne pas dépasser 80 % d'utilisation de la capacité de stockage de votre niveau de stockage SSD. Cela garantit le bon fonctionnement de la hiérarchisation et entraîne une surcharge pour les nouvelles données. Si le niveau de stockage de votre SSD est constamment supérieur à 80 % d'utilisation de la capacité de stockage, vous pouvez augmenter la capacité de votre niveau de stockage SSD. Pour plus d'informations, consultez Mise à jour du système de fichiers, du stockage SSD et des IOPS.

Vous pouvez consulter le stockage SSD disponible d'un système de fichiers et la distribution globale du stockage dans la console Amazon FSx. Le graphique de la capacité de stockage SSD disponible affiche la quantité de capacité de stockage SSD disponible sur un système de fichiers au fil du temps. Le graphique de distribution du stockage montre comment la capacité de stockage globale d'un système de fichiers est actuellement répartie en 3 catégories :

- Niveau du pool de capacités
- Niveau SSD : disponible
- Niveau SSD : d'occasion

Vous pouvez surveiller l'utilisation de la capacité de stockage SSD de votre système de fichiers dans le AWS Management Console, en suivant la procédure suivante.

Pour surveiller la capacité de stockage de niveau SSD disponible dans le système de fichiers (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Choisissez Systèmes de fichiers dans la colonne de navigation de gauche, puis choisissez le système de ONTAP fichiers pour lequel vous souhaitez consulter les informations relatives à la capacité de stockage. La page détaillée du système de fichiers apparaît.
3. Dans le deuxième panneau, choisissez l'onglet Surveillance et performances, puis sélectionnez Stockage. Les graphiques de capacité de stockage principale disponible et d'utilisation de la capacité de stockage par agrégat sont affichés.

Création d'une alarme d'utilisation de la capacité de stockage d'un système de fichiers

Nous vous recommandons de ne pas dépasser un taux d'utilisation moyen de la capacité de stockage SSD de 80 % sur une base continue. Des pics occasionnels d'utilisation du stockage SSD supérieurs à 80 % sont acceptables. Le maintien d'un taux d'utilisation moyen inférieur à 80 % vous permet de disposer d'une capacité suffisante pour augmenter votre espace de stockage sans rencontrer de problèmes. La procédure suivante indique comment créer une CloudWatch alarme qui vous avertit lorsque le taux d'utilisation du stockage SSD de votre système de fichiers approche les 80 %.

Pour créer une alarme SCU dans un système de fichiers

Vous pouvez utiliser cette `StorageCapacityUtilization` métrique pour créer une alarme qui se déclenche lorsqu'un ou plusieurs de vos systèmes de fichiers FSx for ONTAP ont atteint un seuil d'utilisation du stockage.

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le volet de navigation de gauche, sous Alarmes, sélectionnez Toutes les alarmes. Choisissez ensuite Créer une alarme. Dans l'assistant de création d'alarme, choisissez Sélectionner une métrique.
3. Dans l'explorateur de graphes, choisissez l'onglet Requête multisource.
4. Dans le générateur de requêtes, choisissez ce qui suit :
   - Pour Namespace, sélectionnez AWS/FSx > Mesures détaillées du système de fichiers.
   - Pour le nom de la métrique, sélectionnez MAX (StorageCapacityUtilization).
   - Pour Filtrer par, vous pouvez éventuellement inclure ou exclure des systèmes de fichiers spécifiques en fonction de leur ID. Si vous laissez le filtre vide, votre alarme se déclenchera lorsque l'un de vos systèmes de fichiers dépassera le seuil d'utilisation de la capacité de stockage de votre alarme.
   - Laissez le reste des options vides, puis choisissez Requête graphique.
5. Choisissez Select metric (Sélectionner une métrique). De retour dans l'assistant, dans la section Métrique, attribuez une étiquette à votre métrique. Nous recommandons de limiter cette période à 5 minutes.
6. Dans Conditions, choisissez le type de seuil statique, chaque fois que votre métrique est supérieure/égale à 80.

7. Choisissez Suivant pour accéder à la page Configurer les actions.

Pour configurer les actions d'alarme

Vous pouvez configurer diverses actions pour que votre alarme se déclenche lorsqu'elle atteint le seuil que vous avez configuré. Dans cet exemple, nous avons choisi une rubrique Simple Notification Service (SNS), mais vous pouvez en apprendre davantage sur d'autres actions dans la section Utilisation des alarmes Amazon dans le guide de l'utilisateur Amazon. CloudWatch CloudWatch

1. Dans la section Notification, choisissez une rubrique SNS pour vous avertir lorsque votre alarme est activéeALARM. Vous pouvez choisir un sujet existant ou en créer un nouveau. Vous recevrez une notification d'abonnement que vous devrez confirmer avant de recevoir des notifications d'alarme à l'adresse e-mail.
2. Choisissez Suivant.

Pour terminer l'alarme

Suivez ces instructions pour terminer le processus de création de votre CloudWatch alarme.

1. Sur la page Ajouter un nom et une description, donnez un nom à votre alarme, et éventuellement une description, puis choisissez Next.
2. Passez en revue tout ce que vous avez configuré dans la page de prévisualisation et de création, puis choisissez Créer une alarme.

Visualisation des économies d'efficacité du stockage

Lorsque cette option est activée, vous pouvez voir la capacité de stockage que vous économisez dans la console Amazon FSx, la CloudWatch console Amazon et la CLI ONTAP.

Pour afficher les économies réalisées en termes d'efficacité du stockage (console)

Les économies d'efficacité du stockage affichées dans la console Amazon FSx pour un système de fichiers FSx for ONTAP incluent les économies réalisées grâce à et. FlexClones SnapShots

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans la liste des systèmes de fichiers, sélectionnez le système de fichiers FSx for ONTAP dont vous souhaitez connaître l'efficacité du stockage et enregistrer des économies.

3. Choisissez Résumé dans l'onglet Surveillance et performances du deuxième panneau de la page de détails du système de fichiers.
4. Le graphique des économies d'efficacité du stockage indique l'espace économisé en pourcentage de la taille logique de vos données et en octets physiques.

Pour afficher les économies réalisées en termes d'efficacité du stockage (ONTAPCLI)

Vous pouvez réaliser des économies en termes d'efficacité du stockage grâce au simple compactage, à la compression et à la déduplication, sans les effets des instantanés, en exécutant la `storage aggregate show-efficiency` commande à l'aide de la CLI. FlexClones ONTAP Pour plus d'informations, consultez la section relative à l'efficacité des agrégats de stockage dans le Centre de NetApp ONTAP documentation.

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *`management_endpoint_ip`* par l'adresse IP du port de gestion du système de fichiers.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Pour plus d'informations, consultez Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.
2. La storage aggregate show-efficiency commande affiche des informations sur l'efficacité du stockage de tous les agrégats. L'efficacité du stockage est affichée à quatre niveaux différents :

   - Total
   - Regrouper
   - Volume
   - Instantané et FlexClone volume

   ```
   ::*> aggr show-efficiency

   Aggregate: aggr1
        Node: node1

   Total Data Reduction Efficiency Ratio:  3.29:1
   ```

```
Total Storage Efficiency Ratio:         4.29:1
Aggregate: aggr2
     Node: node1

Total Data Reduction Efficiency Ratio:  4.50:1
Total Storage Efficiency Ratio:         5.49:1

cluster::*> aggr show-efficiency -details

Aggregate: aggr1
     Node: node1

Total Data Reduction Ratio:                    2.39:1
Total Storage Efficiency Ratio:                4.29:1

Aggregate level Storage Efficiency
(Aggregate Deduplication and Data Compaction): 1.00:1
Volume Deduplication Efficiency:               5.03:1
Compression Efficiency:                        1.00:1

Snapshot Volume Storage Efficiency:            8.81:1
FlexClone Volume Storage Efficiency:           1.00:1
Number of Efficiency Disabled Volumes:         1

Aggregate: aggr2
     Node: node1
Total Data Reduction Ratio:                    2.39:1
Total Storage Efficiency Ratio:                4.29:1

Aggregate level Storage Efficiency
(Aggregate Deduplication and Data Compaction): 1.00:1
Volume Deduplication Efficiency:               5.03:1
Compression Efficiency:                        1.00:1

Snapshot Volume Storage Efficiency:            8.81:1
FlexClone Volume Storage Efficiency:           1.00:1
Number of Efficiency Disabled Volumes:         1
```

Modification de la capacité de stockage SSD et des IOPS provisionnées

Vous pouvez augmenter le stockage SSD d'un système de fichiers et augmenter ou diminuer le nombre d'IOPS sur SSD provisionnés en utilisant la console Amazon FSx, le et l'API. AWS CLI

Pour mettre à jour la capacité de stockage SSD ou les IOPS provisionnées pour un système de fichiers (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation de gauche, choisissez Systèmes de fichiers. Dans la liste des systèmes de fichiers, sélectionnez le système de fichiers FSx for ONTAP pour lequel vous souhaitez mettre à jour la capacité de stockage SSD et le nombre d'E/S par seconde du SSD.
3. Choisissez Actions > Mettre à jour la capacité de stockage. Ou, dans la section Résumé, choisissez Mettre à jour à côté de la valeur de capacité de stockage SSD du système de fichiers.

   La boîte de dialogue Mettre à jour la capacité de stockage SSD et les IOPS s'affiche.

Update SSD storage capacity and IOPS

File system ID

fs-01234567890abcdef

Current configuration

SSD storage capacity: 4096 GiB
IOPS mode: Automatic (3 IOPS per GiB of SSD storage)
SSD IOPS: 12288

SSD storage capacity

☑ Modify storage capacity

Input type

◉ Percentage
○ Absolute

Desired % increase

10 %

Minimum 4506 GiB (10% above current); Maximum 1048576 GiB.

Provisioned SSD IOPS

◉ Automatic (3 IOPS per GiB of SSD storage)
○ User-provisioned

Configuration preview

Attribute	Current configuration	New configuration
SSD storage capacity	4,096 GiB (2,048 GiB per HA pair)	4,506 GiB (2,253 GiB per HA pair)
	Mode: Automatic	Mode: Automatic

4. Pour augmenter la capacité de stockage SSD, choisissez Modifier la capacité de stockage.
5. Pour Type d'entrée, choisissez l'une des options suivantes :
   - Pour saisir la nouvelle capacité de stockage SSD sous forme de pourcentage de variation par rapport à la valeur actuelle, choisissez Pourcentage.
   - Pour saisir la nouvelle valeur en GiB, choisissez Absolute.
6. En fonction du type d'entrée, entrez une valeur pour le % d'augmentation souhaité.
   - Dans Pourcentage, entrez la valeur d'augmentation en pourcentage. Cette valeur doit être supérieure d'au moins 10 % à la valeur actuelle.
   - Pour Absolute, entrez la nouvelle valeur en GiB, jusqu'à la valeur maximale autorisée de 196 608 GiB.
7. Pour les IOPS de SSD provisionnées, vous avez deux options pour modifier le nombre d'IOPS de SSD provisionnées pour votre système de fichiers :
   - Si vous souhaitez qu'Amazon FSx adapte automatiquement les IOPS de votre SSD afin de maintenir 3 IOPS par GiB de capacité de stockage SSD (jusqu'à un maximum de 160 000), choisissez Automatique.
   - Si vous souhaitez spécifier le nombre d'IOPS SSD, choisissez User-provisioned. Entrez un nombre absolu d'IOPS au moins trois fois supérieur à la quantité de GiB de votre niveau de stockage SSD, et inférieur ou égal à 160 000.

> **Note**
>
> Pour plus d'informations sur le nombre maximal d'IOPS SSD que vous pouvez configurer pour votre système de fichiers FSx for ONTAP, consultez. Impact de la capacité de débit sur les performances

8. Choisissez Mettre à jour.

> **Note**
>
> Au bas de l'invite, un aperçu de la configuration de votre nouvelle capacité de stockage SSD et des IOPS de votre SSD s'affiche. Pour les systèmes de fichiers scale-out, la valeur par paire HA est également affichée.

Pour mettre à jour la capacité de stockage SSD et les IOPS provisionnées pour un système de fichiers (CLI)

Pour mettre à jour la capacité de stockage SSD et les IOPS provisionnées pour un système de fichiers FSx for ONTAP, utilisez la AWS CLI commande update-file-systemou l'action API équivalente. UpdateFileSystem Définissez les paramètres suivants avec vos valeurs :

- `--file-system-id`Défini sur l'ID du système de fichiers que vous mettez à jour.
- Pour augmenter la capacité de stockage de votre SSD, définissez `--storage-capacity` la valeur de capacité de stockage cible, qui doit être supérieure d'au moins 10 % à la valeur actuelle.
- Pour modifier les IOPS de votre SSD provisionné, utilisez la `--ontap-configuration` `DiskIopsConfiguration` propriété. Cette propriété comporte deux paramètres, à `Iops` savoir `Mode` :
  - Si vous souhaitez spécifier le nombre d'IOPS provisionnées, utilisez `Iops=`*`number_of_IOPS`* (jusqu'à un maximum de 160 000) et. `Mode=USER_PROVISIONED` La valeur d'IOPS doit être supérieure ou égale à trois fois la capacité de stockage SSD demandée. Si vous n'augmentez pas la capacité de stockage, la valeur d'IOPS doit être supérieure ou égale à trois fois la capacité de stockage SSD actuelle.
  - Si vous souhaitez qu'Amazon FSx augmente automatiquement les IOPS de votre SSD, utilisez `Mode=AUTOMATIC` et n'utilisez pas le paramètre. `Iops` Amazon FSx conservera automatiquement 3 IOPS par GiB de capacité de stockage SSD allouée (jusqu'à un maximum de 160 000).

> **Note**
>
> Pour plus d'informations sur le nombre maximal d'IOPS SSD que vous pouvez configurer pour votre système de fichiers FSx for ONTAP, consultez. Impact de la capacité de débit sur les performances

L'exemple suivant augmente le stockage SSD du système de fichiers à 2 000 GiB et définit le nombre d'IOPS SSD provisionnées par l'utilisateur à 7 000.

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--storage-capacity 2000 \
--ontap-configuration 'DiskIopsConfiguration={Iops=7000,Mode=USER_PROVISIONED}'
```

Pour suivre la progression de la mise à jour, utilisez la describe-file-systems AWS CLI commande. Recherchez la `AdministrativeActions` section dans le résultat.

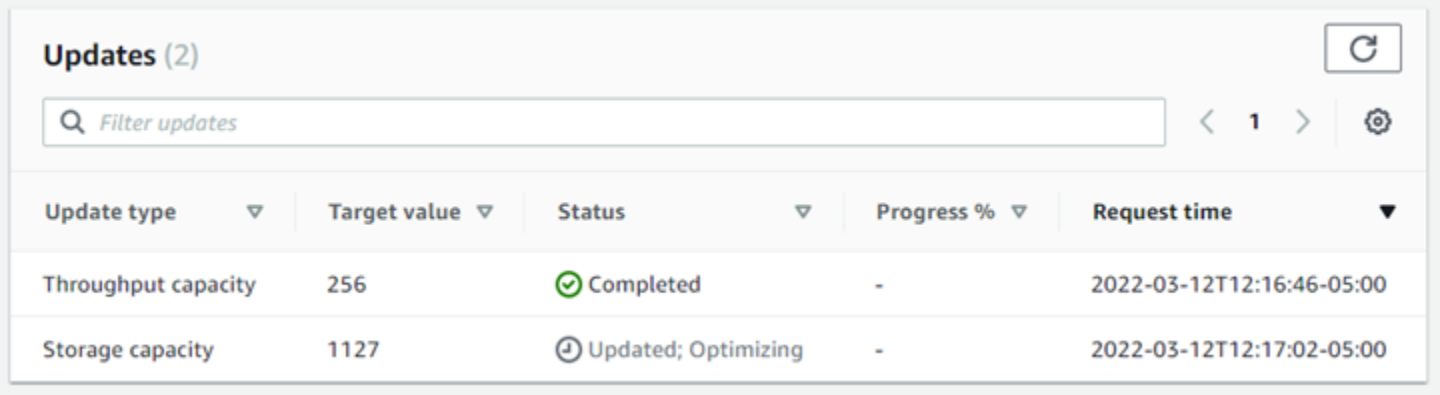
Pour plus d'informations, consultez le AdministrativeActionmanuel Amazon FSx for NetApp ONTAP API Reference.

Surveillance de la capacité de stockage et des mises à jour des IOPS

Vous pouvez suivre la progression de la mise à jour de la capacité de stockage SSD et des IOPS à l'aide de la console, de la CLI et de l'API Amazon FSx.

Pour surveiller le stockage et les mises à jour des IOPS (console)

Dans l'onglet Mises à jour de la page des détails du système de fichiers de votre système de fichiers FSx for ONTAP, vous pouvez consulter les 10 mises à jour les plus récentes pour chaque type de mise à jour.



Pour les mises à jour de la capacité de stockage SSD et des IOPS, vous pouvez consulter les informations suivantes :

Type de mise à jour

Les types pris en charge sont la capacité de stockage, le mode et les IOPS. Les valeurs Mode et IOPS sont répertoriées pour toutes les demandes de capacité de stockage et de dimensionnement des IOPS.

Valeur cible

Valeur que vous avez spécifiée pour mettre à jour la capacité de stockage SSD ou le nombre d'E/S par seconde du système de fichiers.

Statut

État actuel de la mise à jour. Les valeurs possibles sont les suivantes :

- En attente : Amazon FSx a reçu la demande de mise à jour, mais n'a pas commencé à la traiter.
- En cours — Amazon FSx traite la demande de mise à jour.
- Mise à jour ; optimisation — Amazon FSx a augmenté la capacité de stockage SSD du système de fichiers. Le processus d'optimisation du stockage rééquilibre désormais vos données en arrière-plan.
- Terminé — La mise à jour s'est terminée avec succès.
- Échec : la demande de mise à jour a échoué. Choisissez le point d'interrogation (?) pour en savoir plus.

% de progression

Affiche la progression du processus d'optimisation du stockage sous forme de pourcentage d'achèvement.

Heure de la demande

Heure à laquelle Amazon FSx a reçu la demande d'action de mise à jour.

Pour surveiller le stockage et les mises à jour des IOPS (CLI)

Vous pouvez afficher et surveiller les demandes d'augmentation de la capacité de stockage SSD du système de fichiers à l'aide de la describe-file-systems AWS CLI commande et de l'opération DescribeFileSystemsAPI. Le `AdministrativeActions` tableau répertorie les 10 actions de mise à jour les plus récentes pour chaque type d'action administrative. Lorsque vous augmentez la capacité de stockage SSD d'un système de fichiers, deux `AdministrativeActions` actions sont générées : une `FILE_SYSTEM_UPDATE` et une `STORAGE_OPTIMIZATION` action.

L'exemple suivant montre un extrait de la réponse d'une commande `describe-file-systems` CLI. Le système de fichiers est en attente d'une action administrative visant à augmenter la capacité de stockage SSD à 2 000 GiB et le nombre d'IOPS du SSD provisionné à 7 000.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586797629.095,
```

```
        "Status": "PENDING",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
             }
        }
    },
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "RequestTime": 1586797629.095,
        "Status": "PENDING"
    }
]
```

Amazon FSx traite `FILE_SYSTEM_UPDATE` d'abord l'action, en ajoutant les nouveaux disques de stockage plus volumineux au système de fichiers. Lorsque le nouveau stockage est disponible pour le système de fichiers, l'`FILE_SYSTEM_UPDATE`état passe à`UPDATED_OPTIMIZING`. La capacité de stockage indique la nouvelle valeur supérieure, et Amazon FSx commence à traiter l'action `STORAGE_OPTIMIZATION` administrative. Ce comportement est illustré dans l'extrait suivant de la réponse d'une commande `describe-file-systems` CLI.

La `ProgressPercent` propriété affiche la progression du processus d'optimisation du stockage. Une fois le processus d'optimisation du stockage terminé avec succès, le statut de l'`FILE_SYSTEM_UPDATE`action passe à`COMPLETED`, et l'`STORAGE_OPTIMIZATION`action n'apparaît plus.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586799169.445,
        "Status": "UPDATED_OPTIMIZING",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
```

```
            }
        }
    },
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "ProgressPercent": 41,
        "RequestTime": 1586799169.445,
        "Status": "IN_PROGRESS"
    }
]
```

Si la demande de mise à jour de la capacité de stockage ou des IOPS échoue, le statut de l'`FILE_SYSTEM_UPDATE`action passe à`FAILED`, comme indiqué dans l'exemple suivant. La `FailureDetails` propriété fournit des informations sur l'échec.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586373915.697,
        "Status": "FAILED",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
            }
        },
        "FailureDetails": {
            "Message": "failure-message"
        }
    }
]
```

Augmenter la capacité de stockage SSD de manière dynamique

Vous pouvez utiliser la solution suivante pour augmenter dynamiquement la capacité de stockage SSD d'un système de fichiers FSx for ONTAP lorsque la capacité de stockage SSD utilisée dépasse un seuil que vous spécifiez. Ce AWS CloudFormation modèle déploie automatiquement tous les composants nécessaires pour définir le seuil de capacité de stockage, l' CloudWatch alarme Amazon

basée sur ce seuil et la AWS Lambda fonction qui augmente la capacité de stockage du système de fichiers.

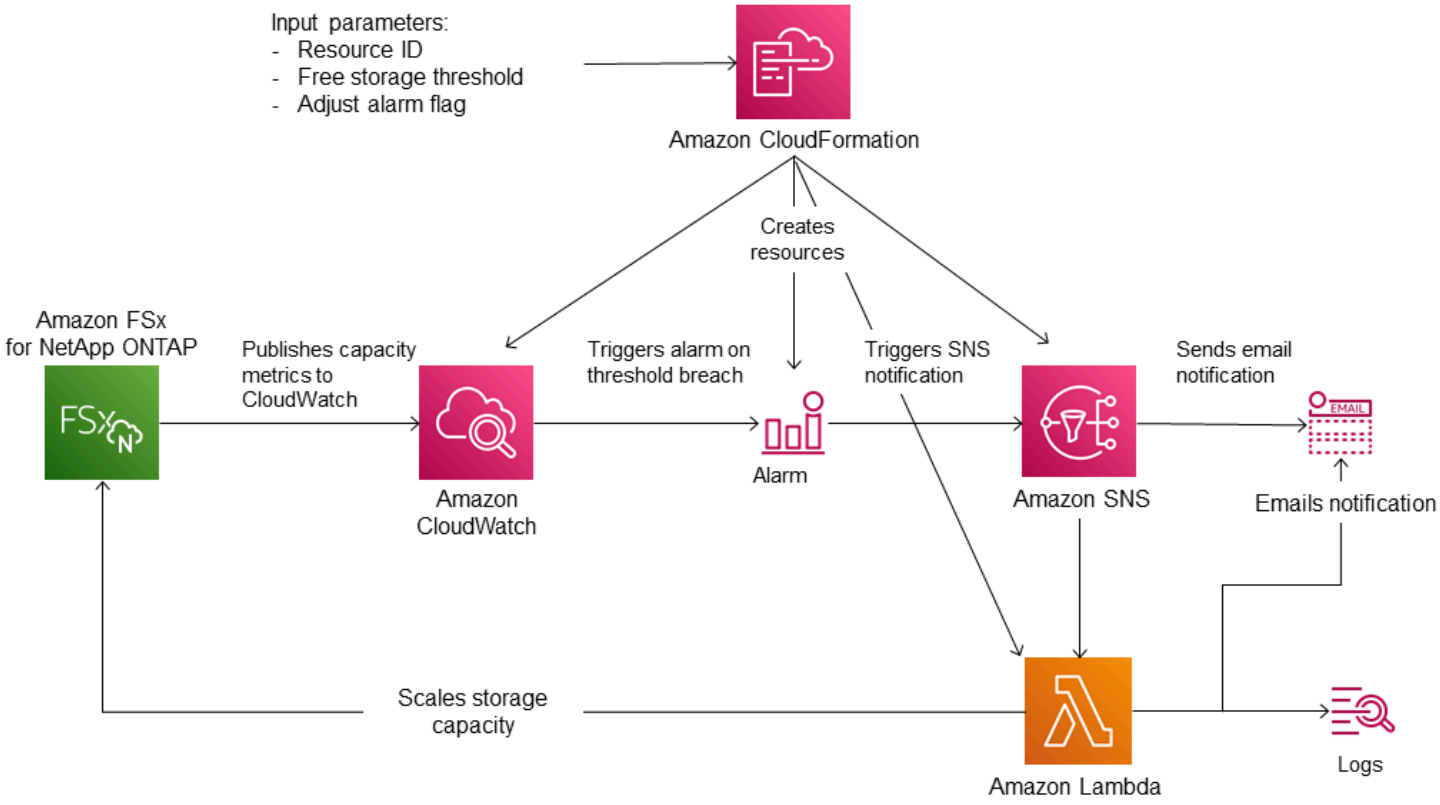
La solution déploie automatiquement tous les composants nécessaires et utilise les paramètres suivants :

- Votre identifiant de système de fichiers FSx for ONTAP.
- Le seuil de capacité de stockage SSD utilisé (valeur numérique). Il s'agit du pourcentage auquel l' CloudWatch alarme sera déclenchée.
- Pourcentage d'augmentation de la capacité de stockage (%).
- Adresse e-mail utilisée pour recevoir les notifications de dimensionnement.

Rubriques

Présentation de l’architecture

Le déploiement de cette solution génère les ressources suivantes dans le AWS Cloud.



Le diagramme suivant illustre les étapes suivantes :

1. Le AWS CloudFormation modèle déploie une CloudWatch alarme, une AWS Lambda fonction, une file d'attente Amazon Simple Notification Service (Amazon SNS) et tous les rôles requis AWS Identity and Access Management (IAM). Le rôle IAM autorise la fonction Lambda à appeler les opérations de l'API Amazon FSx.
2. CloudWatch déclenche une alarme lorsque la capacité de stockage utilisée du système de fichiers dépasse le seuil spécifié et envoie un message à la file d'attente Amazon SNS. Une alarme n'est déclenchée que lorsque la capacité utilisée du système de fichiers dépasse le seuil en continu pendant une période de 5 minutes.
3. La solution déclenche ensuite la fonction Lambda qui est abonnée à cette rubrique Amazon SNS.
4. La fonction Lambda calcule la nouvelle capacité de stockage du système de fichiers en fonction du pourcentage d'augmentation spécifié et définit la nouvelle capacité de stockage du système de fichiers.
5. L'état d' CloudWatch alarme d'origine et les résultats des opérations de la fonction Lambda sont envoyés à la file d'attente Amazon SNS.

Pour recevoir des notifications concernant les actions effectuées en réponse à l' CloudWatch alarme, vous devez confirmer votre inscription à la rubrique Amazon SNS en suivant le lien fourni dans l'e-mail de confirmation d'abonnement.

AWS CloudFormation modèle

Cette solution permet AWS CloudFormation d'automatiser le déploiement des composants utilisés pour augmenter automatiquement la capacité de stockage d'un système de fichiers FSx for ONTAP. Pour utiliser cette solution, téléchargez le SxOntapDynamicStorageScaling AWS CloudFormation modèle F.

Le modèle utilise les paramètres décrits ci-dessous. Passez en revue les paramètres du modèle et leurs valeurs par défaut, puis modifiez-les en fonction des besoins de votre système de fichiers.

FileSystemId

Aucune valeur par défaut. ID du système de fichiers dont vous souhaitez augmenter automatiquement la capacité de stockage.

LowFreeDataStorageCapacityThreshold

Aucune valeur par défaut. Spécifie le seuil de capacité de stockage utilisée à partir duquel déclencher une alarme et augmenter automatiquement la capacité de stockage du système de fichiers, spécifié en pourcentage (%) de la capacité de stockage actuelle du système de fichiers. Le système de fichiers est considéré comme ayant une faible capacité de stockage libre lorsque le stockage utilisé dépasse ce seuil.

EmailAddress

Aucune valeur par défaut. Spécifie l'adresse e-mail à utiliser pour l'abonnement SNS et reçoit les alertes relatives au seuil de capacité de stockage.

PercentIncrease

La valeur par défaut est de 20 %. Spécifie le montant d'augmentation de la capacité de stockage, exprimé en pourcentage de la capacité de stockage actuelle.

> **Note**
>
> Le dimensionnement du stockage est tenté une fois chaque fois que l' CloudWatch alarme passe à l'`ALARM`état. Si l'utilisation de la capacité de stockage de votre SSD reste

supérieure au seuil après une tentative de dimensionnement du stockage, l'opération de dimensionnement du stockage n'est pas tentée à nouveau.

MaxF B SxSizeinGi

La valeur par défaut est 196608. Spécifie la capacité de stockage maximale prise en charge pour le stockage SSD.

Déploiement automatisé avec AWS CloudFormation

La procédure suivante configure et déploie une AWS CloudFormation pile pour augmenter automatiquement la capacité de stockage d'un système de fichiers FSx for ONTAP. Le déploiement prend quelques minutes. Pour plus d'informations sur la création d'une CloudFormation pile, consultez la section Création d'une pile sur la AWS CloudFormation console dans le Guide de AWS CloudFormation l'utilisateur.

> **Note**
>
> La mise en œuvre de cette solution entraîne la facturation des AWS services associés. Pour plus d'informations, consultez les pages de détail des tarifs de ces services.

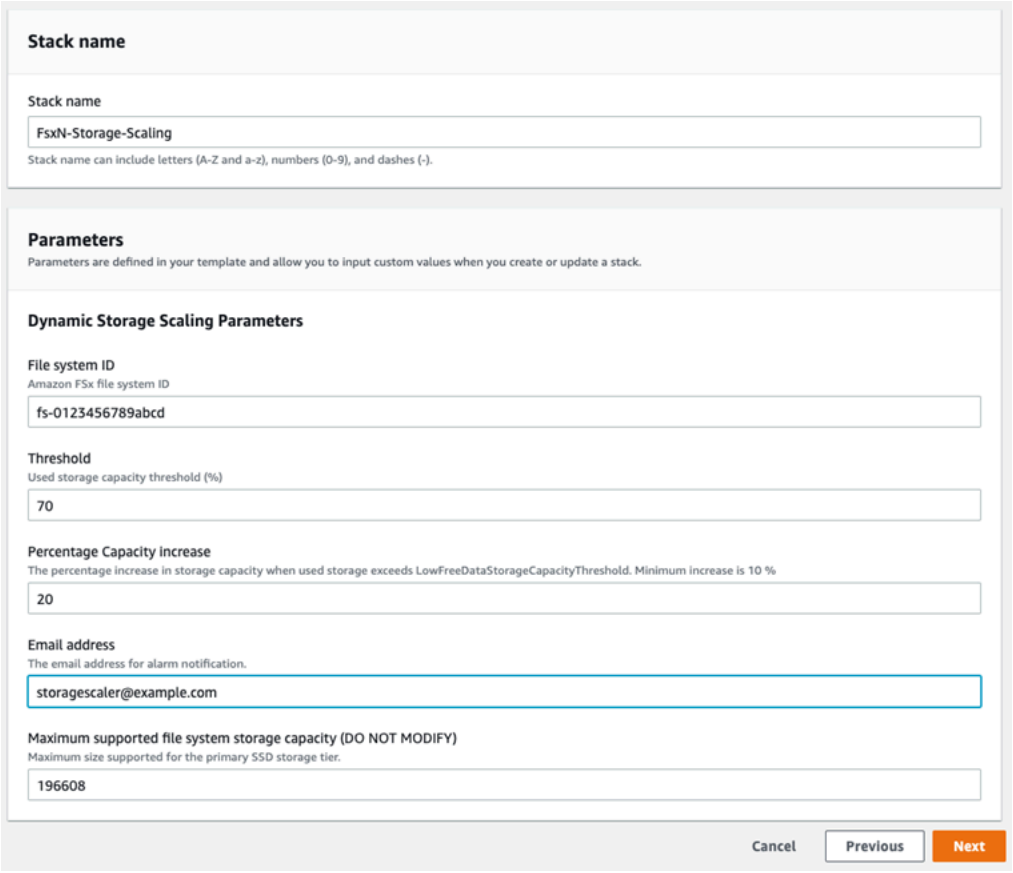
Avant de commencer, vous devez disposer de l'ID du système de fichiers Amazon FSx qui s'exécute dans Amazon Virtual Private Cloud (Amazon VPC) dans votre. Compte AWS Pour plus d'informations sur la création de ressources Amazon FSx, consultez. Commencer à utiliser Amazon FSx pour ONTAP NetApp

Pour lancer la pile de solutions d'augmentation automatique de la capacité de stockage

1. Téléchargez le SxOntapDynamicStorageScaling AWS CloudFormation modèle F.

   > **Note**
   >
   > Amazon FSx n'est actuellement disponible que dans certaines AWS régions. Vous devez lancer cette solution dans une AWS région où Amazon FSx est disponible. Pour plus d'informations, consultez la section Points de terminaison et quotas Amazon FSx dans le. Références générales AWS

2. Dans la AWS CloudFormation console, choisissez Create stack > Avec de nouvelles ressources.
3. Choose Template est prêt. Dans la section Spécifier le modèle, choisissez Télécharger un fichier modèle et chargez le modèle que vous avez téléchargé.
4. Dans Spécifier les détails de la pile, entrez les valeurs de votre solution d'augmentation automatique de la capacité de stockage.



5. Entrez un nom de pile.
6. Pour les paramètres, passez en revue les paramètres du modèle et modifiez-les en fonction des besoins de votre système de fichiers. Ensuite, sélectionnez Suivant.

> **Note**
>
> Pour recevoir des notifications par e-mail lorsque ce CloudFormation modèle tente de dimensionner, confirmez l'e-mail d'abonnement SNS que vous recevez après le déploiement du modèle.

7. Entrez les paramètres d'options que vous souhaitez pour votre solution personnalisée, puis choisissez Next.

8. Pour Révision, vérifiez et confirmez les paramètres de la solution. Vous devez cocher la case indiquant que le modèle crée des ressources IAM.
9. Choisissez Créer pour déployer la pile.

Vous pouvez consulter l'état de la pile dans la AWS CloudFormation console dans la colonne État. Vous devriez voir le statut CREATE_COMPLETE dans quelques minutes.

Mise à jour de la pile

Une fois la pile créée, vous pouvez la mettre à jour en utilisant le même modèle et en fournissant de nouvelles valeurs pour les paramètres. Pour plus d'informations, consultez la section Mise à jour des piles directement dans le guide de l'AWS CloudFormation utilisateur.

Capacité de stockage en volume

Les volumes FSx for ONTAP sont des ressources virtuelles que vous utilisez pour regrouper les données, déterminer le mode de stockage des données et le type d'accès à vos données. Les volumes, comme les dossiers, ne consomment pas eux-mêmes la capacité de stockage du système de fichiers. Seules les données stockées dans un volume consomment du stockage SSD et, en fonction de la politique de hiérarchisation du volume, du stockage en pool de capacité. Vous définissez la taille d'un volume lorsque vous le créez, et vous pouvez modifier sa taille ultérieurement. Vous pouvez surveiller et gérer la capacité de stockage de vos volumes FSx pour ONTAP à l'aide de l'API AWS CLI et de la AWS Management Console CLI ONTAP.

Rubriques

- Hiérarchisation des données de volume
- Instantanés et capacité de stockage en volume
- Capacité du fichier de volume
- Mettre à jour la capacité de stockage d'un volume
- Activation du dimensionnement automatique du volume
- Surveillance de la capacité de stockage des volumes
- Définition de la politique de hiérarchisation d'un volume
- Réglage du nombre minimum de jours de refroidissement
- Définition de la politique de récupération d'un volume dans le cloud
- Affichage de la capacité de fichier d'un volume

- Augmenter le nombre maximum de fichiers sur un volume
- Activation du mode d'écriture dans le cloud d'un volume

Hiérarchisation des données de volume

Un système de fichiers Amazon FSx for NetApp ONTAP comporte deux niveaux de stockage : le stockage principal et le stockage par pool de capacité. Le stockage principal est un stockage SSD haute performance, évolutif et provisionné spécialement conçu pour la partie active de votre ensemble de données. Le stockage en pool de capacité est un niveau de stockage entièrement élastique pouvant atteindre des pétaoctets et optimisé en termes de coûts pour les données rarement consultées.

Les données de chaque volume sont automatiquement hiérarchisées en fonction du niveau de stockage du pool de capacité en fonction de la politique de hiérarchisation, de la période de refroidissement et des paramètres de seuil du volume. Les sections suivantes décrivent les politiques de hiérarchisation des ONTAP volumes et les seuils utilisés pour déterminer à quel moment les données sont hiérarchisées par rapport au pool de capacités.

Politiques de hiérarchisation des volumes

Vous déterminez comment utiliser les niveaux de stockage de votre système de fichiers FSx for ONTAP en choisissant la politique de hiérarchisation pour chaque volume du système de fichiers. Vous choisissez la politique de hiérarchisation lorsque vous créez un volume, et vous pouvez la modifier à tout moment à l'aide de la console Amazon FSx AWS CLI, de l'API ou à l'NetApp aide d'outils de gestion. Vous pouvez choisir l'une des politiques suivantes qui déterminent quelles données, le cas échéant, sont hiérarchisées en fonction de la capacité de stockage du pool.

> **Note**
>
> La hiérarchisation peut déplacer les données de vos fichiers et vos données de capture vers le niveau du pool de capacités. Toutefois, les métadonnées des fichiers restent toujours au niveau SSD. Pour plus d’informations, consultez Comment est utilisé le stockage SSD.

- Auto : cette politique déplace toutes les données confidentielles (données utilisateur et instantanés) vers le niveau du pool de capacités. Le taux de refroidissement des données est déterminé par la période de refroidissement de la politique, qui est par défaut de 31 jours, et peut être configuré sur

des valeurs comprises entre 2 et 183 jours. Lorsque les blocs de données froids sous-jacents sont lus de manière aléatoire (comme dans le cas d'un accès classique aux fichiers), ils sont chauffés et écrits sur le niveau de stockage principal. Lorsque des blocs de données froids sont lus de manière séquentielle (par exemple, par une analyse antivirus), ils restent froids et restent sur le niveau de stockage du pool de capacité. Il s'agit de la politique par défaut lors de la création d'un volume à l'aide de la console Amazon FSx.

- Snapshot uniquement : cette politique déplace uniquement les données des snapshots vers le niveau de stockage du pool de capacité. La fréquence à laquelle les instantanés sont hiérarchisés par rapport au pool de capacités est déterminée par la période de refroidissement de la politique, qui est définie par défaut sur 2 jours, et peut être configurée sur des valeurs comprises entre 2 et 183 jours. Lorsque les données d'un instantané à froid sont lues, elles sont chauffées et écrites sur le niveau de stockage principal. Il s'agit de la politique par défaut lors de la création d'un volume à l' AWS CLI aide de l'API Amazon FSx ou de la CLI NetApp ONTAP.
- Tout : cette politique marque toutes les données utilisateur et les données instantanées comme étant froides et les stocke au niveau du pool de capacités. Lorsque les blocs de données sont lus, ils restent froids et ne sont pas écrits sur le niveau de stockage principal. Lorsque des données sont écrites sur un volume soumis à la politique de hiérarchisation complète, elles sont toujours initialement écrites sur le niveau de stockage SSD, puis hiérarchisées sur le pool de capacités par un processus en arrière-plan. Notez que les métadonnées des fichiers restent toujours au niveau SSD.
- Aucune : cette politique conserve toutes les données de votre volume sur le niveau de stockage principal et empêche leur transfert vers le stockage en pool de capacité. Si vous définissez cette politique à un volume après avoir utilisé une autre politique, les données existantes du volume qui se trouvaient dans le pool de capacité de stockage sont déplacées vers le stockage SSD par un processus en arrière-plan, à condition que l'utilisation de votre SSD soit inférieure à 90 %. Ce processus en arrière-plan peut être accéléré en lisant intentionnellement les données ou en modifiant la politique de récupération dans le cloud de votre volume. Pour plus d’informations, consultez Politiques de récupération dans le cloud.

Il est recommandé, lors de la migration de données que vous prévoyez de stocker à long terme dans un pool de capacité de stockage, d'appliquer la politique de hiérarchisation automatique à votre volume. Avec la hiérarchisation automatique, les données sont stockées sur le niveau de stockage SSD pendant au moins 2 jours (en fonction de la période de refroidissement du volume) avant d'être déplacées vers le niveau du pool de capacité. La conservation des données sur le stockage SSD pendant au moins 2 jours permet à ONTAP de réaliser des économies de compression et de déduplication après le traitement sur vos données, qui sont préservées lorsque les données sont

hiérarchisées en fonction du pool de capacité. ONTAP exécute uniquement la compression et la déduplication après le traitement pour les données stockées sur SSD. Le choix de cette politique peut donc vous aider à optimiser vos économies de stockage à long terme. Vous pouvez également optimiser les vitesses de transfert des premières sauvegardes que vous créez de vos volumes, car les données sauvegardées se trouvent sur un stockage SSD.

Pour plus d'informations sur la définition ou la modification de la politique de hiérarchisation d'un volume, consultezDéfinition de la politique de hiérarchisation d'un volume.

Période de refroidissement échelonnée

La période de refroidissement échelonnée d'un volume définit le temps nécessaire pour que les données du niveau SSD soient marquées comme froides. La période de refroidissement s'applique aux politiques de hiérarchisation `Auto` et `Snapshot-only` de hiérarchisation. Vous pouvez définir la période de refroidissement sur une valeur comprise entre 2 et 183 jours. Pour plus d'informations sur le réglage de la période de refroidissement, consultezRéglage du nombre minimum de jours de refroidissement.

Les données sont hiérarchisées 24 à 48 heures après l'expiration de leur période de refroidissement. La hiérarchisation est un processus d'arrière-plan qui consomme les ressources du réseau et dont la priorité est inférieure à celle des demandes destinées aux clients. Les activités de hiérarchisation sont limitées lorsqu'il y a des demandes continues adressées aux clients.

Politiques de récupération dans le cloud

La politique de récupération dans le cloud d'un volume définit les conditions qui spécifient à quel moment les données lues depuis le niveau du pool de capacités peuvent être promues vers le niveau SSD. Lorsque la politique de récupération dans le cloud est définie sur une valeur autre que`Default`, elle remplace le comportement de récupération de la politique de hiérarchisation de votre volume. Un volume peut avoir l'une des politiques de récupération dans le cloud suivantes :

- Par défaut : cette politique récupère les données hiérarchisées en fonction de la politique de hiérarchisation sous-jacente du volume. Il s'agit de la politique de récupération dans le cloud par défaut pour tous les volumes.
- Jamais : cette politique ne récupère jamais de données hiérarchisées, que les lectures soient séquentielles ou aléatoires. Cela revient à définir la politique de hiérarchisation de votre volume sur Tous, sauf que vous pouvez l'utiliser avec d'autres politiques (Auto, Snapshot uniquement) pour hiérarchiser les données en fonction de la période de refroidissement minimale plutôt qu'immédiatement.

- En cours de lecture : cette règle récupère les données hiérarchisées pour toutes les lectures de données pilotées par le client. Cette politique n'a aucun effet lors de l'utilisation de la politique All tiering.
- Promouvoir : cette politique marque toutes les données d'un volume qui se trouvent dans le pool de capacités en vue de leur extraction vers le niveau SSD. Les données sont marquées lors de la prochaine exécution du scanner de hiérarchisation quotidienne en arrière-plan. Cette politique est avantageuse pour les applications dont les charges de travail cycliques s'exécutent rarement, mais qui nécessitent des performances de niveau SSD pour s'exécuter. Cette politique n'a aucun effet lors de l'utilisation de la politique All tiering.

Pour plus d'informations sur la définition de la politique de récupération dans le cloud d'un volume, consultezDéfinition de la politique de récupération d'un volume dans le cloud.

Seuils de hiérarchisation

L'utilisation de la capacité de stockage SSD d'un système de fichiers détermine ONTAP le mode de gestion du comportement de hiérarchisation pour tous vos volumes. Sur la base de l'utilisation de la capacité de stockage SSD d'un système de fichiers, les seuils suivants définissent le comportement de hiérarchisation tel que décrit. Pour plus d'informations sur la façon de surveiller l'utilisation de la capacité du niveau de stockage SSD d'un volume, consultezSurveillance de la capacité de stockage des volumes.

> **Note**
>
> Nous vous recommandons de ne pas dépasser 80 % d'utilisation de la capacité de stockage de votre niveau de stockage SSD. Pour les systèmes de fichiers évolutifs, cette recommandation s'applique à la fois à l'utilisation moyenne totale de tous les agrégats de votre système de fichiers et à l'utilisation de chaque agrégat individuel. Cela garantit le bon fonctionnement de la hiérarchisation et entraîne une surcharge pour les nouvelles données. Si le niveau de stockage de votre SSD est constamment supérieur à 80 % d'utilisation de la capacité de stockage, vous pouvez augmenter la capacité de votre niveau de stockage SSD. Pour plus d'informations, consultez Mise à jour du système de fichiers, du stockage SSD et des IOPS.

FSx for ONTAP utilise les seuils de capacité de stockage suivants pour gérer la hiérarchisation des volumes :

- <= 50 % d'utilisation du niveau de stockage SSD : à ce seuil, le niveau de stockage SSD est considéré comme sous-utilisé, et seuls les volumes qui appliquent la politique de hiérarchisation complète ont des données hiérarchisées en fonction de la capacité de stockage du pool de stockage. Les volumes dotés de politiques Auto et Snapshot uniquement ne hiérarchisent pas les données à ce seuil.
- > 50 % d'utilisation du niveau de stockage SSD : les volumes soumis à des politiques de hiérarchisation automatique et basées uniquement sur les instantanés hiérarchisent les données en fonction du nombre minimum de jours de refroidissement définis par hiérarchisation. Le paramètre par défaut est de 31 jours.
- >= 90 % d'utilisation du niveau de stockage SSD — À partir de ce seuil, Amazon FSx donne la priorité à la préservation de l'espace dans le niveau de stockage SSD. Les données confidentielles provenant du niveau du pool de capacités ne sont plus déplacées vers le niveau de stockage SSD lorsqu'elles sont lues pour des volumes à l'aide des politiques Auto et Snapshot uniquement.
- >= 98 % d'utilisation du niveau de stockage SSD : toutes les fonctionnalités de hiérarchisation s'arrêtent lorsque le niveau de stockage SSD atteint ou dépasse 98 % d'utilisation. Vous pouvez continuer à lire depuis les niveaux de stockage, mais vous ne pouvez pas écrire sur les niveaux.

Instantanés et capacité de stockage en volume

Un instantané est une image en lecture seule d'un volume Amazon FSx for NetApp ONTAP à un moment donné. Les instantanés offrent une protection contre la suppression ou la modification accidentelle de fichiers de vos volumes. Grâce aux instantanés, vos utilisateurs peuvent facilement visualiser et restaurer des fichiers ou des dossiers individuels à partir d'un instantané antérieur.

Les instantanés sont stockés avec les données de votre système de fichiers, et ils consomment la capacité de stockage du système de fichiers. Toutefois, les instantanés consomment de la capacité de stockage uniquement pour les portions de fichiers modifiées depuis le dernier instantané. Les instantanés ne sont pas inclus dans les sauvegardes des volumes de votre système de fichiers.

Les instantanés sont activés par défaut sur vos volumes, selon la politique de capture par défaut. Les instantanés sont stockés dans le `.snapshot` répertoire situé à la racine d'un volume. Vous pouvez gérer la capacité de stockage en volume pour les instantanés de la manière suivante :

- Politiques relatives aux instantanés : sélectionnez une politique de capture intégrée ou choisissez une politique personnalisée que vous avez créée dans la CLI ONTAP ou l'API REST.
- Supprimer manuellement les instantanés : récupérez de la capacité de stockage en supprimant les instantanés manuellement.

- Création d'une politique de suppression automatique des instantanés : créez une politique qui supprime un plus grand nombre de clichés que la politique de capture d'écran par défaut.
- Désactiver les instantanés automatiques : économisez la capacité de stockage en désactivant les instantanés automatiques.

Pour plus d'informations, consultez Utilisation des instantanés.

Capacité du fichier de volume

Les volumes Amazon FSx for NetApp ONTAP disposent de pointeurs de fichiers utilisés pour stocker les métadonnées des fichiers, telles que le nom du fichier, l'heure du dernier accès, les autorisations, la taille, et pour servir de pointeurs vers des blocs de données. Ces pointeurs de fichiers sont appelés inodes, et chaque volume possède une capacité limitée pour le nombre d'inodes, appelée capacité du fichier de volume. Lorsque le nombre de fichiers disponibles (inodes) d'un volume est épuisé ou qu'il en manque, vous ne pouvez pas y écrire de données supplémentaires.

Le nombre d'objets du système de fichiers (fichiers, répertoires, copies instantanées) qu'un volume peut contenir est déterminé par le nombre d'inodes qu'il contient. Le nombre d'inodes dans un volume augmente proportionnellement à la capacité de stockage du volume (et au nombre de composants du volume pour FlexGroup les volumes). Par défaut, les FlexVol volumes (ou FlexGroup composants) dont la capacité de stockage est supérieure ou égale à 648 GiB possèdent tous le même nombre d'inodes : 21 251 126. Si vous créez un volume supérieur à 648 GiB et que vous souhaitez qu'il contienne plus de 21 251 126 inodes, vous devez augmenter le nombre maximum d'inodes (fichiers) manuellement. Pour plus d'informations sur l'affichage du nombre maximal de fichiers pour un volume, consultezAffichage de la capacité de fichier d'un volume.

Le nombre d'inodes par défaut sur un volume est de 1 inode pour 32 KiB de capacité de stockage du volume, jusqu'à une taille de volume de 648 GiB. Pour un volume de 1 GiB :

Volume_Size_in_bytes × (1 fichier ÷ inode_size_in_bytes) = nombre_maximum_de_fichiers

1 073 741 824 octets × (1 fichier ÷ 32 768 octets) = 32 768 fichiers

Vous pouvez augmenter le nombre maximum d'inodes qu'un volume peut contenir, jusqu'à un maximum de 1 inode pour 4 KiB de capacité de stockage. Pour un volume de 1 GiB, cela augmente le nombre maximum d'inodes ou de fichiers de 32 768 à 262 144 :

1 073 741 824 octets × (1 fichier ÷ 4 096 octets) = 262 144 fichiers

Un volume FSx for ONTAP peut contenir un maximum de 2 milliards d'inodes.

Pour plus d'informations sur la modification du nombre maximal de fichiers qu'un volume peut stocker, consultezAugmenter le nombre maximum de fichiers sur un volume.

Mettre à jour la capacité de stockage d'un volume

Vous pouvez gérer la capacité de stockage des volumes en augmentant ou en diminuant manuellement la taille des volumes à l' AWS Management Console aide de l'API AWS CLI et de la CLI ONTAP. Vous pouvez également activer le dimensionnement automatique du volume afin qu'il augmente ou diminue automatiquement lorsqu'il atteint certains seuils de capacité de stockage utilisée. Vous utilisez la CLI ONTAP pour gérer le dimensionnement automatique des volumes.

Pour modifier la capacité de stockage d'un volume (console)

- Vous pouvez augmenter ou diminuer la capacité de stockage d'un volume à l'aide de la console Amazon FSx et de l' AWS CLI API. Pour plus d'informations, consultez Mettre à jour un volume.

Vous pouvez également utiliser la ONTAP CLI pour modifier la capacité de stockage d'un volume à l'aide de la `volume modify`commande.

Pour modifier la taille d'un volume (CLI ONTAP)

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *`management_endpoint_ip`* par l'adresse IP du port de gestion du système de fichiers.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Pour plus d'informations, consultez Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.
2. Utilisez la commande volume modify ONTAP CLI pour modifier la capacité de stockage d'un volume. Exécutez la commande suivante en utilisant vos données à la place des valeurs suivantes :

   - *`svm_name`*Remplacez-le par le nom de la machine virtuelle de stockage (SVM) sur laquelle le volume est créé.
   - Remplacez *`vol_name`*par le nom du volume que vous souhaitez redimensionner.
   - Remplacez-le *`vol_size`*par la nouvelle taille du volume dans le format *`integer`*`[KB|MB|GB|TB|PB]`, par exemple `100GB` pour augmenter la taille du volume à 100 gigaoctets.

```
::> volume modify -vserver svm_name -volume vol_name -size vol_size
```

Activation du dimensionnement automatique du volume

Dimensionnement automatique du volume afin qu'il atteigne automatiquement une taille spécifiée lorsqu'il atteint un seuil d'espace utilisé. Vous pouvez le faire pour les types de FlexVol volumes (le type de volume par défaut pour FSx for ONTAP) à l'aide de la commande ONTAP `volume autosize`CLI.

Pour activer le dimensionnement automatique des volumes (CLI ONTAP)

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *`management_endpoint_ip`* par l'adresse IP du port de gestion du système de fichiers.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Pour plus d'informations, consultez Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.
2. Utilisez la `volume autosize` commande comme indiqué, en remplaçant les valeurs suivantes :

   - Remplacez *`svm_name`*par le nom de la SVM sur laquelle le volume a été créé.
   - Remplacez *`vol_name`*par le nom du volume que vous souhaitez redimensionner.
   - Remplacez-le *`grow_threshold`*par un pourcentage d'espace utilisé (tel que`90`) à partir duquel le volume augmentera automatiquement (jusqu'à la *`max_size`*valeur).
   - *`max_size`*Remplacez-le par la taille maximale que le volume peut atteindre. Utilisez le format *`integer`*`[KB|MB|GB|TB|PB]`; par exemple,`300TB`. La taille maximale est de 300 To. La valeur par défaut est de 120 % de la taille du volume.
   - Remplacez *`min_size`* par la taille minimale à laquelle le volume sera réduit. Utilisez le même format que pour *`max_size`*.
   - Remplacez *`shrink_threshold`* par le pourcentage d'espace utilisé auquel la taille du volume diminuera automatiquement.

```
::> volume autosize -vserver svm_name -volume vol_name -mode grow_shrink -
grow-threshold-percent grow_threshold -maximum-size max_size -shrink-threshold-
percent shrink_threshold -minimum-size min_size
```

Surveillance de la capacité de stockage des volumes

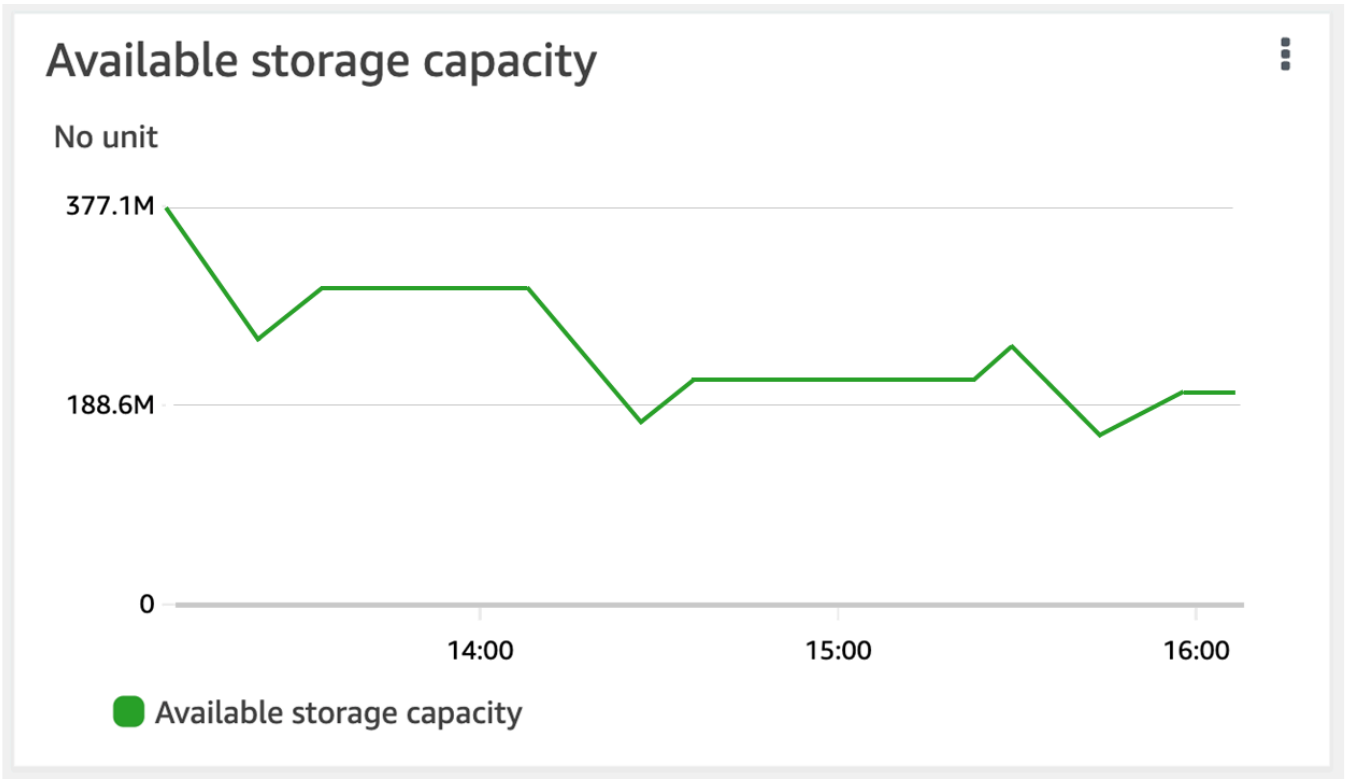
Vous pouvez consulter le stockage disponible d'un volume et sa distribution dans et dans AWS Management Console la CLI NetApp ONTAP. AWS CLI

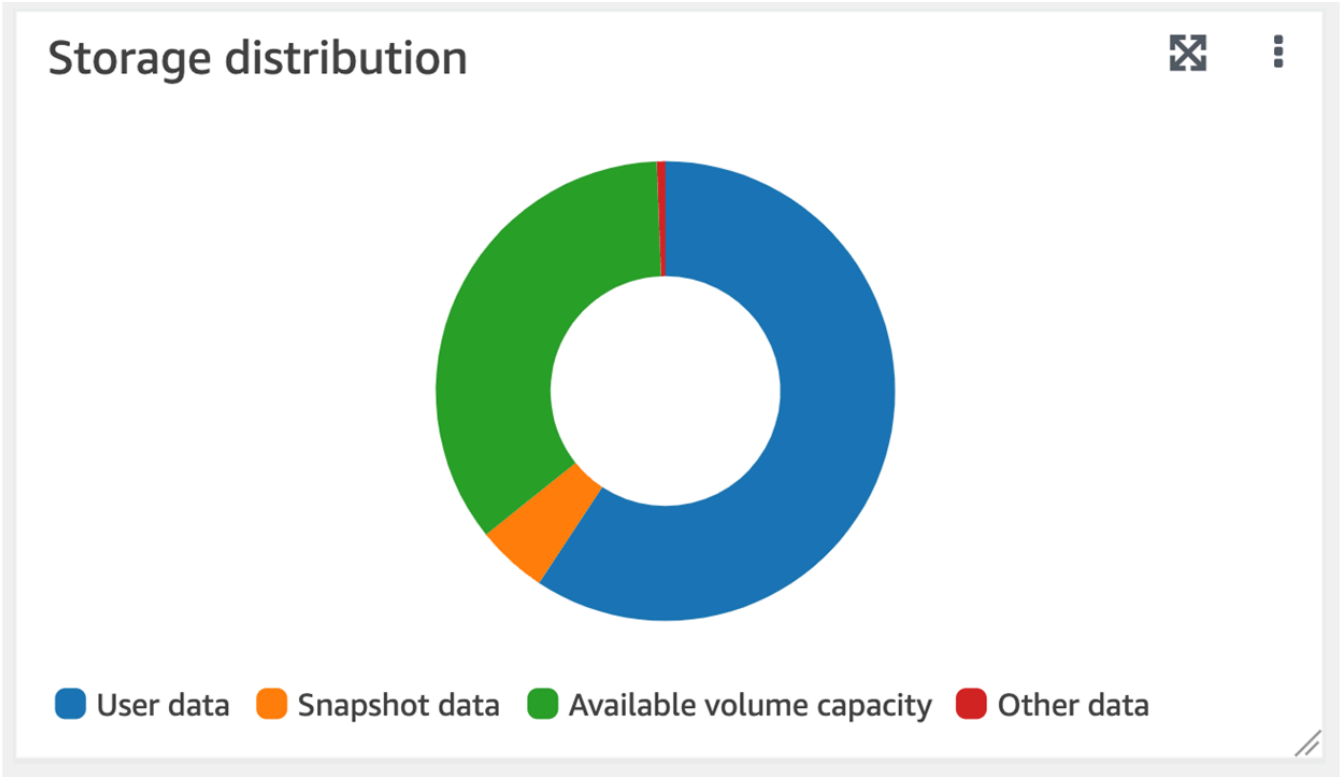
Pour surveiller la capacité de stockage d'un volume (console)

Le graphique de stockage disponible affiche la quantité de capacité de stockage disponible sur un volume au fil du temps. Le graphique de distribution du stockage montre comment la capacité de stockage d'un volume est actuellement répartie en 4 catégories :

- Données utilisateur
- Données instantanées
- Capacité de volume disponible
- Autres données

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Choisissez Volumes dans la colonne de navigation de gauche, puis choisissez le volume ONTAP pour lequel vous souhaitez consulter les informations de capacité de stockage. La page détaillée du volume apparaît.
3. Dans le deuxième panneau, choisissez l'onglet Surveillance. Les graphiques du stockage disponible et de la distribution du stockage s'affichent, ainsi que plusieurs autres graphiques.


Available storage capacity
No unit
377.1M
188.6M
0
14:00
15:00
16:00
Available storage capacity


Storage distribution
User data
Snapshot data
Available volume capacity
Other data

Pour surveiller la capacité de stockage d'un volume (ONTAPCLI)

Vous pouvez surveiller la façon dont la capacité de stockage de votre volume est consommée à l'aide de la commande `volume show-space` ONTAP CLI. Pour plus d'informations, consultez `volume show-space`le Centre de NetApp ONTAP documentation.

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *`management_endpoint_ip`* par l'adresse IP du port de gestion du système de fichiers.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Pour plus d'informations, consultez Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.

2. Consultez l'utilisation de la capacité de stockage d'un volume en exécutant la commande suivante, en remplaçant les valeurs suivantes :

   - Remplacez *`svm_name`*par le nom de la SVM sur laquelle le volume a été créé.
   - Remplacez *`vol_name`*par le nom du volume pour lequel vous définissez la politique de hiérarchisation des données.

   ```
   ::> volume show-space -vserver svm_name -volume vol_name
   ```

   Si la commande aboutit, vous obtiendrez un résultat similaire à ce qui suit :

   ```
   Vserver : svm_name
   Volume  : vol_name
   Feature                                     Used      Used%
   --------------------------------     ----------     ------
   User Data                                140KB         0%
   Filesystem Metadata                    164.4MB         1%
   Inodes                                 10.28MB         0%
   Snapshot Reserve                       563.2MB         5%
   Deduplication                             12KB         0%
   Snapshot Spill                          9.31GB        85%
   Performance Metadata                     668KB         0%

   Total Used                             10.03GB        91%
   ```

```
Total Physical Used                          10.03GB        91%
```

Le résultat de cette commande indique la quantité d'espace physique occupé par les différents types de données sur ce volume. Il indique également le pourcentage de la capacité totale du volume consommé par chaque type de données. Dans cet exemple, `Snapshot Spill` et `Snapshot Reserve` consommez au total 90 % de la capacité du volume.

`Snapshot Reserve`indique la quantité d'espace disque réservée au stockage des copies de snapshots. Si l'espace de stockage des copies Snapshot dépasse l'espace réservé, il se répand dans le système de fichiers et cette quantité est indiquée ci-dessous. `Snapshot Spill`

Pour augmenter la quantité d'espace disponible, vous pouvez soit augmenter la taille du volume, soit supprimer des instantanés que vous n'utilisez pas, comme indiqué dans les procédures suivantes.

Pour les types de FlexVol volumes (type de volume par défaut pour les volumes FSx pour ONTAP), vous pouvez également activer le dimensionnement automatique des volumes. Lorsque vous activez le dimensionnement automatique, la taille du volume augmente automatiquement lorsqu'elle atteint certains seuils. Vous pouvez également désactiver les instantanés automatiques. Ces deux fonctionnalités sont expliquées dans les sections suivantes.

Définition de la politique de hiérarchisation d'un volume

Vous pouvez modifier la politique de hiérarchisation d'un volume à l'aide de l' AWS Management Console API AWS CLI et de la CLI ONTAP.

Pour modifier la politique de hiérarchisation des données d'un volume (console)

Utilisez la procédure suivante pour modifier la politique de hiérarchisation des données d'un volume à l'aide du. AWS Management Console

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Choisissez Volumes dans le volet de navigation de gauche, puis choisissez le volume ONTAP pour lequel vous souhaitez modifier la politique de hiérarchisation des données.
3. Choisissez Mettre à jour le volume dans le menu déroulant Actions. La fenêtre Mettre à jour le volume apparaît.
4. Pour la politique de hiérarchisation du pool de capacités, choisissez la nouvelle politique pour le volume. Pour plus d’informations, consultez Politiques de hiérarchisation des volumes.
5. Choisissez Mettre à jour pour appliquer la nouvelle politique au volume.

Pour définir la politique de hiérarchisation (CLI) d'un volume

- Modifiez la politique de hiérarchisation d'un volume à l'aide de la commande update-volume CLI UpdateVolume(action équivalente de l'API Amazon FSx). L'exemple de commande CLI suivant définit la politique de hiérarchisation des données d'un volume sur. SNAPSHOT_ONLY

```
aws fsx update-volume \
    --volume-id fsxvol-abcde0123456789f
    --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
```

En cas de réussite de la demande, le système répond par la description du volume.

```
{
    "Volume": {
        "CreationTime": "2021-10-05T14:27:44.332000-04:00",
        "FileSystemId": "fs-abcde0123456789f",
        "Lifecycle": "CREATED",
        "Name": "vol1",
        "OntapConfiguration": {
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "UNIX",
            "SizeInMegabytes": 1048576,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abc0123de456789f",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "CoolingPeriod": 2,
                "Name": "SNAPSHOT_ONLY"
            },
            "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcde0123456789f/fsvol-abc012def3456789a",
        "VolumeId": "fsvol-abc012def3456789a",
        "VolumeType": "ONTAP"
    }
}
```

Pour modifier la politique de hiérarchisation d'un volume (CLI ONTAP)

Vous utilisez la commande `volume modify` ONTAP CLI pour définir la politique de hiérarchisation d'un volume. Pour plus d'informations, consultez `volume modify`le centre de documentation NetApp ONTAP.

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *`management_endpoint_ip`* par l'adresse IP du port de gestion du système de fichiers.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Pour plus d'informations, consultez Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.

2. Entrez dans le mode avancé ONTAP CLI à l'aide de la commande suivante.

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. Utilisez la commande suivante pour modifier la politique de hiérarchisation des données de volume, en remplaçant les valeurs suivantes :

   - Remplacez *`svm_name`*par le nom de la SVM sur laquelle le volume a été créé.
   - Remplacez *`vol_name`*par le nom du volume pour lequel vous définissez la politique de hiérarchisation des données.
   - Remplacez *`tiering_policy`*par la politique souhaitée. Les valeurs valides sont `snapshot-only`, `auto`, `all` ou `none`. Pour plus d'informations, consultez Politiques de hiérarchisation des volumes.

   ```
   FSx::> volume modify -vserver svm_name -volume vol_name -tiering-
   policy tiering_policy
   ```

Réglage du nombre minimum de jours de refroidissement

Le nombre minimum de jours de refroidissement pour un volume définit le seuil utilisé pour déterminer quelles données sont chaudes et quelles données sont froides. Vous pouvez définir le nombre minimum de jours de refroidissement d'un volume à l'aide d'une API AWS CLI et de la CLI ONTAP.

Pour définir le nombre minimum de jours de refroidissement d'un volume (CLI)

- Modifiez la configuration d'un volume à l'aide de la commande update-volume CLI (UpdateVolumeaction équivalente de l'API Amazon FSx). L'exemple de commande CLI suivant définit un volume `CoolingPeriod` sur 104 jours.

```
aws fsx update-volume \
    --volume-id fsxvol-abcde0123456789f
    --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
aws fsx update-volume --volume-id fsvol-006530558c14224ac --ontap-configuration
 TieringPolicy={CoolingPeriod=104}
```

Le système répond avec la description du volume en cas de réussite de la demande.

```
{
    "Volume": {
        "CreationTime": "2021-10-05T14:27:44.332000-04:00",
        "FileSystemId": "fs-abcde0123456789f",
        "Lifecycle": "CREATED",
        "Name": "vol1",
        "OntapConfiguration": {
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "UNIX",
            "SizeInMegabytes": 1048576,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abc0123de456789f",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "CoolingPeriod": 104,
                "Name": "SNAPSHOT_ONLY"
            },
            "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
            "OntapVolumeType": "RW"
```

```
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcde0123456789f/fsvol-abc012def3456789a",
        "VolumeId": "fsvol-abc012def3456789a",
        "VolumeType": "ONTAP"
    }
}
```

Pour définir le nombre minimum de jours de refroidissement d'un volume (CLI ONTAP)

Utilisez la commande `volume modify` ONTAP CLI pour définir le nombre minimum de jours de refroidissement pour un volume existant. Pour plus d'informations, consultez `volume modify`le centre de documentation NetApp ONTAP.

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *`management_endpoint_ip`* par l'adresse IP du port de gestion du système de fichiers.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Pour plus d'informations, consultez Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.

2. Entrez dans le mode avancé ONTAP CLI à l'aide de la commande suivante.

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. Utilisez la commande suivante pour modifier le nombre minimal de jours de refroidissement de votre volume par hiérarchisation, en remplaçant les valeurs suivantes :

   - Remplacez *`svm_name`*par le nom de la SVM sur laquelle le volume a été créé.
   - Remplacez *`vol_name`*par le nom du volume pour lequel vous définissez les jours de refroidissement.
   - Remplacez *`cooling_days`* par le nombre entier souhaité compris entre 2 et 183.

```
FSx::> volume modify -vserver svm_name -volume vol_name -tiering-minimum-cooling-
days cooling_days
```

Le système répond comme suit en cas de réussite de la demande.

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

Définition de la politique de récupération d'un volume dans le cloud

Utilisez la commande `volume modify` ONTAP CLI pour définir la politique de récupération dans le cloud pour un volume existant. Pour plus d'informations, consultez `volume modify`le centre de documentation NetApp ONTAP.

Pour définir la politique de récupération dans le cloud d'un volume (CLI ONTAP)

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *`management_endpoint_ip`* par l'adresse IP du port de gestion du système de fichiers.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Pour plus d'informations, consultez Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.
2. Entrez dans le mode avancé ONTAP CLI à l'aide de la commande suivante.

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```
3. Utilisez la commande suivante pour définir la politique de récupération du volume dans le cloud, en remplaçant les valeurs suivantes :

   - Remplacez *`svm_name`*par le nom de la SVM sur laquelle le volume a été créé.

- Remplacez *vol_name*par le nom du volume pour lequel vous définissez la politique de récupération dans le cloud.
- Remplacez *retrieval_policy* par la valeur souhaitée`default`, soit`on-read`,`never`, soit`promote`.

```
FSx::> volume modify -vserver svm_name -volume vol_name -cloud-retrieval-
policy retrieval_policy
```

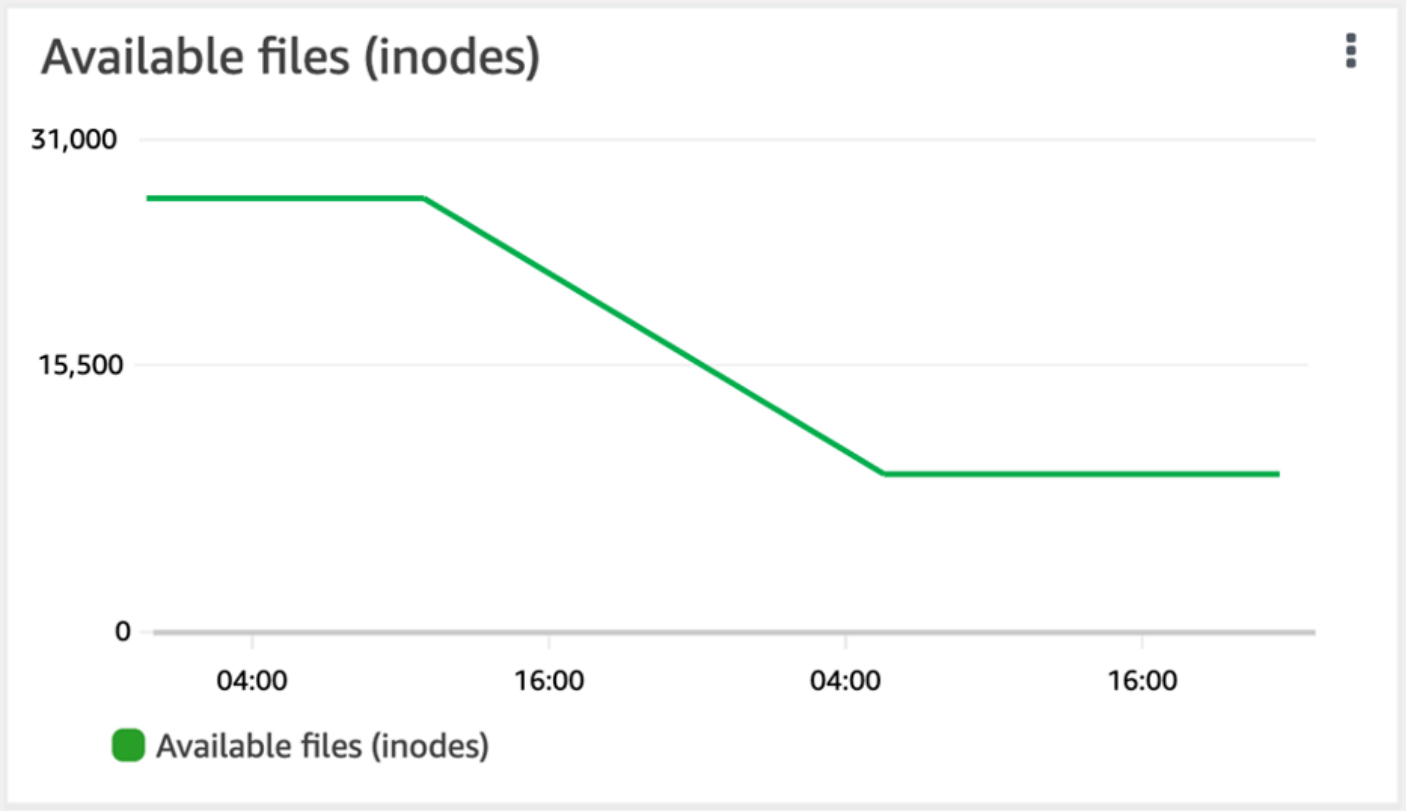
Le système répond comme suit en cas de réussite de la demande.

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

Affichage de la capacité de fichier d'un volume

Vous pouvez utiliser l'une des méthodes suivantes pour afficher le nombre maximum de fichiers autorisés et le nombre de fichiers déjà utilisés sur un volume.

- Les mesures de CloudWatch volume `FilesCapacity` et`FilesUsed`.
- Dans la console Amazon FSx, accédez au graphique des fichiers disponibles (inodes) dans l'onglet Surveillance de votre volume. L'image suivante montre les fichiers disponibles (inodes) sur un volume décroissant au fil du temps.



Augmenter le nombre maximum de fichiers sur un volume

Les volumes FSx for ONTAP peuvent manquer de capacité de fichier lorsque le nombre d'inodes ou de pointeurs de fichiers disponibles est épuisé.

Pour augmenter le nombre maximum de fichiers sur un volume (ONTAPCLI)

Vous utilisez la commande `volume modify` ONTAP CLI pour augmenter le nombre maximum de fichiers sur un volume. Pour plus d'informations, consultez `volume modify`le Centre de NetApp ONTAP documentation.

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *`management_endpoint_ip`* par l'adresse IP du port de gestion du système de fichiers.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

Pour plus d'informations, consultez Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.

2. Effectuez l'une des actions suivantes en fonction de votre cas d'utilisation. Remplacez *svm_name*et *vol_name*par vos valeurs.

   - Pour configurer un volume afin qu'il dispose toujours du nombre maximum de fichiers (inodes) disponibles, effectuez les opérations suivantes :

     1. Passez en mode avancé dans la CLI ONTAP à l'aide de la commande suivante.

        ```
        ::> set adv
        ```

     2. Après avoir exécuté cette commande, vous verrez ce résultat. Entrez y pour continuer.

        ```
        Warning: These advanced commands are potentially dangerous; use them only
         when
        directed to do so by NetApp personnel.
        Do you want to continue? {y|n}: y
        ```

     3. Entrez la commande suivante pour toujours utiliser le nombre maximum de fichiers sur le volume :

        ```
        ::> volume modify -vserver svm_name -volume vol_name -files-set-maximum true
        ```

   - Pour spécifier manuellement le nombre total de fichiers autorisés sur le volume*max_number_files* = (current_size_of_volume) × (1 file ÷ 4 KiB), avec une valeur maximale de 2 milliards, utilisez la commande suivante :

     ```
     ::> volume modify -vserver svm_name -volume vol_name -files max_number_files
     ```

Activation du mode d'écriture dans le cloud d'un volume

Utilisez la commande `volume modify` ONTAP CLI pour activer ou désactiver le mode d'écriture dans le cloud pour un volume existant. Pour plus d'informations, consultez `volume modify`le centre de documentation NetApp ONTAP.

Les conditions requises pour configurer le mode d'écriture dans le cloud sont les suivantes :

- Le volume doit être un volume existant. Vous ne pouvez activer cette fonctionnalité que sur un volume existant.

- Le volume doit être un volume de lecture-écriture (RW).
- Le volume doit respecter la politique de hiérarchisation complète. Pour plus d'informations sur la modification de la politique de hiérarchisation d'un volume, consultezDéfinition de la politique de hiérarchisation d'un volume.

Le mode d'écriture dans le cloud est utile dans des cas tels que les migrations, par exemple, lorsque de grandes quantités de données sont transférées vers un système de fichiers à l'aide du protocole NFS.

Pour définir le mode d'écriture dans le cloud d'un volume (CLI ONTAP)

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *`management_endpoint_ip`* par l'adresse IP du port de gestion du système de fichiers.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Pour plus d'informations, consultez Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.
2. Entrez dans le mode avancé ONTAP CLI à l'aide de la commande suivante.

   ```
   FSx::> set -privilege advanced
   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```
3. Utilisez la commande suivante pour définir le mode d'écriture dans le cloud du volume, en remplaçant les valeurs suivantes :

   - Remplacez *`svm_name`*par le nom de la SVM sur laquelle le volume a été créé.
   - Remplacez *`vol_name`*par le nom du volume pour lequel vous configurez le mode d'écriture dans le cloud.
   - Remplacez *`vol_cw_mode`* par soit `true` pour activer le mode d'écriture dans le cloud sur le volume, soit `false` pour le désactiver.

```
FSx::> volume modify -vserver svm_name -volume vol_name -is-cloud-write-
enabled vol_cw_mode
```

Le système répond comme suit en cas de réussite de la demande.

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

Protection de vos données

Au-delà de la réplication automatique des données de votre système de fichiers pour garantir une durabilité élevée, Amazon FSx vous propose les options suivantes pour mieux protéger les données stockées sur vos systèmes de fichiers :

- Les sauvegardes natives d'Amazon FSx répondent à vos besoins en matière de conservation des sauvegardes et de conformité au sein d'Amazon FSx. Vous pouvez également l'utiliser AWS Backup pour gérer, automatiser et protéger de manière centralisée vos sauvegardes Services AWS dans le cloud.
- Les instantanés permettent à vos utilisateurs d'annuler facilement les modifications apportées aux fichiers et de comparer les versions des fichiers en restaurant les versions précédentes.
- Réplication de votre système de fichiers Amazon FSx vers un second système de fichiers pour assurer la protection et la restauration des données. La réplication, lorsqu'elle est activée, s'effectue automatiquement et de manière planifiée.
- SnapLockpeut protéger vos fichiers en les faisant passer à l'état WORM (Write Once, Read Many), qui empêche toute modification ou suppression pendant une période de conservation spécifiée.

Rubriques

Utilisation des sauvegardes

Avec FSx for ONTAP, vous pouvez effectuer des sauvegardes quotidiennes automatiques et des sauvegardes initiées par l'utilisateur des volumes de votre système de fichiers. Les sauvegardes FSx for ONTAP sont effectuées par volume, de sorte que chaque sauvegarde ne contient que les données d'un volume spécifique. Les sauvegardes Amazon FSx sont extrêmement durables et incrémentielles.

Toutes les sauvegardes Amazon FSx (sauvegardes quotidiennes automatiques et sauvegardes initiées par l'utilisateur) sont incrémentielles. Cela signifie que seules les données du volume qui ont changé après votre dernière sauvegarde sont enregistrées. Cela permet de réduire le temps

nécessaire à la création de la sauvegarde et le stockage requis pour celle-ci, ce qui permet de réduire les coûts de stockage en évitant de dupliquer les données. Lorsque vous supprimez une sauvegarde, seules les données propres à cette sauvegarde sont supprimées. Chaque sauvegarde Amazon FSx contient toutes les informations nécessaires pour créer un nouveau volume à partir de la sauvegarde, ce qui permet de restaurer efficacement un point-in-time instantané du volume du système de fichiers.

La création de sauvegardes régulières pour vos volumes est une bonne pratique qui permet de répondre à vos besoins en matière de conservation des données et de conformité. Il est facile d'utiliser les sauvegardes Amazon FSx, qu'il s'agisse de créer des sauvegardes, de restaurer à partir d'une sauvegarde ou de supprimer une sauvegarde.

Amazon FSx prend en charge la sauvegarde de ONTAP FlexVol volumes (sur tous les systèmes de fichiers) et de FlexGroup volumes dotés d'une valeur `OntapVolumeType` de `RW` (lecture-écriture).

> **Note**
>
> Amazon FSx ne prend pas en charge la sauvegarde de volumes de protection des données (DP), de volumes de partage de charge (LS) ou de volumes de destination. FlexCache

Le nombre de sauvegardes que vous pouvez stocker par système de fichiers et par volume est limité. Pour plus d'informations, consultez Les quotas que vous pouvez augmenter et Quotas de ressources pour chaque système de fichiers.

Rubriques

- Création d'une sauvegarde initiée par l'utilisateur
- Restauration d'une sauvegarde sur un nouveau volume
- Suppression d'une sauvegarde

Comment fonctionnent les sauvegardes

Les sauvegardes Amazon FSx utilisent des instantanés (point-in-timeimages en lecture seule de vos volumes) pour maintenir l'incrémentalité entre les sauvegardes. Chaque fois qu'une sauvegarde est effectuée, Amazon FSx prend d'abord un instantané de votre volume. L'instantané de sauvegarde est stocké dans votre volume et consomme de l'espace sur le niveau de stockage de votre SSD. Amazon FSx compare ensuite cet instantané à l'instantané de sauvegarde précédent (s'il en existe un) et copie uniquement les données modifiées dans votre sauvegarde.

S'il n'existe aucun instantané de sauvegarde antérieur, l'intégralité du contenu de l'instantané de sauvegarde le plus récent est copié dans votre sauvegarde. Une fois le dernier instantané de sauvegarde pris avec succès, Amazon FSx supprime l'instantané de sauvegarde précédent. L'instantané utilisé pour la dernière sauvegarde reste dans votre volume jusqu'à ce que la sauvegarde suivante soit effectuée, lorsque le processus se répète. Pour optimiser les coûts de stockage des sauvegardes, ONTAP préserve l'efficacité du stockage d'un volume et permet de réaliser des économies lors de ses sauvegardes.

Amazon FSx ne peut pas sauvegarder les volumes hors ligne.

Besoins de stockage

Pour effectuer des sauvegardes de vos volumes, votre volume et votre système de fichiers doivent disposer d'une capacité de stockage SSD suffisante pour stocker un instantané de sauvegarde. Lorsque vous prenez un instantané de sauvegarde, la capacité de stockage supplémentaire consommée par l'instantané ne peut pas faire en sorte que le volume dépasse 98 % d'utilisation du stockage SSD. Dans ce cas, la sauvegarde échouera. Vous pouvez augmenter le stockage SSD d'un volume ou d'un système de fichiers à tout moment pour garantir que vos sauvegardes ne seront pas interrompues.

Utilisation de sauvegardes quotidiennes automatiques

Les sauvegardes quotidiennes automatiques des volumes de votre système de fichiers sont activées par défaut lorsque vous créez un système de fichiers. Vous pouvez activer ou désactiver les sauvegardes quotidiennes automatiques d'un système de fichiers à tout moment. Les sauvegardes

quotidiennes automatiques ont lieu pendant la fenêtre de sauvegarde quotidienne, qui est automatiquement définie lorsque vous créez un système de fichiers. Vous pouvez modifier la fenêtre de sauvegarde quotidienne à tout moment. Nous vous recommandons de choisir une heure de la journée pour vos sauvegardes quotidiennes en dehors des heures de fonctionnement normales pour les applications qui utilisent vos volumes afin d'améliorer les performances de sauvegarde. Pour plus d'informations, consultez Performances de sauvegarde et de restauration.

Vous pouvez définir la période de conservation des sauvegardes quotidiennes automatiques entre 1 et 90 jours dans la console lors de la création d'un système de fichiers ou à tout moment. La période de conservation quotidienne automatique des sauvegardes par défaut est de 30 jours. Le service supprime une sauvegarde quotidienne automatique une fois sa période de conservation expirée. À l'aide de la CLI ou de l'API, vous pouvez définir la période de rétention entre 0 et 90 jours ; la définir sur 0 désactive les sauvegardes quotidiennes automatiques.

La fenêtre de sauvegarde quotidienne et la période de conservation des sauvegardes sont des paramètres au niveau du système de fichiers qui s'appliquent à tous les volumes de votre système de fichiers. Vous pouvez utiliser la console Amazon FSx AWS CLI, ou l'API pour modifier la fenêtre de sauvegarde et la période de conservation des sauvegardes pour vos systèmes de fichiers, et pour activer ou désactiver les sauvegardes quotidiennes automatiques. Pour plus d'informations, consultez Mettre à jour un système de fichiers.

Vous ne pouvez pas créer de sauvegarde de volume si le volume est hors ligne. Pour plus d'informations, consultez Sauvegardes et volumes hors ligne.

> **Note**
>
> Les sauvegardes quotidiennes automatiques ont une durée de conservation maximale de 90 jours, mais les sauvegardes initiées par l'utilisateur que vous créez, y compris les sauvegardes créées à l'aide de celles-ci AWS Backup, sont conservées indéfiniment à moins que vous ou le AWS Backup service ne les supprimiez.

Vous pouvez supprimer manuellement une sauvegarde quotidienne automatique à l'aide de la console, de la CLI et de l'API. Lorsque vous supprimez un volume, vous supprimez également les sauvegardes quotidiennes automatiques de ce volume. Amazon FSx offre la possibilité de créer une sauvegarde finale d'un volume avant de le supprimer. La sauvegarde finale est conservée indéfiniment, sauf si vous la supprimez. Pour plus d'informations, consultezSuppression de sauvegardes.

Utilisation de sauvegardes initiées par l'utilisateur

Avec Amazon FSx, vous pouvez effectuer des sauvegardes manuelles des volumes de votre système de fichiers à tout moment à l'aide de l'API AWS Management Console AWS CLI, et. Vos sauvegardes initiées par l'utilisateur sont incrémentielles par rapport aux autres sauvegardes qui peuvent avoir été créées pour un volume et sont conservées pour toujours, sauf si vous les supprimez. Les sauvegardes initiées par l'utilisateur sont conservées même après la suppression du volume ou du système de fichiers sur lequel les sauvegardes ont été créées. Vous pouvez supprimer des sauvegardes initiées par l'utilisateur uniquement à l'aide de la console, de l'API ou de la CLI Amazon FSx. Ils ne sont jamais automatiquement supprimés par Amazon FSx. Pour plus d'informations, consultez Suppression de sauvegardes.

Vous ne pouvez pas créer de sauvegarde de volume si le volume est hors ligne. Pour plus d'informations, consultez Sauvegardes et volumes hors ligne.

Copier des balises dans les sauvegardes

Lorsque vous créez ou mettez à jour un volume à l'aide de la CLI ou de l'API, vous pouvez `CopyTagsToBackups` activer la copie automatique des balises de votre volume dans ses sauvegardes. Toutefois, si vous ajoutez des balises lors de la création d'une sauvegarde initiée par l'utilisateur, notamment en nommant une sauvegarde lorsque vous utilisez la console, le service ne copie pas les balises du volume, même s'il `CopyTagsToBackups` est activé.

Performances de sauvegarde et de restauration

De nombreux facteurs peuvent influencer les performances des opérations de sauvegarde et de restauration. Les opérations de sauvegarde et de restauration sont des processus en arrière-plan, ce qui signifie qu'elles ont une priorité moindre par rapport aux opérations d'E/S du client. Les opérations d'E/S du client incluent la lecture et l'écriture de données NFS, CIFS et iSCSI. Tous les processus en arrière-plan, y compris les opérations de sauvegarde et de restauration, n'utilisent que la partie inutilisée de la capacité de débit de votre système de fichiers et peuvent prendre de quelques minutes à quelques heures en fonction de la taille de votre sauvegarde et de la capacité de débit inutilisée de votre système de fichiers.

Les autres facteurs qui affectent les performances de sauvegarde et de restauration incluent le niveau de stockage dans lequel vos données sont stockées et le profil du jeu de données. Nous vous recommandons de créer les premières sauvegardes de vos volumes lorsque la plupart des données se trouvent sur un stockage SSD. Les ensembles de données contenant principalement de petits fichiers auront généralement des performances inférieures à celles des ensembles de données de

taille similaire contenant principalement des fichiers volumineux. Cela est dû au fait que le traitement d'un grand nombre de petits fichiers consomme plus de cycles de processeur et de surcharge réseau que le traitement de moins de fichiers volumineux.

En règle générale, vous pouvez vous attendre aux taux de sauvegarde suivants lorsque vous sauvegardez des données stockées dans le niveau de stockage SSD :

- 750 Mbits/s sur plusieurs sauvegardes simultanées contenant principalement des fichiers volumineux.
- 100 Mo/s sur plusieurs sauvegardes simultanées contenant principalement de petits fichiers.

En général, vous pouvez vous attendre aux taux de restauration suivants :

- 250 Mbits/s sur plusieurs restaurations simultanées contenant principalement des fichiers volumineux.
- 100 Mbits/s sur plusieurs restaurations simultanées contenant principalement de petits fichiers.

Utilisation AWS Backup avec Amazon FSx

AWS Backup est un moyen simple et économique de protéger vos données en sauvegardant vos volumes Amazon FSx for NetApp ONTAP. AWS Backup est un service de sauvegarde unifié conçu pour simplifier la création, la restauration et la suppression des sauvegardes, tout en fournissant des rapports et des audits améliorés. AWS Backup facilite le développement d'une stratégie de sauvegarde centralisée à des fins de conformité légale, réglementaire et professionnelle. AWS Backup simplifie également la protection AWS de vos volumes de stockage, de vos bases de données et de vos systèmes de fichiers en fournissant un emplacement central où vous pouvez effectuer les opérations suivantes :

- Configurez et auditez les AWS ressources que vous souhaitez sauvegarder.
- Automatiser la planification des sauvegardes.
- Définir des stratégies de conservation.
- Surveillez toutes les activités récentes de sauvegarde, de copie et de restauration.

AWS Backup utilise la fonctionnalité de sauvegarde intégrée d'Amazon FSx. Les sauvegardes créées à l'aide de la AWS Backup console présentent le même niveau de cohérence et de performance du système de fichiers, sont incrémentielles par rapport à toutes les autres sauvegardes Amazon FSx

que vous effectuez de votre volume (initiées par l'utilisateur ou automatiques) et offrent les mêmes options de restauration que les sauvegardes effectuées via la console Amazon FSx. Si vous gérez AWS Backup ces sauvegardes, vous bénéficiez de fonctionnalités supplémentaires, telles que la possibilité de créer des sauvegardes planifiées toutes les heures. Vous pouvez ajouter une couche de défense supplémentaire pour protéger les sauvegardes contre les suppressions involontaires ou malveillantes en les stockant dans un AWS Backup coffre-fort.

Les sauvegardes créées par AWS Backup sont considérées comme des sauvegardes initiées par l'utilisateur et sont prises en compte dans le quota de sauvegarde initié par l'utilisateur pour Amazon FSx. Pour plus d'informations, consultez Les quotas que vous pouvez augmenter. Vous pouvez afficher et restaurer les sauvegardes créées par AWS Backup la console, la CLI et l'API Amazon FSx. Toutefois, vous ne pouvez pas supprimer les sauvegardes créées par AWS Backup la console, la CLI ou l'API Amazon FSx. Pour plus d'informations, voir Getting Started with AWS Backup dans le guide du AWS Backup développeur.

AWS Backup Impossible de sauvegarder des volumes hors ligne.

Restauration des sauvegardes sur un nouveau volume

Vous pouvez restaurer une sauvegarde de volume sur un nouveau volume, en restaurant efficacement un point-in-time instantané d'un volume à l'aide de la console, de la CLI ou de l'API.

Lors de la restauration d'une sauvegarde, toutes les données sont d'abord écrites sur le niveau de stockage SSD avant que le service ne commence à hiérarchiser les données sur le stockage du pool de capacité conformément à la politique de hiérarchisation que vous avez définie pour le volume restauré. Lors de la restauration d'une sauvegarde sur un volume avec une politique de hiérarchisation de`All`, un processus d'arrière-plan périodique hiérarchise les données vers le pool de capacités. Lors de la restauration d'une sauvegarde sur un volume soumis à une politique de hiérarchisation de `Snapshot Only` ou`Auto`, les données sont hiérarchisées en fonction du pool de capacités si l'utilisation du SSD pour le système de fichiers est supérieure à 50 %, et le taux de refroidissement est déterminé par la période de refroidissement de la politique de hiérarchisation.

Lorsque vous restaurez une sauvegarde de FlexGroup volume sur un système de fichiers dont le nombre de paires de haute disponibilité (HA) est différent de celui du système de fichiers d'origine, Amazon FSx peut ajouter des volumes constitutifs supplémentaires pour garantir une distribution uniforme des composants.

Pour step-by-step obtenir des instructions sur la restauration d'une sauvegarde sur un nouveau volume, reportez-vous àRestauration d'une sauvegarde sur un nouveau volume.

> **Note**
>
> Un volume restauré possède toujours le même style de volume que le volume d'origine. Vous ne pouvez pas modifier le style du volume lors de la restauration.

Suppression de sauvegardes

Vous pouvez supprimer les sauvegardes quotidiennes automatiques et les sauvegardes initiées par l'utilisateur de vos volumes. La suppression d'une sauvegarde est une action permanente irrécupérable. Toutes les données d'une sauvegarde supprimée sont également supprimées. Ne supprimez pas une sauvegarde si vous n'êtes pas certain de ne pas en avoir besoin à nouveau à l'avenir. Pour obtenir des instructions expliquant comment supprimer des sauvegardes, consultezSuppression d'une sauvegarde.

Vous ne pouvez pas supprimer les sauvegardes créées par AWS Backup, qui ont un type AWS Backup, dans la console, la CLI ou l'API Amazon FSx. Pour plus d'informations sur la suppression des sauvegardes créées par AWS Backup, consultez la section Suppression de sauvegardes dans le manuel du AWS Backup développeur.

Vous ne pouvez pas supprimer la sauvegarde d'un volume s'il est hors ligne. Pour plus d'informations, consultez Sauvegardes et volumes hors ligne.

> **Important**
>
> Ne supprimez pas le cliché commun du volume car il est utilisé pour maintenir l'incrémentalité entre vos sauvegardes. La suppression de l'instantané commun du volume fera en sorte que la sauvegarde suivante portera sur l'ensemble du volume plutôt que sur une simple sauvegarde incrémentielle.

Sauvegardes et volumes hors ligne

Vous ne pouvez pas créer ou supprimer des sauvegardes de volumes si ce volume est hors ligne. Utilisez la commande `volume show`ONTAPCLI pour déterminer l'état et le statut actuels d'un volume.

Pour remettre en ligne un volume hors ligne, utilisez la commande `volume online`ONTAPCLI comme dans l'exemple suivant :

```
::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

Création d'une sauvegarde initiée par l'utilisateur

La procédure suivante décrit comment utiliser la console Amazon FSx pour créer une sauvegarde d'un volume initiée par l'utilisateur.

Vous ne pouvez pas créer de sauvegarde de volume si le volume est hors ligne. Pour plus d'informations, consultez Sauvegardes et volumes hors ligne.

Pour créer une sauvegarde d'un volume initiée par l'utilisateur (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Accédez à Systèmes de fichiers et choisissez le système de ONTAP fichiers pour lequel vous souhaitez sauvegarder un volume.
3. Choisissez l'onglet Volumes.
4. Choisissez le volume que vous souhaitez sauvegarder.
5. Dans Actions, sélectionnez Créer une sauvegarde.
6. Dans la boîte de dialogue Créer une sauvegarde qui s'ouvre, donnez un nom à votre sauvegarde. Les noms de sauvegarde peuvent comporter au maximum 256 caractères Unicode, y compris des lettres, des espaces blancs, des chiffres et des caractères spéciaux. + - = _ :/
7. Choisissez Créer une sauvegarde.

Vous venez de créer une sauvegarde de l'un des volumes de votre système de fichiers. Vous pouvez trouver un tableau de toutes vos sauvegardes dans la console Amazon FSx en choisissant Sauvegardes dans la barre de navigation de gauche. Vous pouvez rechercher le nom que vous avez donné à votre sauvegarde, et le tableau filtre pour n'afficher que les résultats correspondants.

Lorsque vous créez une sauvegarde initiée par l'utilisateur comme décrit dans cette procédure, elle possède le type `USER_INITIATED` et le `CREATING` statut jusqu'à ce qu'elle soit entièrement disponible.

Restauration d'une sauvegarde sur un nouveau volume

Les procédures suivantes décrivent comment restaurer une sauvegarde FSx for ONTAP sur un nouveau volume à l'aide du et. AWS Management Console AWS CLI

Pour restaurer une sauvegarde de volume sur un nouveau volume (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation, choisissez Backups, puis choisissez la sauvegarde du volume FSx for ONTAP que vous souhaitez restaurer.
3. Dans le menu Actions en haut à droite, choisissez Restaurer la sauvegarde. La page Créer un volume à partir d'une sauvegarde apparaît.
4. Choisissez le système de fichiers FSx for ONTAP et la machine virtuelle de stockage sur lesquels vous souhaitez restaurer la sauvegarde dans les menus déroulants.
5. Sous Détails du volume, vous pouvez sélectionner plusieurs options. Entrez d'abord le nom du volume. Vous pouvez utiliser jusqu'à 203 caractères alphanumériques ou soulignés (_).
6. Pour Taille du volume, entrez un nombre entier compris entre 20 et 314572800 pour spécifier la taille en mégaoctets (MiB).
7. Pour le type de volume, choisissez Read-Write (RW) pour créer un volume lisible et inscriptible ou Data Protection (DP) pour créer un volume en lecture seule pouvant être utilisé comme destination d'une relation or. NetApp SnapMirror SnapVault Pour plus d’informations, consultez Types de volume.
8. Pour le chemin de jonction, entrez un emplacement dans le système de fichiers pour monter le volume. Le nom doit être précédé d'une barre oblique, par exemple`/vol3`.
9. Pour l'efficacité du stockage, choisissez Activé pour activer les fonctionnalités d'ONTAPefficacité du stockage (déduplication, compression et compactage). Pour plus d’informations, consultez FSx pour l'efficacité du stockage ONTAP.
10. Pour le style de sécurité des volumes, choisissez Unix (Linux), NTFS ou Mixed. Le style de sécurité d'un volume détermine si la préférence est donnée aux ACL NTFS ou UNIX pour l'accès multiprotocole. Le mode MIXED n'est pas requis pour l'accès multiprotocole et n'est recommandé qu'aux utilisateurs expérimentés.
11. Pour la politique de capture instantanée, choisissez une politique de capture instantanée pour le volume. Pour plus d'informations sur les politiques relatives aux instantanés, consultezRègles relatives aux snapshots.

Si vous choisissez Politique personnalisée, vous devez spécifier le nom de la politique dans le champ Politique personnalisée. La politique personnalisée doit déjà exister sur la SVM ou dans le système de fichiers. Vous pouvez créer une politique de capture d'écran personnalisée à l'aide de la ONTAP CLI ou de l'API REST. Pour plus d'informations, consultez la section Création d'une politique de capture instantanée dans la documentation NetApp ONTAP du produit.

12. Pour la période de refroidissement de la politique de hiérarchisation, les valeurs valides sont de 2 à 183 jours. La période de refroidissement de la politique de hiérarchisation d'un volume définit le nombre de jours avant que les données auxquelles il n'est pas possible d'accéder soient signalées comme froides et transférées vers le stockage en pool de capacité. Ce paramètre n'affecte que les `Snapshot-only` politiques `Auto` et.
13. Dans la section Avancé, pour SnapLockConfiguration, vous pouvez laisser le paramètre Désactivé par défaut ou choisir Activé pour configurer un SnapLock volume. Pour plus d'informations sur la configuration d'un SnapLock Compliance volume ou d'un SnapLock Enterprise volume, reportez-vous Création d'un volume SnapLock de conformité aux sections etCréation d'un volume SnapLock Enterprise. Pour plus d'informations sur SnapLock, consultez Protégez vos données avec SnapLock.
14. Choisissez Confirmer pour créer le volume.

Pour restaurer une sauvegarde de volume sur un nouveau volume (CLI)

Utilisez la commande create-volume-from-backupCLI ou la commande CreateVolumeFromBackupAPI équivalente pour restaurer une sauvegarde de volume sur un nouveau volume.

- ```
  $ aws fsx create-volume-from-backup --backup-id backup-08e6fc1133fff3532 \
        --name demo --ontap-configuration JunctionPath=/demo, SizeInMegabytes=100000,
   \
        StorageVirtualMachineId=svm-0f04a9c7c27e1908b, TieringPolicy={Name=ALL}
  ```

  La réponse du système en cas de demande réussie :

  ```
  {
        "Volume": {
            "CreationTime": 1692721488.428,
            "FileSystemId": "fs-07ab735385276ed60",
            "Lifecycle": "CREATING",
            "Name": "demo",
  ```
  ```

```
            "OntapConfiguration": {
                "FlexCacheEndpointType": "NONE",
                "JunctionPath": "/demo",
                "SizeInMegabytes": 100000,
                "StorageEfficiencyEnabled": true,
                "StorageVirtualMachineId": "svm-0f04a9c7c27e1908b",
                "StorageVirtualMachineRoot": false,
                "TieringPolicy": {
                    "Name": "ALL"
                },
                "OntapVolumeType": "DP",
                "SnapshotPolicy": "default",
                "CopyTagsToBackups": false,
            },
            "ResourceARN": "arn:aws:fsx:us-east-1:752825163408:volume/
fs-07ab735385276ed60/fsvol-0b6ec764c9c5f654a",
            "VolumeId": "fsvol-0b6ec764c9c5f654a",
            "VolumeType": "ONTAP",

        }
    }
```


Suppression d'une sauvegarde

Vous pouvez supprimer les sauvegardes quotidiennes automatiques et les sauvegardes initiées par l'utilisateur à l'aide de la console, de la CLI et de l'API Amazon FSx, comme décrit dans les procédures suivantes.

Pour supprimer des sauvegardes créées à l'aide de AWS Backup, consultez la section Suppression de sauvegardes dans le guide du AWS Backup développeur.

Pour supprimer une sauvegarde (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le tableau de bord de la console, choisissez Sauvegardes dans la barre de navigation de gauche.
3. Choisissez la sauvegarde que vous souhaitez supprimer dans le tableau des sauvegardes, puis choisissez Supprimer la sauvegarde.
4. Dans la boîte de dialogue Supprimer les sauvegardes qui s'ouvre, vérifiez que l'ID de la sauvegarde affiché est celui de la sauvegarde que vous souhaitez supprimer.

5. Vérifiez que la case est cochée pour la sauvegarde que vous souhaitez supprimer.
6. Choisissez Supprimer les sauvegardes.

Votre sauvegarde et toutes les données incluses sont désormais définitivement et irrémédiablement supprimées.

Pour supprimer une sauvegarde (CLI)

- Utilisez la commande de la CLI delete-backup ou l'action DeleteBackup API équivalente pour supprimer une sauvegarde de volume FSx for ONTAP, comme illustré dans l'exemple suivant.

```
$ aws fsx delete-backup --backup-id backup-a0123456789abcdef
```

La réponse du système inclut l'ID de la sauvegarde supprimée et son état de cycle de vie, `DELETED` indiquant que la demande a été acceptée.

```
{
    "BackupId": "backup-a0123456789abcdef",
    "Lifecycle": "DELETED"
}
```

Utilisation des instantanés

Un instantané est une image en lecture seule d'un volume Amazon FSx for NetApp ONTAP à un moment donné. Les instantanés offrent une protection contre la suppression ou la modification accidentelle de fichiers de vos volumes. Grâce aux instantanés, vos utilisateurs peuvent facilement afficher et restaurer des fichiers ou des dossiers individuels à partir d'un instantané antérieur afin d'annuler les modifications, de récupérer du contenu supprimé et de comparer les versions de fichiers.

Un instantané contient les données modifiées depuis le dernier instantané, ce qui consomme la capacité de stockage SSD du système de fichiers. Les instantanés ne sont inclus dans aucune sauvegarde de volume. Les instantanés sont activés par défaut sur vos volumes à l'aide de la politique des `default` instantanés. Les instantanés sont stockés dans le `.snapshot` répertoire situé à la racine d'un volume. Vous pouvez stocker un maximum de 1 023 instantanés par volume à tout moment. Une fois cette limite atteinte, vous devez supprimer un instantané existant avant de pouvoir créer un nouvel instantané de votre volume.

Rubriques

Règles relatives aux snapshots

La politique relative aux instantanés définit la manière dont le système crée des instantanés pour un volume. La politique précise à quel moment créer des instantanés, combien de copies conserver et comment les nommer. Il existe trois politiques de capture d'écran intégrées pour FSx for ONTAP :

- `default`
- `default-1weekly`
- `none`

Par défaut, chaque volume est associé à la politique de `default` capture instantanée du système de fichiers. Nous recommandons d'utiliser cette politique pour la plupart des charges de travail.

La `default` politique crée automatiquement des instantanés selon le calendrier suivant, les copies les plus anciennes étant supprimées pour faire de la place aux nouvelles copies :

- Un maximum de six instantanés pris toutes les heures, cinq minutes après l'heure.
- Deux instantanés quotidiens au maximum pris du lundi au samedi, 10 minutes après minuit.
- Un maximum de deux instantanés hebdomadaires pris chaque dimanche, 15 minutes après minuit.

> **Note**
>
> Les heures des instantanés sont basées sur le fuseau horaire du système de fichiers, qui est défini par défaut sur le temps universel coordonné (UTC). Pour plus d'informations sur la modification du fuseau horaire, consultez la section Affichage et réglage du fuseau horaire du système dans la documentation de NetApp support.

La `default-1weekly` politique fonctionne de la même manière que la `default` politique, sauf qu'elle ne conserve qu'un seul instantané du planning hebdomadaire.

La none politique ne prend aucun instantané. Vous pouvez attribuer cette politique aux volumes pour empêcher la prise de clichés automatiques.

Vous pouvez également créer une politique de capture personnalisée à l'aide de la CLI ONTAP ou de l'API REST. Pour plus d'informations, consultez la section Création d'une politique de capture instantanée dans la documentation du produit NetApp ONTAP. Vous pouvez choisir une politique de capture instantanée lors de la création ou de la mise à jour d'un volume dans la console Amazon FSx AWS CLI, l'API Amazon FSx ou l'API Amazon FSx. Pour plus d'informations, consultez Création de volumes et Mettre à jour un volume.

Restauration de fichiers et de dossiers individuels

À l'aide des instantanés de votre système de fichiers Amazon FSx, vos utilisateurs peuvent rapidement restaurer les versions précédentes de fichiers ou de dossiers individuels. Cela leur permet de récupérer les fichiers supprimés ou modifiés stockés sur le système de fichiers partagé. Ils le font en libre-service directement sur leur bureau sans l'assistance d'un administrateur. Cette approche en libre-service augmente la productivité et réduit la charge de travail administrative.

Les clients Linux et macOS peuvent afficher des instantanés dans le `.snapshot` répertoire situé à la racine d'un volume. Les clients Windows peuvent afficher des instantanés dans l'`Previous Versions`onglet de l'Explorateur Windows (en cliquant avec le bouton droit sur un fichier ou un dossier).

Restaurer des fichiers à partir de snapshots

Pour restaurer un fichier à partir d'un instantané (clients Linux et macOS)

1. Si le fichier d'origine existe toujours et que vous ne voulez pas qu'il soit remplacé par le fichier dans un instantané, utilisez votre client Linux ou macOS pour renommer le fichier d'origine ou déplacez-le dans un autre répertoire.
2. Dans le `.snapshot` répertoire, recherchez le cliché contenant la version du fichier que vous souhaitez restaurer.
3. Copiez le fichier du `.snapshot` répertoire vers le répertoire dans lequel le fichier existait à l'origine.

Pour restaurer un fichier à partir d'un instantané (clients Windows)

Les utilisateurs de clients Windows peuvent restaurer des fichiers dans des versions antérieures à l'aide de l'interface familière de l'explorateur de fichiers Windows.

1. Pour restaurer un fichier, les utilisateurs choisissent le fichier à restaurer, puis choisissent Restaurer les versions précédentes dans le menu contextuel (clic droit).
2. Les utilisateurs peuvent ensuite consulter et restaurer une version précédente à partir de la liste des versions précédentes.

Les données des instantanés sont en lecture seule. Si vous souhaitez apporter des modifications aux fichiers et dossiers répertoriés dans l'onglet Versions précédentes, vous devez enregistrer une copie des fichiers et dossiers que vous souhaitez modifier dans un emplacement accessible en écriture et apporter des modifications aux copies.

Suppression d’instantanés

Les instantanés consomment de la capacité de stockage uniquement pour les données d'un volume qui a changé depuis le dernier instantané. C'est pourquoi, si votre charge de travail écrit des données rapidement, les instantanés provenant d'anciennes données peuvent occuper une part importante de la capacité de stockage d'un volume.

Par exemple, la sortie de la commande `volume show-space`ONTAPCLI indique 140 Ko de`User Data`. Cependant, le volume disposait de 9,8 Go `User Data` avant la suppression des données utilisateur. Même si vous avez supprimé les fichiers de votre volume, un instantané peut toujours faire

référence à d'anciennes données utilisateur. De ce fait, `Snapshot Reserve` et `Snapshot Spill` dans l'exemple précédent, cela occupe un total de 9,8 Go d'espace, même s'il n'y a pratiquement aucune donnée utilisateur sur le volume.

Pour libérer de l'espace sur les volumes, vous pouvez supprimer les anciens instantanés dont vous n'avez plus besoin. Vous pouvez le faire en créant une politique de suppression automatique des instantanés ou en supprimant manuellement les instantanés. La suppression d'un instantané entraîne la suppression des données modifiées enregistrées sur le cliché.

Création d'une politique de suppression automatique des instantanés

Vous pouvez créer une politique pour supprimer automatiquement les instantanés lorsque l'espace disponible sur votre volume est insuffisant. Utilisez la commande volume snapshot autodelete modify ONTAP CLI pour établir une politique de suppression automatique pour un volume.

Lorsque vous utilisez cette commande, utilisez vos données pour remplacer les valeurs d'espace réservé suivantes :

- Remplacez *svm_name* par le nom de la SVM sur laquelle le volume a été créé.
- Remplacez *vol_name* par le nom du volume.

Pour `-trigger`, attribuez l'une des valeurs suivantes :

- `volume` — À utiliser `volume` si vous souhaitez que le seuil à partir duquel les instantanés sont supprimés corresponde à un seuil de capacité totale du volume utilisé. Les seuils de capacité du volume utilisé qui déclenchent la suppression des instantanés sont déterminés par la taille de votre volume, le seuil variant de 85 à 98 % de la capacité utilisée. Les petits volumes ont un seuil plus petit, tandis que les volumes plus grands ont un seuil plus grand.
- `snap_reserve` — À utiliser `snap_reserve` si vous souhaitez que les instantanés soient supprimés en fonction de ce qui peut être conservé dans votre réserve d'instantanés.

```
::> volume snapshot autodelete modify -vserver svm_name -volume vol_name -enabled true
 -trigger [volume|snap_reserve]
```

Pour plus d'informations, consultez la commande de modification automatique du volume snapshot dans le centre de documentation NetApp ONTAP.

Supprimer des instantanés

Utilisez la commande volume snapshot deleteONTAPCLI pour supprimer manuellement les instantanés, en remplaçant les valeurs d'espace réservé suivantes par vos données :

- Remplacez *svm_name*par le nom de la SVM sur laquelle le volume a été créé.
- Remplacez *vol_name*par le nom du volume.
- Remplacez *snapshot_name*par le nom de l'instantané. Cette commande prend en charge les caractères génériques (*) pour *snapshot_name*. Par conséquent, vous pouvez supprimer tous les instantanés horaires, par exemple en utilisant`hourly*`.

> **Important**
>
> Si les sauvegardes Amazon FSx sont activées, Amazon FSx conserve un instantané de la dernière sauvegarde Amazon FSx de chaque volume. Ces instantanés sont utilisés pour maintenir l'incrémentalité entre les sauvegardes et ne doivent pas être supprimés à l'aide de cette méthode.

```
FsxIdabcdef01234567892::> volume snapshot delete -vserver svm_name -volume vol_name -
snapshot snapshot_name
```

Désactivation des instantanés automatiques

Les instantanés automatiques sont activés par la politique de capture d'écran par défaut pour les volumes de votre système de fichiers FSx for ONTAP. Si vous n'avez pas besoin d'instantanés de vos données (par exemple, si vous utilisez des données de test), vous pouvez désactiver les instantanés en définissant la politique d'instantanés du volume de manière à none utiliser l' AWS Management Console API, et la ONTAP CLI, comme décrit dans les procédures suivantes. AWS CLI

Pour désactiver les instantanés automatiques (AWS console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Accédez à Systèmes de fichiers et choisissez le système de fichiers ONTAP pour lequel vous souhaitez mettre à jour un volume.
3. Choisissez l'onglet Volumes.

4. Choisissez le volume que vous souhaitez mettre à jour.
5. Pour Actions, choisissez Mettre à jour le volume.

   La boîte de dialogue Mettre à jour le volume s'affiche avec les paramètres actuels du volume.
6. Pour la politique des instantanés, choisissez None.
7. Choisissez Mettre à jour pour mettre à jour le volume.

Pour désactiver les instantanés automatiques (AWS CLI)

- Utilisez la commande AWS update-volume CLI (ou la commande UpdateVolumeAPI équivalente) pour définir le `SnapshotPolicy` tonone, comme indiqué dans l'exemple suivant.

```
aws fsx update-volume \
    --volume-id fsvol-1234567890abcdefa \
    --name new_vol \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
           SizeInMegabytes=2048,SnapshotPolicy=none, \
           StorageEfficiencyEnabled=true, \
           TieringPolicy=all
```

Pour désactiver les instantanés automatiques (ONTAPCLI)

Définissez la politique d'instantanés du volume afin d'utiliser la politique none par défaut pour désactiver les instantanés automatiques.

1. Utilisez la commande `volume snapshot policy show`ONTAPCLI pour afficher la none politique.

```
::> snapshot policy show -policy none

Vserver: FsxIdabcdef01234567892
                         Number of Is
Policy Name              Schedules Enabled Comment
------------------------ --------- ------- ----------------------------------
none                               0 false   Policy for no automatic snapshots.
    Schedule               Count     Prefix                SnapMirror Label
    ---------------------- -----     --------------------- -------------------
    -                          -     -                     -
```

2. Utilisez la commande `volume modify`ONTAPCLi pour définir la politique de capture instantanée du volume none afin de désactiver les instantanés automatiques. Remplacez les valeurs d'espace réservé suivantes par vos données :

   - *svm_name*— utilisez le nom de votre SVM.
   - *vol_name*— utilisez le nom de votre volume.

   Lorsque vous êtes invité à continuer, entrez**y**.

```
::> volume modify -vserver svm_name -volume vol_name -snapshot-policy none

Warning: You are changing the Snapshot policy on volume "vol_name" to "none".
 Snapshot copies on this volume
        that do not match any of the prefixes of the new Snapshot policy will not
 be deleted. However, when
        the new Snapshot policy takes effect, depending on the new retention
 count, any existing Snapshot copies
        that continue to use the same prefixes might be deleted. See the 'volume
 modify' man page for more information.
Do you want to continue? {y|n}: y
Volume modify successful on volume vol_name of Vserver svm_name.
```

Réserve d'instantanés

La réserve de copies instantanées définit un pourcentage spécifique de la capacité de stockage d'un volume pour le stockage des copies instantanées, avec une valeur par défaut de 5 %. La réserve de copies de snapshots doit disposer d'un espace suffisant pour les copies de snapshots, y compris les sauvegardes de volumes. Si le nombre de copies d'instantanés dépasse l'espace réservé aux instantanés, vous devez supprimer les copies d'instantanés existantes du système de fichiers actif afin de récupérer la capacité de stockage nécessaire à l'utilisation du système de fichiers. Vous pouvez également modifier le pourcentage d'espace disque alloué aux copies Snapshot.

Chaque fois que les instantanés consomment plus de 100 % de la réserve de snapshots, ils commencent à occuper l'espace de stockage SSD principal. Ce processus s'appelle Snapshot Spill. Lorsque les instantanés continuent d'occuper l'espace du système de fichiers actif, le système de fichiers risque d'être saturé. Si le système de fichiers est saturé à cause de la fuite de snapshots, vous ne pouvez créer des fichiers qu'après avoir supprimé suffisamment de snapshots.

Lorsque suffisamment d'espace disque est disponible pour les snapshots dans la réserve de snapshots, la suppression de fichiers du niveau SSD principal libère de l'espace disque pour les nouveaux fichiers, tandis que les copies de snapshots qui font référence à ces fichiers ne consomment que l'espace de la réserve de copies de snapshots.

Comme il n'existe aucun moyen d'empêcher les snapshots de consommer plus d'espace disque que la quantité qui leur est réservée (réserve de snapshots), il est important de réserver suffisamment d'espace disque pour les snapshots afin que le niveau SSD principal dispose toujours de l'espace disponible pour créer de nouveaux fichiers ou modifier des fichiers existants.

Si un instantané est créé alors que les disques sont pleins, la suppression de fichiers du niveau SSD principal ne crée aucun espace libre, car toutes ces données sont également référencées par le cliché nouvellement créé. Vous devez supprimer le snapshot afin de libérer de l'espace afin de créer ou de mettre à jour des fichiers.

Vous pouvez modifier la quantité de réserve de snapshots sur un volume à l'aide de la NetApp ONTAP CLI. Pour plus d'informations, consultez Mise à jour de la réserve de snapshots du volume.

Mise à jour de la réserve de snapshots du volume

Vous pouvez modifier le montant de la réserve de snapshots sur un volume à l'aide de la NetApp ONTAP CLI ou de l'API, comme décrit dans la procédure suivante.

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *`management_endpoint_ip`* par l'adresse IP du port de gestion du système de fichiers.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Pour plus d'informations, consultez Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.

2. Utilisez la commande `snap reserve` ONTAP CLI pour modifier le pourcentage d'espace disque utilisé pour la réserve de copies Snapshot. Remplacez *`vol_name`* par le nom du volume, et *`percent`* `with the percent of disk space you want to reserve for Snapshot copies.`

   ```
   ::> snap reserve vol_name percent
   ```

L'exemple suivant modifie la réserve de snapshots pour le volume 1 à 25 % de la capacité de stockage du volume.

```
::> snap reserve vol1 25
```

Réplication planifiée à l'aide NetApp SnapMirror

Vous pouvez l'utiliser NetApp SnapMirror pour planifier la réplication périodique de votre système de fichiers FSx for ONTAP vers ou depuis un second système de fichiers. Cette fonctionnalité est disponible pour les déploiements régionaux et interrégionaux.

NetApp SnapMirror réplique les données à des vitesses élevées, afin de garantir une haute disponibilité des données et une réplication rapide des données sur les systèmes ONTAP, que vous effectuiez une réplication entre deux systèmes de fichiers Amazon FSx dans AWS ou depuis un système sur site vers. AWS La réplication peut être planifiée toutes les 5 minutes, mais les intervalles doivent être soigneusement choisis en fonction des RPO (objectifs de point de restauration), des RTO (objectifs de temps de restauration) et de considérations relatives aux performances.

Lorsque vous répliquez des données vers des systèmes NetApp de stockage et que vous mettez continuellement à jour les données secondaires, vos données sont mises à jour et restent disponibles chaque fois que vous en avez besoin. Aucun serveur de réplication externe n'est requis. Pour plus d'informations sur l'utilisation NetApp SnapMirror pour répliquer vos données, consultez la section En savoir plus sur le service de réplication dans la documentation NetApp BlueXP.

Vous pouvez créer un volume de destination de protection des données (DP) pour NetApp SnapMirror utiliser la console Amazon FSx, le, et l'API Amazon FSx AWS CLI, en plus de la NetApp CLI ONTAP et de l'API REST. Pour plus d'informations sur la création d'un volume de destination à l'aide de la console Amazon FSx AWS CLI, consultez. Création de volumes

Vous pouvez utiliser NetApp BlueXP ou la CLI NetApp ONTAP pour planifier la réplication de votre système de fichiers.

> **Note**
>
> Il existe deux types de SnapMirror réplication : au niveau du volume SnapMirror et SVM Disaster Recovery (SVMDR). Seule la SnapMirror réplication au niveau du volume est prise en charge par FSx for ONTAP.

Utiliser NetApp BlueXP pour planifier la réplication

Vous pouvez utiliser NetApp BlueXP pour configurer la réplication SnapMirror sur votre système de fichiers FSx for ONTAP. Pour plus d'informations, consultez la section Réplication de données entre systèmes dans la documentation NetApp BlueXP.

Utilisation de la CLI NetApp ONTAP pour planifier la réplication

Vous pouvez utiliser la CLI NetApp ONTAP pour configurer la réplication planifiée des volumes. Pour plus d'informations, consultez la section Gestion de la réplication de SnapMirror volumes dans le centre de documentation NetApp ONTAP.

Protégez vos données avec SnapLock

SnapLockest une fonctionnalité qui vous permet de protéger vos fichiers en les faisant passer à l'état WORM (Write Once, Read Many), qui empêche toute modification ou suppression pendant une période de conservation spécifiée. Vous pouvez l'utiliser SnapLock pour respecter les réglementations, pour protéger les données critiques contre les attaques de ransomware et pour fournir un niveau de protection supplémentaire à vos données contre toute modification ou suppression.

Amazon FSx for NetApp ONTAP prend en charge les modes de rétention Compliance et Enterprise avec. SnapLock Pour plus d'informations, consultez Conformité d'SnapLock et SnapLockEntreprise.

Vous pouvez créer des SnapLock volumes sur FSx pour les systèmes de fichiers ONTAP créés le 13 juillet 2023 ou après cette date. Les systèmes de fichiers existants seront pris SnapLock en charge lors d'une prochaine période de maintenance hebdomadaire.

Rubriques

Fonctionnement d'SnapLock

SnapLockpeut vous aider à respecter les objectifs réglementaires et de gouvernance en empêchant la suppression, la modification ou le changement de nom de vos fichiers. Lorsque vous créez un SnapLock volume, vous validez vos fichiers pour qu'ils soient stockés en écriture unique, en lecture multiple (WORM) et vous définissez des périodes de conservation pour les données. Vos fichiers peuvent être stockés dans un état non effaçable et non inscriptible pendant une période déterminée ou indéfiniment.

> **Important**
>
> Vous devez indiquer si un volume utilisera SnapLock les paramètres au moment de sa création. Un SnapLock non-volume ne peut pas être converti en SnapLock volume après sa création.

Modes de conservation

SnapLockpropose deux modes de rétention : Compliance et Enterprise. Amazon FSx for NetApp ONTAP prend en charge les deux. Ils ont différents cas d'utilisation et certaines fonctionnalités diffèrent, mais ils protègent tous deux vos données contre toute modification ou suppression à l'aide du modèle WORM. Le tableau suivant explique certaines des similitudes et des différences entre ces modes de rétention.

Fonctionnalité SnapLock	Conformité d'SnapLock	SnapLockEntreprise
Description	Les fichiers transférés vers WORM sur un volume de conformité ne peuvent pas être supprimés avant l'expiration de leur période de conservation.	Les fichiers transférés vers WORM sur un volume Enterprise peuvent être supprimés par les utilisateurs autorisés avant l'expiration de leur période de conservat ion à l'aide de la suppression privilégiée.
Cas d'utilisation	• Pour répondre à des mandats spécifiques au gouvernement ou à l'industr	• Pour améliorer l'intégrité des données et la conformité interne d'une entreprise.

Fonctionnalité SnapLock	Conformité d'SnapLock	SnapLockEntreprise
	ie tels que la règle 17a-4 (f) de la SEC, la règle 4511 de la FINRA et le règlement 1.31 de la CFTC. • Pour vous protéger contre les attaques de rançongic iels.	• Pour tester les paramètres de rétention avant d'utiliser SnapLock Compliance.
Commission automatique	Oui	Oui
Rétention basée sur les événements (EBR)*	Oui	Oui
Maintien légal*	Oui	Non
Suppression privilégiée	Non	Oui
Mode d'ajout de volumes	Oui	Oui
SnapLockvolumes des journaux d'audit	Oui	Oui

* Les opérations EBR et Legal Hold sont prises en charge dans la ONTAP CLI et l'API REST.

administrateur SnapLock

Vous devez disposer de privilèges d'SnapLockadministrateur pour effectuer certaines actions sur les SnapLock volumes. SnapLockles privilèges d'administrateur sont définis dans le `vsadmin-snaplock` rôle de la ONTAP CLI. Vous devez être administrateur de cluster pour créer un compte d'administrateur de machine virtuelle de stockage (SVM) doté du rôle d'SnapLockadministrateur.

Vous pouvez effectuer les actions suivantes avec le `vsadmin-snaplock` rôle dans la ONTAP CLI :

- Gérez votre propre compte utilisateur, votre mot de passe local et vos informations clés
- Gérez les volumes, à l'exception des volumes mobiles
- Gérez les quotas, les qtrees, les copies instantanées et les fichiers
- Réaliser SnapLock des actions, notamment la suppression privilégiée et la conservation légale

- Configuration des protocoles NFS (Network File System) et SMB (Server Message Block)
- Configuration des services DNS (Domain Name System), LDAP (Lightweight Directory Access Protocol) et NIS (Network Information Service)
- Surveillance des tâches

La procédure suivante explique comment créer un SnapLock administrateur dans la ONTAP CLI. Vous devez être connecté en tant qu'administrateur de cluster sur une connexion sécurisée, telle que le protocole Secure Shell (SSH) pour effectuer cette tâche.

Pour créer un compte administrateur de SVM avec le rôle vsadmin-snaplock dans la CLI ONTAP

- Exécutez la commande suivante. Remplacez *SVM_name* et *SnapLockAdmin*par vos propres informations.

```
cluster1::> security login create -vserver SVM_name -user-or-group-
name SnapLockAdmin -application ssh -authentication-method password -role vsadmin-
snaplock
```

SnapLockvolumes des journaux d'audit

Un volume de journaux SnapLock d'audit contient des journaux SnapLock d'audit, qui contiennent les horodatages d'événements tels que le moment où un SnapLock administrateur a été créé, le moment où des opérations de suppression privilégiées ont été exécutées ou le moment où un blocage légal a été placé sur des fichiers. Le volume du journal SnapLock d'audit est un enregistrement non effaçable des événements.

Vous devez créer un volume de journal SnapLock d'audit dans la même SVM que le SnapLock volume pour effectuer les actions suivantes :

- Pour activer ou désactiver la suppression privilégiée sur un volume SnapLock Enterprise.
- Appliquer la suspension légale à un fichier d'un volume de SnapLock conformité.

> ⚠ Warning
>
> - La période de conservation minimale d'un volume de journal SnapLock d'audit est de six mois. Jusqu'à l'expiration de cette période de conservation, le volume du journal SnapLock

d'audit ainsi que la SVM et le système de fichiers qui y sont associés ne peuvent pas être supprimés, même si le volume a été créé en mode SnapLock Enterprise.

- Si un fichier est supprimé à l'aide de la suppression privilégiée et que sa durée de conservation est supérieure à celle du volume, le volume du journal d'audit hérite de la période de conservation du fichier. Par exemple, si un fichier dont la durée de conservation est de 10 mois est supprimé à l'aide de la suppression privilégiée et que la période de conservation du volume du journal d'audit est de six mois, la période de conservation du volume du journal d'audit est prolongée à 10 mois.

Vous ne pouvez avoir qu'un seul volume de journal d'SnapLockaudit actif dans une SVM, mais il peut être partagé par plusieurs SnapLock volumes de la SVM. Pour monter un volume de journal SnapLock d'audit avec succès, définissez le chemin de jonction sur`/snaplock_audit_log`. Aucun autre volume ne peut utiliser ce chemin de jonction, y compris les volumes qui ne sont pas des volumes de journaux d'audit.

Les journaux SnapLock d'audit se trouvent dans le `/snaplock_log` répertoire situé à la racine du volume des journaux d'audit. Les opérations de suppression privilégiées sont enregistrées dans le `privdel_log` sous-répertoire. Les opérations de début et de fin de Legal Hold sont enregistrées/`snaplock_log/legal_hold_logs/`. Tous les autres journaux sont stockés dans le `system_log` sous-répertoire.

Vous pouvez créer un volume de journal SnapLock d'audit à l'aide de la console Amazon FSx, de l'API Amazon FSxAWS CLI, de la ONTAP CLI et de l'API REST.

> **Note**
>
> Un volume de protection des données (DP) ne peut pas être utilisé comme volume de journal d'SnapLockaudit.

La procédure suivante explique comment créer un volume de journal SnapLock d'audit sur la console Amazon FSx.

Pour créer un volume de journal SnapLock d'audit, la console Amazon FSx

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Suivez la procédure de création d'un nouveau volume dansCréation de volumes.

3. Dans la section Avancé, pour SnapLock Configuration, choisissez Activé.

   Cochez la case pour accuser réception de l'avertissement concernant l'activation SnapLock sur le volume.
4. Pour le volume du journal d'audit, sélectionnez Activé.

   Assurez-vous que le chemin de jonction est défini sur`/snaplock_audit_log`.
5. Suivez le reste de la procédure de création d'un nouveau volume dansCréation de volumes.
6. Choisissez Confirmer pour créer le volume.

Pour activer le volume du journal SnapLock d'audit avec l'API Amazon FSx, utilisez `AuditLogVolume` le. `CreateSnaplockConfiguration`

Accès à vos données dans un SnapLock volume

Vous pouvez utiliser des protocoles de fichiers ouverts tels que NFS et SMB pour accéder à vos données dans un SnapLock volume. L'écriture de données sur un SnapLock volume ou la lecture de données protégées par WORM n'ont aucun impact sur les performances.

Vous pouvez copier des fichiers entre SnapLock volumes avec NFS et SMB, mais ils ne conserveront pas leurs propriétés WORM sur le volume de destinationSnapLock. Vous devez réattribuer les fichiers copiés à WORM pour éviter qu'ils ne soient modifiés ou supprimés. Pour plus d'informations, consultez Validation de fichiers à l'état WORM.

Vous pouvez également répliquer SnapLock des données avecSnapMirror, mais les volumes source et de destination doivent être des SnapLock volumes dotés du même mode de conservation (par exemple, les deux doivent être Compliance ou Enterprise).

Conformité d'SnapLock

Amazon FSx for NetApp ONTAP prend en charge SnapLock les volumes de conformité.

Utilisation de SnapLock la conformité

Cette section décrit les cas d'utilisation et les considérations relatives au mode de conservation de la conformité.

Cas d'utilisation relatifs à SnapLock la conformité

Vous pouvez choisir le mode de conservation de la conformité pour les cas d'utilisation suivants.

- Vous pouvez utiliser SnapLock Compliance pour répondre à des mandats gouvernementaux ou sectoriels tels que la règle 17a-4 (f) de la SEC, la règle 4511 de la FINRA et le règlement 1.31 de la CFTC. SnapLock La conformité sur Amazon FSx for NetApp ONTAP a été évaluée par rapport à ces mandats et réglementations par. Cohasset Associates Pour plus d'informations, consultez le rapport d'évaluation de la conformité pour Amazon FSx for NetApp ONTAP.
- Vous pouvez utiliser SnapLock la conformité pour compléter ou améliorer une stratégie complète de protection des données afin de lutter contre les attaques de ransomware.

Considérations relatives à SnapLock la conformité

Voici quelques points importants à prendre en compte concernant le mode de conservation de la conformité.

- Une fois qu'un fichier est passé à l'état WORM (Write Once, Read Many) sur un volume SnapLock Compliance, il ne peut être supprimé avant l'expiration de sa période de conservation par aucun utilisateur.
- Un volume de SnapLock conformité ne peut être supprimé que lorsque les périodes de conservation de tous les fichiers WORM du volume ont expiré et que les fichiers WORM ont été supprimés du volume.
- Vous ne pouvez pas renommer un volume SnapLock Compliance après sa création.
- Vous pouvez l'utiliser SnapMirror pour répliquer des fichiers WORM, mais le volume source et le volume de destination doivent avoir le même mode de rétention (par exemple, les deux doivent être conformes).
- Un volume de SnapLock conformité ne peut pas être converti en volume d'SnapLockentreprise, et inversement.

Création d'un volume SnapLock de conformité

Vous pouvez créer un volume de SnapLock conformité à l'aide de la console Amazon FSx, de l'API Amazon FSxAWS CLI, de la ONTAP CLI et de l'API REST.

Pour créer un volume de SnapLock conformité avec l'API Amazon FSx, utilisez `SnaplockType` le. `CreateSnaplockConfiguration`

La procédure suivante explique comment créer un volume SnapLock Compliance sur la console Amazon FSx.

Pour créer un volume SnapLock Compliance sur la console Amazon FSx

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Suivez la procédure de création d'un nouveau volume dansCréation de volumes.
3. Dans la section Avancé, pour SnapLock Configuration, choisissez Activé.

   Cochez la case pour accuser réception de l'avertissement concernant l'activation SnapLock sur le volume.
4. Pour le mode de rétention, choisissez Conformité.
5. Pour le volume du journal d'audit, choisissez entre Activé et Désactivé.

   Si vous choisissez Activé, assurez-vous que le chemin de jonction est défini sur`/snaplock_audit_log`.

   Pour plus d'informations, consultez SnapLockvolumes des journaux d'audit.
6. Pour Période de rétention, entrez les valeurs de rétention par défaut, de rétention minimale et de rétention maximale. Choisissez ensuite une unité correspondante pour chacune d'elles.

   Pour plus d'informations, consultez Travailler avec la période de conservation dans SnapLock.
7. Pour Autocommit, choisissez entre Activé et Désactivé.

   Si vous choisissez Activé, pour la période de validation automatique, entrez une valeur et choisissez une unité de validation automatique correspondante.

   Vous pouvez spécifier une valeur comprise entre 5 minutes et 10 ans.

   Pour plus d'informations, consultez Commission automatique.
8. Pour le mode d'ajout de volume, choisissez entre Activé et Désactivé.

   Pour plus d'informations, consultez Mode d'ajout de volumes.
9. Suivez le reste de la procédure de création d'un nouveau volume dansCréation de volumes.
10. Choisissez Confirmer pour créer le volume.

SnapLockEntreprise

Amazon FSx pour NetApp ONTAP prend en charge SnapLock les volumes d'entreprise.

Utilisation de l'SnapLockentreprise

Cette section décrit les cas d'utilisation et les considérations relatives au mode de rétention d'entreprise.

Cas d'utilisation pour SnapLock Enterprise

Vous pouvez choisir le mode de rétention Enterprise pour les cas d'utilisation suivants.

- Vous pouvez utiliser SnapLock Enterprise pour autoriser uniquement des utilisateurs spécifiques à supprimer des fichiers.
- Vous pouvez utiliser SnapLock Enterprise pour améliorer l'intégrité des données et la conformité interne de votre entreprise.
- Vous pouvez utiliser SnapLock Enterprise pour tester les paramètres de rétention avant d'utiliser SnapLock Compliance.

Considérations relatives à l'utilisation SnapLock d'Enterprise

Voici quelques points importants à prendre en compte concernant le mode de rétention d'entreprise.

- Vous pouvez l'utiliser SnapMirror pour répliquer des fichiers WORM, mais le volume source et le volume de destination doivent avoir le même mode de rétention (par exemple, les deux doivent être Enterprise).
- Un SnapLock volume ne peut pas être converti de la version Enterprise à la version Compliance, ni de la version Compliance à la version Enterprise.
- SnapLockEnterprise ne prend pas en charge Legal Hold.

Suppression privilégiée

L'une des principales différences entre SnapLock Enterprise et SnapLock Compliance est qu'un SnapLock administrateur peut activer la suppression privilégiée sur un volume SnapLock Enterprise pour autoriser la suppression d'un fichier avant l'expiration de sa période de conservation. L'SnapLockadministrateur est le seul utilisateur autorisé à supprimer des fichiers d'un volume SnapLock Enterprise auquel sont appliquées des politiques de rétention actives. Pour plus d'informations, consultez administrateur SnapLock.

Vous pouvez activer ou désactiver la suppression privilégiée à l'aide de la console Amazon FSx, de l'API Amazon FSxAWS CLI, de la ONTAP CLI et de l'API REST. Pour activer la suppression

privilégiée, vous devez d'abord créer un volume de journal SnapLock d'audit dans la même SVM que le SnapLock volume. Pour plus d'informations, consultez SnapLockvolumes des journaux d'audit.

Pour activer la suppression privilégiée avec l'API Amazon FSx, utilisez `PrivilegedDelete` le. `CreateSnaplockConfiguration`

La procédure suivante explique comment activer la suppression privilégiée sur la console Amazon FSx.

Pour activer la suppression privilégiée sur un volume SnapLock Enterprise sur la console Amazon FSx

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Suivez la procédure de création d'un nouveau volume dansCréation de volumes.
3. Dans la section Avancé, pour SnapLock Configuration, choisissez Activé.

   Cochez la case pour accuser réception de l'avertissement concernant l'activation SnapLock sur le volume.
4. Pour le mode de rétention, choisissez Enterprise.
5. Pour Privileged Delete, choisissez Enabled.
6. Suivez le reste de la procédure de création d'un nouveau volume dansCréation de volumes.
7. Choisissez Confirmer pour créer le volume.

> **Note**
>
> Vous ne pouvez pas émettre de commande de suppression privilégiée pour supprimer un fichier WORM (Write Once, Read Many) dont la période de conservation a expiré. Vous pouvez effectuer une opération de suppression normale après l'expiration de la période de rétention.

Vous pouvez choisir de désactiver définitivement la suppression privilégiée, mais cette action est irréversible. Si la suppression privilégiée est définitivement désactivée, il n'est pas nécessaire qu'un volume de journal SnapLock d'audit soit associé au volume SnapLock Enterprise.

Pour désactiver définitivement la suppression privilégiée avec l'API Amazon FSx, utilisez `PrivilegedDelete` le. `CreateSnaplockConfiguration`

Pour désactiver définitivement la suppression privilégiée sur un volume SnapLock Enterprise sur la console Amazon FSx

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Suivez la procédure de création d'un nouveau volume dansCréation de volumes.
3. Dans la section Avancé, pour SnapLock Configuration, choisissez Activé.

   Cochez la case pour accuser réception de l'avertissement concernant l'activation SnapLock sur le volume.
4. Pour le mode de rétention, choisissez Enterprise.
5. Pour Privileged Delete, choisissez Désactivé définitivement.
6. Suivez le reste de la procédure de création d'un nouveau volume dansCréation de volumes.
7. Choisissez Confirmer pour créer le volume.

Création d'un volume SnapLock Enterprise

Vous pouvez créer un volume SnapLock Enterprise à l'aide de la console Amazon FSx, de l'API Amazon FSxAWS CLI, de la ONTAP CLI et de l'API REST.

Pour créer un volume SnapLock d'entreprise avec l'API Amazon FSx, utilisez `SnaplockType` le. `CreateSnaplockConfiguration`

Pour créer un volume SnapLock Enterprise sur la console Amazon FSx

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Suivez la procédure de création d'un nouveau volume dansCréation de volumes.
3. Dans la section Avancé, pour SnapLock Configuration, choisissez Activé.

   Cochez la case pour accuser réception de l'avertissement concernant l'activation SnapLock sur le volume.
4. Pour le mode de rétention, choisissez Enterprise.
5. Pour le volume du journal d'audit, choisissez entre Activé et Désactivé.

   Si vous choisissez Activé, assurez-vous que le chemin de jonction est défini sur`/snaplock_audit_log`.

Pour plus d'informations, consultez SnapLockvolumes des journaux d'audit.

6. Pour Période de rétention, entrez les valeurs de rétention par défaut, de rétention minimale et de rétention maximale. Choisissez ensuite une unité correspondante pour chacune d'elles.

   Pour plus d'informations, consultez Travailler avec la période de conservation dans SnapLock.

7. Pour Autocommit, choisissez entre Activé et Désactivé.

   Si vous choisissez Activé, pour la période de validation automatique, entrez une valeur et choisissez une unité de validation automatique correspondante.

   Vous pouvez spécifier une valeur comprise entre 5 minutes et 10 ans.

   Pour plus d'informations, consultez Commission automatique.

8. Pour Privileged Delete, choisissez entre Activé, Désactivé et Désactivé définitivement.

   Pour plus d'informations, consultez Suppression privilégiée.

9. Pour le mode d'ajout de volume, choisissez entre Activé et Désactivé.

   Pour plus d'informations, consultez Mode d'ajout de volumes.

10. Suivez le reste de la procédure de création d'un nouveau volume dansCréation de volumes.
11. Choisissez Confirmer pour créer le volume.

Contourner le mode Enterprise

Si vous utilisez la console Amazon FSx ou l'API Amazon FSx, vous devez disposer de l'`fsx:BypassSnapLockEnterpriseRetention`autorisation IAM pour supprimer un volume SnapLock Enterprise contenant des fichiers WORM soumis à des politiques de rétention actives.

Pour plus d'informations, consultez Supprimer des SnapLock volumes.

Travailler avec la période de conservation dans SnapLock

Lorsque vous créez un SnapLock volume, vous pouvez définir une période de rétention par défaut pour le volume, ou vous pouvez définir explicitement la période de rétention pour les fichiers WORM (Write Once Read Many). Pendant la période de conservation, vous ne pouvez ni supprimer ni modifier les fichiers protégés par Worm. La période de conservation est utilisée pour calculer la durée de conservation. Par exemple, si vous transférez un fichier vers WORM le 14 juillet 2023 à minuit et

que vous fixez la période de conservation à cinq ans, la durée de conservation s'étendra jusqu'au 14 juillet 2028 à minuit.

Pour plus d'informations sur WORM, consultezValidation de fichiers à l'état WORM.

Politiques relatives aux périodes de conservation

La durée de conservation est déterminée par les valeurs que vous attribuez aux paramètres suivants :

- Rétention par défaut : période de conservation par défaut attribuée à un fichier WORM si vous ne fournissez pas de période de conservation explicite pour celui-ci.
- Rétention minimale : période de conservation la plus courte qui peut être attribuée à un fichier WORM.
- Rétention maximale : période de rétention la plus longue qui peut être attribuée à un fichier WORM.

> **Note**
>
> Même après l'expiration de la période de conservation, vous ne pouvez pas modifier un fichier WORM. Vous pouvez uniquement le supprimer ou définir une nouvelle période de conservation pour réactiver la protection WORM.

Vous pouvez définir la période de conservation en utilisant plusieurs unités de temps différentes. Le tableau suivant répertorie les plages spécifiques prises en charge.

Type	Valeur	Remarques
Secondes	0 - 65 535	
Minutes	0 - 65 535	
Heures	0 À 24	
Jours	0 à 365	
cal.	0 -12	
Années	0 À 100	

Type	Valeur	Remarques
Infini	-	Conserve les fichiers pour toujours. Disponible pour la rétention par défaut, la rétention maximale et la rétention minimale.
Non spécifié*	-	Conserve les fichiers jusqu'à ce que vous définissiez une période de conservation. Disponible uniquement pour la rétention par défaut.

* Lorsque vous transférez des fichiers vers WORM avec une période de conservation non spécifiée, la période de conservation minimale configurée pour le SnapLock volume leur est attribuée. Lorsque vous passez les fichiers protégés par Worm à une durée de conservation absolue, la nouvelle période de conservation doit être supérieure à la période minimale que vous avez définie pour les fichiers précédemment.

Période de conservation expirée

Une fois la période de conservation d'un fichier WORM expirée, vous pouvez supprimer le fichier ou définir une nouvelle période de conservation pour réactiver la protection WORM. Les fichiers WORM ne sont pas automatiquement supprimés après l'expiration de leur période de conservation. Vous ne pouvez toujours pas modifier le contenu d'un fichier WORM, même après l'expiration de sa période de conservation.

Définition de la durée de conservation d'un SnapLock volume

Vous pouvez définir la période de rétention d'un SnapLock volume à l'aide de la console Amazon FSx, de l'API Amazon FSxAWS CLI, de la ONTAP CLI et de l'API REST.

Pour définir la période de rétention avec l'API Amazon FSx, utilisez la `SnaplockRetentionPeriod`configuration.

La procédure suivante explique comment définir la période de rétention sur la console Amazon FSx.

Pour définir la période de rétention d'un SnapLock volume sur la console Amazon FSx

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Suivez la procédure de création d'un nouveau volume dansCréation de volumes.
3. Dans la section Avancé, pour SnapLock Configuration, choisissez Activé.

   Cochez la case pour accuser réception de l'avertissement concernant l'activation SnapLock sur le volume.
4. Pour Période de rétention, entrez les valeurs de rétention par défaut, de rétention minimale et de rétention maximale. Choisissez ensuite une unité correspondante pour chacune d'elles.
5. Suivez le reste de la procédure de création d'un nouveau volume dansCréation de volumes.
6. Choisissez Confirmer pour créer le volume.

Validation de fichiers à l'état WORM

Cette section explique comment faire passer vos fichiers à l'état WORM (Write Once, Read Many). Il aborde également le mode d'ajout de volumes, qui permet d'écrire des données de manière incrémentielle dans des fichiers protégés par WORM.

Commission automatique

Vous pouvez utiliser la validation automatique pour transférer des fichiers vers WORM s'ils n'ont pas été modifiés pendant la période que vous spécifiez. Vous pouvez activer la validation automatique à l'aide de la console Amazon FSx, de AWS CLI l'API Amazon FSx, de la ONTAP CLI et de l'API REST.

Vous pouvez spécifier une période de validation automatique comprise entre cinq minutes et 10 ans. Le tableau suivant répertorie les plages spécifiques prises en charge.

Unit	Valeur
Minutes	5 - 65 535
Heures	1 - 65 535

Unit	Valeur
Jours	1 - 3 650
cal.	1 à 120
Années	1 à 10

Pour activer la validation automatique avec l'API Amazon FSx, `AutocommitPeriod` utilisez dans le. `CreateSnaplockConfiguration`

La procédure suivante explique comment activer la validation automatique sur la console Amazon FSx.

Pour activer la validation automatique sur la console Amazon FSx

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Suivez la procédure de création d'un nouveau volume dansCréation de volumes.
3. Dans la section Avancé, pour SnapLock Configuration, choisissez Activé.

   Cochez la case pour accuser réception de l'avertissement concernant l'activation SnapLock sur le volume.
4. Pour Autocommit, choisissez Enabled.
5. Pour la période de validation automatique, entrez une valeur et choisissez une unité de validation automatique correspondante.

   Vous pouvez spécifier une valeur comprise entre 5 minutes et 10 ans.
6. Suivez le reste de la procédure de création d'un nouveau volume dansCréation de volumes.
7. Choisissez Confirmer pour créer le volume.

Mode d'ajout de volumes

Vous ne pouvez pas modifier les données existantes dans un fichier protégé par Worm. SnapLockCela vous permet toutefois de protéger les données existantes à l'aide de fichiers pouvant être ajoutés par WORM. Par exemple, vous pouvez générer des fichiers journaux ou conserver les données de streaming audio ou vidéo tout en y écrivant des données de manière incrémentielle.

Vous pouvez activer ou désactiver le mode d'ajout de volumes à l'aide de la console Amazon FSx, de l'API AWS CLI Amazon FSx, de la CLI et de l'API REST. ONTAP

Exigences relatives à la mise à jour du mode d'ajout de volumes

- Le SnapLock volume doit être démonté.
- Le SnapLock volume doit être vide de copies instantanées et de données utilisateur.

Pour activer le mode d'ajout de volume avec l'API Amazon FSx, utilisez dans le. `VolumeAppendModeEnabled` `CreateSnaplockConfiguration`

La procédure suivante explique comment activer le mode d'ajout de volume sur la console Amazon FSx.

Pour activer le mode d'ajout de volumes sur la console Amazon FSx

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Suivez la procédure de création d'un nouveau volume dansCréation de volumes.
3. Dans la section Avancé, pour SnapLock Configuration, choisissez Activé.

   Cochez la case pour accuser réception de l'avertissement concernant l'activation SnapLock sur le volume.
4. Pour le mode d'ajout de volume, choisissez Activé.
5. Suivez le reste de la procédure de création d'un nouveau volume dansCréation de volumes.
6. Choisissez Confirmer pour créer le volume.

Rétention basée sur les événements (EBR)

Vous pouvez utiliser la rétention basée sur les événements (EBR) pour créer des politiques personnalisées avec des périodes de conservation associées. Par exemple, vous pouvez transférer tous les fichiers d'un chemin spécifié vers WORM et définir la période de conservation d'un an à l'aide des `snaplock event-retention apply` commandes `snaplock event-retention policy create` et. Lorsque vous utilisez EBR, vous devez spécifier un volume, un répertoire ou un fichier. La période de conservation que vous sélectionnez lorsque vous créez la politique EBR est appliquée à tous les fichiers situés dans le chemin spécifié.

L'EBR est pris en charge par la ONTAP CLI et l'API REST.

> **Note**
>
> ONTAPne prend pas en charge l'EBR avec des FlexGroup volumes.

Les procédures suivantes expliquent comment créer, appliquer, modifier et supprimer une politique EBR. Vous devez être SnapLock administrateur (avoir le `vsadmin-snaplock` rôle) pour effectuer ces tâches dans la ONTAP CLI. Pour plus d'informations, consultez administrateur SnapLock.

Pour créer une politique EBR dans la CLI ONTAP

Exécutez la commande suivante. Remplacez *p1* et *« 10 ans »* par vos propres informations.

```
vs1::> snaplock event-retention policy create -name p1 -retention-period "10 years"
```

Pour appliquer une politique EBR dans la CLI ONTAP

Exécutez la commande suivante. Remplacez *p1* et *slc* par vos propres informations. Vous pouvez ajouter un chemin après la barre oblique (/) si vous souhaitez spécifier un chemin particulier pour la politique EBR. Dans le cas contraire, cette commande applique la politique EBR à tous les fichiers du volume.

```
vs1::> snaplock event-retention apply -policy-name p1 -volume slc -path /
```

Pour modifier une politique EBR dans la CLI ONTAP

Exécutez la commande suivante. Remplacez *p1* et *« 5 ans »* par vos propres informations.

```
vs1::> snaplock event-retention policy modify -name p1 -retention-period "5 years"
```

Pour supprimer une politique EBR dans la CLI ONTAP

Exécutez la commande suivante. Remplacez *p1* par vos propres informations.

```
vs1::> snaplock event-retention policy delete -name p1
```

Commandes associées dans le centre de NetApp documentation :

- Annulation de la rétention des événements par snaplock

- serveurs d'affichage Snaplock Event Retention
- émission de rétention d'événements SnapLock
- afficher la politique de rétention des événements de snaplock

Maintien légal

Vous pouvez conserver les fichiers WORM pour une durée indéterminée grâce à Legal Hold. Legal Hold est généralement utilisé à des fins de litige. Un fichier WORM soumis à une suspension légale ne peut pas être supprimé tant que la suspension légale n'est pas levée.

Legal Hold est pris en charge par la ONTAP CLI et l'API REST.

> **Note**
>
> ONTAPne prend pas en charge la conservation légale des FlexGroup volumes.

Les procédures suivantes expliquent comment démarrer et mettre fin à une suspension légale. Vous devez être SnapLock administrateur (avoir le `vsadmin-snaplock` rôle) pour effectuer ces tâches dans la ONTAP CLI. Pour plus d'informations, consultez administrateur SnapLock.

Pour démarrer une conservation légale sur un fichier d'un volume de SnapLock conformité à l'aide de la ONTAP CLI

Exécutez la commande suivante. *Remplacez litigation1, slc_vol1 et file1 par vos propres informations.*

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

Pour démarrer un blocage légal sur tous les fichiers d'un volume de SnapLock conformité à l'aide de la ONTAP CLI

Exécutez la commande suivante. Remplacez *litigation1* et *slc_vol1* par vos propres informations.

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -path /
```

Pour mettre fin à un blocage légal sur un fichier d'un volume de SnapLock conformité à l'aide de la ONTAP CLI

Exécutez la commande suivante. *Remplacez litigation1, slc_vol1 et file1 par vos propres informations.*

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

Pour mettre fin à une suspension légale de tous les fichiers d'un volume de SnapLock conformité à l'aide de la ONTAP CLI

Exécutez la commande suivante. Remplacez *litigation1* et *slc_vol1* par vos propres informations.

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -path /
```

> **Note**
>
> Nous vous recommandons de surveiller la commande à l'`-operation-status`aide de la `snaplock legal-hold show` commande lorsque vous émettez une suspension légale pour vous assurer qu'elle n'échoue pas.

Commandes associées dans le centre de NetApp documentation :

- Snaplock Legal-Hold Abort
- fichiers de vidage légaux SnapLock
- litiges relatifs à la détention légale de Snapock
- émission Snaplock Legal Hold

Sauvegarde de SnapLock volumes

Vous pouvez sauvegarder des SnapLock volumes pour renforcer la protection des données. Lorsque vous restaurez un SnapLock volume, ses paramètres d'origine, tels que la rétention par défaut, la rétention minimale et la rétention maximale, sont préservés. Les paramètres Write once, read many (WORM) et Legal Hold sont également préservés.

> **Note**
>
> Vous ne pouvez pas sauvegarder un SnapLock FlexGroup volume.

Vous pouvez restaurer la sauvegarde d'un SnapLock volume en tant que SnapLock volume SnapLock ou non. Toutefois, vous ne pouvez pas restaurer la sauvegarde d'un SnapLock non-volume en tant que SnapLock volume.

Pour plus d'informations sur les sauvegardes, consultez Utilisation des sauvegardes.

Supprimer des SnapLock volumes

Vous pouvez supprimer un volume SnapLock Compliance si les périodes de conservation de tous les fichiers WORM (écriture une fois, lecture multiple) qu'il contient ont expiré.

> **Note**
>
> Lorsque vous fermez un compte contenant SnapLock Enterprise ou des Compliance volumes AWS et Compte AWS que FSx for ONTAP suspend votre compte pendant 90 jours avec vos données intactes. Si vous ne rouvrez pas votre compte pendant ces 90 jours, il AWS supprime vos données, y compris les données en SnapLock volume, quels que soient vos paramètres de conservation.

Vous pouvez supprimer un volume SnapLock Enterprise à tout moment si vous disposez des autorisations appropriées. Vous devez être un administrateur Amazon FSx. En outre, que vous utilisiez la console Amazon FSx ou l'API Amazon FSx, vous devez disposer de l'autorisation IAM `fsx:BypassSnapLockEnterpriseRetention` IAM pour supprimer un volume SnapLock Enterprise contenant des données WORM avec une politique de rétention active.

> **Warning**
>
> La période de conservation minimale d'un volume de journal SnapLock d'audit est de six mois. Tant que cette période de conservation n'est pas expirée, vous ne pouvez pas supprimer le volume du journal d'SnapLockaudit, la machine virtuelle de stockage (SVM) ou le système de fichiers associé à la SVM, même si le volume a été créé en mode Enterprise. SnapLock Pour plus d'informations, consultez SnapLockvolumes des journaux d'audit.

Pour supprimer un volume SnapLock Enterprise sur la console Amazon FSx

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation de gauche, sélectionnez Volumes.
3. Choisissez le volume que vous souhaitez supprimer.
4. Dans Actions, choisissez Supprimer le volume.
5. Pour Bypass SnapLock Enterprise Retention, choisissez Yes.
6. Dans la boîte de dialogue de confirmation, choisissez l'une des options suivantes pour Créer une sauvegarde finale :

   - Choisissez Oui pour effectuer une sauvegarde finale du volume. Le nom de la sauvegarde finale s'affiche.
   - Choisissez Non si vous ne souhaitez pas effectuer de sauvegarde finale du volume. Il vous est demandé de confirmer qu'une fois le volume supprimé, les sauvegardes automatiques ne sont plus disponibles.
7. Confirmez la suppression du volume **`delete`** en saisissant le champ Confirmer la suppression.
8. Choisissez Supprimer le (s) volume (s).

Utilisation de Microsoft Active Directory dans FSx pour ONTAP

Amazon FSx fonctionne avec Microsoft Active Directory pour s'intégrer à vos environnements existants. Active Directory est le service d'annuaire Microsoft utilisé pour stocker des informations sur les objets du réseau et pour aider les administrateurs et les utilisateurs à trouver et à utiliser ces informations. Ces objets incluent généralement des ressources partagées, telles que des serveurs de fichiers, des comptes d'utilisateurs et d'ordinateurs du réseau.

Vous pouvez éventuellement associer vos machines virtuelles de stockage (SVM) FSx for ONTAP à votre domaine Active Directory pour authentifier les utilisateurs et contrôler l'accès au niveau des fichiers et des dossiers. Les clients SMB (Server Message Block) peuvent ensuite utiliser leur identité utilisateur existante dans Active Directory pour s'authentifier et accéder aux volumes de SVM. Vos utilisateurs peuvent utiliser leurs identités existantes pour contrôler l'accès à des fichiers et dossiers individuels. En outre, vous pouvez migrer vos fichiers et dossiers existants ainsi que leurs configurations de liste de contrôle d'accès (ACL) vers Amazon FSx sans aucune modification.

Lorsque vous associez Amazon FSx for NetApp ONTAP à un Active Directory, vous associez les SVM du système de fichiers à Active Directory de manière indépendante. Cela signifie que vous pouvez avoir un système de fichiers dont certaines SVM sont jointes à un Active Directory et d'autres qui ne le sont pas.

Une fois qu'une SVM est jointe à Active Directory, vous pouvez mettre à jour les propriétés de configuration Active Directory suivantes :

- Adresses IP des serveurs DNS
- Nom d'utilisateur et mot de passe du compte de service Active Directory autogéré

Rubriques

Conditions requises pour joindre une SVM à un Microsoft AD autogéré

Avant de joindre une SVM FSx for ONTAP à un domaine Microsoft AD autogéré, assurez-vous que votre Active Directory et votre réseau répondent aux exigences décrites dans les sections suivantes.

Rubriques

Exigences relatives à Active Directory sur site

Assurez-vous que vous disposez déjà d'un Microsoft AD sur site ou d'un autre outil autogéré auquel vous pouvez joindre la SVM. Cet Active Directory doit avoir la configuration suivante :

- Le niveau fonctionnel du domaine du contrôleur de domaine Active Directory est Windows Server 2000 ou supérieur.
- Active Directory utilise un nom de domaine qui n'est pas au format SLD (Single Label Domain). Amazon FSx ne prend pas en charge les domaines SLD.
- Si des sites Active Directory sont définis, assurez-vous que les sous-réseaux du VPC associé à votre système de fichiers FSx for ONTAP sont définis dans les mêmes sites Active Directory et qu'il n'existe aucun conflit entre vos sous-réseaux VPC et les sous-réseaux de vos sites Active Directory.

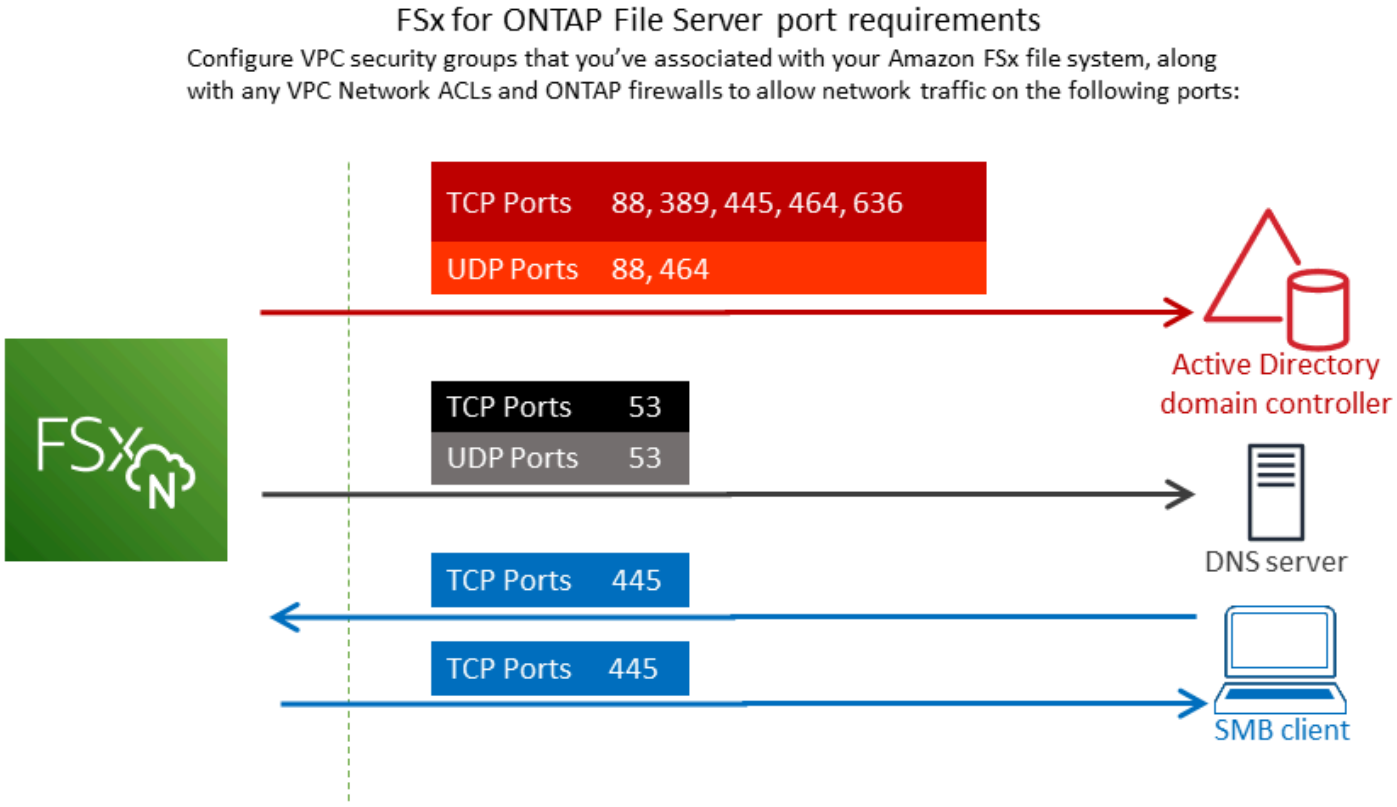
> **Note**
>
> Si vous l'utilisez AWS Directory Service, FSx for ONTAP ne permet pas de joindre des SVM au Simple Active Directory.

Exigences en matière de configuration du réseau

Assurez-vous que les configurations réseau suivantes sont en place et que les informations associées sont à votre disposition.

> **Important**
>
> Pour qu'une SVM puisse rejoindre Active Directory, vous devez vous assurer que les ports décrits dans cette rubrique autorisent le trafic entre tous les contrôleurs de domaine Active Directory et les deux adresses IP iSCSI (interfaces logiques iscsi_1 et iscsi_2 (LIFS)) de la SVM.

- Les adresses IP du serveur DNS et du contrôleur de domaine Active Directory.
- Connectivité entre le VPC Amazon dans lequel vous créez le système de fichiers et votre Active Directory autogéré à l'aide de AWS Direct Connect, AWS VPNou. AWS Transit Gateway
- Le groupe de sécurité et les ACL du réseau VPC pour les sous-réseaux sur lesquels vous créez le système de fichiers doivent autoriser le trafic sur les ports et dans les directions indiquées dans le schéma suivant.



Le rôle de chaque port est décrit dans le tableau suivant.

Protocole	Ports	Rôle
TCP/UDP	53	Système de nom de domaine (DNS)
TCP/UDP	88	Authentification Kerberos
TCP/UDP	389	Protocole LDAP (Lightweight Directory Access Protocol)
TCP	445	Partage de fichiers SMB avec les services d'annuaire
TCP/UDP	464	Changement/définition de mot de passe
TCP	636	Protocole LDAP (Lightweight Directory Access Protocol) via TLS/SSL (LDAPS)

- Ces règles de trafic doivent également être reflétées sur les pare-feux qui s'appliquent à chacun des contrôleurs de domaine Active Directory, des serveurs DNS, des clients FSx et des administrateurs FSx.

> **Important**
>
> Alors que les groupes de sécurité Amazon VPC nécessitent que les ports soient ouverts uniquement dans le sens où le trafic réseau est initié, la plupart des pare-feux Windows et des ACL de réseau VPC nécessitent que les ports soient ouverts dans les deux sens.

Exigences relatives aux comptes de service Active Directory

Assurez-vous que vous disposez d'un compte de service dans votre Microsoft AD autogéré doté d'autorisations déléguées pour associer des ordinateurs au domaine. Un compte de service est un compte utilisateur de votre Active Directory autogéré auquel certaines tâches ont été déléguées.

Au minimum, les autorisations suivantes doivent être déléguées au compte de service dans l'unité d'organisation à laquelle vous rejoignez la SVM :

- Possibilité de réinitialiser les mots de passe

- Possibilité d'empêcher les comptes de lire et d'écrire des données
- Possibilité de définir la `msDS-SupportedEncryptionTypes` propriété sur les objets de l'ordinateur
- Capacité validée d'écrire sur le nom d'hôte DNS
- Capacité validée d'écrire dans le nom du principal de service
- Possibilité de créer et de supprimer des objets informatiques
- Aptitude validée à lire et à écrire les restrictions du compte

Il s'agit de l'ensemble minimal d'autorisations requises pour joindre des objets informatiques à votre Active Directory. Pour plus d'informations, consultez la rubrique de documentation de Windows Server Erreur : l'accès est refusé lorsque des utilisateurs non administrateurs auxquels le contrôle a été délégué tentent de joindre des ordinateurs à un contrôleur de domaine.

Pour en savoir plus sur la création d'un compte de service doté des autorisations appropriées, consultezDélégation d'autorisations à votre compte de service Amazon FSx.

> **Important**
>
> Amazon FSx nécessite un compte de service valide pendant toute la durée de vie de votre système de fichiers Amazon FSx. Amazon FSx doit être en mesure de gérer entièrement le système de fichiers et d'effectuer des tâches qui l'obligent à dissocier et à joindre des ressources à votre domaine Active Directory. Ces tâches incluent le remplacement d'un système de fichiers ou d'une SVM défaillants ou l'application de correctifs au logiciel NetApp ONTAP. Gardez vos informations de configuration Active Directory à jour avec Amazon FSx, y compris les informations d'identification du compte de service. Pour en savoir plus, veuillez consulter la section Maintien à jour de votre configuration Active Directory avec Amazon FSx.

Si c'est la première fois que vous utilisez AWS FSx for ONTAP, assurez-vous d'avoir effectué les étapes de configuration initiales avant de commencer votre intégration à Active Directory. Pour de plus amples informations, veuillez consulter Configuration de FSx pour ONTAP.

> **Important**
>
> Ne déplacez pas les objets informatiques créés par Amazon FSx dans l'unité d'organisation après la création de vos SVM, et ne supprimez pas votre Active Directory alors que votre SVM y est jointe. Dans ce cas, vos SVM seront mal configurées.

Bonnes pratiques d'utilisation d'Active Directory

Voici quelques suggestions et directives à prendre en compte lorsque vous associez des SVM Amazon FSx for NetApp ONTAP à votre Microsoft Active Directory autogéré. Notez qu'elles sont recommandées en tant que meilleures pratiques, mais qu'elles ne sont pas obligatoires.

Délégation d'autorisations à votre compte de service Amazon FSx

Assurez-vous de configurer le compte de service que vous fournissez à Amazon FSx avec les autorisations minimales requises. En outre, séparez l'unité organisationnelle (UO) des autres domaines concernés par le contrôleur de domaine.

Pour associer des SVM Amazon FSx à votre domaine, assurez-vous que le compte de service dispose d'autorisations déléguées. Les membres du groupe des administrateurs de domaine disposent des autorisations suffisantes pour effectuer cette tâche. Toutefois, il est recommandé d'utiliser un compte de service qui ne dispose que des autorisations minimales nécessaires pour ce faire. La procédure suivante explique comment déléguer uniquement les autorisations nécessaires pour joindre les SVM FSx for ONTAP à votre domaine.

Effectuez cette procédure sur un ordinateur joint à votre annuaire et sur lequel le composant logiciel enfichable MMC Active Directory User and Computers est installé.

Pour créer un compte de service pour votre domaine Microsoft Active Directory

1. Assurez-vous d'être connecté en tant qu'administrateur de domaine pour votre domaine Microsoft Active Directory.
2. Ouvrez le composant logiciel enfichable MMC Active Directory User and Computers.
3. Dans le volet des tâches, développez le nœud de domaine.
4. Localisez et ouvrez le menu contextuel (clic droit) de l'unité d'organisation que vous souhaitez modifier, puis choisissez Déléguer le contrôle.

5. Sur la page Assistant de délégation de contrôle, choisissez Next.
6. Choisissez Ajouter pour ajouter un utilisateur ou un groupe spécifique aux utilisateurs et groupes sélectionnés, puis cliquez sur Suivant.
7. Sur la page Tâches à déléguer, sélectionnez Créer une tâche personnalisée à déléguer, puis choisissez Suivant.
8. Choisissez Uniquement les objets suivants dans le dossier, puis choisissez Objets informatiques.
9. Choisissez Créer les objets sélectionnés dans ce dossier et Supprimer les objets sélectionnés dans ce dossier. Ensuite, sélectionnez Suivant.
10. Sous Afficher ces autorisations, assurez-vous que les options Général et Spécifique à la propriété sont sélectionnées.
11. Pour Autorisations, choisissez ce qui suit :

    - Réinitialisation du mot
    - Lire et écrire les restrictions du compte
    - Écriture validée sur le nom d'hôte DNS
    - Écriture validée sur le nom principal du service
    - Rédiger des MSDs- SupportedEncryptionTypes
12. Cliquez sur Suivant, puis sur Terminer.
13. Fermez le composant logiciel enfichable MMC Active Directory User and Computers.

> ⚠ Important
>
> Ne déplacez pas les objets informatiques créés par Amazon FSx dans l'unité d'organisation après la création de vos SVM. Cela entraînera une mauvaise configuration de vos SVM.

Maintien à jour de votre configuration Active Directory avec Amazon FSx

Pour une disponibilité ininterrompue de vos SVM Amazon FSx, mettez à jour la configuration Active Directory (AD) autogérée d'une SVM lorsque vous modifiez votre configuration AD autogérée.

Supposons, par exemple, que votre AD utilise une politique de réinitialisation des mots de passe basée sur le temps. Dans ce cas, dès que le mot de passe est réinitialisé, assurez-vous de mettre à jour le mot de passe du compte de service avec Amazon FSx. Pour ce faire, utilisez la console

Amazon FSx, l'API Amazon FSx ou. AWS CLI De même, si les adresses IP du serveur DNS changent pour votre domaine Active Directory, mettez à jour les adresses IP du serveur DNS avec Amazon FSx dès que le changement se produit.

En cas de problème avec la mise à jour de la configuration AD autogérée, l'état de la SVM passe à Mauvaise configuration. Cet état affiche un message d'erreur et une action recommandée à côté de la description de la SVM dans la console, l'API et la CLI. En cas de problème lié à la configuration Active Directory de votre SVM, veillez à prendre les mesures correctives recommandées pour les propriétés de configuration. Si le problème est résolu, vérifiez que l'état de votre SVM passe à Créé.

Pour plus d'informations, consultez Mettre à jour la configuration Active Directory d'une SVM existante à l'aide de l' AWS Management ConsoleAPI AWS CLI,, et et Modifier une configuration Active Directory à l'aide de la CLI ONTAP.

Utilisation de groupes de sécurité pour limiter le trafic au sein de votre VPC

Pour limiter le trafic réseau dans votre cloud privé virtuel (VPC), vous pouvez mettre en œuvre le principe du moindre privilège dans votre VPC. En d'autres termes, vous pouvez limiter les autorisations au minimum nécessaire. Pour ce faire, utilisez les règles des groupes de sécurité. Pour en savoir plus, veuillez consulter la section Groupes de sécurité Amazon VPC.

Création de règles de groupe de sécurité sortant pour l'interface réseau de votre système de fichiers

Pour plus de sécurité, envisagez de configurer un groupe de sécurité avec des règles de trafic sortant. Ces règles doivent autoriser le trafic sortant uniquement vers vos contrôleurs de domaines AD autogérés ou au sein du sous-réseau ou du groupe de sécurité. Appliquez ce groupe de sécurité au VPC associé à l'interface Elastic Network Interface de votre système de fichiers Amazon FSx. Pour en savoir plus, consultez Contrôle d'accès au système de fichiers avec Amazon VPC.

Joindre des SVM à un Microsoft Active Directory

Votre organisation peut gérer les identités et les appareils à l'aide d'un Active Directory, que ce soit sur site ou dans le cloud. Avec FSx for ONTAP, vous pouvez associer vos SVM directement à votre domaine Active Directory existant de la manière suivante :

- Joindre de nouvelles SVM à un Active Directory lors de la création :

  - À l'aide de l'option de création standard de la console Amazon FSx pour créer un nouveau système de fichiers FSx for ONTAP, vous pouvez associer la SVM par défaut à un Active Directory autogéré. Pour de plus amples informations, veuillez consulter Pour créer un système de fichiers (console).
  - Utilisation de la console Amazon FSx ou de l'API Amazon FSx pour créer une nouvelle SVM sur un système de fichiers FSx for ONTAP existant. AWS CLI Pour de plus amples informations, veuillez consulter Création d'une machine virtuelle de stockage.
- Joindre des SVM existantes à un Active Directory :
  - Utilisation de l'API AWS Management Console AWS CLI, et pour joindre une SVM à un Active Directory et pour réessayer de joindre une SVM à Active Directory en cas d'échec de la première tentative de connexion. Vous pouvez également mettre à jour certaines propriétés de configuration Active Directory pour les SVM déjà jointes à un Active Directory. Pour de plus amples informations, veuillez consulter Gestion des configurations Active Directory des SVM.
  - Utilisation de la CLI NetApp ONTAP ou de l'API REST pour joindre, réessayer ou dissocier des configurations SVM Active Directory. Pour de plus amples informations, veuillez consulter Gestion de la configuration Active Directory de votre SVM à l'aide de la CLI NetApp .

> ⚠ Important
>
> - Amazon FSx enregistre les enregistrements DNS pour une SVM uniquement si vous utilisez Microsoft DNS comme service DNS par défaut. Si vous utilisez un DNS tiers, vous devez configurer les entrées DNS manuellement pour vos SVM Amazon FSx après les avoir créées.
> - Si vous l'utilisez AWS Managed Microsoft AD, vous devez spécifier un groupe tel que les administrateurs FSx AWS délégués, les administrateurs AWS délégués ou un groupe personnalisé doté d'autorisations déléguées sur l'unité d'organisation.

Lorsque vous associez une SVM FSx for ONTAP directement à un Active Directory autogéré, la SVM réside dans la même forêt Active Directory (le conteneur logique supérieur d'une configuration Active Directory qui contient des domaines, des utilisateurs et des ordinateurs) et dans le même domaine Active Directory que vos utilisateurs et les ressources existantes, y compris les serveurs de fichiers existants.

Informations nécessaires pour joindre une SVM à un Active Directory

Vous devez fournir les informations suivantes concernant votre Active Directory lorsque vous associez une SVM à un Active Directory, quelle que soit l'opération d'API que vous choisissez :

- Nom NetBIOS de l'objet informatique Active Directory à créer pour votre SVM. Il s'agit du nom de la SVM dans Active Directory, qui doit être unique au sein de votre Active Directory. N'utilisez pas le nom NetBIOS du domaine d'origine. Le nom NetBIOS ne peut pas dépasser 15 caractères.
- Le nom de domaine complet (FQDN) de votre Active Directory. Le FQDN ne peut pas dépasser 255 caractères.

  > **Note**
  >
  > Le FQDN ne peut pas être au format SLD (Single Label Domain). Amazon FSx ne prend pas en charge les domaines SLD.

- Jusqu'à trois adresses IP des serveurs DNS ou des hôtes de domaine de votre domaine.

  Les adresses IP du serveur DNS et les adresses IP du contrôleur de domaine Active Directory peuvent se situer dans n'importe quelle plage d'adresses IP, sauf :

  - Des adresses IP qui entrent en conflit avec les adresses IP appartenant à Amazon Web Services à cet égard. Région AWS Pour obtenir la liste des adresses AWS IP par région, consultez les plages d'adresses AWS IP.
  - Adresses IP comprises dans la plage de blocs CIDR suivante : 198.19.0.0/16
- Nom d'utilisateur et mot de passe d'un compte de service sur votre domaine Active Directory, à utiliser par Amazon FSx pour joindre la SVM au domaine Active Directory. Pour plus d'informations sur les exigences relatives aux comptes de service, consultezExigences relatives aux comptes de service Active Directory.
- (Facultatif) Unité organisationnelle (UO) du domaine auquel vous joignez la SVM.

  > **Note**
  >
  > Si vous associez votre SVM à un AWS Directory Service Active Directory, vous devez fournir une unité d'organisation qui se trouve dans l'unité d'organisation par défaut qui AWS Directory Service crée pour les objets de répertoire associés. AWS Cela est dû au fait que le AWS Directory Service ne donne pas accès à l'unité d'organisation par défaut de votre Active `Computers` Directory. Par exemple, si votre domaine

Active Directory est`example.com`, vous pouvez spécifier l'unité d'organisation suivante :`OU=Computers,OU=example,DC=example,DC=com`.

- (Facultatif) Le groupe de domaines auquel vous déléguez l'autorité pour effectuer des actions administratives sur votre système de fichiers. Par exemple, ce groupe de domaines peut gérer les partages de fichiers Windows SMB, s'approprier des fichiers et des dossiers, etc. Si vous ne spécifiez pas ce groupe, Amazon FSx délègue cette autorité au groupe des administrateurs de domaine de votre domaine Active Directory par défaut.

Gestion des configurations Active Directory des SVM

Cette section décrit comment utiliser l'API AWS Management Console AWS CLI, FSx et la CLI ONTAP pour effectuer les opérations suivantes :

- Joindre une SVM existante à un Active Directory
- Modification de la configuration Active Directory d'une SVM existante
- Supprimer les SVM d'un Active Directory

Pour supprimer une SVM d'un Active Directory, vous devez utiliser la NetApp CLI ONTAP.

Rubriques

- Joindre une SVM à un Active Directory à l'aide de AWS Management Console l'API AWS CLI et
- Mettre à jour la configuration Active Directory d'une SVM existante à l'aide de l' AWS Management ConsoleAPI AWS CLI,, et
- Gestion de la configuration Active Directory de votre SVM à l'aide de la CLI NetApp

Joindre une SVM à un Active Directory à l'aide de AWS Management Console l'API AWS CLI et

Pour joindre une SVM existante à un Active Directory, procédez comme suit. Dans cette procédure, la SVM n'est pas déjà jointe à un Active Directory.

Pour joindre une SVM à un Active Directory () AWS Management Console

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.

2. Choisissez la SVM que vous souhaitez associer à un Active Directory :

   - Dans le volet de navigation de gauche, sélectionnez Systèmes de fichiers, puis choisissez le système de fichiers ONTAP contenant la SVM que vous souhaitez mettre à jour.
   - Choisissez l'onglet Machines virtuelles de stockage.

     —Ou—

   - Pour afficher la liste de toutes les SVM disponibles, dans le volet de navigation de gauche, développez ONTAP et choisissez Machines virtuelles de stockage. La liste de toutes les SVM de votre compte Région AWS s'affiche.

   Sélectionnez dans la liste la SVM que vous souhaitez associer à un Active Directory.
3. Dans le coin supérieur droit du panneau récapitulatif de la SVM, choisissez Actions > Joindre/Mettre à jour Active Directory. La fenêtre Joindre la SVM à un Active Directory apparaît.
4. Entrez les informations suivantes pour l'Active Directory auquel vous souhaitez rejoindre la SVM :

   - Nom NetBIOS de l'objet informatique Active Directory à créer pour votre SVM. Il s'agit du nom de la SVM dans Active Directory, qui doit être unique au sein de votre Active Directory. N'utilisez pas le nom NetBIOS du domaine d'origine. Le nom NetBIOS ne peut pas dépasser 15 caractères.
   - Le nom de domaine complet (FQDN) de votre Active Directory. Le nom de domaine ne peut pas dépasser 255 caractères.
   - Adresses IP des serveurs DNS : adresses IPv4 des serveurs DNS de votre domaine.
   - Nom d'utilisateur du compte de service : nom d'utilisateur du compte de service dans votre Active Directory existant. N'incluez pas de préfixe ou de suffixe de domaine. Par exemple, pour`EXAMPLE\ADMIN`, utiliser uniquement`ADMIN`.
   - Mot de passe du compte de service : mot de passe du compte de service.
   - Confirmer le mot de passe : mot de passe du compte de service.
   - (Facultatif) Unité organisationnelle (UO) : nom du chemin unique de l'unité organisationnelle à laquelle vous souhaitez joindre votre SVM.
   - Groupe d'administrateurs de systèmes de fichiers délégués : nom du groupe de votre Active Directory qui peut administrer votre système de fichiers.

Si vous utilisez AWS Managed Microsoft AD, vous devez spécifier un groupe tel que les administrateurs FSx AWS délégués, les administrateurs AWS délégués ou un groupe personnalisé doté d'autorisations déléguées sur l'unité d'organisation.

Si vous rejoignez un Active Directory autogéré, utilisez le nom du groupe dans votre Active Directory. Le groupe par défaut est`Domain Admins`.

5. Choisissez Join Active Directory pour associer la SVM à Active Directory en utilisant la configuration que vous avez fournie.

Pour joindre une SVM à un Active Directory (AWS CLI)

- Pour joindre une SVM FSx for ONTAP à un Active Directory, utilisez la commande update-storage-virtual-machineCLI (ou l'opération UpdateStorageVirtualMachineAPI équivalente), comme indiqué dans l'exemple suivant.

```
aws fsx update-storage-virtual-machine \
  --storage-virtual-machine-id svm-abcdef0123456789a\
  --active-directory-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
    OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",
\
    FileSystemAdministratorsGroup="FSxAdmins",UserName="FSxService",\
    Password="password", \
    DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

Après avoir créé avec succès la machine virtuelle de stockage, Amazon FSx renvoie sa description au format JSON, comme illustré dans l'exemple suivant.

```
{
  "StorageVirtualMachine": {
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
```

```
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATED",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],

  }
}
```

Mettre à jour la configuration Active Directory d'une SVM existante à l'aide de l' AWS Management ConsoleAPI AWS CLI,, et

Pour mettre à jour la configuration Active Directory d'une SVM déjà jointe à Active Directory, procédez comme suit.

Pour mettre à jour la configuration Active Directory d'une SVM () AWS Management Console

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Choisissez la SVM à mettre à jour comme suit :

   - Dans le volet de navigation de gauche, choisissez Systèmes de fichiers, puis choisissez le système de fichiers ONTAP contenant la SVM que vous souhaitez mettre à jour.
   - Choisissez l'onglet Machines virtuelles de stockage.

   —Ou—

   - Pour afficher la liste de toutes les SVM disponibles, dans le volet de navigation de gauche, développez ONTAP et choisissez Machines virtuelles de stockage.

   Sélectionnez dans la liste la SVM que vous souhaitez mettre à jour.
3. Dans le panneau récapitulatif de la SVM, choisissez Actions > Joindre/Mettre à jour Active Directory. La fenêtre de configuration Active Directory de Update SVM apparaît.
4. Vous pouvez mettre à jour les propriétés de configuration Active Directory suivantes dans cette fenêtre.

   - Adresses IP des serveurs DNS : adresses IPv4 des serveurs DNS de votre domaine.
   - Nom d'utilisateur du compte de service : nom d'utilisateur du compte de service dans votre Active Directory existant. N'incluez pas de préfixe ou de suffixe de domaine. Pour `EXAMPLE\ADMIN`, utilisez `ADMIN`.
   - Mot de passe du compte de service : mot de passe du compte de service Active Directory.
5. Après avoir saisi vos mises à jour, choisissez Mettre à jour Active Directory pour effectuer les modifications.

Pour mettre à jour la configuration Active Directory d'une SVM déjà jointe à Active Directory, procédez comme suit.

Pour mettre à jour la configuration Active Directory d'une SVM () AWS CLI

- Pour mettre à jour la configuration Active Directory d'une SVM avec l'API AWS CLI or, utilisez la commande update-storage-virtual-machineCLI (ou une opération UpdateStorageVirtualMachineAPI équivalente), comme indiqué dans l'exemple suivant.

```
aws fsx update-storage-virtual-machine \
    --storage-virtual-machine-id svm-abcdef0123456789a\
    --active-directory-configuration \
    SelfManagedActiveDirectoryConfiguration='{UserName="FSxService",\
    Password="password", \
    DnsIps=["10.0.1.18"]}'
```

Gestion de la configuration Active Directory de votre SVM à l'aide de la CLI NetApp

Vous pouvez utiliser la CLI NetApp ONTAP pour joindre et dissocier votre SVM à un Active Directory, et pour modifier la configuration d'une SVM Active Directory existante.

Joindre une SVM à un Active Directory à l'aide de la CLI ONTAP

Vous pouvez joindre des SVM existantes à un Active Directory à l'aide de la CLI ONTAP, comme décrit dans la procédure suivante. Vous pouvez le faire même si votre SVM est déjà jointe à un Active Directory.

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *management_endpoint_ip* par l'adresse IP du port de gestion du système de fichiers.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Pour de plus amples informations, veuillez consulter Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.
2. Créez une entrée DNS pour votre Active Directory en fournissant le nom DNS complet du répertoire (`corp.example.com`) et au moins une adresse IP du serveur DNS.

```
::>vserver services name-service dns create -vserver svm_name -
domains corp.example.com -name-servers dns_ip_1, dns_ip_2
```

Pour vérifier la connexion à vos serveurs DNS, exécutez la commande suivante. Remplacez *svm_name* par vos propres informations.

```
FsxId0ae30e5b7f1a50b6a::>vserver services name-service dns check -vserver svm_name

                            Name Server
Vserver       Name Server     Status       Status Details
------------ --------------- ------------ --------------------------
svm_name      172.31.14.245   up           Response time (msec): 0
svm_name      172.31.25.207   up           Response time (msec): 1
2 entries were displayed.
```

3. Pour associer votre SVM à Active Directory, exécutez la commande suivante. Notez que vous devez spécifier un nom `computer_name` qui n'existe pas encore dans votre Active Directory et fournir le nom DNS du répertoire pour `-domain`. Pour cela `-OU`, entrez les unités d'organisation auxquelles vous souhaitez associer la SVM, ainsi que le nom DNS complet au format DC.

```
::>vserver cifs create -vserver svm_name -cifs-server computer_name -
domain corp.example.com -OU OU=Computers,OU=example,DC=corp,DC=example,DC=com
```

Pour vérifier l'état de votre connexion Active Directory, exécutez la commande suivante :

```
::>vserver cifs check -vserver svm_name

             Vserver : svm_name
                  Cifs NetBIOS Name : svm_netBIOS_name
                        Cifs Status : Running
                               Site : Default-First-Site-Name
Node Name       DC Server Name  DC Server IP    Status   Status Details
--------------- --------------  --------------- ------   --------------
FsxId0ae30e5b7f1a50b6a-01
                corp.example.com
                                172.31.14.245   up       Response time (msec): 5
FsxId0ae30e5b7f1a50b6a-02
                corp.example.com
                                172.31.14.245   up       Response time (msec): 20
2 entries were displayed.
```

4. Si vous ne pouvez pas accéder aux partages après cette inscription, déterminez si le compte que vous utilisez pour accéder au partage dispose d'autorisations. Par exemple, si vous utilisez le `Admin` compte par défaut (un administrateur délégué) avec un Active Directory AWS géré, vous devez exécuter la commande suivante dans ONTAP. `netbios_domain`Correspond au nom de domaine de votre Active Directory (pour`corp.example.com`, le nom `netbios_domain` utilisé ici est`example`).

```
FsxId0123456789a::>vserver cifs users-and-groups local-group add-members -vserver
 svm_name -group-name BUILTIN\Administrators -member-names netbios_domain\admin
```

Modifier une configuration Active Directory à l'aide de la CLI ONTAP

Vous pouvez utiliser la CLI ONTAP pour modifier une configuration Active Directory existante.

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *`management_endpoint_ip`* par l'adresse IP du port de gestion du système de fichiers.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

   Pour de plus amples informations, veuillez consulter Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.

2. Exécutez la commande suivante pour arrêter temporairement le serveur CIFS de la SVM :

```
FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
```

3. Si vous devez modifier les entrées DNS de votre Active Directory, exécutez la commande suivante :

```
::>vserver services name-service dns modify -vserver svm_name -
domains corp.example.com -name-servers dns_ip_1,dns_ip_2
```

   Vous pouvez valider l'état de connexion aux serveurs DNS de votre Active Directory à l'aide de la `vserver services name-service dns check -vserver svm_name` commande.

```
::>vserver services name-service dns check -vserver svm_name
```

```
                                Name Server
Vserver       Name Server       Status       Status Details
------------- ---------------- ------------ --------------------------
svmciad       dns_ip_1          up           Response time (msec): 1
svmciad       dns_ip_2          up           Response time (msec): 1
2 entries were displayed.
```

4. Si vous devez modifier la configuration d'Active Directory elle-même, vous pouvez modifier les champs existants à l'aide de la commande suivante, en remplaçant :

   - *`nom_ordinateur, si vous souhaitez modifier le nom`* NetBIOS (compte machine) de la SVM.
   - *`domain_name`*, si vous souhaitez modifier le nom du domaine. Cela doit correspondre à l'entrée de domaine DNS indiquée à l'étape 3 de cette section (`corp.example.com`).
   - `organizational_unit`, si vous souhaitez modifier l'unité d'organisation (`OU=Computers,OU=example,DC=corp,DC=example,DC=com`).

   Vous devrez saisir à nouveau les informations d'identification Active Directory que vous avez utilisées pour associer cet appareil à Active Directory.

   ```
   ::>vserver cifs modify -vserver svm_name -cifs-server computer_name -
   domain domain_name -OU organizational_unit
   ```

   Vous pouvez vérifier l'état de votre connexion Active Directory à l'aide de la `vserver cifs check -vserver svm_name` commande.

5. Lorsque vous avez terminé de modifier votre configuration Active Directory et DNS, réactivez le serveur CIFS en exécutant la commande suivante :

   ```
   ::>vserver cifs modify -vserver svm_name -status-admin up
   ```

Dissocier un Active Directory de votre SVM à l'aide de la NetApp CLI ONTAP

La CLI NetApp ONTAP peut également être utilisée pour dissocier votre SVM d'un Active Directory en suivant les étapes ci-dessous :

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante.

Remplacez *management_endpoint_ip* par l'adresse IP du port de gestion du système de fichiers.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Pour de plus amples informations, veuillez consulter Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.

2. Supprimez le serveur CIFS qui a dissocié votre appareil d'Active Directory en exécutant la commande suivante. Pour qu'ONTAP supprime le compte de machine associé à votre SVM, veuillez fournir les informations d'identification que vous avez initialement utilisées pour associer la SVM à Active Directory.

```
FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
```

3. Si vous devez modifier les entrées DNS de votre Active Directory, exécutez la commande suivante :

```
FsxId0123456789a::vserver cifs delete -vserver svm_name

In order to delete an Active Directory machine account for the CIFS server, you
 must supply the name and password of a Windows account with
sufficient privileges to remove computers from the "CORP.ADEXAMPLE.COM" domain.

Enter the user name: user_name

Enter the password:

Warning: There are one or more shares associated with this CIFS server
         Do you really want to delete this CIFS server and all its shares? {y|n}: y
```

4. Supprimez les serveurs DNS de votre Active Directory en exécutant la commande suivante :

```
::vserver services name-service dns delete -vserver svm_name
```

Si vous voyez un avertissement comme celui-ci, indiquant qu'il `dns` doit être supprimé en tant que tel, `ns-switch` et si vous ne prévoyez pas de rattacher cet appareil à un Active Directory, vous pouvez supprimer les entrées. `ns-switch`

```
Warning: "DNS" is present as one of the sources in one or more ns-switch databases
 but no valid DNS configuration was found for Vserver
        "svm_name". Remove "DNS" from ns-switch using the "vserver services name-
service ns-switch" command. Configuring "DNS" as a source
        in the ns-switch setting when there is no valid configuration can cause
 protocol access issues.
```

5. (Facultatif) Supprimez les `ns-switch` entrées pour en `dns` exécutant la commande suivante. Vérifiez l'ordre des sources, puis supprimez l'`dns`entrée de la `hosts` base de données en modifiant le `sources` afin qu'il ne contienne que les autres sources répertoriées. Dans cet exemple, la seule autre source est`files`.

```
::>vserver services name-service ns-switch show -vserver svm_name -database hosts

                    Vserver: svm_name
Name Service Switch Database: hosts
   Name Service Source Order: files, dns
```

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

6. (Facultatif) Supprimez l'`dns`entrée en modifiant le `sources` pour l'hôte de base de données afin de l'inclure uniquement`files`.

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

Amazon FSx pour NetApp les performances d'ONTAP

Vous trouverez ci-dessous une présentation des performances du système de fichiers Amazon FSx for NetApp ONTAP, avec une discussion sur les options de performance et de débit disponibles, ainsi que des conseils utiles en matière de performances.

Rubriques

Comment les performances sont mesurées pour les systèmes de fichiers FSx for ONTAP

Les performances du système de fichiers sont mesurées par sa latence, son débit et ses opérations d'E/S par seconde (IOPS).

Latence

Amazon FSx for NetApp ONTAP fournit des latences de fonctionnement des fichiers inférieures à la milliseconde avec le stockage sur disque SSD, et des dizaines de millisecondes de latence pour le stockage en pool de capacité. En outre, Amazon FSx dispose de deux couches de mise en cache de lecture sur chaque serveur de fichiers, à savoir les lecteurs NVMe (mémoire non volatile express) et les disques en mémoire, afin de réduire encore les latences lorsque vous accédez aux données les plus fréquemment lues.

Débit et IOPS

Chaque système de fichiers Amazon FSx fournit jusqu'à des dizaines de Gbit/s de débit et des millions d'IOPS. Le débit et les IOPS spécifiques que votre charge de travail peut générer sur votre système de fichiers dépendent de la capacité de débit totale et de la configuration de la capacité de

stockage de votre système de fichiers, ainsi que de la nature de votre charge de travail, notamment de la taille de l'ensemble de travail actif.

Support pour SMB, multicanal et NFS nconnect

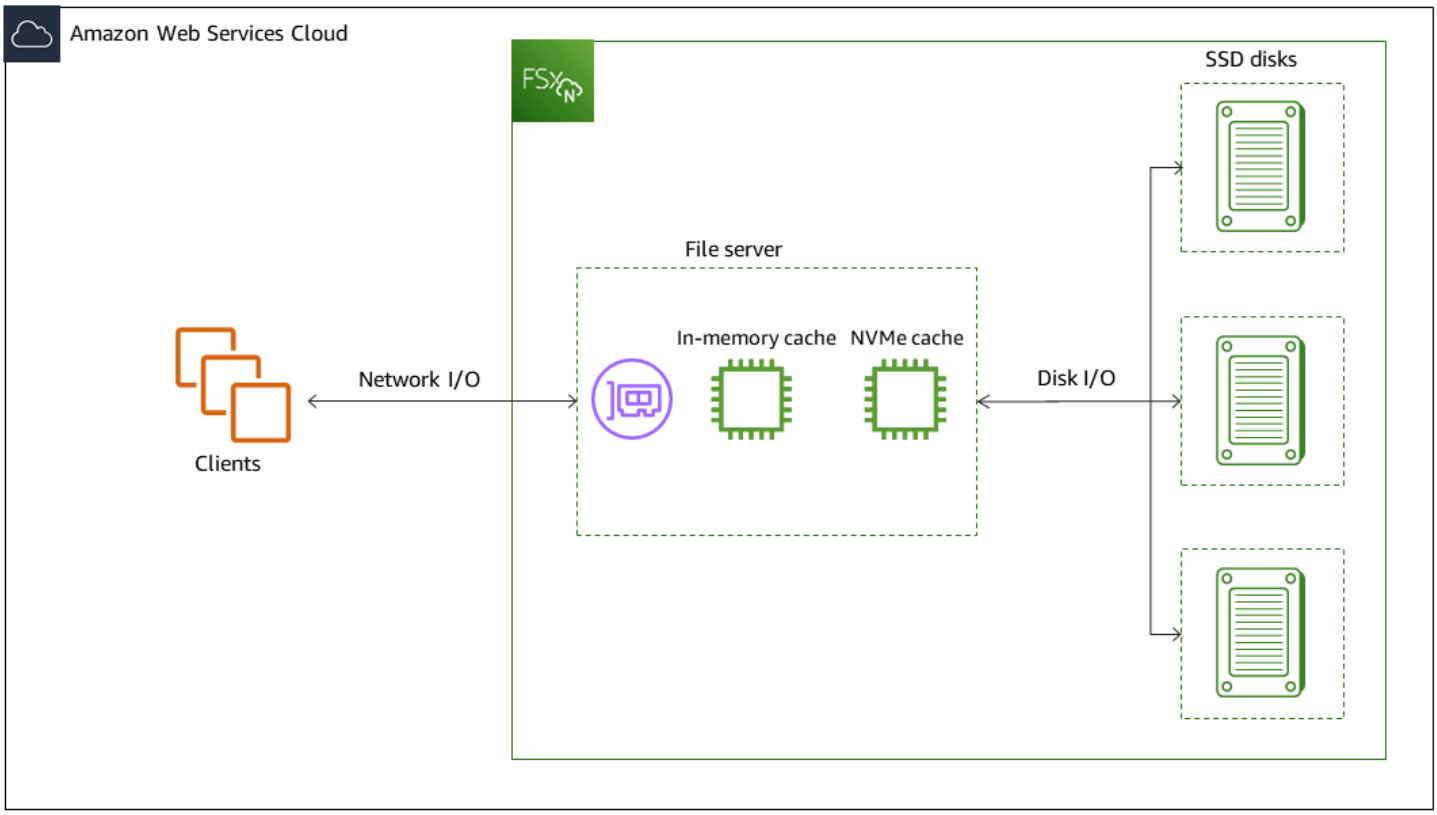
Avec Amazon FSx, vous pouvez configurer SMB Multicanal pour fournir plusieurs connexions entre ONTAP et clients au cours d'une seule session SMB. SMB Multicanal utilise plusieurs connexions réseau entre le client et le serveur simultanément pour agréger la bande passante réseau afin d'optimiser l'utilisation. Pour plus d'informations sur l'utilisation de la NetApp ONTAP CLI pour configurer le multicanal SMB, voir Configuration du multicanal SMB pour les performances et la redondance.

Les clients NFS peuvent utiliser l'option de `nconnect` montage pour associer plusieurs connexions TCP (jusqu'à 16) à un seul montage NFS. Un tel client NFS multiplexe les opérations de fichiers sur plusieurs connexions TCP de manière circulaire et obtient ainsi un débit supérieur à partir de la bande passante réseau disponible. Support de NFSv3 et NFSv4.1+. `nconnect` La bande passante réseau des instances Amazon EC2 décrit la limite de bande passante de 5 Gbit/s par flux réseau en duplex intégral. Vous pouvez surmonter cette limite en utilisant plusieurs flux réseau `nconnect` ou en utilisant le multicanal SMB. Consultez la documentation de votre client NFS pour vérifier s'il `nconnect` est pris en charge dans votre version client. Pour plus d'informations sur la NetApp ONTAP prise en charge den`connect`, consultez la section ONTAPprise en charge de NFSv4.1.

Détails des performances

Pour comprendre en détail le modèle de performance Amazon FSx for NetApp ONTAP, vous pouvez examiner les composants architecturaux d'un système de fichiers Amazon FSx. Les instances de calcul de vos clients, qu'elles existent sur site AWS ou sur site, accèdent à votre système de fichiers via une ou plusieurs interfaces réseau élastiques (ENI). Ces interfaces réseau se trouvent dans le VPC Amazon que vous associez à votre système de fichiers. Derrière chaque système de fichiers ENI se trouve un serveur de NetApp ONTAP fichiers qui fournit des données via le réseau aux clients accédant au système de fichiers. Amazon FSx fournit un cache en mémoire rapide et un cache NVMe sur chaque serveur de fichiers afin d'améliorer les performances des données les plus fréquemment consultées. Les disques SSD hébergeant les données de votre système de fichiers sont connectés à chaque serveur de fichiers.

Ces composants sont illustrés dans le schéma suivant.



Les principales caractéristiques de performance d'un système de fichiers Amazon FSx for NetApp ONTAP qui déterminent le débit global et les performances d'IOPS correspondent à ces composants architecturaux (interface réseau, cache en mémoire, cache NVMe et volumes de stockage).

- Performances d'E/S réseau : débit/IOPS des demandes entre les clients et le serveur de fichiers (agrégé)
- Taille du cache en mémoire et NVMe sur le serveur de fichiers : taille du poste de travail actif pouvant être utilisé pour la mise en cache
- Performances d'E/S du disque : débit/IOPS des demandes entre le serveur de fichiers et les disques de stockage

Deux facteurs déterminent ces caractéristiques de performance de votre système de fichiers : la quantité totale d'IOPS du SSD et la capacité de débit que vous configurez pour celui-ci. Les deux premières caractéristiques de performance (performances d'E/S réseau et taille de cache en mémoire et NVMe) sont uniquement déterminées par la capacité de débit, tandis que la troisième (performances d'E/S du disque) est déterminée par une combinaison de capacité de débit et d'IOPS du SSD.

Les charges de travail basées sur des fichiers sont généralement élevées, caractérisées par des périodes courtes et intenses d'E/S élevées avec de longues périodes d'inactivité entre les rafales. Pour prendre en charge les charges de travail élevées, outre les vitesses de base qu'un système de fichiers peut supporter 24 heures sur 24, 7 jours sur 7, Amazon FSx permet d'atteindre des vitesses plus élevées pendant des périodes de temps, à la fois pour les opérations d'E/S réseau et d'E/S sur disque. Amazon FSx utilise un mécanisme de crédit d'E/S réseau pour allouer le débit et les IOPS en fonction de l'utilisation moyenne. Les systèmes de fichiers accumulent des crédits lorsque leur débit et leur utilisation d'IOPS sont inférieurs à leurs limites de base, et peuvent utiliser ces crédits lorsqu'ils effectuent des opérations d'E/S.

Les opérations d'écriture utilisent deux fois plus de bande passante réseau que les opérations de lecture. Une opération d'écriture doit être répliquée sur le serveur de fichiers secondaire. Ainsi, une seule opération d'écriture double le débit du réseau.

Impact du type de déploiement sur les performances

Vous pouvez créer deux types de systèmes de fichiers avec FSx for ONTAP. Les systèmes de fichiers dotés d'une seule paire de serveurs de fichiers à haute disponibilité (HA) sont appelés systèmes de fichiers évolutifs. Les systèmes de fichiers comportant plusieurs paires HA sont appelés systèmes de fichiers scale-out. Pour plus d’informations, consultez Paires à haute disponibilité (HA).

Les systèmes de fichiers multi-AZ et mono-AZ FSx for ONTAP fournissent des latences de fonctionnement des fichiers constantes inférieures à la milliseconde avec le stockage SSD et des dizaines de millisecondes de latence avec le stockage en pool de capacité. En outre, les systèmes de fichiers répondant aux exigences suivantes fournissent un cache de lecture NVMe afin de réduire les latences de lecture et d'augmenter les IOPS pour les données fréquemment lues :

- Systèmes de fichiers multi-AZ
- Systèmes de fichiers mono-AZ créés après le 28 novembre 2022 avec une capacité de débit d'au moins 2 Gbit/s

Les tableaux suivants indiquent la capacité de débit que les systèmes de fichiers peuvent atteindre en fonction de facteurs tels que le nombre de paires de haute disponibilité (HA) et Régions AWS la disponibilité.

Scale-up

Ces spécifications de performances s'appliquent aux systèmes de fichiers à mise à l'échelle.

Débit maximal du stockage SSD par paire HA pour les systèmes de fichiers évolutifs

	Région USA Est (Ohio), Région USA Est (Virginie du Nord), Région USA Ouest (Oregon) et Europe (Irlande)		Tous les autres sites Régions AWS où FSx for ONTAP est disponible	
	Débit de lecture (Mo/s)	Débit d'écriture (Mo/s)	Débit de lecture (Mo/s)	Débit d'écriture (Mo/s)
Mono-AZ	4 096 *	1 000	2 048	750
Multi-AZ	4 096 *	1 800	2 048	1 300

> **Note**
>
> * Pour fournir une capacité de débit de 4 Gbit/s, votre système de fichiers doit être configuré avec un minimum de 5 120 GiB de capacité de stockage SSD et 160 000 IOPS SSD.

Scale-out

Ces spécifications de performances s'appliquent aux systèmes de fichiers évolutifs.

Débit maximal du stockage SSD par paire HA pour les systèmes de fichiers évolutifs

	Débit de lecture (Mo/s)	Débit d'écriture (Mo/s)
Scale-out mono-AZ	6 144*	1 100*

> **Note**
>
> * Par paire HA (jusqu'à 12). Pour plus d'informations, consultez Paires à haute disponibilité (HA).

Impact de la capacité de stockage sur les performances

Le débit de disque et les niveaux d'IOPS maximaux que votre système de fichiers peut atteindre sont les plus faibles des valeurs suivantes :

- le niveau de performance du disque fourni par vos serveurs de fichiers, en fonction de la capacité de débit que vous sélectionnez pour votre système de fichiers
- le niveau de performance du disque fourni par le nombre d'IOPS SSD que vous allouez à votre système de fichiers

Par défaut, le stockage SSD de votre système de fichiers fournit les niveaux de débit de disque et d'IOPS suivants :

- Débit du disque (Mo/s par TiB de stockage) : 768
- IOPS sur disque (IOPS par TiB de stockage) : 3 072

Impact de la capacité de débit sur les performances

Chaque système de fichiers Amazon FSx possède une capacité de débit que vous configurez lors de sa création. La capacité de débit de votre système de fichiers détermine le niveau de performance des E/S du réseau, c'est-à-dire la vitesse à laquelle chacun des serveurs de fichiers hébergeant votre système de fichiers peut transmettre des données de fichiers sur le réseau aux clients qui y accèdent. Des niveaux de capacité de débit plus élevés s'accompagnent d'une plus grande quantité de mémoire et de stockage NVMe (NVMe) pour la mise en cache des données sur chaque serveur de fichiers, ainsi que de niveaux de performances d'E/S de disque supérieurs pris en charge par chaque serveur de fichiers.

Vous pouvez éventuellement fournir un niveau plus élevé d'IOPS SSD lors de la création de votre système de fichiers. Le niveau maximal d'IOPS SSD que votre système de fichiers peut atteindre est également dicté par la capacité de débit de votre système de fichiers, même lors du provisionnement d'IOPS SSD supplémentaires.

Les tableaux suivants présentent l'ensemble complet des spécifications relatives à la capacité de débit, ainsi que les niveaux de référence et de rafale, ainsi que la quantité de mémoire pour la mise en cache sur le serveur de fichiers dans le fichier correspondant. Régions AWS

Single-AZ (scale-up)

Ces spécifications de performances s'appliquent aux systèmes de fichiers scale-up mono-AZ créés après le 28 novembre 2022 dans les conditions spécifiées. Régions AWS

Spécifications de performance pour les systèmes de fichiers suivants Régions AWS : USA Est (Virginie du Nord), USA Est (Ohio), USA Ouest (Oregon) et Europe (Irlande)

FSxcapacité de débit (Mbits/s)	Capacité de débit du réseau (Mbits/s)		IOPS du réseau	Mise en cache en mémoire (Go)	Mise en cache de lecture NVMe (Go)	Débit du disque (Mbits/s)		IOPS du disque SSD *	
	Base de référence	Éclater				Base de référence	Éclater	Base de référence	Éclater
128	188	1 500	Des dizaines de milliers de données de référence	16	–	128	1 250	6 000	40 000
256	375	1 500		32	–	256	1 250	12 000	40 000
512	750	1 500	Base de référence de centaines de milliers	64	–	512	1 250	20 000	40 000
1,024	1 500	–		128	–	1,024	1 250	40 000	–
2 048	3 125	–		256	1 900	2 048	–	80 000	–
4 096	6 250	–		512	5 400	4 096	–	160 000	–

> **Note**
>
> * Les IOPS de votre SSD ne sont utilisées que lorsque vous accédez à des données qui ne sont pas mises en cache dans le cache en mémoire ou dans le cache NVMe de votre serveur de fichiers.

Ces spécifications de performances s'appliquent aux systèmes de fichiers scale-up mono-AZ dans tous les autres systèmes où Régions AWS FSx for ONTAP est disponible.

Spécifications de performance pour les systèmes de fichiers dans tous les autres pays Régions AWS où FSx for ONTAP est disponible

Capacité de débit FSx (Mo/s)	Capacité de débit du réseau (Mbits/s)		IOPS du réseau	Mise en cache en mémoire (Go)	Débit du disque (Mbits/s)		IOPS du disque SSD *	
	Base de référence	Éclater			Base de référence	Éclater	Base de référence	Éclater
128	150	1 250	Des dizaines de milliers de données de référence	16	128	600	6 000	18 750
256	300	1 250		32	256	600	12 000	18 750
512	625	1 250	Base de référence de centaines	64	512	600	18 750	–
1,024	1 500	–		128	1,024	–	40 000	–
2 048	3 125	–		256	2 048	–	80 000	–

Capacité de débit FSx (Mo/s)	Capacité de débit du réseau (Mbits/s)	IOPS du réseau	Mise en cache en mémoire (Go)	Débit du disque (Mbits/s)	IOPS du disque SSD *
		de milliers			

> **Note**
>
> * Les IOPS de votre SSD ne sont utilisées que lorsque vous accédez à des données qui ne sont pas mises en cache dans le cache en mémoire ou dans le cache NVMe de votre serveur de fichiers.

Single-AZ (scale-out)

Ces spécifications de performances s'appliquent aux systèmes de fichiers évolutifs.

Spécifications de performance pour les systèmes de fichiers évolutifs

Capacité de débit FSx (Mo/s)	Capacité de débit du réseau (Mbits/s)		IOPS du réseau	Mise en cache en mémoire (Go)	Débit du disque (Mbits/s)		IOPS du disque SSD *	
	Base de référence	Éclater			Base de référence	Éclater	Base de référence	Éclater
3 072**	6 250	–	Base de référence de centaines	128	3 072	–	100 000	–
6 144**	12 500	–		256	6 144	–	200 000	–

Capacité de débit FSx (Mo/s)	Capacité de débit du réseau (Mbits/s)	IOPS du réseau de milliers	Mise en cache en mémoire (Go)	Débit du disque (Mbits/s)	IOPS du disque SSD *

> **Note**
>
> * Les IOPS de votre SSD ne sont utilisées que lorsque vous accédez à des données qui ne sont pas mises en cache dans le cache en mémoire ou dans le cache NVMe de votre serveur de fichiers.
> ** Par paire HA (jusqu'à 12). Pour plus d'informations, consultez Paires à haute disponibilité (HA).

Multi-AZ (scale-up)

Ces spécifications de performances s'appliquent aux systèmes de fichiers de mise à l'échelle multi-AZ créés après le 28 novembre 2022 dans les conditions spécifiées. Régions AWS

Spécifications de performance pour les systèmes de fichiers suivants Régions AWS : USA Est (Virginie du Nord), USA Est (Ohio), USA Ouest (Oregon) et Europe (Irlande)

Capacité de débit FSx (Mo/s)	Capacité de débit du réseau (Mbits/s)		IOPS du réseau	Mise en cache en mémoire (Go)	Mise en cache NVMe (Go)	Débit du disque (Mbits/s)		IOPS du disque SSD *	
	Base de référence	Éclater				Base de référence	Éclater	Base de référence	Éclater

Capacité de débit FSx (Mo/s)	Capacité de débit du réseau (Mbits/s)		IOPS du réseau	Mise en cache en mémoire (Go)	Mise en cache NVMe (Go)	Débit du disque (Mbits/s)		IOPS du disque SSD *	
128	188	1 500	Des dizaines de milliers de données de référence	16	238	128	1 250	6 000	40 000
256	375	1 500		32	475	256	1 250	12 000	40 000
512	750	1 500	Base de référence de centaines de milliers	64	950	512	1 250	20 000	40 000
1,024	1 500	–		128	1 900	1,024	1 250	40 000	–
2 048	3 125	–		256	3,800	2 048	–	80 000	–
4 096	6 250	–		512	7 600	4 096	–	160 000	–

> **Note**
>
> * Les IOPS de votre SSD ne sont utilisées que lorsque vous accédez à des données qui ne sont pas mises en cache dans le cache en mémoire ou dans le cache NVMe de votre serveur de fichiers.

Ces spécifications de performances s'appliquent aux systèmes de fichiers à mise à l'échelle multi-AZ dans tous les autres systèmes où Régions AWS FSx for ONTAP est disponible.

Spécifications de performance pour les systèmes de fichiers dans tous les autres pays Régions AWS où FSx for ONTAP est disponible

Capacité de débit FSx (Mo/s)	Capacité de débit du réseau (Mbits/s)		IOPS du réseau	Mise en cache en mémoire (Go)	Mise en cache NVMe (Go)	Débit du disque (Mbits/s)		IOPS du disque SSD *	
	Base de référence	Éclater				Base de référence	Éclater	Base de référence	Éclater
128	150	1 250	Des dizaines de milliers de données de référence	16	150	128	600	6 000	18 750
256	300	1 250		32	300	256	600	12 000	18 750
512	625	1 250	Base de référence de centaines de milliers	64	600	512	600	18 750	–
1,024	1 500	–		128	1 200	1,024	–	40 000	–
2 048	3 125	–		256	2 400	2 048	–	80 000	–

> **Note**
>
> * Les IOPS de votre SSD ne sont utilisées que lorsque vous accédez à des données qui ne sont pas mises en cache dans le cache en mémoire ou dans le cache NVMe de votre serveur de fichiers.

Exemple : capacité de stockage et capacité de débit

L'exemple suivant illustre l'impact de la capacité de stockage et de débit sur les performances du système de fichiers.

Un système de fichiers évolutif configuré avec une capacité de stockage SSD de 2 TiB et une capacité de débit de 512 Mo/s possède les niveaux de débit suivants :

- Débit réseau : 625 Mo/s en ligne de base et 1 250 Mo/s en rafale (voir le tableau des capacités de débit)
- Débit du disque : 512 Mo/s en ligne de base et 600 Mo/s en rafale.

Votre charge de travail accédant au système de fichiers sera donc en mesure de générer un débit de base allant jusqu'à 625 Mo/s et un débit en rafale de 1 250 Mo/s pour les opérations de fichiers effectuées sur des données activement consultées mises en cache dans le cache en mémoire du serveur de fichiers et dans le cache NVMe.

Administration de FSx pour les ressources ONTAP

À l' AWS Management Console aide de la CLI et de l'API ONTAP, vous pouvez effectuer les actions administratives suivantes pour les ressources FSx for ONTAP : AWS CLI

- Création, liste, mise à jour et suppression de systèmes de fichiers, de machines virtuelles de stockage (SVM), de volumes, de sauvegardes et de balises.
- Gestion de l'accès, des comptes administratifs et des mots de passe, des exigences en matière de mots de passe, des protocoles SMB et iSCSI, de l'accessibilité au réseau pour les cibles de montage des systèmes de fichiers existants

Rubriques

Gestion de FSx pour les systèmes de fichiers ONTAP

Un système de fichiers est la principale ressource Amazon FSx, comme un cluster ONTAP sur site. Vous spécifiez la capacité de stockage et le débit du disque SSD (Solid State Drive) pour votre

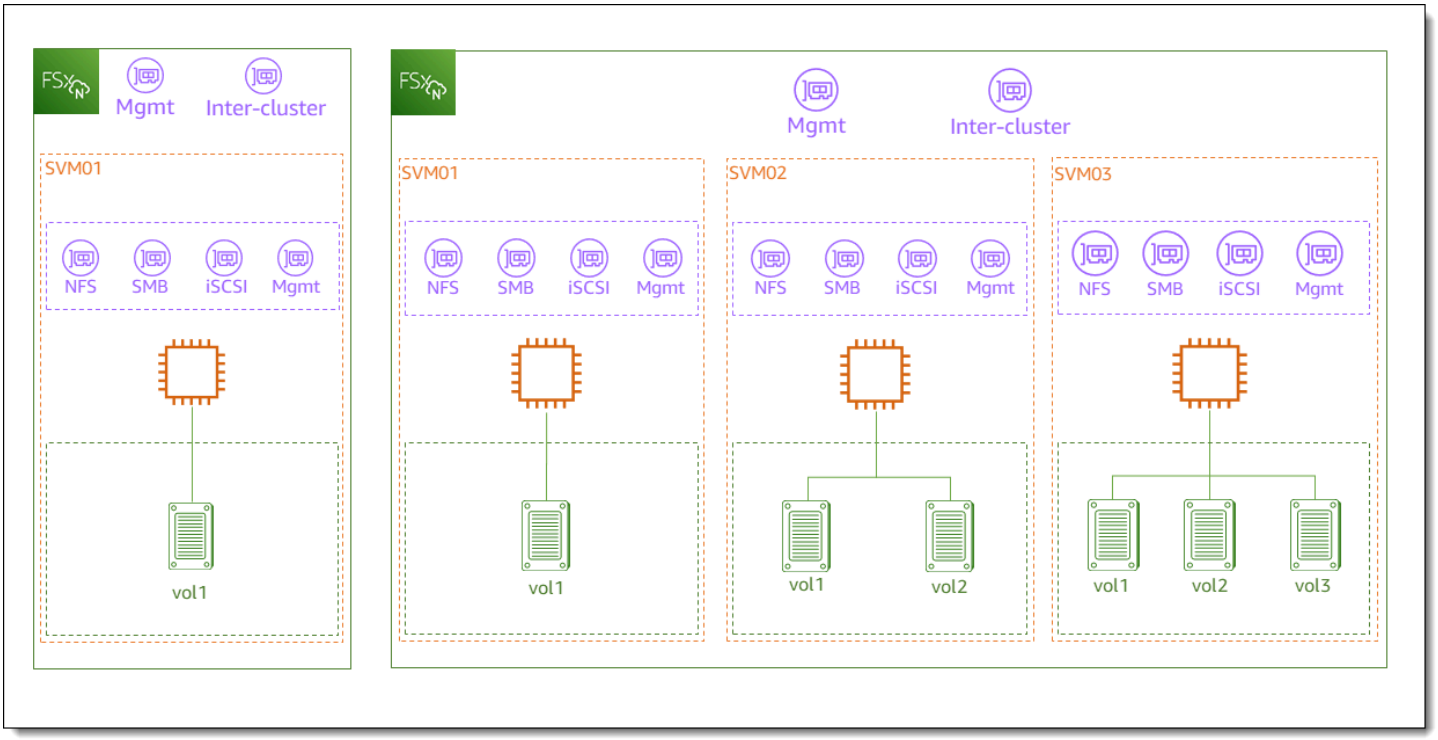
système de fichiers, puis vous choisissez un cloud privé virtuel (VPC) dans lequel créer le système de fichiers. Chaque système de fichiers possède un point de terminaison de gestion que vous pouvez utiliser pour gérer les ressources et les données à l'aide de la CLI ONTAP ou de l'API REST.

Ressources du système de fichiers

Un système de fichiers Amazon FSx for NetApp ONTAP est composé des ressources principales suivantes :

- Le matériel physique du système de fichiers lui-même, qui inclut les serveurs de fichiers et les supports de stockage.
- Une ou plusieurs paires de serveurs de fichiers à haute disponibilité (HA) hébergeant vos machines virtuelles de stockage (SVM). Les systèmes de fichiers scale-up possèdent une paire HA, tandis que les systèmes de fichiers scale-out possèdent au moins deux paires HA. Chaque paire HA possède un pool de stockage appelé agrégat. L'ensemble des agrégats répartis sur toutes les paires HA constitue le niveau de stockage de votre SSD.
- Une ou plusieurs machines virtuelles de stockage (SVM) hébergeant les volumes du système de fichiers et disposant de leurs propres informations d'identification et de gestion des accès.
- Un ou plusieurs volumes qui organisent virtuellement vos données et qui sont montés par vos clients.

L'image suivante illustre l'architecture d'un système de fichiers FSx pour ONTAP évolutif avec une paire HA, ainsi que la relation entre ses ressources principales. Le système de fichiers FSx for ONTAP sur la gauche est le système de fichiers le plus simple, avec une SVM et un volume. Le système de fichiers sur la droite comporte plusieurs SVM, certaines SVM comportant plusieurs volumes. Les systèmes de fichiers et les SVM ont chacun plusieurs points de terminaison de gestion, et les SVM ont également des points de terminaison d'accès aux données.



Lorsque vous créez un système de fichiers FSx for ONTAP, vous définissez les propriétés suivantes :

- Type de déploiement : type de déploiement de votre système de fichiers (multi-AZ ou mono-AZ). Les systèmes de fichiers mono-AZ répliquent vos données et offrent un basculement automatique au sein d'une seule zone de disponibilité, ainsi que des systèmes de fichiers évolutifs. Les systèmes de fichiers multi-AZ offrent une résilience accrue en répliquant également vos données et en prenant en charge le basculement entre plusieurs zones de disponibilité au sein d'une même zone. Région AWS
- Capacité de stockage — Il s'agit de la quantité de stockage SSD, jusqu'à 192 tebioctets (TiB) pour les systèmes de fichiers scale-up et 1 pebioctet (PiB) pour les systèmes de fichiers scale-out.
- IOPS SSD : par défaut, chaque gigaoctet de stockage SSD inclut trois IOPS SSD (jusqu'au maximum pris en charge par la configuration de votre système de fichiers). Vous pouvez éventuellement provisionner des IOPS SSD supplémentaires selon vos besoins.
- Capacité de débit : vitesse soutenue à laquelle le serveur de fichiers peut traiter les données.
- Mise en réseau : VPC et sous-réseaux pour les points de terminaison de gestion et d'accès aux données créés par votre système de fichiers. Pour un système de fichiers multi-AZ, vous définissez également une plage d'adresses IP et des tables de routage.
- Chiffrement : clé AWS Key Management Service (AWS KMS) utilisée pour chiffrer les données du système de fichiers au repos.

- Accès administratif — Vous pouvez spécifier le mot de passe de l'`fsxadmin`utilisateur. Vous pouvez utiliser cet utilisateur pour administrer le système de fichiers à l'aide de la CLI NetApp ONTAP et de l'API REST.

Vous pouvez gérer FSx pour les systèmes de fichiers ONTAP à l'aide de la NetApp CLI ONTAP ou de l'API REST. Vous pouvez également configurer SnapMirror des SnapVault relations entre un système de fichiers Amazon FSx et un autre déploiement ONTAP (y compris un autre système de fichiers Amazon FSx). Chaque système de fichiers FSx for ONTAP possède les points de terminaison suivants qui permettent d'accéder aux applications : NetApp

- Gestion : utilisez ce point de terminaison pour accéder à la CLI NetApp ONTAP via Secure Shell (SSH) ou pour utiliser l'API REST NetApp ONTAP avec votre système de fichiers.
- Intercluster : utilisez ce point de terminaison lors de la configuration de la réplication à l'aide NetApp SnapMirror ou de la mise en cache à l'aide de. NetApp FlexCache

Pour plus d’informations, consultez Gestion des ressources FSx for ONTAP à l'aide d'applications NetApp et Réplication planifiée à l'aide NetApp SnapMirror.

Paires à haute disponibilité (HA)

Chaque système de fichiers FSx for ONTAP est alimenté par une ou plusieurs paires de serveurs de fichiers à haute disponibilité (HA) dans une configuration de veille active. Dans cette configuration, il existe un serveur de fichiers préféré qui gère activement le trafic et un serveur de fichiers secondaire qui prend le relais si le serveur actif n'est pas disponible. Les systèmes de fichiers évolutifs FSx for ONTAP sont alimentés par une paire HA, qui fournit une capacité de débit allant jusqu'à 4 Gbit/s et 160 000 E/S par seconde sur SSD. Les systèmes de fichiers scale-out FSx for ONTAP sont alimentés par un maximum de 12 paires HA, qui peuvent fournir une capacité de débit allant jusqu'à 72 Gbit/s et 2 400 000 IOPS SSD (6 Gbit/s de capacité de débit et 200 000 IOPS SSD par paire HA).

Lorsque vous créez votre système de fichiers à partir de la console Amazon FSx, Amazon FSx recommande le nombre de paires HA que vous devez utiliser en fonction du stockage SSD souhaité. Vous pouvez également choisir manuellement le nombre de paires HA en fonction de votre charge de travail et de vos exigences en matière de performances. Nous vous recommandons d'utiliser une seule paire HA si les exigences de votre système de fichiers sont satisfaites par une capacité de débit maximale de 4 Gbit/s et 160 000 E/S par seconde sur SSD, et plusieurs paires HA si vos charges de travail nécessitent des niveaux d'évolutivité des performances supérieurs.

Chaque paire HA possède un agrégat, qui est un ensemble logique de disques physiques.

> **Note**
>
> Vous ne pouvez pas ajouter de paires HA aux systèmes de fichiers existants. Au lieu de cela, vous pouvez migrer des données entre des systèmes de fichiers (avec différentes paires HA) en utilisant SnapMirror ou en restaurant vos données d'une sauvegarde vers un nouveau système de fichiers. AWS DataSync

Création de FSx pour les systèmes de fichiers ONTAP

Cette section explique comment créer un système de fichiers FSx pour ONTAP à l'aide de la console Amazon FSx ou de AWS CLI l'API Amazon FSx. Vous pouvez créer un système de fichiers dans un cloud privé virtuel (VPC) dont vous êtes le propriétaire ou dans un VPC qu'un autre utilisateur Compte AWS a partagé avec vous. Vous devez tenir compte de certaines considérations lors de la création d'un système de fichiers multi-AZ dans un VPC auquel vous participez. Ces considérations sont expliquées dans cette rubrique.

Par défaut, lorsque vous créez un nouveau système de fichiers à partir de la console Amazon FSx, Amazon FSx crée automatiquement un système de fichiers avec une seule machine virtuelle de stockage (SVM) et un volume, ce qui permet un accès rapide aux données des instances Linux via le protocole NFS (Network File System). Lors de la création du système de fichiers, vous pouvez éventuellement associer la SVM à un Active Directory pour permettre aux clients Windows et macOS d'y accéder via le protocole SMB (Server Message Block). Une fois votre système de fichiers créé, vous pouvez créer des SVM et des volumes supplémentaires selon vos besoins.

Pour créer un système de fichiers (console)

Cette procédure utilise l'option de création standard pour créer un système de fichiers FSx for ONTAP avec une configuration que vous personnalisez en fonction de vos besoins. Pour plus d'informations sur l'utilisation de l'option de création rapide pour créer rapidement un système de fichiers avec un ensemble de paramètres de configuration par défaut, voirÉtape 1 : créer un système de fichiers Amazon FSx pour NetApp ONTAP.

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Sur le tableau de bord, choisissez Créer un système de fichiers.

3. Sur la page Sélectionner le type de système de fichiers, pour les options du système de fichiers, choisissez Amazon FSx for NetApp ONTAP, puis Next.
4. Dans la section Méthode de création, choisissez Création standard.
5. Dans la section Détails du système de fichiers, fournissez les informations suivantes :

   - Dans Nom du système de fichiers - facultatif, entrez le nom de votre système de fichiers. Il est plus facile de trouver et de gérer vos systèmes de fichiers lorsque vous les nommez. Vous pouvez utiliser un maximum de 256 lettres Unicode, espaces blancs et chiffres, plus les caractères spéciaux suivants : + - =. _ :/
   - Pour le type de déploiement, choisissez Multi-AZ ou Single-AZ.
     - Les systèmes de fichiers multi-AZ répliquent vos données et prennent en charge le basculement entre plusieurs zones de disponibilité au même endroit. Région AWS
     - Les systèmes de fichiers mono-AZ répliquent vos données et offrent un basculement automatique au sein d'une seule zone de disponibilité.

     > **Note**
     >
     > Choisissez Single-AZ si vous souhaitez avoir la possibilité de créer un système de fichiers avec au moins deux paires de haute disponibilité (HA) (jusqu'à 12). Pour plus d'informations, consultez Paires à haute disponibilité (HA).

     Pour plus d'informations, consultez Disponibilité et durabilité.
   - Pour la capacité de stockage SSD, entrez la capacité de stockage de votre système de fichiers, en gibioctets (GiB). Entrez un nombre entier compris entre 1 024 et 1 048 576 GiB (jusqu'à 1 pébioctet [PiB]).

     Vous pouvez augmenter la capacité de stockage selon vos besoins à tout moment après avoir créé le système de fichiers. Pour plus d'informations, consultez Gestion de la capacité de stockage.
   - Pour les IOPS de SSD provisionnés, vous avez deux options pour configurer le nombre d'IOPS pour votre système de fichiers :
     - Choisissez Automatique (valeur par défaut) si vous souhaitez qu'Amazon FSx provisionne automatiquement 3 IOPS par GiB de stockage SSD.
     - Choisissez Provisionné par l'utilisateur si vous souhaitez spécifier le nombre d'IOPS. Vous pouvez provisionner un maximum de 200 000 IOPS sur SSD par système de fichiers.

> **Note**
>
> Vous pouvez augmenter les IOPS de votre SSD provisionné après avoir créé le système de fichiers. N'oubliez pas que le niveau maximal d'IOPS sur SSD que votre système de fichiers peut atteindre dépend également de la capacité de débit de votre système de fichiers, même lors du provisionnement d'IOPS supplémentaires sur SSD. Pour plus d'informations, consultez Impact de la capacité de débit sur les performances et Gestion de la capacité de stockage.

- Pour ce qui est de la capacité de débit, deux options s'offrent à vous pour déterminer votre capacité de débit en mégaoctets par seconde (Mo/s) :
  - Choisissez Capacité de débit recommandée si vous souhaitez qu'Amazon FSx choisisse automatiquement la capacité de débit en fonction de la quantité de capacité de stockage que vous avez choisie.
  - Choisissez Spécifier la capacité de débit si vous souhaitez spécifier le montant de la capacité de débit. Si vous choisissez cette option, une liste déroulante de capacité de débit apparaît et est renseignée en fonction du type de déploiement que vous avez choisi. Vous pouvez également choisir le nombre de paires HA (jusqu'à 12). Pour plus d'informations, consultez Paires à haute disponibilité (HA).

  La capacité de débit est la vitesse soutenue à laquelle le serveur de fichiers hébergeant votre système de fichiers peut traiter les données. Pour plus d'informations, consultez Amazon FSx pour NetApp les performances d'ONTAP.

6. Dans la section Mise en réseau, fournissez les informations suivantes :

   - Pour Virtual Private Cloud (VPC), choisissez le VPC que vous souhaitez associer à votre système de fichiers.
   - Pour les groupes de sécurité VPC, vous pouvez choisir un groupe de sécurité à associer à l'interface réseau de votre système de fichiers. Si vous n'en spécifiez aucun, Amazon FSx associera le groupe de sécurité par défaut du VPC à votre système de fichiers.
   - Spécifiez un sous-réseau pour votre serveur de fichiers. Si vous créez un système de fichiers multi-AZ, choisissez également un sous-réseau de secours pour le serveur de fichiers de secours.
   - (Multi-AZ uniquement) Pour les tables de routage VPC, spécifiez les tables de routage VPC pour créer les points de terminaison de votre système de fichiers. Sélectionnez toutes les

tables de routage VPC associées aux sous-réseaux dans lesquels se trouvent vos clients. Par défaut, Amazon FSx sélectionne la table de routage par défaut de votre VPC. Pour plus d'informations, consultez Accès aux données depuis l'extérieur du VPC de déploiement.

> **Note**
>
> Amazon FSx gère ces tables de routage pour les systèmes de fichiers multi-AZ à l'aide d'une authentification basée sur des balises. Ces tables de routage sont étiquetées avec`Key: AmazonFSx; Value: ManagedByAmazonFSx`. Lors de la création de FSx pour les systèmes de fichiers ONTAP Multi-AZ à l'aide de AWS CloudFormation nous vous recommandons d'ajouter la balise manuellement. `Key: AmazonFSx; Value: ManagedByAmazonFSx`

- (Multi-AZ uniquement) La plage d'adresses IP du point de terminaison indique la plage d'adresses IP dans laquelle sont créés les points de terminaison permettant d'accéder à votre système de fichiers.

  Trois options s'offrent à vous pour la plage d'adresses IP du point de terminaison :

  - Plage d'adresses IP non allouée provenant de votre VPC : Amazon FSx choisit les 64 dernières adresses IP de la plage d'adresses CIDR principale du VPC à utiliser comme plage d'adresses IP de point de terminaison pour le système de fichiers. Cette plage est partagée entre plusieurs systèmes de fichiers si vous sélectionnez cette option plusieurs fois.

    > **Note**
    >
    > Cette option est grisée si l'une des 64 dernières adresses IP de la plage CIDR principale d'un VPC est utilisée par un sous-réseau. Dans ce cas, vous pouvez toujours choisir une plage d'adresses intégrée au VPC (c'est-à-dire une plage qui ne se trouve pas à la fin de votre plage d'adresses CIDR principale ou une plage qui se trouve dans une plage d'adresses CIDR secondaire de votre VPC) en choisissant l'option Entrer une plage d'adresses IP.

  - Pour Sous-réseau préféré, spécifiez un sous-réseau pour votre serveur de fichiers. Si vous créez un système de fichiers multi-AZ, choisissez également un sous-réseau de secours pour le serveur de fichiers de secours.

- (Multi-AZ uniquement) Pour les tables de routage VPC, spécifiez les tables de routage VPC pour créer les points de terminaison de votre système de fichiers. Sélectionnez toutes les tables de routage VPC associées aux sous-réseaux dans lesquels se trouvent vos clients. Par défaut, Amazon FSx sélectionne la table de routage par défaut de votre VPC.
- (Multi-AZ uniquement) La plage d'adresses IP du point de terminaison indique la plage d'adresses IP dans laquelle sont créés les points de terminaison permettant d'accéder à votre système de fichiers.

  Trois options s'offrent à vous pour la plage d'adresses IP du point de terminaison :

  - Plage d'adresses IP non allouée provenant de votre VPC : Amazon FSx choisit les 64 dernières adresses IP de la plage d'adresses CIDR principale du VPC à utiliser comme plage d'adresses IP de point de terminaison pour le système de fichiers. Cette plage est partagée entre plusieurs systèmes de fichiers si vous sélectionnez cette option plusieurs fois.

    > **Note**
    >
    > Cette option est grisée si l'une des 64 dernières adresses IP de la plage CIDR principale d'un VPC est utilisée par un sous-réseau. Dans ce cas, vous pouvez toujours choisir une plage d'adresses intégrée au VPC (c'est-à-dire une plage qui ne se trouve pas à la fin de votre plage d'adresses CIDR principale ou une plage qui se trouve dans une plage d'adresses CIDR secondaire de votre VPC) en choisissant l'option Entrer une plage d'adresses IP.

  - Plage d'adresses IP flottante en dehors de votre VPC : Amazon FSx choisit une plage d'adresses 198.19.x.0/24 qui n'est pas déjà utilisée par d'autres systèmes de fichiers dotés du même VPC et des mêmes tables de routage.
  - Entrez une plage d'adresses IP — Vous pouvez fournir une plage d'adresses CIDR de votre choix. La plage d'adresses IP que vous choisissez peut se trouver à l'intérieur ou à l'extérieur de la plage d'adresses IP du VPC, à condition qu'elle ne chevauche aucun sous-réseau.

    > **Note**
    >
    > Ne choisissez aucune plage comprise dans les plages CIDR suivantes, car elles sont incompatibles avec FSx for ONTAP :
    >
    > - 0.0.0,0/8

- 127,0.0.0/8
- 198,19,0,0/20
- 224,0.0.0/4
- 240,0,0,0/4
- 255,255,255,255/32

7. Dans la section Sécurité et chiffrement, pour Clé de chiffrement, choisissez la clé de chiffrement AWS Key Management Service (AWS KMS) qui protège les données inactives de votre système de fichiers.
8. Pour le mot de passe administratif du système de fichiers, entrez un mot de passe sécurisé pour l'`fsxadmin`utilisateur. Confirmez le mot de passe.

   Vous pouvez utiliser l'`fsxadmin`utilisateur pour administrer votre système de fichiers à l'aide de la CLI ONTAP et de l'API REST. Pour plus d'informations sur l'`fsxadmin`utilisateur, consultezGestion des systèmes de fichiers à l'aide de la ONTAP CLI.
9. Dans la section Configuration de la machine virtuelle de stockage par défaut, fournissez les informations suivantes :

   - Dans le champ Nom de la machine virtuelle de stockage, indiquez le nom de la machine virtuelle de stockage. Vous pouvez utiliser un maximum de 47 caractères alphanumériques, plus le caractère spécial de soulignement (_).
   - Pour le mot de passe administratif de la SVM, vous pouvez éventuellement choisir Spécifier un mot de passe et fournir un mot de passe pour l'utilisateur de `vsadmin` la SVM. Vous pouvez utiliser l'`vsadmin`utilisateur pour administrer la SVM à l'aide de la CLI ONTAP ou de l'API REST. Pour plus d'informations sur l'`vsadmin`utilisateur, consultezGestion des SVM à l'aide de la CLI ONTAP.

     Si vous choisissez Ne pas spécifier de mot de passe (valeur par défaut), vous pouvez toujours utiliser l'`fsxadmin`utilisateur du système de fichiers pour gérer votre système de fichiers à l'aide de la CLI ONTAP ou de l'API REST, mais vous ne pouvez pas utiliser `vsadmin` l'utilisateur de votre SVM pour faire de même.
   - Dans la section Active Directory, vous pouvez associer un Active Directory à la SVM. Pour plus d'informations, consultez Utilisation de Microsoft Active Directory dans FSx pour ONTAP.

     Si vous ne souhaitez pas associer votre SVM à un Active Directory, choisissez Ne pas joindre un Active Directory.

Si vous souhaitez associer votre SVM à un domaine Active Directory autogéré, choisissez Join an Active Directory et fournissez les informations suivantes pour votre Active Directory :

- Nom NetBIOS de l'objet informatique Active Directory à créer pour votre SVM. Le nom NetBIOS ne peut pas dépasser 15 caractères.
- Le nom de domaine complet de votre Active Directory. Le nom de domaine ne peut pas dépasser 255 caractères.
- Adresses IP des serveurs DNS : adresses IPv4 des serveurs DNS (Domain Name System) de votre domaine.
- Nom d'utilisateur du compte de service : nom d'utilisateur du compte de service dans votre Active Directory existant. N'incluez pas de préfixe ou de suffixe de domaine.
- Mot de passe du compte de service : mot de passe du compte de service.
- Confirmer le mot de passe : mot de passe du compte de service.
- (Facultatif) Unité organisationnelle (UO) : nom du chemin unique de l'unité organisationnelle à laquelle vous souhaitez joindre votre système de fichiers.
- Groupe d'administrateurs de systèmes de fichiers délégués : nom du groupe de votre Active Directory qui peut administrer votre système de fichiers.

  Si vous en utilisez AWS Managed Microsoft AD, vous devez spécifier un groupe tel que les administrateurs FSx AWS délégués, les administrateurs AWS délégués ou un groupe personnalisé doté d'autorisations déléguées sur l'unité d'organisation.

  Si vous adhérez à un AD autogéré, utilisez le nom du groupe dans votre AD. Le groupe par défaut est`Domain Admins`.

10. Dans la section Configuration du volume par défaut, fournissez les informations suivantes pour le volume par défaut créé avec votre système de fichiers :

    - Dans le champ Nom du volume, saisissez le nom du volume. Vous pouvez utiliser jusqu'à 203 caractères alphanumériques ou soulignés (_).
    - (Systèmes de fichiers évolutifs uniquement) Pour le style de volume, choisissez FlexVolsoit FlexGroup. FlexVolles volumes sont des volumes à usage général dont la taille peut atteindre 300 TiB. FlexGrouples volumes sont destinés à des charges de travail à hautes performances et peuvent atteindre une taille de 20 PiB.
    - Pour Taille du volume, entrez un nombre entier compris entre 800 Go (GiB) et 2 000 pebioctets (PiB).

- Pour le type de volume, choisissez Read-Write (RW) pour créer un volume lisible et inscriptible ou Data Protection (DP) pour créer un volume en lecture seule pouvant être utilisé comme destination d'une relation or. NetApp SnapMirror SnapVault Pour plus d'informations, consultez Types de volume.
- Pour le chemin de jonction, entrez un emplacement dans le système de fichiers pour monter le volume. Le nom doit être précédé d'une barre oblique, par exemple `/vol3`.
- Pour l'efficacité du stockage, choisissez Activé pour activer les fonctionnalités d'efficacité du stockage ONTAP (déduplication, compression et compactage). Pour plus d'informations, consultez FSx pour l'efficacité du stockage ONTAP.
- Pour le style de sécurité du volume, choisissez entre Unix (Linux), NTFS et Mixed pour le volume. Pour plus d'informations, consultez Style de sécurité des volumes.
- Pour la politique de capture instantanée, choisissez une politique de capture instantanée pour le volume. Pour plus d'informations sur les politiques relatives aux instantanés, consultezRègles relatives aux snapshots.

  Si vous choisissez Politique personnalisée, vous devez spécifier le nom de la politique dans le champ Politique personnalisée. La politique personnalisée doit déjà exister sur la SVM ou dans le système de fichiers. Vous pouvez créer une politique de capture personnalisée à l'aide de la CLI ONTAP ou de l'API REST. Pour plus d'informations, consultez la section Création d'une politique de capture instantanée dans la documentation du produit NetApp ONTAP.

11. Dans la section Hiérarchisation du stockage du volume par défaut, pour la politique de hiérarchisation du pool de capacité, choisissez la politique de hiérarchisation du pool de stockage pour le volume, qui peut être Auto (valeur par défaut), Snapshot uniquement, Tout ou Aucune. Pour plus d'informations sur les politiques de hiérarchisation des pools de capacités, consultezPolitiques de hiérarchisation des volumes.

    Pour la période de refroidissement de la politique de hiérarchisation, si vous avez défini la hiérarchisation du stockage sur l'une ou l'autre des valeurs `Auto` et `Snapshot-only` policies.valid sont comprises entre 2 et 183 jours. La période de refroidissement de la politique de hiérarchisation d'un volume définit le nombre de jours avant que les données auxquelles il n'est pas possible d'accéder soient signalées comme froides et transférées vers le stockage en pool de capacité.

12. Dans Backup and maintenance (facultatif), vous pouvez définir les options suivantes :

    - Pour la sauvegarde automatique quotidienne, choisissez Activé pour les sauvegardes quotidiennes automatiques. Cette option est activée par défaut.

- Pour la fenêtre de sauvegarde automatique quotidienne, définissez l'heure en temps universel coordonné (UTC) à laquelle vous souhaitez que la fenêtre de sauvegarde automatique quotidienne commence. La fenêtre est de 30 minutes à partir de cette heure spécifiée. Cette fenêtre ne peut pas chevaucher la fenêtre de sauvegarde hebdomadaire pour la maintenance.
- Pour la période de conservation automatique des sauvegardes, définissez une période comprise entre 1 et 90 jours pendant laquelle vous souhaitez conserver les sauvegardes automatiques.
- Pour la fenêtre de maintenance hebdomadaire, vous pouvez définir l'heure de la semaine à laquelle vous souhaitez que la fenêtre de maintenance commence. Le jour 1 est le lundi, le 2 est le mardi, et ainsi de suite. La fenêtre est de 30 minutes à partir de cette heure spécifiée. Cette fenêtre ne peut pas être superposée à la fenêtre de sauvegarde automatique quotidienne.

13. Pour les balises (facultatif), vous pouvez saisir une clé et une valeur pour ajouter des balises à votre système de fichiers. Une balise est une paire clé-valeur distinguant majuscules et minuscules qui vous permet de gérer, de filtrer et de rechercher votre système de fichiers.

    Choisissez Suivant.

14. Vérifiez la configuration du système de fichiers qui s'affiche sur la page Create file system (Créer un système de fichiers). À titre de référence, notez les paramètres du système de fichiers que vous pouvez modifier une fois le système de fichiers créé.
15. Choisissez Create file system (Créer un système de fichiers).

Pour créer un système de fichiers (CLI)

- Pour créer un système de fichiers FSx for ONTAP, utilisez la commande CLI create-file-system (ou l'opération équivalente de l'API CreateFilesystème), comme indiqué dans l'exemple suivant.

```
aws fsx create-file-system \
    --file-system-type ONTAP \
    --storage-capacity 1024 \
    --storage-type SSD \
    --security-group-ids security-group-id \

    --subnet-ids subnet-abcdef1234567890b subnet-abcdef1234567890c \
    --ontap-configuration DeploymentType=MULTI_AZ_1,
        ThroughputCapacity=512,PreferredSubnetId=subnet-abcdef1234567890b
```

Une fois le système de fichiers créé avec succès, Amazon FSx renvoie la description du système de fichiers au format JSON, comme indiqué dans l'exemple suivant.


```
{
  "FileSystem": {
    "OwnerId": "111122223333",
    "CreationTime": 1625066825.306,
    "FileSystemId": "fs-0123456789abcdef0",
    "FileSystemType": "ONTAP",
    "Lifecycle": "CREATING",
    "StorageCapacity": 1024,
    "StorageType": "SSD",
    "VpcId": "vpc-11223344556677aab",
    "SubnetIds": [
      "subnet-abcdef1234567890b",
      "subnet-abcdef1234567890c"
    ],
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "ResourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/
fs-0123456789abcdef0",
    "Tags": [],
    "OntapConfiguration": {
      "DeploymentType": "MULTI_AZ_HA_1",
      "EndpointIpAddressRange": "198.19.0.0/24",
      "Endpoints": {
        "Management": {
          "DnsName": "management.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        },
        "Intercluster": {
          "DnsName": "intercluster.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        }
      },
      "DiskIopsConfiguration": {
                "Mode": "AUTOMATIC",
                "Iops": 3072
      },
      "PreferredSubnetId": "subnet-abcdef1234567890b",
      "RouteTableIds": [
        "rtb-abcdef1234567890e",
        "rtb-abcd1234ef567890b"
      ],
      "ThroughputCapacity": 512,
```

```
      "WeeklyMaintenanceStartTime": "4:10:00"
    }
  }
}
```

> **Note**
>
> Contrairement au processus de création d'un système de fichiers dans la console, la commande `create-file-system` CLI et le fonctionnement de l'`CreateFileSystem`API ne créent pas de SVM ou de volume par défaut. Pour créer une SVM, voir Création d'une machine virtuelle de stockage ; pour créer un volume, voirCréation de volumes.

Création de systèmes de fichiers FSx pour ONTAP dans des sous-réseaux partagés

Le partage VPC permet Comptes AWS à plusieurs de créer des ressources dans des clouds privés virtuels (VPC) partagés et gérés de manière centralisée. Dans ce modèle, le compte propriétaire du VPC (propriétaire) partage un ou plusieurs sous-réseaux avec d'autres comptes (participants) appartenant à la même organisation. AWS Organizations

Les comptes participants peuvent créer des systèmes de fichiers FSx pour ONTAP mono-AZ ou multi-AZ dans un sous-réseau VPC que le compte propriétaire a partagé avec eux. Pour qu'un compte participant puisse créer un système de fichiers multi-AZ, le compte propriétaire doit également autoriser Amazon FSx à modifier les tables de routage dans les sous-réseaux partagés au nom du compte participant. Pour plus d’informations, consultez Gestion du support VPC partagé pour les systèmes de fichiers multi-AZ.

> **Note**
>
> Il est de la responsabilité du compte du participant de se coordonner avec le propriétaire du VPC afin d'empêcher la création de sous-réseaux VPC ultérieurs qui chevaucheraient le CIDR intégré au VPC des systèmes de fichiers du participant. Si les sous-réseaux se chevauchent, le trafic vers le système de fichiers peut être interrompu.

Exigences et considérations requises pour les sous-réseaux partagés

Lorsque vous créez des systèmes de fichiers FSx for ONTAP dans des sous-réseaux partagés, tenez compte des points suivants :

- Le propriétaire du sous-réseau VPC doit partager un sous-réseau avec un compte participant avant que ce compte puisse y créer un système de fichiers FSx for ONTAP.
- Vous ne pouvez pas lancer de ressources en utilisant le groupe de sécurité par défaut du VPC, car il appartient au propriétaire. En outre, les comptes de participants ne peuvent pas lancer de ressources à l'aide de groupes de sécurité appartenant à d'autres participants ou au propriétaire.
- Dans un sous-réseau partagé, le participant et le propriétaire contrôlent séparément les groupes de sécurité au sein de leur compte respectif. Le compte propriétaire peut voir les groupes de sécurité créés par les participants, mais ne peut effectuer aucune action sur ceux-ci. Si le compte propriétaire souhaite supprimer ou modifier ces groupes de sécurité, le participant qui a créé le groupe de sécurité doit prendre les mesures nécessaires.
- Les comptes participants peuvent afficher, créer, modifier et supprimer des systèmes de fichiers mono-AZ et leurs ressources associées dans des sous-réseaux que le compte propriétaire a partagés avec eux.
- Les comptes participants peuvent créer, afficher, modifier et supprimer des systèmes de fichiers multi-AZ et leurs ressources associées dans des sous-réseaux que le compte propriétaire a partagés avec eux. En outre, le compte propriétaire doit également accorder au service Amazon FSx les autorisations nécessaires pour modifier les tables de routage dans les sous-réseaux partagés au nom du compte du participant. Pour plus d'informations, consultez Gestion du support VPC partagé pour les systèmes de fichiers multi-AZ.
- Le propriétaire du VPC partagé ne peut pas afficher, modifier ou supprimer les ressources créées par un participant dans le sous-réseau partagé. Cela s'ajoute aux ressources VPC auxquelles chaque compte a un accès différent. Pour plus d'informations, consultez la section Responsabilités et autorisations des propriétaires et des participants dans le guide de l'utilisateur Amazon VPC.

Pour plus d'informations, consultez Partager votre VPC avec d'autres comptes dans le guide de l'utilisateur Amazon VPC.

Lors du partage d'un sous-réseau VPC

Lorsque vous partagez vos sous-réseaux avec des comptes participants qui créeront des systèmes de fichiers FSx pour ONTAP dans les sous-réseaux partagés, vous devez effectuer les opérations suivantes :

- Le propriétaire du VPC doit l'utiliser pour partager en toute sécurité AWS Resource Access Manager des VPC et des sous-réseaux avec d'autres. Comptes AWS Pour plus d'informations, consultez la section Partage de vos AWS ressources dans le guide de AWS Resource Access Manager l'utilisateur.
- Le propriétaire du VPC doit partager un ou plusieurs VPC avec un compte participant. Pour plus d'informations, consultez Partager votre VPC avec d'autres comptes dans le guide de l'utilisateur d'Amazon Virtual Private Cloud.
- Pour que les comptes participants puissent créer des systèmes de fichiers FSx for ONTAP Multi-AZ, le propriétaire du VPC doit également accorder au service Amazon FSx les autorisations nécessaires pour créer et modifier des tables de routage dans les sous-réseaux partagés au nom des comptes participants. Cela est dû au fait que les systèmes de fichiers multi-AZ FSx for ONTAP utilisent des adresses IP flottantes afin que les clients connectés puissent effectuer une transition fluide entre le serveur de fichiers préféré et le serveur de secours lors d'un événement de basculement. Lorsqu'un événement de basculement se produit, Amazon FSx met à jour toutes les routes de toutes les tables de routage associées au système de fichiers pour qu'elles pointent vers le serveur de fichiers actuellement actif.

Gestion du support VPC partagé pour les systèmes de fichiers multi-AZ

Les comptes propriétaires peuvent déterminer si les comptes participants peuvent ou non créer des systèmes de fichiers FSx pour ONTAP multi-AZ dans des sous-réseaux VPC que le propriétaire a partagés avec les participants à l'aide de l'API,, et de l'API AWS CLI, comme décrit dans AWS Management Console les sections suivantes.

Pour gérer le partage VPC pour les systèmes de fichiers multi-AZ (console)

Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.

1. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
2. Localisez les paramètres VPC partagés Multi-AZ sur la page Paramètres.

    - Pour activer le partage VPC pour les systèmes de fichiers multi-AZ dans les sous-réseaux VPC que vous partagez, choisissez Activer les mises à jour des tables de routage depuis les comptes des participants.
    - Pour désactiver le partage VPC pour les systèmes de fichiers multi-AZ dans tous les VPC que vous possédez, choisissez Désactiver les mises à jour des tables de routage depuis les comptes des participants. L'écran de confirmation s'affiche.

> **Important**
>
> Nous recommandons vivement de supprimer les systèmes de fichiers multi-AZ créés par les participants dans le VPC partagé avant de désactiver cette fonctionnalité. Une fois la fonctionnalité désactivée, ces systèmes de fichiers entrent dans un `MISCONFIGURED` état et risquent de devenir indisponibles.

3. Entrez **`confirm`** et choisissez Confirmer pour désactiver la fonctionnalité.

Pour gérer le partage VPC pour les systèmes de fichiers multi-AZ ()AWS CLI

1. Pour afficher le paramètre actuel du partage VPC multi-AZ, utilisez la commande CLI describe-shared-vpc-configuration, ou la commande API équivalente, illustrée ci-dessous : DescribeSharedVpcConfiguration

   ```
   $ aws fsx describe-shared-vpc-configuration
   ```

   Le service répond à une demande acceptée comme suit :

   ```
   {
       "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
   }
   ```

2. Pour gérer la configuration VPC partagée multi-AZ, utilisez la commande CLI update-shared-vpc-configuration ou la commande API équivalente. UpdateSharedVpcConfiguration L'exemple suivant active le partage VPC pour les systèmes de fichiers multi-AZ.

   ```
   $ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts true
   ```

   Le service répond à une demande acceptée comme suit :

   ```
   {
       "EnableFsxRouteTableUpdatesFromParticipantAccounts": "true"
   }
   ```

3. Pour désactiver cette fonctionnalité, `EnableFsxRouteTableUpdatesFromParticipantAccounts` réglez-la sur`false`, comme indiqué dans l'exemple suivant.

```
$ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-
participant-accounts false
```

Le service répond à une demande acceptée comme suit :

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
}
```

Mettre à jour un système de fichiers

Cette rubrique décrit les propriétés d'un système de fichiers existant que vous pouvez mettre à jour, ainsi que les procédures permettant de le faire à l'aide de la console et de la CLI.

Vous pouvez mettre à jour les propriétés du système de fichiers FSx for ONTAP suivantes à l'aide de la console Amazon FSx, de l'API Amazon FSx et de AWS CLI l'API Amazon FSx :

- Sauvegardes quotidiennes automatiques. Active ou désactive les sauvegardes quotidiennes automatiques, modifie la fenêtre de sauvegarde et la période de conservation des sauvegardes. Pour plus d'informations sur les sauvegardes, consultez Utilisation de sauvegardes quotidiennes automatiques.
- Fenêtre de maintenance hebdomadaire. Définit le jour de la semaine et l'heure auxquels Amazon FSx effectue la maintenance et les mises à jour du système de fichiers. Pour plus d'informations sur la fenêtre de maintenance, consultezOptimisation des performances avec les fenêtres de maintenance Amazon FSx.
- Mot de passe administratif du système de fichiers. Modifie le mot de passe de l'`fsxadmin`utilisateur du système de fichiers. Vous pouvez utiliser l'`fsxadmin`utilisateur pour administrer votre système de fichiers à l'aide de la CLI ONTAP et de l'API REST. Pour plus d'informations sur l'`fsxadmin`utilisateur, consultezGestion des systèmes de fichiers à l'aide de la ONTAP CLI.
- Tables de routage Amazon VPC. Avec Multi-AZ FSx pour les systèmes de fichiers ONTAP, les points de terminaison que vous utilisez pour accéder aux données via NFS ou SMB et les points de

terminaison de gestion pour accéder à la CLI ONTAP, à l'API et à BlueXP utilisent des adresses IP flottantes dans les tables de routage Amazon VPC que vous associez à votre système de fichiers. Vous pouvez associer les nouvelles tables de routage que vous créez à vos systèmes de fichiers multi-AZ existants, ce qui vous permet de configurer quels clients peuvent accéder à vos données même si votre réseau évolue. Vous pouvez également dissocier (supprimer) les tables de routage existantes de votre système de fichiers.

> **Note**
>
> Amazon FSx gère les tables de routage VPC pour les systèmes de fichiers multi-AZ à l'aide d'une authentification basée sur des balises. Ces tables de routage sont étiquetées avec`Key: AmazonFSx; Value: ManagedByAmazonFSx`. Lorsque vous créez ou mettez à jour des systèmes de fichiers multi-AZ FSx pour ONTAP, AWS CloudFormation nous vous recommandons d'ajouter la balise manuellement. `Key: AmazonFSx; Value: ManagedByAmazonFSx`

Pour mettre à jour un système de fichiers (console)

Les procédures suivantes fournissent des instructions sur la manière de mettre à jour un système de fichiers FSx for ONTAP existant à l'aide du. AWS Management Console

Pour mettre à jour les sauvegardes quotidiennes automatiques

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Pour afficher la page de détails du système de fichiers, dans le volet de navigation de gauche, sélectionnez Systèmes de fichiers, puis choisissez le système de fichiers FSx for ONTAP que vous souhaitez mettre à jour.
3. Choisissez l'onglet Sauvegardes dans le deuxième panneau de la page.
4. Choisissez Mettre à jour.
5. Modifiez les paramètres de sauvegarde quotidienne automatique pour ce système de fichiers.
6. Choisissez Save pour enregistrer les changements.

Pour mettre à jour le créneau de maintenance hebdomadaire

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.

2. Pour afficher la page de détails du système de fichiers, dans le volet de navigation de gauche, sélectionnez Systèmes de fichiers, puis choisissez le système de fichiers FSx for ONTAP que vous souhaitez mettre à jour.
3. Choisissez l'onglet Administration dans le deuxième panneau de la page.
4. Dans le volet Maintenance, sélectionnez Mettre à jour.
5. Modifiez le moment où la fenêtre de maintenance hebdomadaire arrive pour ce système de fichiers.
6. Choisissez Save pour enregistrer les changements.

Pour modifier le mot de passe administratif du système de fichiers

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Pour afficher la page de détails du système de fichiers, dans le volet de navigation de gauche, sélectionnez Systèmes de fichiers, puis choisissez le système de fichiers FSx for ONTAP que vous souhaitez mettre à jour.
3. Choisissez l'onglet Administration.
4. Dans le volet d'administration ONTAP, choisissez Mettre à jour sous le mot de passe administrateur ONTAP.
5. Dans la boîte de dialogue Mettre à jour les informations d'identification de l'administrateur ONTAP, entrez un nouveau mot de passe dans le champ du mot de passe administratif ONTAP.
6. Utilisez le champ Confirmer le mot de passe pour confirmer le mot de passe.
7. Choisissez Mettre à jour les informations d'identification pour enregistrer votre modification.

> **Note**
>
> Si vous recevez un message d'erreur indiquant que le nouveau mot de passe ne répond pas aux exigences du mot de passe, vous pouvez utiliser la commande `security login role config show`ONTAPCLI pour afficher les paramètres du mot de passe requis sur le système de fichiers. Pour plus d'informations, notamment pour savoir comment modifier le paramètre du mot de passe, consultezLa mise à jour du mot de passe du `fsxadmin` compte échoue.

Pour mettre à jour les tables de routage VPC sur les systèmes de fichiers multi-AZ

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Pour afficher la page de détails du système de fichiers, dans le volet de navigation de gauche, sélectionnez Systèmes de fichiers, puis choisissez le système de fichiers FSx for ONTAP que vous souhaitez mettre à jour.
3. Pour Actions, choisissez Gérer les tables de routage. Cette option n'est disponible que pour les systèmes de fichiers multi-AZ.
4. Dans la boîte de dialogue Gérer les tables de routage, effectuez l'une des opérations suivantes :
   - Pour associer une nouvelle table de routage VPC, sélectionnez une table de routage dans la liste déroulante Associer de nouvelles tables de routage, puis choisissez Associer.
   - Pour dissocier une table de routage VPC existante, sélectionnez une table de routage dans le volet Tables de routage actuelles, puis choisissez Dissocier.
5. Choisissez Fermer.

Pour mettre à jour un système de fichiers (CLI)

La procédure suivante montre comment mettre à jour un système de fichiers FSx for ONTAP existant à l'aide du. AWS CLI

1. Pour mettre à jour la configuration d'un système de fichiers FSx for ONTAP, utilisez la commande CLI update-file-system (ou l'opération équivalente de l'API UpdateFilesystème), comme indiqué dans l'exemple suivant.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration
 AutomaticBackupRetentionDays=30,DailyAutomaticBackupStartTime=01:00, \
      WeeklyMaintenanceStartTime=1:01:30,AddRouteTableIds=rtb-0123abcd, \
      FsxAdminPassword=new-fsx-admin-password
```

2. Pour désactiver les sauvegardes quotidiennes automatiques, définissez la `AutomaticBackupRetentionDays` propriété sur 0.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration AutomaticBackupRetentionDays=0
```

Suppression d’un système de fichiers

Vous pouvez supprimer un système de fichiers FSx for ONTAP à l'aide de la console Amazon FSx, de AWS CLI l'API et des SDK Amazon FSx.

Pour supprimer un système de fichiers :

- Utilisation de la console : suivez la procédure décrite dansÉtape 3 : Nettoyer les ressources.
- À l'aide de la CLI ou de l'API : supprimez d'abord tous les volumes et SVM de votre système de fichiers. Utilisez ensuite la commande delete-file-system CLI ou DeleteFilel'opération System API.

Affichage des détails du système de fichiers

Vous pouvez consulter les informations de configuration détaillées de votre système de fichiers FSx for ONTAP à l'aide de la console Amazon FSx, de l'API et des SDK AWS CLI pris en charge. AWS

Pour afficher des informations détaillées sur le système de fichiers, procédez comme suit :

- Utilisation de la console : choisissez un système de fichiers pour afficher la page détaillée des systèmes de fichiers. Le panneau Résumé indique l'ID du système de fichiers, l'état du cycle de vie, le type de déploiement, la capacité de stockage SSD, la capacité de débit, les IOPS provisionnées, les zones de disponibilité et l'heure de création.

  Les onglets suivants fournissent des informations de configuration détaillées et permettent de modifier les propriétés qui peuvent être modifiées :
  - Réseau et sécurité
  - Surveillance et performances : affiche les CloudWatch alarmes que vous avez créées, ainsi que les mesures et les avertissements pour les catégories suivantes :
    - Résumé : résumé de haut niveau des mesures d'activité du système de fichiers
    - Capacité de stockage du système de fichiers
    - Performances du serveur de fichiers et du disque

    Pour plus d’informations, consultez Surveillance avec Amazon CloudWatch.
  - Administration : affiche les informations d'administration du système de fichiers suivantes :
    - Les DNS noms et IP adresses des points de terminaison interclusters et de gestion du système de fichiers.
    - Le nom ONTAP d'utilisateur de l'administrateur.

    - L'option permettant de mettre à jour le mot de passe ONTAP administrateur.
  - Liste des SVM du système de fichiers
  - Liste des volumes du système de fichiers
  - Paramètres de sauvegarde : modifiez les paramètres de sauvegarde quotidienne automatique du système de fichiers.
  - Mises à jour : indique l'état des mises à jour initiées par l'utilisateur et apportées à la configuration du système de fichiers.
  - Balises : afficher, modifier, ajouter, supprimer des paires clé:valeur de balises.
- Utilisation de la CLI ou de l'API : utilisez la commande CLI describe-file-systems ou DescribeFilel'opération Systems API.

État du système de fichiers FSx for ONTAP

Vous pouvez consulter l'état d'un système de fichiers Amazon FSx à l'aide de la console Amazon FSx, de la AWS CLI commande describe-file-systems ou des systèmes d'exploitation des API. DescribeFile

État du système de fichiers	Description
DISPONIBLE	Le système de fichiers a été créé avec succès et est prêt à être utilisé.
CREAtioN	Amazon FSx est en train de créer un nouveau système de fichiers.
SUPPRESSION	Amazon FSx est en train de supprimer un système de fichiers existant.
MAL CONFIGURÉ	Le système de fichiers est mal configuré mais peut être restauré.
ÉCHEC	1. Le système de fichiers est défaillant et Amazon FSx ne parvient pas à le récupérer. 2. Lors de la création d'un nouveau système de fichiers, Amazon FSx n'a pas pu créer de nouveau système de fichiers.

Gestion de FSx pour les machines virtuelles de stockage ONTAP

Dans FSx for ONTAP, les volumes sont hébergés sur des serveurs de fichiers virtuels appelés machines virtuelles de stockage (SVM). Une SVM est un serveur de fichiers isolé doté de ses propres identifiants administratifs et de points de terminaison pour administrer les données et y accéder. Lorsque vous accédez aux données dans FSx for ONTAP, vos clients et postes de travail montent un volume, un partage SMB ou un LUN iSCSI hébergé par une SVM en utilisant le point de terminaison (adresse IP) de la SVM.

Amazon FSx crée automatiquement une SVM par défaut sur votre système de fichiers lorsque vous créez un système de fichiers à l'aide du. AWS Management Console Vous pouvez créer des SVM supplémentaires sur votre système de fichiers à tout moment à l'aide de la console ou de l'API et des SDK Amazon FSx. AWS CLI Vous ne pouvez pas créer de SVM à l'aide de la CLI ONTAP ou de l'API REST.

Vous pouvez associer vos SVM à un Microsoft Active Directory pour l'authentification et l'autorisation d'accès aux fichiers. Pour plus d’informations, consultez Utilisation de Microsoft Active Directory dans FSx pour ONTAP.

Nombre maximum de SVM par système de fichiers

Le tableau suivant indique le nombre maximum de SVM que vous pouvez créer pour un système de fichiers. Le nombre maximum de SVM dépend de la capacité de débit allouée en mégaoctets par seconde (Mbits/s).

Type de déploiement	Quantité de capacité de débit (Mbits/s)	Nombre maximum de SVM par système de fichiers
Mono-AZ (mise à l'échelle) et multi-AZ (mise à l'échelle)	128	6
	256	6
	512	14
	1,024	14
	2 048	24
	4 096	24

Type de déploiement	Quantité de capacité de débit (Mbits/s)	Nombre maximum de SVM par système de fichiers
Mono-AZ (scale-out)	N'importe quel compte	5

Rubriques

- Création d'une machine virtuelle de stockage
- Mise à jour d'une machine virtuelle de stockage
- Supprimer une machine virtuelle de stockage (SVM)
- Affichage des détails de configuration des machines virtuelles de stockage

Création d'une machine virtuelle de stockage

Vous pouvez créer une SVM FSx pour ONTAP à l'aide de l'API AWS Management Console, et AWS CLI.

Le nombre maximum de SVM que vous pouvez créer pour un système de fichiers dépend du type de déploiement de celui-ci et de la capacité de débit allouée. Pour plus d'informations, consultez Nombre maximum de SVM par système de fichiers.

Propriétés de la SVM

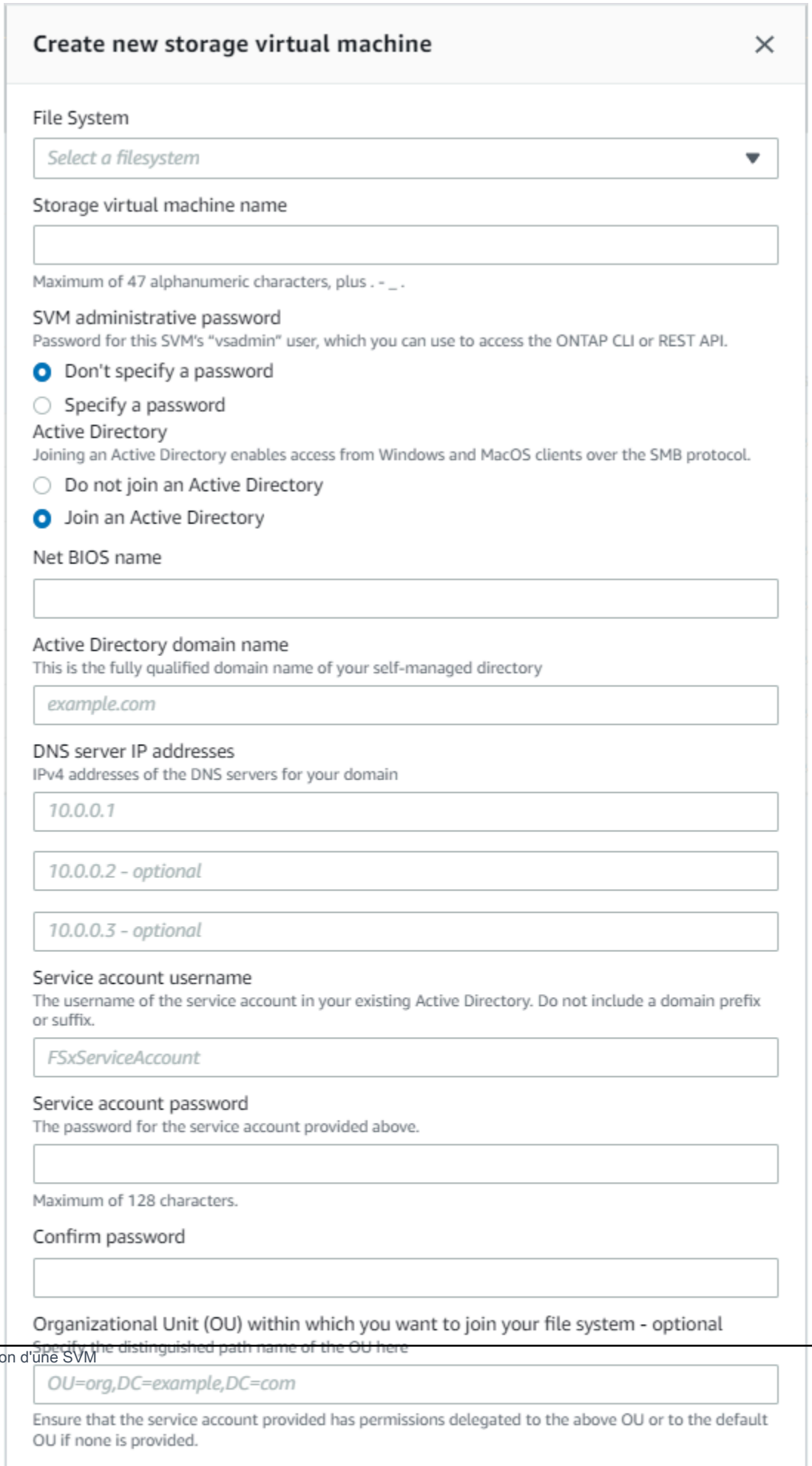
Lors de la création d'une SVM, vous définissez les propriétés suivantes :

- Le système de fichiers FSx for ONTAP auquel il appartient.
- Configuration Microsoft Active Directory (AD) — Vous pouvez éventuellement associer votre SVM à un AD autogéré pour l'authentification et le contrôle d'accès des clients Windows et macOS. Pour plus d'informations, consultez Utilisation de Microsoft Active Directory dans FSx pour ONTAP.
- Style de sécurité du volume racine — Définissez le style de sécurité du volume racine (Unix, NTFS ou mixte) en fonction du type de clients que vous utilisez pour accéder à vos données dans la SVM. Pour plus d'informations, consultez Style de sécurité des volumes.
- Le mot de passe administratif de la SVM : vous pouvez éventuellement définir le mot de passe de l'utilisateur de la SVM. `vsadmin` Pour plus d'informations, consultez Gestion des SVM à l'aide de la CLI ONTAP.

Pour créer une machine virtuelle de stockage (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation de gauche, choisissez Storage virtual machines.
3. Choisissez Créer une nouvelle machine virtuelle de stockage.

   La boîte de dialogue Créer une nouvelle machine virtuelle de stockage apparaît.


Create new storage virtual machine
File System
Select a filesystem
Storage virtual machine name
Maximum of 47 alphanumeric characters, plus . - _ .
SVM administrative password
Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.
Don't specify a password
Specify a password
Active Directory
Joining an Active Directory enables access from Windows and MacOS clients over the SMB protocol.
Do not join an Active Directory
Join an Active Directory
Net BIOS name
Active Directory domain name
This is the fully qualified domain name of your self-managed directory
example.com
DNS server IP addresses
IPv4 addresses of the DNS servers for your domain
10.0.0.1
10.0.0.2 - optional
10.0.0.3 - optional
Service account username
The username of the service account in your existing Active Directory. Do not include a domain prefix or suffix.
FSxServiceAccount
Service account password
The password for the service account provided above.
Maximum of 128 characters.
Confirm password
Organizational Unit (OU) within which you want to join your file system - optional
Specify the distinguished path name of the OU here
OU=org,DC=example,DC=com
Ensure that the service account provided has permissions delegated to the above OU or to the default OU if none is provided.

4. Pour Système de fichiers, choisissez le système de fichiers sur lequel créer la machine virtuelle de stockage.
5. Dans le champ Nom de la machine virtuelle de stockage, indiquez le nom de la machine virtuelle de stockage. Vous pouvez utiliser un maximum de 47 caractères alphanumériques, plus le caractère spécial de soulignement (_).
6. Pour le mot de passe administratif de la SVM, vous pouvez éventuellement choisir Spécifier un mot de passe et fournir un mot de passe pour l'utilisateur de `vsadmin` cette SVM. Vous pouvez utiliser l'`vsadmin`utilisateur pour administrer la SVM à l'aide de la CLI ONTAP ou de l'API REST. Pour plus d'informations sur l'`vsadmin`utilisateur, consultezGestion des SVM à l'aide de la CLI ONTAP.

   Si vous choisissez Ne pas spécifier de mot de passe (valeur par défaut), vous pouvez toujours utiliser l'`fsxadmin`utilisateur du système de fichiers pour gérer votre système de fichiers à l'aide de la CLI ONTAP ou de l'API REST, mais vous ne pouvez pas utiliser `vsadmin` l'utilisateur de votre SVM pour faire de même.
7. Pour Active Directory, vous disposez des options suivantes :

   - Si vous n'associez pas votre système de fichiers à un Active Directory (AD), choisissez Ne pas joindre un Active Directory.
   - Si vous associez votre SVM à un domaine AD autogéré, choisissez Joindre un Active Directory et fournissez les informations suivantes pour votre AD. Pour plus d'informations, consultez Conditions requises pour joindre une SVM à un Microsoft AD autogéré.
     - Nom NetBIOS de l'objet informatique Active Directory à créer pour votre SVM. Le nom NetBIOS ne peut pas dépasser 15 caractères. C'est le nom de cette SVM dans Active Directory.
     - Le nom de domaine complet (FQDN) de votre Active Directory. Le FQDN ne peut pas dépasser 255 caractères.
     - Adresses IP des serveurs DNS : adresses IPv4 des serveurs DNS de votre domaine.
     - Nom d'utilisateur du compte de service : nom d'utilisateur du compte de service dans votre Active Directory existant. N'incluez pas de préfixe ou de suffixe de domaine. Pour `EXAMPLE\ADMIN`, utilisez `ADMIN`.
     - Mot de passe du compte de service : mot de passe du compte de service.
     - Confirmer le mot de passe : mot de passe du compte de service.
     - (Facultatif) Unité organisationnelle (UO) : nom du chemin unique de l'unité organisationnelle à laquelle vous souhaitez joindre votre système de fichiers.

- Groupe d'administrateurs de systèmes de fichiers délégués : nom du groupe de votre AD qui peut administrer votre système de fichiers.

  Si vous utilisez AWS Managed Microsoft AD, vous devez spécifier un groupe tel que les administrateurs FSx AWS délégués, les administrateurs AWS délégués ou un groupe personnalisé doté d'autorisations déléguées sur l'unité d'organisation.

  Si vous adhérez à un AD autogéré, utilisez le nom du groupe dans votre AD. Le groupe par défaut est`Domain Admins`.

8. Pour le style de sécurité du volume racine de la SVM, choisissez le style de sécurité de la SVM en fonction du type de clients qui accèdent à vos données. Choisissez Unix (Linux) si vous accédez principalement à vos données via des clients Linux ; choisissez NTFS si vous accédez principalement à vos données via des clients Windows. Pour plus d'informations, consultez Style de sécurité des volumes.
9. Choisissez Confirmer pour créer la machine virtuelle de stockage.

Vous pouvez suivre la progression de la mise à jour sur la page détaillée des systèmes de fichiers, dans la colonne État du volet Machines virtuelles de stockage. La machine virtuelle de stockage est prête à être utilisée lorsque son statut est créé.

Pour créer une machine virtuelle de stockage (CLI)

- Pour créer une machine virtuelle de stockage (SVM) FSx for ONTAP, utilisez la commande create-storage-virtual-machineCLI (ou l'opération CreateStorageVirtualMachineAPI équivalente), comme indiqué dans l'exemple suivant.

```
aws fsx create-storage-virtual-machine \
    --file-system-id fs-0123456789abcdef0 \
    --name svm1 \
    --svm-admin-password password \
    --active-directory-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAd
 \
UserName="FSxService",Password="password", \
   DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

Après avoir créé avec succès la machine virtuelle de stockage, Amazon FSx renvoie sa description au format JSON, comme illustré dans l'exemple suivant.


```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
```

```
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}
```

Mise à jour d'une machine virtuelle de stockage

Vous pouvez mettre à jour les propriétés de configuration de la machine virtuelle de stockage (SVM) suivantes à l'aide de la console Amazon FSx et de l' AWS CLI API Amazon FSx :

- Mot de passe du compte administratif de la SVM.
- Configuration Active Directory (AD) de la SVM : vous pouvez joindre une SVM à un AD ou modifier la configuration AD d'une SVM déjà jointe à un AD. Pour plus d'informations, consultez Gestion des configurations Active Directory des SVM.

Pour mettre à jour les informations d'identification du compte administrateur de la SVM (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Choisissez la SVM à mettre à jour comme suit :
   - Dans le volet de navigation de gauche, choisissez Systèmes de fichiers, puis le système de fichiers ONTAP pour lequel vous souhaitez mettre à jour une SVM.
   - Choisissez l'onglet Machines virtuelles de stockage.

     —Ou—
   - Pour afficher la liste de toutes les SVM actuellement disponibles Compte AWS dans votre environnement Région AWS, développez ONTAP et sélectionnez Machines virtuelles de stockage.
3. Choisissez la machine virtuelle de stockage que vous souhaitez mettre à jour.
4. Choisissez Actions > Mettre à jour le mot de passe administrateur. La fenêtre Mettre à jour les informations d'identification administratives de la SVM s'affiche.
5. Entrez le nouveau mot de passe de l'`vsadmin`utilisateur, puis confirmez-le.

6. Choisissez Mettre à jour les informations d'identification pour enregistrer le nouveau mot de passe.

Pour mettre à jour les informations d'identification du compte administrateur de la SVM (CLI)

- Pour mettre à jour la configuration d'une FSx for ONTAP SVM, utilisez la commande update-storage-virtual-machineCLI (ou l'opération UpdateStorageVirtualMachineAPI équivalente), comme indiqué dans l'exemple suivant.

```
aws fsx update-storage-virtual-machine \
--storage-virtual-machine-id svm-abcdef01234567890 \
--svm-admin-password new-svm-password \
```

Après avoir créé avec succès la machine virtuelle de stockage, Amazon FSx renvoie sa description au format JSON, comme illustré dans l'exemple suivant.

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
```

```
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef01234567890",
    "StorageVirtualMachineId": "svm-abcdef01234567890",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}
```

Supprimer une machine virtuelle de stockage (SVM)

Vous ne pouvez supprimer une SVM FSx for ONTAP qu'à l'aide de la console Amazon FSx, de l'API et de l'API. AWS CLI Avant de pouvoir supprimer une SVM, vous devez d'abord supprimer tous les volumes non root attachés à la SVM.

> **Important**
>
> Il n'est pas possible de supprimer une SVM à l'aide de la NetApp CLI ou de l'API ONTAP.

> **Note**
>
> Avant de supprimer une machine virtuelle de stockage, assurez-vous qu'aucune application n'accède aux données de la SVM et que vous avez supprimé tous les volumes non root attachés à la SVM.

Pour supprimer une machine virtuelle de stockage (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Choisissez la SVM que vous souhaitez supprimer comme suit :

   - Dans le volet de navigation de gauche, choisissez Systèmes de fichiers, puis le système de fichiers ONTAP pour lequel vous souhaitez supprimer une SVM.
   - Choisissez l'onglet Machines virtuelles de stockage.

   —Ou—

   - Pour afficher la liste de toutes les SVM disponibles, développez ONTAP et choisissez Machines virtuelles de stockage.

   Sélectionnez dans la liste la SVM que vous souhaitez supprimer.
3. Dans l'onglet Volumes, consultez la liste des volumes attachés à la SVM. Si des volumes autres que root sont attachés à la SVM, vous devez les supprimer avant de pouvoir supprimer la SVM. Pour plus d'informations, consultez Suppression d'un volume.
4. Choisissez Supprimer la machine virtuelle de stockage dans le menu Actions.
5. Dans la boîte de dialogue de confirmation de suppression, choisissez Supprimer la machine virtuelle de stockage.

Pour supprimer une machine virtuelle de stockage (CLI)

- Pour supprimer une machine virtuelle de stockage FSx for ONTAP, utilisez la commande delete-storage-virtual-machineCLI (ou l'opération DeleteStorageVirtualMachineAPI équivalente), comme indiqué dans l'exemple suivant.

```
aws fsx delete-storage-virtual-machine --storage-virtual-machine-id svm-
abcdef0123456789d
```

Affichage des détails de configuration des machines virtuelles de stockage

Vous pouvez voir les machines virtuelles de stockage FSx for ONTAP qui se trouvent actuellement sur votre système de fichiers à l'aide de la console Amazon FSx, de l'API Amazon FSx et de AWS CLI l'API Amazon FSx.

Pour afficher une machine virtuelle de stockage sur votre système de fichiers :

- Utilisation de la console : choisissez un système de fichiers pour afficher sa page détaillée sur les systèmes de fichiers. Pour répertorier toutes les machines virtuelles de stockage du système de fichiers, choisissez l'onglet Machines virtuelles de stockage, puis choisissez la machine virtuelle de stockage que vous souhaitez afficher.
- Utilisation de la CLI ou de l'API : utilisez la commande describe-storage-virtual-machinesCLI ou l'opération DescribeStorageVirtualMachinesAPI.

  La réponse du système est une liste de descriptions complètes de toutes les SVM de votre compte. Région AWS

Gestion de FSx pour les volumes ONTAP

Chaque machine virtuelle de stockage (SVM) d'un système de fichiers FSx for ONTAP peut comporter un ou plusieurs volumes. Un volume est un conteneur de données isolé pour des fichiers, des répertoires ou des unités logiques de stockage (LUN) iSCSI. Les volumes sont dotés d'un provisionnement léger, ce qui signifie qu'ils consomment de la capacité de stockage uniquement pour les données qu'ils contiennent.

Vous pouvez accéder à un volume à partir de clients Linux, Windows ou macOS via le protocole NFS (Network File System), le protocole SMB (Server Message Block) ou le protocole iSCSI (Internet Small Computer Systems Interface) en créant un LUN iSCSI (stockage par blocs partagé). FSx for ONTAP prend également en charge l'accès multiprotocole (accès NFS et SMB simultanés) au même volume.

Vous pouvez créer des volumes à l' AWS Management Console aide de AWS CLI l'API Amazon FSx ou NetApp BlueXP. Vous pouvez également utiliser le point de terminaison administratif de votre système de fichiers ou de votre SVM pour créer, mettre à jour et supprimer des volumes à l'aide de la NetApp CLI ONTAP ou de l'API REST.

> **Note**
>
> Vous pouvez créer 500 volumes par paire HA, jusqu'à 1 000 volumes pour toutes les paires HA. FlexGrouples volumes de constituants sont pris en compte dans cette limite. Par défaut, il existe huit volumes constitutifs par agrégat, parFlexGroup.

Lorsque vous créez un volume, vous définissez les propriétés suivantes :

- Style de volume — Le style de volume peut être FlexVol soitFlexGroup.
- Nom du volume : nom du volume.
- Type de volume : le type de volume peut être en lecture-écriture (RW) ou en protection des données (DP). Les volumes DP sont en lecture seule et sont utilisés comme destination dans une relation NetApp SnapMirror orSnapVault.
- Taille du volume : il s'agit de la quantité maximale de données que le volume peut stocker, quel que soit le niveau de stockage.
- Chemin de jonction — Il s'agit de l'emplacement dans l'espace de noms de la SVM où le volume est monté.
- Efficacité du stockage : les fonctionnalités d'efficacité du stockage, notamment le compactage, la compression et la déduplication des données, permettent de réaliser des économies de stockage typiques de 65 % pour les charges de travail de partage de fichiers à usage général.
- Style de sécurité du volume (Unix, NTFS ou mixte) : détermine le type d'autorisations utilisé pour accéder aux données sur le volume lors de l'autorisation des utilisateurs.
- Hiérarchisation des données — La politique de hiérarchisation définit les données stockées dans le niveau rentable du pool de capacités.
- Période de refroidissement de la politique de hiérarchisation : définit le moment où les données sont marquées comme froides et déplacées vers le stockage du pool de capacité.
- Politique relative aux instantanés : les politiques relatives aux instantanés définissent la manière dont le système crée des instantanés pour un volume. Vous pouvez choisir entre trois politiques prédéfinies ou utiliser une politique personnalisée que vous avez créée à l'aide de la CLI ONTAP ou de l'API REST.
- Copier les balises dans les sauvegardes : Amazon FSx copie automatiquement toutes les balises de vos volumes vers les sauvegardes à l'aide de cette option. Vous pouvez définir cette option à l'aide de l' AWS CLI API ou Amazon FSx.

Rubriques

Styles de volume

FSx for ONTAP propose deux styles de volumes que vous pouvez utiliser à des fins différentes. Vous pouvez créer l'un FlexVol ou l'autre FlexGroup des volumes à l'aide de la console Amazon FSx, de l' AWS CLI API Amazon FSx et de l'API Amazon FSx.

- FlexVolles volumes offrent l'expérience la plus simple pour les systèmes de fichiers dotés d'une paire de haute disponibilité (HA) et constituent le style de volume par défaut pour les systèmes de fichiers évolutifs. La taille minimale d'un FlexVol volume est de 20 mégaoctets (Mo) et la taille maximale est de 314 572 800 Mo.
- FlexGrouples volumes sont composés de plusieurs FlexVol volumes constitutifs, ce qui leur permet d'offrir des performances et une évolutivité de stockage supérieures à celles des FlexVol volumes destinés à des systèmes de fichiers comportant plusieurs paires HA. FlexGrouples volumes sont le style de volume par défaut pour les systèmes de fichiers scale-out. La taille minimale d'un FlexGroup volume est de 100 gibioctets (GiB) par constituant, et la taille maximale est de 20 pebioctets (PiB).

Vous pouvez convertir un volume avec le FlexVol style en style à l'FlexGroupaide de la ONTAP CLI, ce qui crée un volume FlexGroup avec un seul constituant. Toutefois, nous vous recommandons de l'utiliser AWS DataSync pour déplacer des données entre un FlexVol volume et un nouveau FlexGroup volume afin de garantir une répartition uniforme des données entre les FlexGroup's composants. Pour plus d’informations, consultez FlexGroupconstituants.

> **Note**
>
> Si vous souhaitez utiliser la ONTAP CLI pour convertir un FlexVol volume en FlexGroup volume, assurez-vous de supprimer toutes les sauvegardes du FlexVol volume avant de le convertir. ONTAPne rééquilibre pas automatiquement les données dans le cadre de la conversion, de sorte que les données peuvent être déséquilibrées entre les FlexGroup composants.

FlexGroupconstituants

Un FlexGroup volume est composé de constituants, qui sont des FlexVol volumes. Par défaut, FSx for ONTAP attribue huit composants à un FlexGroup volume par paire HA.

Lorsque vous créez votre FlexGroup volume, sa taille est répartie uniformément entre ses composants. Par exemple, si vous créez un FlexGroup volume de 800 gigaoctets (Go) avec huit composants, chaque composant a une taille de 100 Go. La taille d'un FlexGroup volume peut être comprise entre 100 Go et 20 PiB, mais la taille totale dépend de la taille des composants. Chaque composant a une taille minimale de 100 Go et une taille maximale de 300 TiB. Par exemple, un FlexGroup volume à huit composants a une taille minimale de 800 Go et une taille maximale de 20 PiB.

ONTAP distribue les données au niveau des fichiers entre les composants. Vous pouvez stocker jusqu'à deux milliards de fichiers dans chaque composant de votre FlexGroup volume.

Lorsque vous mettez à jour la taille de votre FlexGroup volume, la nouvelle taille est répartie uniformément entre ses composants existants.

Vous pouvez également ajouter d'autres composants à votre FlexGroup volume à l'aide de la ONTAP CLI ou de l'API REST. Toutefois, nous vous recommandons de ne le faire que si vous avez besoin d'une capacité de stockage supplémentaire et que tous vos composants ont déjà atteint leur taille maximale (300 TiB par composant). L'ajout de composants peut entraîner un déséquilibre des données et des E/S entre les composants. Tant que les composants ne sont pas équilibrés, il est possible que le débit d'écriture soit inférieur de 5 à 10 % à celui d'un FlexGroup volume équilibré. Lorsque de nouvelles données sont écrites dans le FlexGroup volume, ONTAP les distribue en priorité aux nouveaux composants jusqu'à ce que les composants soient équilibrés. Si vous ajoutez de nouveaux composants, nous vous recommandons de choisir un nombre pair et de ne pas dépasser huit par agrégat.

> **Note**
>
> Si vous ajoutez de nouveaux composants, vos instantanés existants deviennent des instantanés partiels ; ils ne peuvent donc pas être utilisés pour restaurer complètement l'état antérieur de votre FlexGroup volume. Les instantanés précédents ne peuvent pas fournir une point-in-time image complète de votre FlexGroup volume car les nouveaux composants n'existaient pas encore. Toutefois, les instantanés partiels peuvent être utilisés pour restaurer des fichiers et des répertoires individuels, pour créer un nouveau volume ou pour effectuer une réplication avec. SnapMirror

Types de volume

FSx for ONTAP propose deux types de volumes que vous pouvez créer à l'aide de la console Amazon FSx, de l'API Amazon FSx et de AWS CLI l'API Amazon FSx.

- Les volumes de lecture-écriture (RW) sont utilisés dans la plupart des cas. Comme leur nom l'indique, ils sont lisibles et inscriptibles.
- Les volumes de protection des données (DP) sont des volumes en lecture seule que vous utilisez comme destination d'une relation NetApp SnapMirror ouSnapVault. Vous devez utiliser des volumes DP lorsque vous souhaitez migrer ou protéger les données d'un seul volume.

FlexVolet les FlexGroup volumes peuvent être soit RW soit DP.

> **Note**
>
> Vous ne pouvez pas mettre à jour le type d'un volume une fois celui-ci créé.

Style de sécurité des volumes

FSx for ONTAP prend en charge 3 styles de sécurité des volumes différents : Unix, NTFS et mixte. Chaque style de sécurité a un effet différent sur la façon dont les autorisations sont gérées pour les données. Vous devez comprendre les différents effets pour vous assurer de sélectionner le style de sécurité adapté à vos besoins.

Il est important de comprendre que les styles de sécurité ne déterminent pas quels types de clients peuvent ou ne peuvent pas accéder aux données. Les styles de sécurité déterminent uniquement le

type d'autorisations que FSx for ONTAP utilise pour contrôler l'accès aux données et le type de client qui peut modifier ces autorisations.

Les deux facteurs que vous utilisez pour déterminer le style de sécurité d'un volume sont le type d'administrateurs qui gèrent le système de fichiers et le type d'utilisateurs ou de services qui accèdent aux données du volume.

Lors de la création d'un volume dans la console, la CLI et l'API Amazon FSx, le style de sécurité est automatiquement défini sur le style de sécurité du volume racine. Vous pouvez modifier le style de sécurité d'un volume à l'aide de l'API AWS CLI or. Vous pouvez modifier ce paramètre une fois le volume créé. Pour plus d'informations, consultez Mettre à jour un volume.

Lorsque vous configurez le style de sécurité sur un volume, tenez compte des besoins de votre environnement pour vous assurer de sélectionner le meilleur style de sécurité afin d'éviter les problèmes liés à la gestion des autorisations. N'oubliez pas que le style de sécurité ne détermine pas quels types de clients peuvent accéder aux données. Le style de sécurité détermine les autorisations utilisées pour autoriser l'accès aux données et les types de clients qui peuvent modifier ces autorisations. Les considérations suivantes peuvent vous aider à choisir le style de sécurité à choisir pour un volume :

- Unix (Linux) — Choisissez ce style de sécurité si le système de fichiers est géré par un administrateur Unix, si la majorité des utilisateurs sont des clients NFS et si une application accédant aux données utilise un utilisateur Unix comme compte de service. Seuls les clients Linux peuvent modifier les autorisations avec le style de sécurité Unix, et les types d'autorisations utilisés sur les fichiers et les répertoires sont les mode-bits ou les ACL NFS v4.x.
- NTFS — Choisissez ce style de sécurité si le système de fichiers est géré par un administrateur Windows, si la majorité des utilisateurs sont des clients PME et si une application accédant aux données utilise un utilisateur Windows comme compte de service. Si un accès Windows est requis pour accéder à un volume, nous vous recommandons d'utiliser le style de sécurité NTFS. Seuls les clients Windows peuvent modifier les autorisations avec le style de sécurité NTFS, et les types d'autorisations utilisés sur les fichiers et les répertoires sont les ACL NTFS.
- Mixte — Il s'agit d'un paramètre avancé. Pour plus d'informations, consultez la rubrique Quels sont les styles de sécurité et leurs effets dans le Centre de NetApp documentation.

Création de volumes

Vous pouvez créer un FSx pour ONTAP FlexVol ou un FlexGroup volume à l'aide de la console Amazon FSx, du, et de AWS CLI l'API Amazon FSx, en plus de l'interface de ligne de NetApp commande (CLI) ONTAP et de l'API REST.

Pour créer un FlexVol volume (console)

> **Note**
>
> Le style de sécurité du volume est automatiquement défini sur le style de sécurité du volume racine.

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation de gauche, sélectionnez Volumes.
3. Choisissez Créer un volume.
4. Pour le type de système de fichiers, choisissez Amazon FSx for NetApp ONTAP.
5. Dans la section Détails du système de fichiers, fournissez les informations suivantes :
   - Dans Système de fichiers, choisissez le système de fichiers sur lequel créer le volume.
   - Pour Machine virtuelle de stockage, choisissez la machine virtuelle de stockage (SVM) sur laquelle créer le volume.
6. Dans la section Style de volume, choisissez FlexVol.
7. Dans la section Détails du volume, fournissez les informations suivantes :
   - Dans le champ Nom du volume, saisissez le nom du volume. Vous pouvez utiliser jusqu'à 203 caractères alphanumériques ou soulignés (_).
   - Pour Taille du volume, entrez un nombre entier compris entre 20 et 314572800 pour spécifier la taille en mégaoctets (MiB).
   - Pour le type de volume, choisissez Read-Write (RW) pour créer un volume lisible et inscriptible ou Data Protection (DP) pour créer un volume en lecture seule pouvant être utilisé comme destination d'une relation or. NetApp SnapMirror SnapVault Pour plus d’informations, consultez Types de volume.
   - Pour le chemin de jonction, entrez un emplacement dans le système de fichiers pour monter le volume. Le nom doit être précédé d'une barre oblique, par exemple `/vol3`.

- Pour l'efficacité du stockage, choisissez Activé pour activer les fonctionnalités d'efficacité du stockage ONTAP (déduplication, compression et compactage). Pour plus d'informations, consultez FSx pour l'efficacité du stockage ONTAP.
- Pour le style de sécurité du volume, choisissez entre Unix (Linux), NTFS et Mixed pour le volume. Pour plus d'informations, consultez Style de sécurité des volumes.
- Pour la politique de capture instantanée, choisissez une politique de capture instantanée pour le volume. Pour plus d'informations sur les politiques relatives aux instantanés, consultezRègles relatives aux snapshots.

  Si vous choisissez Politique personnalisée, vous devez spécifier le nom de la politique dans le champ Politique personnalisée. La politique personnalisée doit déjà exister sur la SVM ou dans le système de fichiers. Vous pouvez créer une politique de capture personnalisée à l'aide de la CLI ONTAP ou de l'API REST. Pour plus d'informations, consultez la section Création d'une politique de capture instantanée dans la documentation du produit NetApp ONTAP.

8. Dans la section Hiérarchisation du stockage, fournissez les informations suivantes :

   - Pour la politique de hiérarchisation du pool de capacités, choisissez la politique de hiérarchisation du pool de stockage pour le volume, qui peut être Auto (par défaut), Snapshot Only, All ou None. Pour plus d'informations, consultez Politiques de hiérarchisation des volumes.
   - Si vous choisissez Auto ou Snapshot Only, vous pouvez définir la période de refroidissement de la politique de hiérarchisation afin de définir le nombre de jours avant que les données non consultées ne soient marquées comme froides et déplacées vers le stockage du pool de capacité. Vous pouvez fournir une valeur comprise entre 2 et 183 jours. Le paramètre par défaut est de 31 jours.

9. Dans la section Avancé, pour SnapLockConfiguration, choisissez entre Activé et Désactivé. Pour plus d'informations sur la configuration d'un volume SnapLock Compliance ou SnapLock d'un volume Enterprise, consultez Création d'un volume SnapLock de conformité etCréation d'un volume SnapLock Enterprise. Pour plus d'informations sur SnapLock, consultez Protégez vos données avec SnapLock.
10. Choisissez Confirmer pour créer le volume.

Vous pouvez suivre la progression de la mise à jour sur la page détaillée des systèmes de fichiers, dans la colonne État du volet Volumes. Le volume est prêt à être utilisé lorsque son statut est créé.

Pour créer un FlexGroup volume (console)

> **Note**
>
> Vous ne pouvez créer des FlexGroup volumes pour des systèmes de fichiers évolutifs qu'à l'aide de la console Amazon FSx. Pour créer des FlexVol volumes pour vos systèmes de fichiers évolutifs, utilisez l'API AWS CLI Amazon FSx ou des outils de gestion. NetApp

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation de gauche, sélectionnez Volumes.
3. Choisissez Créer un volume.
4. Pour le type de système de fichiers, choisissez Amazon FSx for NetApp ONTAP.
5. Dans la section Détails du système de fichiers, fournissez les informations suivantes :
   - Dans Système de fichiers, choisissez le système de fichiers sur lequel créer le volume.
   - Pour Machine virtuelle de stockage, choisissez la machine virtuelle de stockage (SVM) sur laquelle créer le volume.
6. Dans la section Style de volume, choisissez FlexGroup.
7. Dans la section Détails du volume, fournissez les informations suivantes :
   - Dans le champ Nom du volume, saisissez le nom du volume. Vous pouvez utiliser jusqu'à 203 caractères alphanumériques ou soulignés (_).
   - Pour Taille du volume, entrez un nombre entier compris entre 800 Go (GiB) et 2 000 pebioctets (PiB).
   - Pour le type de volume, choisissez Read-Write (RW) pour créer un volume lisible et inscriptible ou Data Protection (DP) pour créer un volume en lecture seule pouvant être utilisé comme destination d'une relation or. NetApp SnapMirror SnapVault Pour plus d’informations, consultez Types de volume.
   - Pour le chemin de jonction, entrez un emplacement dans le système de fichiers pour monter le volume. Le nom doit être précédé d'une barre oblique, par exemple `/vol3`.
   - Pour l'efficacité du stockage, choisissez Activé pour activer les fonctionnalités d'efficacité du stockage ONTAP (déduplication, compression et compactage). Pour plus d’informations, consultez FSx pour l'efficacité du stockage ONTAP.

- Pour le style de sécurité du volume, choisissez entre Unix (Linux), NTFS et Mixed pour le volume. Pour plus d'informations, consultez Style de sécurité des volumes.

  > **Note**
  >
  > Le style de sécurité du volume est automatiquement défini sur le style de sécurité du volume racine.

- Pour la politique de capture instantanée, choisissez une politique de capture instantanée pour le volume. Pour plus d'informations sur les politiques relatives aux instantanés, consultezRègles relatives aux snapshots.

  Si vous choisissez Politique personnalisée, vous devez spécifier le nom de la politique dans le champ Politique personnalisée. La politique personnalisée doit déjà exister sur la SVM ou dans le système de fichiers. Vous pouvez créer une politique de capture personnalisée à l'aide de la CLI ONTAP ou de l'API REST. Pour plus d'informations, consultez la section Création d'une politique de capture instantanée dans la documentation du produit NetApp ONTAP.

8. Dans la section Hiérarchisation du stockage, fournissez les informations suivantes :

   - Pour la politique de hiérarchisation du pool de capacités, choisissez la politique de hiérarchisation du pool de stockage pour le volume, qui peut être Auto (par défaut), Snapshot Only, All ou None. Pour plus d'informations, consultez Politiques de hiérarchisation des volumes.
   - Si vous choisissez Auto ou Snapshot Only, vous pouvez définir la période de refroidissement de la politique de hiérarchisation afin de définir le nombre de jours avant que les données non consultées ne soient marquées comme froides et déplacées vers le stockage du pool de capacité. Vous pouvez fournir une valeur comprise entre 2 et 183 jours. Le paramètre par défaut est de 31 jours.

9. Dans la section Avancé, pour SnapLockConfiguration, choisissez entre Activé et Désactivé. Pour plus d'informations sur la configuration d'un volume SnapLock Compliance ou SnapLock d'un volume Enterprise, consultez Création d'un volume SnapLock de conformité etCréation d'un volume SnapLock Enterprise. Pour plus d'informations sur SnapLock, consultez Protégez vos données avec SnapLock.

10. Choisissez Confirmer pour créer le volume.

Vous pouvez suivre la progression de la mise à jour sur la page détaillée des systèmes de fichiers, dans la colonne État du volet Volumes. Le volume est prêt à être utilisé lorsque son statut est créé.

Pour créer un volume (CLI)

- Pour créer un volume FSx for ONTAP, utilisez la commande de la CLI create-volume (ou l'opération CreateVolumeAPI équivalente), comme indiqué dans l'exemple suivant.

```
aws fsx create-volume \
    --volume-type ONTAP \
    --name vol1 \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/
vol1,SecurityStyle=NTFS, \
          SizeInMegabytes=1024,SnapshotPolicy=default, \
          StorageVirtualMachineId=svm-abcdef0123456789a,OntapVolumeType=RW, \
          StorageEfficiencyEnabled=true
```

Après avoir créé le volume avec succès, Amazon FSx renvoie sa description au format JSON, comme illustré dans l'exemple suivant.

```
{
    "Volume": {
        "CreationTime": "2022-08-12T13:03:37.625000-04:00",
        "FileSystemId": "fs-abcdef0123456789c",
        "Lifecycle": "CREATING",
        "Name": "vol1",
        "OntapConfiguration": {
            "CopyTagsToBackups": true,
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "NTFS",
            "SizeInMegabytes": 1024,
            "SnapshotPolicy": "default",
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abcdef0123456789a",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "Name": "NONE"
            },
            "OntapVolumeType": "RW"
        },
```

```
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-abcdef0123456789c/
fsvol-abcdef0123456789b",
        "VolumeId": "fsvol-abcdef0123456789b",
        "VolumeType": "ONTAP"


    }
}
```

Vous pouvez également créer un nouveau volume en restaurant une sauvegarde d'un volume sur un nouveau volume. Pour plus d'informations, consultez Restauration des sauvegardes sur un nouveau volume.

Mettre à jour un volume

Vous pouvez mettre à jour la configuration d'un volume FSx pour ONTAP à l'aide de la console Amazon FSx, du, et de AWS CLI l'API Amazon FSx, en plus de l'interface de ligne de NetApp commande (CLI) ONTAP et de l'API REST. Vous pouvez modifier les propriétés suivantes d'un volume FSx for ONTAP existant :

- Nom du volume
- Sentier de jonction
- Taille du volume
- Efficacité du stockage
- Politique de hiérarchisation du pool de capacités
- Style de sécurité des volumes
- Politique relative aux instantanés
- Période de refroidissement de la politique de hiérarchisation
- Copier les balises dans les sauvegardes (à l'aide de l'API AWS CLI et Amazon FSx)

Pour plus d'informations, consultez Gestion de FSx pour les volumes ONTAP.

Pour mettre à jour la configuration d'un volume (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Accédez à Systèmes de fichiers et choisissez le système de fichiers ONTAP pour lequel vous souhaitez mettre à jour un volume.

3. Choisissez l'onglet Volumes.
4. Choisissez le volume que vous souhaitez mettre à jour.
5. Pour Actions, choisissez Mettre à jour le volume.

   La boîte de dialogue Mettre à jour le volume s'affiche avec les paramètres actuels du volume.
6. Pour Junction path, entrez un emplacement existant dans le système de fichiers pour monter le volume. Le nom doit être précédé d'une barre oblique, telle que `/vol1`.
7. Pour la taille du volume, vous pouvez augmenter ou diminuer la taille du volume dans la plage spécifiée dans la console Amazon FSx. Pour les FlexVol volumes, la taille maximale est de 300 TiB. Pour les FlexGroup volumes, la taille maximale est de 300 TiB multipliés par le nombre total de volumes constitutifs que vous FlexGroup possédez, jusqu'à un maximum de 20 PiB.
8. Pour l'efficacité du stockage, choisissez Activé pour activer les fonctionnalités d'efficacité du stockage ONTAP (déduplication, compression et compactage), ou choisissez Désactivé pour les désactiver.
9. Pour la politique de hiérarchisation du pool de capacité, choisissez une nouvelle politique de hiérarchisation du pool de stockage pour le volume, qui peut être Auto (par défaut), Snapshot uniquement, All ou None. Pour plus d'informations sur les politiques de hiérarchisation des pools de capacités, consultezPolitiques de hiérarchisation des volumes.
10. Pour le style de sécurité des volumes, choisissez Unix (Linux), NTFS ou Mixed. Le style de sécurité d'un volume détermine si la préférence est donnée aux ACL NTFS ou UNIX pour l'accès multiprotocole. Le mode MIXED n'est pas requis pour l'accès multiprotocole et n'est recommandé qu'aux utilisateurs expérimentés.
11. Pour la politique de capture instantanée, choisissez une politique de capture instantanée pour le volume. Pour plus d'informations sur les politiques relatives aux instantanés, consultezRègles relatives aux snapshots.

    Si vous choisissez Politique personnalisée, vous devez spécifier le nom de la politique dans le champ Politique personnalisée. La politique personnalisée doit déjà exister sur la SVM ou dans le système de fichiers. Vous pouvez créer une politique de capture personnalisée à l'aide de la CLI ONTAP ou de l'API REST. Pour plus d'informations, consultez la section Création d'une politique de capture instantanée dans la documentation du produit NetApp ONTAP.
12. Pour la période de refroidissement de la politique de hiérarchisation, les valeurs valides sont de 2 à 183 jours. La période de refroidissement de la politique de hiérarchisation d'un volume définit le nombre de jours avant que les données auxquelles il n'est pas possible d'accéder soient

signalées comme froides et transférées vers le stockage en pool de capacité. Ce paramètre n'affecte que les `Snapshot-only` politiques `Auto` et.

13. Choisissez Mettre à jour pour mettre à jour le volume.

Pour mettre à jour la configuration d'un volume (CLI)

- Pour mettre à jour la configuration d'un volume FSx for ONTAP, utilisez la commande update-volume CLI (ou l'opération UpdateVolumeAPI équivalente), comme indiqué dans l'exemple suivant.

```
aws fsx update-volume \
    --volume-id fsvol-1234567890abcdefa \
    --name new_vol \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
           SizeInMegabytes=2048,SnapshotPolicy=default-1weekly, \
           StorageEfficiencyEnabled=true, \
           TieringPolicy=all
```

Suppression d'un volume

Vous pouvez supprimer un volume FSx for ONTAP à l'aide de la console Amazon FSx, du, et de l'API Amazon FSx, en plus de AWS CLI l'interface de ligne de NetApp commande (CLI) ONTAP et de l'API REST.

> **Important**
>
> Vous ne pouvez supprimer des volumes à l'aide de la console, de l'API ou de la CLI Amazon FSx que si les sauvegardes Amazon FSx sont activées sur le volume.

> **Important**
>
> Lorsque vous supprimez un volume à l'aide de la console Amazon FSx, vous avez la possibilité d'effectuer une sauvegarde finale du volume. Vous pouvez créer de nouveaux volumes à partir de sauvegardes. Nous vous recommandons de choisir d'effectuer une sauvegarde finale comme meilleure pratique. Si vous n'en avez plus besoin au bout d'un certain temps, vous pouvez supprimer cette sauvegarde de volume ainsi que les autres

sauvegardes de volume créées manuellement. Lorsque vous supprimez un volume à l'aide de la commande `delete-volume` CLI, Amazon FSx effectue une sauvegarde finale par défaut.

Avant de supprimer un volume, assurez-vous qu'aucune application n'accède aux données du volume que vous souhaitez supprimer.

Pour supprimer un volume (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation de gauche, choisissez Systèmes de fichiers, puis choisissez le système de fichiers ONTAP dont vous souhaitez supprimer un volume.
3. Choisissez l'onglet Volumes.
4. Choisissez le volume que vous souhaitez supprimer.
5. Pour Actions, choisissez Supprimer le volume.
6. Dans la boîte de dialogue de confirmation, pour Créer une sauvegarde finale, vous avez deux options :
   - Choisissez Oui pour effectuer une sauvegarde finale du volume. Le nom de la sauvegarde finale s'affiche.
   - Choisissez Non si vous ne souhaitez pas effectuer de sauvegarde finale du volume. Il vous est demandé de confirmer qu'une fois le volume supprimé, les sauvegardes automatiques ne sont plus disponibles.
7. Confirmez la suppression du volume en saisissant supprimer dans le champ Confirmer la suppression.
8. Choisissez Supprimer le ou les volumes.

Pour supprimer un volume (CLI)

- Pour supprimer un volume FSx for ONTAP, utilisez la commande CLI delete-volume (ou l'opération DeleteVolumeAPI équivalente), comme indiqué dans l'exemple suivant.

```
aws fsx delete-volume --volume-id fsvol-1234567890abcde
```

Affichage d'un volume

Vous pouvez consulter les volumes FSx pour ONTAP qui se trouvent actuellement sur votre système de fichiers à l'aide de la console Amazon FSx, de AWS CLI l'API et des SDK Amazon FSx.

Pour consulter les volumes de votre système de fichiers :

- Utilisation de la console : choisissez un système de fichiers pour afficher la page détaillée des systèmes de fichiers. Cliquez sur l'onglet Volumes pour répertorier tous les volumes du système de fichiers, puis choisissez le volume que vous souhaitez afficher.
- Utilisation de la CLI ou de l'API : utilisez la commande de la CLI describe-volumes ou l'opération DescribeVolumesAPI.

Création d'un LUN iSCSI

Ce processus décrit comment créer un LUN iSCSI sur un système de fichiers de mise à l'échelle Amazon FSx for NetApp ONTAP à l'aide de la commande ONTAP CLI. NetApp lun create Pour plus d'informations, consultez lun createle centre de documentation NetApp ONTAP.

> **Note**
>
> Le protocole iSCSI n'est pas pris en charge pour les systèmes de fichiers évolutifs.

Ce processus suppose qu'un volume a déjà été créé sur votre système de fichiers. Pour plus d'informations, consultez Création de volumes.

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *management_endpoint_ip* par l'adresse IP du port de gestion du système de fichiers.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Pour plus d'informations, consultez Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.
2. Créez un LUN à l'aide de la commande lun create NetApp CLI, en remplaçant les valeurs suivantes :

- ***svm_name***- Nom de la machine virtuelle de stockage (SVM) fournissant la cible iSCSI. L'hôte utilise cette valeur pour atteindre le LUN.
- ***vol_name***- Le nom du volume hébergeant le LUN.
- ***lun_name***- Le nom que vous souhaitez attribuer au LUN.
- ***size***- La taille, en octets, du LUN. La taille maximale du LUN que vous pouvez créer est de 128 To.

> **Note**
>
> Nous vous recommandons d'utiliser un volume supérieur d'au moins 5 % à la taille de votre LUN. Cette marge laisse de la place pour les captures d'écran du volume.

- ***ostype***- Le système d'exploitation de l'hôte, `windows_2008` soit`linux`. Utilisable `windows_2008` pour toutes les versions de Windows ; cela garantit que le LUN dispose d'un décalage de bloc approprié pour le système d'exploitation et optimise les performances.

> **Note**
>
> Nous vous recommandons d'activer l'allocation d'espace sur votre LUN. Lorsque l'allocation d'espace est activée, ONTAP peut informer votre hôte lorsque le LUN est épuisé et peut récupérer de l'espace lorsque vous supprimez des données du LUN.

Pour plus d'informations, consultez la documentation `lun create`de la CLI NetApp ONTAP.

```
> lun create -vserver svm_name -path /vol/vol_name/lun_name -size size -
ostype ostype -space-allocation enabled
```

```
Created a LUN of size 10g (10737418240)
```

3. Vérifiez que le LUN est créé, en ligne et mappé.

```
> lun show
```

Le système répond avec le résultat suivant :

```
Vserver   Path                            State   Mapped   Type         Size
--------- ------------------------------- ------- -------- ------------ --------
svm_name
          /vol/vol_name/lun_name          online  unmapped windows_2008 10GB
```

Étapes suivantes

Maintenant que vous avez créé un LUN iSCSI, l'étape suivante du processus d'utilisation d'un LUN iSCSI comme stockage par blocs consiste à mapper le LUN à un. `igroup` Pour plus d'informations, consultez Montage de LUN iSCSI sur un client Linux ou Montage de LUN iSCSI sur un client Windows.

Gestion des actions des PME

Pour gérer les partages de fichiers SMB sur votre système de fichiers Amazon FSx, vous pouvez utiliser l'interface graphique des dossiers partagés de Microsoft Windows. L'interface utilisateur des dossiers partagés fournit un emplacement central pour gérer tous les dossiers partagés de votre machine virtuelle de stockage (SVM). Les procédures suivantes expliquent comment créer, mettre à jour et supprimer vos partages de fichiers.

> **Note**
>
> Vous pouvez également gérer les partages de fichiers SMB à l'aide du gestionnaire de NetApp système. Pour plus d'informations, consultez Utilisation NetApp de System Manager avec BlueXP.

Pour connecter des dossiers partagés à votre système de fichiers Amazon FSx

1. Lancez votre instance Amazon EC2 et connectez-la au Microsoft Active Directory auquel votre système de fichiers Amazon FSx est joint. Pour ce faire, choisissez l'une des procédures suivantes dans le guide AWS Directory Service d'administration :

   - Rejoignez facilement une instance Windows EC2
   - Joindre manuellement une instance Windows

2. Connectez-vous à votre instance en tant qu'utilisateur membre du groupe des administrateurs du système de fichiers. Pour plus d'informations, consultez la section Connexion à votre instance Windows dans le guide de l'utilisateur Amazon EC2.
3. Ouvrez le menu Démarrer et exécutez fsmgmt.msc à l'aide de la commande Exécuter en tant qu'administrateur. Cela ouvre l'outil graphique des dossiers partagés.
4. Pour Action, choisissez Connect to another computer.
5. Pour Autre ordinateur, entrez le nom DNS de votre machine virtuelle de stockage (SVM), par exemple**`netbios_name.corp.example.com`**.

   Pour trouver le nom DNS de votre SVM sur la console Amazon FSx, choisissez Storage virtual machines, choisissez votre SVM, puis faites défiler la page jusqu'à Endpoints jusqu'à ce que vous trouviez le nom DNS SMB. Vous pouvez également obtenir le nom DNS dans la réponse de l'opération d'DescribeStorageVirtualMachinesAPI.
6. Choisissez OK. Une entrée pour votre système de fichiers Amazon FSx apparaît ensuite dans la liste de l'outil Dossiers partagés.

Maintenant que Shared Folders est connecté à votre système de fichiers Amazon FSx, vous pouvez gérer les partages de fichiers Windows sur le système de fichiers en effectuant les actions suivantes :

> **Note**
>
> Nous vous recommandons de localiser vos partages SMB sur un volume autre que votre volume racine.

- Créer un nouveau partage de fichiers : dans l'outil Dossiers partagés, choisissez Shares dans le volet de gauche pour voir les partages actifs de votre système de fichiers Amazon FSx. Les volumes sont affichés montés sur le chemin choisi lors de leur création. Choisissez Nouveau partage et complétez l'assistant de création d'un dossier partagé.

  Vous devez créer le dossier local avant de créer le nouveau partage de fichiers. Vous pouvez le faire comme suit :

  - À l'aide de l'outil Dossiers partagés : choisissez Parcourir lorsque vous spécifiez le chemin d'un dossier local, choisissez Créer un nouveau dossier pour créer le dossier local.
  - À l'aide de la ligne de commande :

```
New-Item -Type Directory -Path \\netbios_name.corp.example.com\C
$volume_path\MyNewFolder
```

- Modifier un partage de fichiers : dans l'outil Dossiers partagés, ouvrez le menu contextuel (clic droit) du partage de fichiers que vous souhaitez modifier dans le volet droit, puis choisissez Propriétés. Modifiez les propriétés et cliquez sur OK.
- Supprimer un partage de fichiers : dans l'outil Dossiers partagés, ouvrez le menu contextuel (clic droit) du partage de fichiers que vous souhaitez supprimer dans le volet droit, puis choisissez Arrêter le partage.

> **Note**
>
> La suppression des partages de fichiers de l'interface graphique n'est possible que si vous vous êtes connecté à fsmgmt.msc en utilisant le nom DNS du système de fichiers Amazon FSx. Si vous vous êtes connecté en utilisant l'adresse IP ou le nom d'alias DNS du système de fichiers, l'option Arrêter le partage ne fonctionnera pas et le partage de fichiers n'est pas supprimé.

Audit d'audit de l'audit

Amazon FSx for NetApp ONTAP prend en charge l'audit des accès des utilisateurs finaux aux fichiers et aux répertoires d'une machine virtuelle de stockage (SVM).

Rubriques

- Présentation de l'audit de l'accès aux fichiers
- Vue d'ensemble des tâches de configuration de l'audit de l'accès aux fichiers

Présentation de l'audit de l'accès aux fichiers

L'audit de l'accès aux fichiers vous permet d'enregistrer les accès des utilisateurs finaux à des fichiers et répertoires individuels en fonction des politiques d'audit que vous définissez. L'audit de l'accès aux fichiers peut vous aider à améliorer la sécurité de votre système et à réduire le risque d'accès non autorisé aux données de votre système. L'audit de l'accès aux fichiers aide vos entreprises à rester en conformité avec les exigences en matière de protection des données, à identifier rapidement les menaces potentielles et à réduire le risque de violation de données.

Pour les accès aux fichiers et aux répertoires, Amazon FSx prend en charge la journalisation des tentatives réussies (par exemple, un utilisateur disposant des autorisations suffisantes accédant à un fichier), des tentatives infructueuses, ou des deux. Vous pouvez également désactiver l'audit d'accès aux fichiers à tout moment.

Par défaut, les journaux des événements d'audit sont stockés au format de`EVTX` fichier, ce qui vous permet de les consulter à l'aide de Microsoft Event Viewer.

Événements d'accès aux PME qui peuvent être audités

Le tableau suivant répertorie les événements d'accès aux fichiers et aux dossiers SMB qui peuvent être audités.

Identifiant de l'événement (EVT/ EVTX)	Événement	Description	Catégorie
560/4656	Ouvrir un objet/Créer un objet	ACCÈS À L'OBJET : Objet (fichier ou répertoire) ouvert	Accès aux fichiers
563/4659	Ouvrir un objet avec l'intention de le supprimer	ACCÈS AUX OBJETS : Un descripteur d'un objet (fichier ou répertoir e) a été demandé avec l'intention de supprimer	Accès aux fichiers
564/460	Suppression d’objet	ACCÈS À L'OBJET : Supprimer l'objet (fichier ou répertoire). ONTAP génère cet événement lorsqu'un client Windows tente de supprimer l'objet (fichier ou répertoire)	Accès aux fichiers

Identifiant de l'événement (EVT/EVTX)	Événement	Description	Catégorie
567/463	Lire l'objet/Écrire un objet/Obtenir les attributs de l'objet/Définir les attributs de l'objet	ACCÈS À L'OBJET : tentative d'accès à un objet (lecture, écriture, obtention d'un attribut, définition d'un attribut) . **Note** Pour cet événement, ONTAP audite uniquement la première opération de lecture SMB et la première opération d'écriture SMB (réussite ou échec) sur un objet. Cela empêche ONTAP de créer des entrées de journal excessives lorsqu'un seul client ouvre un objet et effectue de nombreuse	Accès aux fichiers

Identifiant de l'événement (EVT/ EVTX)	Événement	Description	Catégorie
		s opération s de lecture ou d'écriture successives sur le même objet.	
N/A/4664	Lien dur	ACCÈS À L'OBJET : Une tentative a été faite pour créer un lien physique	Accès aux fichiers
N/A/N/A Numéro d'événement ONTAP 9999	Renommez l'objet	ACCÈS À L'OBJET : Objet renommé. Il s'agit d'un événement ONTAP. Il n'est actuellement pas pris en charge par Windows en tant qu'événement unique.	Accès aux fichiers
N/A/N/A Numéro d'événement ONTAP 9998	Dissocier un objet	ACCÈS À L'OBJET : Objet non lié. Il s'agit d'un événement ONTAP. Il n'est actuellement pas pris en charge par Windows en tant qu'événement unique.	Accès aux fichiers

Événements d'accès NFS pouvant être audités

Les événements d'accès aux fichiers et aux dossiers NFS suivants peuvent être audités.

- READ
- OPEN
- CLOSE
- READDIR
- WRITE
- SETATTR
- CREATE
- LIEN
- OPENATTR
- SUPPRIMER
- GETATTR
- VÉRIFIER
- NVÉRIFIER
- RENAME

Vue d'ensemble des tâches de configuration de l'audit de l'accès aux fichiers

La configuration de FSx pour ONTAP à des fins d'audit de l'accès aux fichiers implique les tâches de haut niveau suivantes :

1. Familiarisez-vous avec les exigences et les considérations relatives à l'audit de l'accès aux fichiers.
2. Créez une configuration d'audit sur une SVM spécifique.
3. Activez l'audit sur cette SVM.
4. Configurez des politiques d'audit sur vos fichiers et répertoires.
5. Consultez les journaux des événements d'audit une fois que FSx pour ONTAP les a émis.

Les détails des tâches sont fournis dans les procédures suivantes.

Répétez les tâches pour toute autre SVM de votre système de fichiers pour laquelle vous souhaitez activer l'audit de l'accès aux fichiers.

Exigences en matière d'audit

Avant de configurer et d'activer la configuration et l'activation de l'audit sur une condition et les points suivants :

- L'audit NFS prend en charge les entrées de contrôle d'accès (ACE) d'audit désignées par typeu, qui génèrent une entrée de journal d'audit lorsque l'accès est tenté à l'objet. Pour l'audit NFS, il n'existe aucun mappage entre les bits de mode et les ACE d'audit. Lors de la conversion des ACL en bits de mode, les ACE d'audit sont ignorées. Lors de la conversion des bits de mode en ACL, les ACE d'audit ne sont pas générés.
- L'audit dépend de l'espace disponible dans les volumes intermédiaires. (Un volume intermédiaire est un volume dédié créé par ONTAP pour stocker des fichiers intermédiaires, qui sont des fichiers binaires intermédiaires sur des nœuds individuels dans lesquels les enregistrements d'audit sont stockés avant leur conversion au format de fichier EVTX ou XML.) Vous devez vous assurer qu'il y a suffisamment d'espace pour les volumes intermédiaires dans les agrégats contenant des volumes audités.
- L'audit dépend de l'espace disponible dans le volume contenant le répertoire dans lequel les journaux d'événements d'audit convertis sont stockés. Vous devez vous assurer qu'il y a suffisamment d'espace dans les volumes utilisés pour stocker les journaux d'événements. Vous pouvez spécifier le nombre de journaux d'audit à conserver dans le répertoire d'audit en utilisant le`-rotate-limit` paramètre lors de la création d'une configuration d'audit, ce qui permet de garantir que l'espace disponible est suffisant pour les journaux d'audit dans le volume.

Création de configurations d'audit sur les SVM

Avant de commencer à auditer les événements liés aux fichiers et aux répertoires, vous devez créer une configuration d'audit sur la machine virtuelle de stockage (SVM). Une fois la configuration d'audit créée, vous devez l'activer sur la configuration d'audit.

Avant d'utiliser la`vserver audit create` commande pour créer la configuration d'audit, assurez-vous que vous avez créé un répertoire à utiliser comme destination pour les journaux et que le répertoire ne contient pas de liens symboliques. Vous spécifiez le répertoire de destination à l'aide du`-destination` paramètre.

Vous pouvez créer une configuration d'audit qui fait pivoter les journaux d'audit en fonction de leur taille ou d'un calendrier, comme suit :

- Pour faire pivoter les journaux d'audit en fonction de leur taille, utilisez cette commande :

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}] [-
rotate-limit integer] [-rotate-size {integer[KB|MB|GB|TB|PB]}]
```

L'exemple suivant crée une configuration d'audit pour la SVM nomméesvm1 qui audite les opérations sur les fichiers et les événements d'ouverture et de fermeture de session CIFS (SMB) (par défaut) en utilisant une rotation basée sur la taille. Le format du journal est le suivantEVTX (par défaut), les journaux sont stockés dans le/audit_log répertoire et vous n'aurez qu'un seul fichier journal à la fois (taille maximale de 200 Mo).

```
vserver audit create -vserver svm1 -destination /audit_log -rotate-size 200MB
```

- Pour alterner les journaux d'audit en fonction d'un calendrier, utilisez cette commande :

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}]
        [-rotate-limit integer] [-rotate-schedule-month chron_month]
        [-rotate-schedule-dayofweek chron_dayofweek] [-rotate-schedule-
day chron_dayofmonth]
        [-rotate-schedule-hour chron_hour] [-rotate-schedule-minute chron_minute]
```

Le-rotate-schedule-minute paramètre est obligatoire si vous configurez la rotation des journaux d'audit basée sur le temps.

L'exemple suivant crée une configuration d'audit pour la SVM nommée à l'svm2aide d'une rotation basée sur le temps. Le format des journaux estEVTX (par défaut) et les journaux d'audit sont renouvelés tous les mois, à 12 h 30, tous les jours de la semaine.

```
vserver audit create -vserver svm2 -destination /audit_log -rotate-size 200MB  -
rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour 12 -
rotate-schedule-minute 30
```

Vous pouvez utiliser le-format paramètre pour spécifier si les journaux d'audit sont créés auEVTX format converti (par défaut) ou au format deXML fichier. LeEVTX format vous permet de visualiser les fichiers journaux avec Microsoft Event Viewer.

Par défaut, les catégories d'événements à auditer sont les événements d'accès aux fichiers (SMB et NFS), les événements d'ouverture et de fermeture de session CIFS (SMB) et les événements de

modification des politiques d'autorisation. Vous pouvez mieux contrôler les événements à enregistrer à l'aide du`-events` paramètre, dont le format est le suivant :

```
-events {file-ops|cifs-logon-logoff|cap-staging|file-share|audit-policy-change|user-account|authorization-policy-change|security-group}
```

Par exemple, l'utilisation`-events file-share` permet d'auditer les événements de partage de fichiers.

Pour plus d'informations sur la`vserver audit create` commande, voir Créer une configuration d'audit.

Activation de l'audit sur une SVM

Une fois que vous avez fini de configurer la configuration d'audit, vous devez activer l'audit sur la SVM. Pour cela, utilisez la commande suivante :

```
vserver audit enable -vserver svm_name
```

Par exemple, utilisez la commande suivante pour activer l'audit sur la commande suivante`svm1` :

```
vserver audit enable -vserver svm1
```

Vous pouvez désactiver l'audit d'accès à tout moment. Par exemple, utilisez la commande suivante pour désactiver l'audit sur la SVM nommée`svm4`.

```
vserver audit disable -vserver svm4
```

Lorsque vous désactivez l'audit, la configuration d'audit n'est pas supprimée sur la SVM, ce qui signifie que vous pouvez réactiver l'audit sur cette SVM à tout moment.

Configuration des politiques d'audit des fichiers et des dossiers

Vous devez configurer des politiques d'audit sur les fichiers et les dossiers que vous souhaitez auditer pour détecter les tentatives d'accès des utilisateurs. Vous pouvez configurer des politiques d'audit pour surveiller à la fois les tentatives d'accès réussies et infructueuses.

Vous pouvez configurer les politiques d'audit SMB et NFS. Les politiques d'audit SMB et NFS ont des exigences de configuration et des fonctionnalités d'audit différentes en fonction du style de sécurité du volume.

Politiques d'audit relatives aux fichiers et répertoires de type sécurisé NTFS

Vous pouvez configurer les politiques d'audit NTFS à l'aide de l'onglet Windows Security ou de l'ONTAP CLI.

Pour configurer les politiques d'audit NTFS (onglet Sécurité Windows)

Vous configurez les politiques d'audit NTFS en ajoutant des entrées aux SACL NTFS associées à un descripteur de sécurité NTFS. Le descripteur de sécurité est ensuite appliqué aux fichiers et répertoires NTFS. Ces tâches sont automatiquement gérées par l'interface graphique de Windows. Le descripteur de sécurité peut contenir des listes de contrôle d'accès discrétionnaires (DACL) pour appliquer des autorisations d'accès aux fichiers et aux dossiers, des SACL pour l'audit des fichiers et des dossiers, ou à la fois des SACL et des DACL.

1. Dans le menu Outils de l'Explorateur Windows, sélectionnez Mapper le lecteur réseau.
2. Complétez la case Map Network Drive :

   a. Choisissez une lettre Drive.
   b. Dans la zone Dossier, tapez le nom du serveur SMB (CIFS) qui contient le partage, contenant les données que vous souhaitez auditer et le nom du partage.
   c. Choisissez Finish (Terminer).

   Le lecteur que vous avez sélectionné est monté et prêt. La fenêtre de l'Explorateur Windows affiche les fichiers et les dossiers contenus dans le partage.
3. Sélectionnez le fichier ou le répertoire pour lequel vous souhaitez activer l'accès d'audit.
4. Cliquez avec le bouton droit droit de la souris sur le fichier ou le répertoire, puis sélectionnez Properties.
5. Choisissez l'onglet Security (Sécurité).
6. Cliquez sur Avancé.
7. Cliquez sur l'onglet Audit.
8. Effectuez les actions souhaitées :

Si vous souhaitez...	Procédez comme suit :
Configurer l'audit pour un nouvel	1. Choisissez Add (Ajouter).

Si vous souhaitez...	Procédez comme suit :
utilisateur ou un nouveau groupe	2. Dans la zone Entrez le nom de l'objet à sélectionner, tapez le nom de l'utilisateur ou du groupe que vous souhaitez ajouter. 3. Sélectionnez OK.
Supprimer l'audit d'un utilisateur ou d'un groupe	1. Dans la zone Entrez le nom de l'objet à sélectionner, sélectionnez l'utilisateur ou le groupe que vous souhaitez supprimer. 2. Choisissez Remove (Supprimer). 3. Sélectionnez OK. 4. Ignorez le reste de cette procédure.
Audit des modifications pour un utilisateur ou un groupe	1. Dans la zone Entrez le nom de l'objet à sélectionner, choisissez l'utilisateur ou le groupe que vous souhaitez modifier. 2. Choisissez Edit (Modifier). 3. Sélectionnez OK.

Si vous configurez l'audit sur un utilisateur ou un groupe ou si vous modifiez l'audit sur un utilisateur ou un groupe existant, la zone Entrée d'audit pour ***l'objet*** s'ouvre.

9. Dans la zone Appliquer à, sélectionnez la manière dont vous souhaitez appliquer cette entrée d'audit.

   Si vous configurez l'audit sur un seul fichier, la case Appliquer à n'est pas active, car elle est définie par défaut sur Cet objet uniquement.

10. Dans la zone Accès, sélectionnez les éléments que vous souhaitez auditer et indiquez si vous souhaitez auditer les événements réussis, les événements d'échec, ou les deux.

    - Pour auditer les événements réussis, cochez la case Succès.
    - Pour auditer les événements de défaillance, cochez la case Échec.

    Choisissez les actions que vous devez surveiller pour répondre à vos exigences de sécurité. Pour plus d'informations sur ces informations sur ces informations, consultez la documentation Windows. Vous pouvez audidit les audits des journaux suivants :

    - Contrôle total

- Traverser le dossier/exécuter le fichier
- Répertorier le dossier/lire les données
- Lire les attributs
- Lire les attributs étendus
- Création de fichiers/écriture de données
- Créer des dossiers/ajouter des données
- Écriture d'attributs
- Écriture d'attributs étendus
- Supprimer des sous-dossiers et des fichiers
- Delete
- Autorisations de lecture
- Modifier les autorisations
- Prenez la propriété

11. Si vous ne souhaitez pas que le paramètre d'audit se propage aux fichiers et dossiers suivants du conteneur d'origine, cochez la case Appliquer ces entrées d'audit aux objets et/ou aux conteneurs de ce conteneur uniquement.
12. Choisissez Apply (Appliquer).
13. Une fois que vous avez fini d'ajouter, de supprimer ou de modifier des entrées d'audit, cliquez sur OK.

    La zone Entrée d'audit pour ***l'objet*** se ferme.
14. Dans la zone Audit, choisissez les paramètres d'héritage pour ce dossier. Choisissez uniquement le niveau minimal qui fournit les événements d'audit répondant à vos exigences de sécurité.

    Vous pouvez choisir l'une des méthodes suivantes.

    - Choisissez l'option Inclure les entrées d'audit héritables depuis la zone parent de cet objet.
    - Choisissez la zone Remplacer toutes les entrées d'audit héritables existantes sur tous les descendants par des entrées d'audit héritables provenant de cet objet.
    - Choisissez les deux cases.
    - Ne choisissez aucune des deux cases.

Si vous définissez des SACL sur un seul fichier, la zone Remplacer toutes les entrées d'audit héritables existantes sur tous les descendants par des entrées d'audit héritables provenant de cet objet n'est pas présente dans la zone Audit.

15. Sélectionnez OK.

Pour configurer les politiques d'audit NTFS (ONTAP CLI)

À l'aide de l'interface de ligne de commande ONTAP, vous pouvez configurer des politiques d'audit NTFS sans avoir à vous connecter aux données via un partage SMB sur un client Windows.

- Vous pouvez configurer les politiques d'audit NTFS à l'aide de la famille de commandes vserver security file-directory.

Par exemple, la commande suivante applique une politique de sécurité nomméep1 à la SVM nomméevs0.

```
vserver security file-directory apply -vserver vs0 -policy-name p1
```

Politiques d'audit relatives aux fichiers et répertoires de type UNIX

Vous configurez l'audit pour les fichiers et répertoires de type UNIX en ajoutant des ACE d'audit (expressions de contrôle d'accès) aux ACL NFS v4.x (listes de contrôle d'accès). Cela vous permet de surveiller certains événements d'accès aux fichiers et répertoires NFS à des fins de sécurité.

> **Note**
>
> Pour NFS v4.x, les ACE discrétionnaires et les ACE du système sont stockés dans la même ACL. Par conséquent, vous devez être prudent lorsque vous ajoutez des ACL d'audit à une ACL existante afin d'éviter de remplacer et de perdre une ACL existante. L'ordre dans lequel vous ajoutez les ACE d'audit à une ACL existante n'a pas d'importance.

Pour configurer les politiques d'audit UNIX

1. Récupérez l'ACL existante pour le fichier ou le répertoire à l'aide de la commandenfs4_getfacl ou d'une commande équivalente.
2. Ajoutez les ACE d'audit souhaités.

3. Appliquez l'ACL mise à jour au fichier ou au répertoire à l'aide de la commandenfs4_setfacl ou d'une commande équivalente.

   Cet exemple utilise l'-aoption pour accorder à un utilisateur (nommétestuser) des autorisations de lecture sur le fichier nomméfile1.

   ```
   nfs4_setfacl -a "A::testuser@example.com:R" file1
   ```

Affichage des journaux d'journaux d'journaux d'audit

Vous pouvez consulter les journaux des événements d'audit enregistrés au format deXML fichierEVTX or.

- EVTXformat de fichier : vous pouvez ouvrir les journauxEVTX d'événements d'audit convertis en tant que fichiers enregistrés à l'aide de Microsoft Event Viewer.

  Vous pouvez utiliser deux options lorsque vous consultez les journaux d'événements à l'aide de l'Observateur d'événements :

  - Vue générale : les informations communes à tous les événements sont affichées pour l'enregistrement de l'événement. Les données spécifiques à l'événement pour l'enregistrement de l'événement ne sont pas affichées. Vous pouvez utiliser la vue détaillée pour afficher des données spécifiques à l'événement.
  - Vue détaillée : une vue conviviale et une vue XML sont disponibles. La vue conviviale et la vue XML affichent à la fois les informations communes à tous les événements et les données spécifiques à l'événement pour l'enregistrement de l'événement.
- XMLformat de fichier : vous pouvez afficher et traiter les journaux d'événements d'audit XML sur des applications tierces prenant en charge le format de fichier XML. Les outils de visualisation XML peuvent être utilisés pour afficher les journaux d'audit à condition de disposer du schéma XML et d'informations sur les définitions des champs XML.

Élargissement de la capacité de stockage SSD et IOPS provisionnées

Lorsque vous avez besoin de stockage supplémentaire pour la partie active de votre ensemble de données, vous pouvez augmenter la capacité de stockage sur disque SSD (Solid State Drive)

de votre système de fichiers Amazon FSx for NetApp ONTAP. Vous pouvez le faire en utilisant la console Amazon FSx, l'API Amazon FSx ou (). AWS Command Line Interface AWS CLI

Vous pouvez également modifier les IOPS du SSD provisionné pour votre système de fichiers, soit lorsque vous augmentez la capacité de stockage du SSD principal, soit en tant qu'action indépendante. Pour plus d'informations sur le dimensionnement de la capacité de stockage SSD principal d'un système de fichiers et sur la quantité d'IOPS allouées, consultez. Mise à jour du système de fichiers, du stockage SSD et des IOPS

Gestion de la capacité de débit

FSx for ONTAP configure la capacité de débit lorsque vous créez le système de fichiers. Vous pouvez modifier la capacité de débit de votre système de fichiers scale-out à tout moment, mais vous ne pouvez pas modifier la capacité de débit de votre système de fichiers scale-out. N'oubliez pas que votre système de fichiers nécessite une configuration spécifique pour atteindre une capacité de débit maximale. Par exemple, pour fournir une capacité de débit de 4 Gbit/s à un système de fichiers évolutif, votre système de fichiers nécessite une configuration avec un minimum de 5 120 GiB de capacité de stockage SSD et 160 000 IOPS SSD. Pour en savoir plus, consultez Impact de la capacité de débit sur les performances.

La capacité de débit est l'un des facteurs qui déterminent la vitesse à laquelle le serveur de fichiers hébergeant le système de fichiers peut traiter les données des fichiers. Des niveaux de capacité de débit plus élevés s'accompagnent de niveaux plus élevés de réseau, d'opérations d'E/S de lecture de disque par seconde (IOPS) et de capacité de mise en cache des données sur le serveur de fichiers. Pour en savoir plus, consultez Performance.

Lorsque vous modifiez la capacité de débit de votre système de fichiers, Amazon FSx remplace le serveur de fichiers qui alimente votre système de fichiers. Les systèmes de fichiers mono-AZ et multi-AZ subissent un basculement et un retour en arrière automatiques au cours de ce processus, qui prend généralement quelques minutes. Les processus de basculement et de restauration sont transparents pour les clients NFS (Network File Sharing), SMB (Server Message Block) et iSCSI (Internet Small Computer Systems Interface), ce qui permet à vos charges de travail de continuer à fonctionner sans interruption ni intervention manuelle. La nouvelle capacité de débit vous est facturée une fois qu'elle est disponible pour votre système de fichiers.

> **Note**
>
> Pour garantir l'intégrité des données pendant les activités de maintenance, FSx for ONTAP ferme tous les verrous opportunistes et termine toutes les opérations d'écriture en attente

sur les volumes de stockage sous-jacents hébergeant votre système de fichiers avant le début de la maintenance. Au cours d'une fenêtre de maintenance planifiée du système de fichiers, les modifications du système (telles que les modifications de votre capacité de débit) peuvent être retardées. La maintenance du système peut entraîner la mise en attente de ces modifications jusqu'à ce qu'elles soient traitées. Pour en savoir plus, consultez the section called “Fenêtres de maintenance”.

Rubriques

Quand modifier la capacité de débit

Amazon FSx s'intègre à Amazon CloudWatch, ce qui vous permet de surveiller les niveaux d'utilisation continue du débit de votre système de fichiers. Le débit et les performances d'IOPS que vous pouvez atteindre dans votre système de fichiers dépendent des caractéristiques spécifiques de votre charge de travail, en plus de la capacité de débit de votre système de fichiers. En règle générale, vous devez prévoir une capacité de débit suffisante pour prendre en charge le débit de lecture de votre charge de travail plus le double du débit d'écriture de votre charge de travail. Vous pouvez utiliser CloudWatch des métriques pour déterminer laquelle de ces dimensions doit être modifiée pour améliorer les performances. Pour en savoir plus, consultez the section called “Comment utiliser FSx pour les métriques ONTAP CloudWatch”.

> **Note**
>
> Vous ne pouvez pas modifier la capacité de débit pour les systèmes de fichiers évolutifs.

Comment les demandes simultanées de débit et de dimensionnement du stockage sont traitées

Vous pouvez demander une mise à jour de la capacité de débit juste avant le début du flux de mise à jour de la capacité de stockage SSD et des IOPS provisionnées ou pendant qu'il est en cours. L'ordre dans lequel Amazon FSx gère les deux demandes est le suivant :

- Si vous soumettez une mise à jour SSD/IOPS et une mise à jour de la capacité de débit en même temps, les deux demandes sont acceptées. La mise à jour SSD/IOPS est priorisée avant la mise à jour de la capacité de débit.
- Si vous soumettez une mise à jour de la capacité de débit alors qu'une mise à jour des SSD/IOPS est en cours, la demande de mise à jour de la capacité de débit est acceptée et mise en file d'attente pour être exécutée après la mise à jour des SSD/IOPS. La mise à jour de la capacité de débit commence après la mise à jour du SSD/IOPS (de nouvelles valeurs sont disponibles) et pendant l'étape d'optimisation. Cela prend généralement moins de 10 minutes.
- Si vous soumettez une mise à jour SSD/IOPS alors qu'une mise à jour de la capacité de débit est en cours, la demande de mise à jour du stockage SSD/IOPS est acceptée et mise en file d'attente pour démarrer une fois la mise à jour de la capacité de débit terminée (une nouvelle capacité de débit est disponible). Cela prend généralement 20 minutes.

Pour plus d'informations sur le stockage SSD et les mises à jour des IOPS provisionnées, consultez. Gestion de la capacité de stockage

Comment modifier la capacité de débit

Vous pouvez modifier la capacité de débit d'un système de fichiers à l'aide de la console Amazon FSx, AWS Command Line Interface du AWS CLI () ou de l'API Amazon FSx.

Pour modifier la capacité de débit d'un système de fichiers (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Accédez à Systèmes de fichiers, puis choisissez le système de fichiers ONTAP dont vous souhaitez augmenter la capacité de débit.
3. Pour Actions, sélectionnez Mettre à jour la capacité de débit. Ou, dans le panneau Résumé, choisissez Mettre à jour à côté de la capacité de débit du système de fichiers.
4. Choisissez la nouvelle valeur pour la capacité de débit dans la liste.

> **Note**
>
> Vous pouvez modifier la capacité de débit de n'importe quel système de fichiers FSx for ONTAP. Toutefois, seuls les systèmes de fichiers créés le 9 décembre 2021 ou après cette date peuvent prendre en charge une capacité de débit de 128 Mo/s ou 256 Mo/s.

5. Choisissez Mettre à jour pour lancer la mise à jour de la capacité de débit.
6. Vous pouvez suivre la progression de la mise à jour sur la page détaillée des systèmes de fichiers, dans l'onglet Mises à jour.

   Vous pouvez suivre la progression de la mise à jour à l'aide de la console Amazon FSx, duAWS CLI, et de l'API. Pour en savoir plus, consultez Surveillance des variations de capacité de débit.

Pour modifier la capacité de débit (CLI) d'un système de fichiers

Pour modifier la capacité de débit d'un système de fichiers, utilisez la AWS CLI commande update-file-system. Définissez les paramètres suivants :

- `--file-system-id`à l'ID du système de fichiers que vous mettez à jour.
- `ThroughputCapacity`à la valeur souhaitée pour mettre à jour le système de fichiers.

Vous pouvez suivre la progression de la mise à jour à l'aide de la console Amazon FSx, duAWS CLI, et de l'API. Pour en savoir plus, consultez Surveillance des variations de capacité de débit.

Surveillance des variations de capacité de débit

Vous pouvez suivre la progression d'une modification de la capacité de débit à l'aide de la console Amazon FSx, de l'API et du. AWS CLI

Surveillance des variations de capacité de débit dans la console

Dans l'onglet Mises à jour de la fenêtre des détails du système de fichiers, vous pouvez consulter les 10 actions de mise à jour les plus récentes pour chaque type d'action de mise à jour.

Pour les actions de mise à jour de la capacité de débit, vous pouvez consulter les informations suivantes.

Type de mise à jour

Les types pris en charge sont la capacité de débit, la capacité de stockage et l'optimisation du stockage.

Valeur cible

La valeur souhaitée pour modifier la capacité de débit du système de fichiers.

Statut

État actuel de la mise à jour. Pour les mises à jour de la capacité de débit, les valeurs possibles sont les suivantes :

- En attente : Amazon FSx a reçu la demande de mise à jour, mais n'a pas commencé à la traiter.
- En cours — Amazon FSx traite la demande de mise à jour.
- Terminé — La mise à jour de la capacité de débit s'est terminée avec succès.
- Échec : la mise à jour de la capacité de débit a échoué. Choisissez le point d'interrogation (?) pour en savoir plus sur les raisons de l'échec de la mise à jour du débit.

Heure de la demande

Heure à laquelle Amazon FSx a reçu la demande de mise à jour.

Surveillance des modifications à l'aide de l'API AWS CLI and

Vous pouvez afficher et surveiller les demandes de modification de la capacité du débit du système de fichiers à l'aide de la commande describe-file-systemsCLI et de l'action DescribeFileSystemsAPI. Le `AdministrativeActions` tableau répertorie les 10 actions de mise à jour les plus récentes pour chaque type d'action administrative. Lorsque vous modifiez la capacité de débit d'un système de fichiers, une action `FILE_SYSTEM_UPDATE` administrative est générée.

L'exemple suivant montre l'extrait de réponse d'une commande `describe-file-systems` CLI. Le système de fichiers a une capacité de débit de 128 Mo/s et une capacité de débit cible de 256 Mo/s.

```
.
.
.
    "ThroughputCapacity": 128,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
```

```
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Lorsqu'Amazon FSx traite l'action avec succès, le statut passe à. `COMPLETED` La nouvelle capacité de débit est alors disponible pour le système de fichiers et apparaît dans la `ThroughputCapacity` propriété. Ceci est illustré dans l'extrait de réponse suivant d'une commande describe-file-systems CLI.

```
.
.
.
    "ThroughputCapacity": 256,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "COMPLETED",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Si la modification de la capacité de débit échoue, le statut passe à`FAILED`, et la `FailureDetails` propriété fournit des informations sur la panne.

Optimisation des performances avec les fenêtres de maintenance Amazon FSx

En tant que service entièrement géré, FSx for ONTAP assure régulièrement la maintenance et les mises à jour de votre système de fichiers. Cette maintenance n'a aucun impact sur la plupart des

charges de travail. Pour les charges de travail sensibles aux performances, vous pouvez parfois remarquer un impact bref (<60 secondes) sur les performances lors de la maintenance ; Amazon FSx vous permet d'utiliser la fenêtre de maintenance pour contrôler le moment où de telles activités de maintenance potentielles se produisent.

L'application de correctifs est peu fréquente, généralement une fois toutes les quelques semaines. Pour les systèmes de fichiers évolutifs, l'application des correctifs ne prend généralement que 30 minutes à compter du début de votre fenêtre de maintenance. Pour les systèmes de fichiers évolutifs, l'application des correctifs prend jusqu'à 90 minutes à compter du début de votre fenêtre de maintenance. Pendant ces quelques minutes, vos systèmes de fichiers basculent et reprennent automatiquement le dessus. Vous choisissez la fenêtre de maintenance lors de la création du système de fichiers. Si vous n'avez aucune préférence horaire, une heure de début de 30 minutes est attribuée.

FSx for ONTAP vous permet d'ajuster votre fenêtre de maintenance en fonction de vos besoins en fonction de votre charge de travail et de vos exigences opérationnelles. Vous pouvez déplacer votre fenêtre de maintenance aussi souvent que nécessaire, à condition qu'une fenêtre de maintenance ait lieu au moins une fois tous les 14 jours. Si un correctif est publié et qu'aucune fenêtre de maintenance ne se produit dans les 14 jours, FSx for ONTAP procédera à la maintenance du système de fichiers afin de garantir sa sécurité et sa fiabilité.

> **Note**
>
> Pour garantir l'intégrité des données pendant les activités de maintenance, FSx for ONTAP ferme tous les verrous opportunistes et termine toutes les opérations d'écriture en attente sur les volumes de stockage sous-jacents hébergeant votre système de fichiers avant le début de la maintenance.

Vous pouvez utiliser la console de gestion Amazon FSx AWS CLI, AWS l'API ou l'un des AWS SDK pour modifier la fenêtre de maintenance de vos systèmes de fichiers.

Pour modifier le créneau de maintenance hebdomadaire (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Choisissez Systèmes de fichiers dans la colonne de navigation de gauche.
3. Choisissez le système de fichiers dont vous souhaitez modifier la fenêtre de maintenance hebdomadaire. La page des détails du système de fichiers récapitulatif apparaît.

4. Choisissez Administration pour afficher le panneau des paramètres d'administration du système de fichiers.
5. Choisissez Mettre à jour pour afficher la fenêtre de maintenance des modifications.
6. Entrez le nouveau jour et l'heure auxquels vous souhaitez que la fenêtre de maintenance hebdomadaire commence.
7. Choisissez Save pour enregistrer les changements. La nouvelle heure de début de maintenance est affichée dans le panneau des paramètres d'administration du système de fichiers.

Pour modifier la fenêtre de maintenance hebdomadaire à l'aide de la commande update-file-systemCLI, consultezPour mettre à jour un système de fichiers (CLI).

Baliser vos ressources Amazon FSx

Pour vous aider à gérer vos systèmes de fichiers et autres ressources Amazon FSx, vous pouvez attribuer vos propres métadonnées à chaque ressource sous la forme de balises. Les balises vous permettent de classer vos AWS ressources de différentes manières, par exemple, par objectif, par propriétaire ou par environnement. Cette catégorisation est utile lorsque vous avez de nombreuses ressources de même type. Elle vous permet d'identifier rapidement une ressource spécifique en fonction des balises que vous lui avez attribuées. Cette rubrique décrit les identifications et explique comment les créer.

Rubriques

- Principes de base des étiquettes
- Identification de vos ressources
- Copier les balises aux sauvegardes
- Restrictions liées aux étiquettes
- Autorisations et balisage

Principes de base des étiquettes

Une balise est une étiquette que vous affectez à une AWS ressource. Chaque balise se compose de deux parties que vous définissez :

- Une clé de balise (par exemple, `CostCenter`, `Environment` ou `Project`). Les clés de balises sont sensibles à la casse.

- Une valeur de balise (par exemple, `111122223333` ou `Production`). Les valeurs de balise sont sensibles à la casse, tout comme les clés de balise. Les valeurs des balises sont facultatives.

Vous pouvez utiliser des balises pour classer vos AWS ressources de différentes manières, par exemple, par objectif, par propriétaire ou par environnement. Par exemple, vous pouvez définir un ensemble de balises pour les systèmes de fichiers Amazon FSx de votre compte, ce qui vous permet de suivre le propriétaire et le niveau de stack de chaque instance.

Nous vous recommandons de concevoir un ensemble de clés d'étiquette répondant à vos besoins pour chaque type de ressource. L'utilisation d'un ensemble de clés de balise cohérent facilite la gestion de vos ressources. Vous pouvez rechercher et filtrer les ressources en fonction des balises que vous ajoutez. Pour plus d'informations sur la mise en œuvre d'une stratégie efficace de balisage des ressources, veuillez consulter Baliser AWS des ressources dans le. Références générales AWS

Points à garder à l'esprit en matière de balisage :

- Les balises n'ont pas de signification sémantique pour Amazon FSx et sont interprétées strictement comme des chaînes de caractères.
- Les balises ne sont pas automatiquement affectées à vos ressources.
- Vous pouvez modifier les clés et valeurs d'identification, et vous pouvez retirer des identifications d'une ressource à tout moment.
- Vous pouvez définir la valeur d'une balise sur une chaîne vide, mais vous ne pouvez pas définir la valeur d'une balise sur`null`.
- Si vous ajoutez une balise ayant la même clé qu'une balise existante sur cette ressource, la nouvelle valeur remplace l'ancienne valeur.
- Si vous supprimez une ressource, les balises associées à celle-ci seront également supprimées.
- Si vous utilisez l'API Amazon FSx, le AWS Command Line Interface (AWS CLI) ou un AWS SDK, vous pouvez effectuer les opérations suivantes :
  - Vous pouvez utiliser l'action d'`TagResource`API pour appliquer des balises aux ressources existantes.
  - Pour certaines actions de création de ressources, vous pouvez spécifier des balises pour une ressource lors de la création de cette dernière. En attribuant des balises aux ressources au moment de la création, vous pouvez supprimer la nécessité d'exécuter des scriptes de balisage personnalisés après la création de ressources.

Si les balises ne peuvent pas être appliquées au cours de la création de ressources, Amazon FSx annule le processus de création de ressources. Ce comportement permet de s'assurer que les ressources sont créées avec des balises ou qu'elles ne sont pas créées du tout, et qu'aucune ressource ne demeure sans balise à tout moment.

> **Note**
>
> Certaines autorisations AWS Identity and Access Management (IAM) sont requises pour que les utilisateurs balisent des ressources à leur création. Pour plus d'informations, veuillez consulter Accorder l’autorisation de baliser les ressources lors de la création.

Identification de vos ressources

Vous pouvez baliser des ressources Amazon FSx qui existent dans votre compte. Si vous utilisez la console Amazon FSx, vous pouvez appliquer des balises aux ressources à l'aide de l'onglet Balises sur l'écran de ressource concerné. Lorsque vous créez des ressources, vous pouvez appliquer une valeur à la clé Name, et vous pouvez appliquer les balises de votre choix lors de la création d'un nouveau système de fichiers. Cependant, même si la console organise des ressources en fonction de la clé Name, cette clé n'a pas de signification sémantique pour le service Amazon FSx.

Pour mettre en œuvre un contrôle détaillé des utilisateurs et des groupes qui peuvent baliser des ressources à leur création, vous pouvez appliquer des autorisations au niveau des ressources basées sur des balises dans vos stratégies IAM aux actions d'API Amazon FSx qui prennent en charge le balisage à la création. En utilisant ces autorisations dans vos stratégies, vous bénéficiez des avantages suivants :

- Vos ressources sont correctement sécurisées depuis la création.
- Les balises étant appliquées immédiatement à vos ressources, toutes les autorisations de niveau ressource basées sur des balises sont effectives immédiatement.
- Vos ressources peuvent être suivies et signalées avec plus de précision.
- Vous pouvez appliquer l'utilisation du balisage sur les nouvelles ressources et contrôler que les clés et valeurs de balise sont définies sur vos ressources.

Pour contrôler les clés et valeurs de balise définies sur vos ressources existantes, vous pouvez appliquer des autorisations au niveau des ressources pour les actions d'API `UntagResource` Amazon FSx `TagResource` et dans vos stratégies IAM.

Pour plus d'informations sur les autorisations requises pour baliser des ressources Amazon FSx à leur création, consultezAccorder l'autorisation de baliser les ressources lors de la création.

Pour plus d'informations sur l'utilisation d'identifications pour restreindre l'accès aux ressources Amazon FSx dans les stratégies IAM, consultez. Utilisation de balises pour contrôler l'accès à vos ressources Amazon FSx

Pour plus d'informations sur le balisage de vos ressources pour la facturation, veuillez consulter Utilisation des balises de répartition des coûts du Guide de l'AWS Billingutilisateur.

Copier les balises aux sauvegardes

Lorsque vous créez ou mettez à jour un volume dans l'API Amazon FSx ouAWS CLI, vous pouvez activer `CopyTagsToBackups` la copie automatique de toutes les balises de vos volumes vers des sauvegardes.

> **Note**
>
> Si vous spécifiez des balises lors de la création d'une sauvegarde initiée par l'utilisateur (y compris la balise nominative lorsque vous créez une sauvegarde à l'aide de la console Amazon FSx), les balises ne sont pas copiées depuis le volume même si vous les avez activées. `CopyTagsToBackups`

Pour plus d'informations sur les sauvegardes, consultez Utilisation des sauvegardes. Pour plus d'informations sur l'activation`CopyTagsToBackups`, consultez Pour créer un volume (CLI) et Pour mettre à jour la configuration d'un volume (CLI) dans le guide de l'utilisateur d'Amazon FSx pour NetApp ONTAP ou UpdateVolumedans la référence CreateVolumede l'API Amazon FSx pour NetApp ONTAP.

Restrictions liées aux étiquettes

Les restrictions de base suivantes s'appliquent aux balises :

- Le nombre maximum d'identifications par ressource est de 50.

- La longueur maximale de clé est de 128 caractères Unicode en UTF-8.
- La longueur maximale de valeur est de 256 caractères Unicode en UTF-8.
- Les caractères autorisés sont les lettres, les espaces et les chiffres représentables en UTF-8, ainsi que les caractères spéciaux suivants : `+ - (tiret) (tiret) = . _ : / @`
- Pour chaque ressource, chaque clé d'identification doit être unique, et chaque clé d'identification peut avoir une seule valeur.
- Les clés et valeurs de balise sont sensibles à la casse.
- Le préfixe `aws:` est réservé à l'utilisation d'AWS. Si une balise possède une clé de balise avec ce préfixe, vous ne pouvez pas modifier ou supprimer la clé ou la valeur de cette balise. Les balises avec le préfixe `aws:` ne sont pas comptabilisées comme vos balises pour la limite de ressources.

Vous ne pouvez pas supprimer une ressource uniquement en fonction de ses balises ; vous devez spécifier l'identificateur de ressource. Par exemple, pour supprimer un système de fichiers que vous avez balisé à l'aide d'une clé de balise appeléeDeleteMe, vous devez utiliser l'DeleteFileSystemaction avec l'identifiant de ressource du système de fichiers, tel quefs-1234567890abcdef0.

Lorsque vous balisez des ressources publiques ou partagées, les balises que vous attribuez ne sont disponibles que pour vous Compte AWS ; personne d'autre n'Compte AWSa accès à ces balises. Pour le contrôle d'accès aux ressources partagées basé sur des balises, chaque Compte AWS utilisateur doit attribuer son propre ensemble de balises pour contrôler l'accès à la ressource.

Autorisations et balisage

Pour plus d'informations sur les autorisations requises pour baliser des ressources Amazon FSx à leur création, consultezAccorder l’autorisation de baliser les ressources lors de la création.

Pour plus d'informations sur l'utilisation d'identifications pour restreindre l'accès aux ressources Amazon FSx dans les stratégies IAM, consultez. Utilisation de balises pour contrôler l'accès à vos ressources Amazon FSx

Gestion des ressources FSx for ONTAP à l'aide d'applications NetApp

Outre les AWS API et SDK AWS Management Console AWS CLI, vous pouvez également utiliser ces outils et applications de NetApp gestion pour gérer vos ressources FSx for ONTAP :

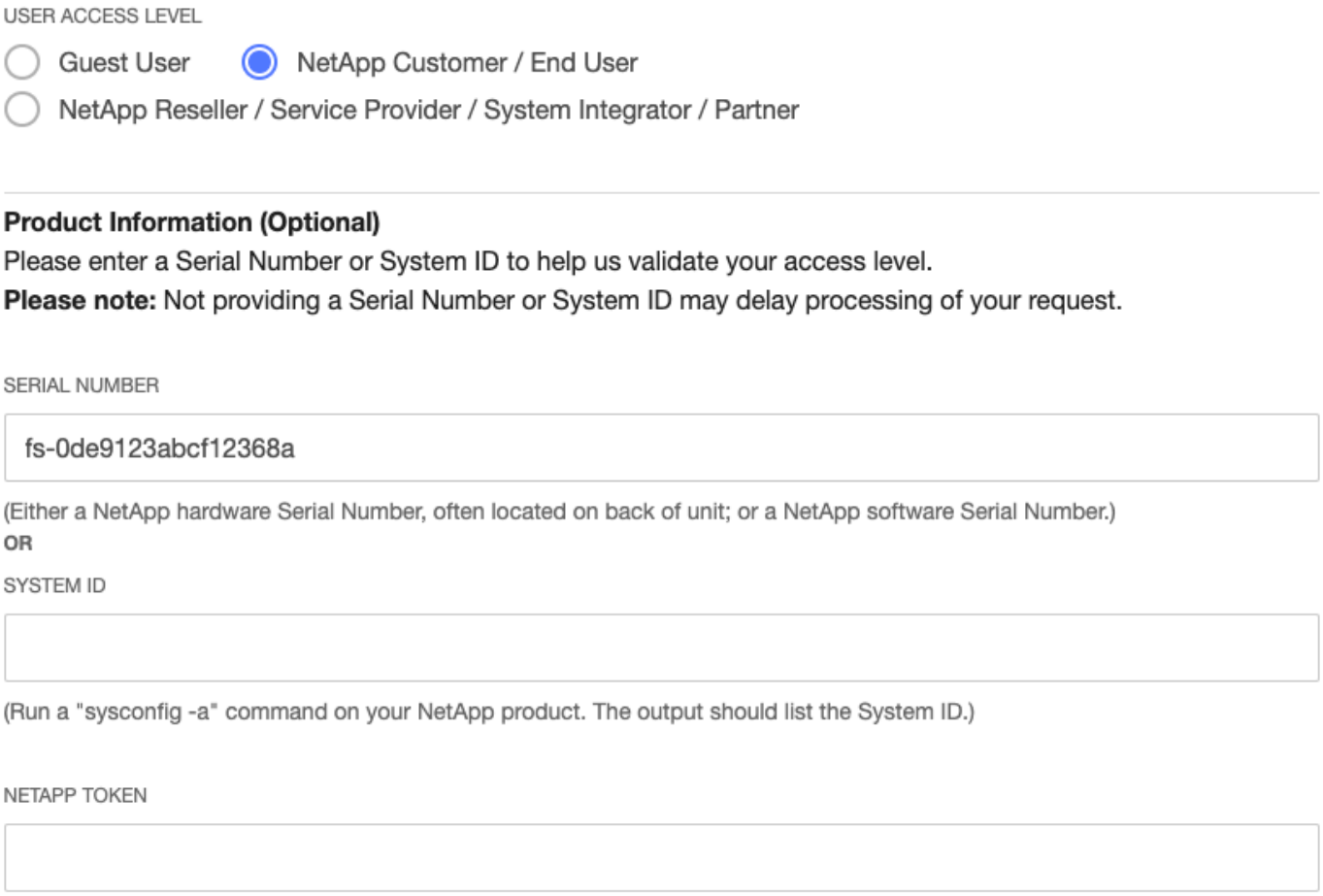
Rubriques

> **Important**
>
> Amazon FSx se synchronise régulièrement ONTAP pour garantir la cohérence. Si vous créez ou modifiez des volumes à l'aide d'NetAppapplications, plusieurs minutes peuvent être nécessaires pour que ces modifications soient prises en compte dans l' AWS Management Console API et les SDK. AWS CLI

Création d'un NetApp compte

Pour télécharger certains NetApp logiciels, tels que BlueXPSnapCenter, et le connecteur ONTAP antivirus, vous devez disposer d'un NetApp compte. Pour créer un NetApp compte, effectuez les étapes suivantes :

1. Accédez à la page d'enregistrement des NetApp utilisateurs et créez un nouveau compte NetApp utilisateur.
2. Complétez le (s) formulaire (s) avec vos informations. Assurez-vous de sélectionner le niveau d'accès NetAppclient/utilisateur final. Dans le champ NUMÉRO DE SÉRIE, copiez et collez l'ID du système de fichiers de votre système de fichiers FSx for ONTAP. Consultez l’exemple suivant:



À quoi s'attendre après votre inscription

Les clients possédant des NetApp produits existants verront leur compte NSS passer au niveau d'accès au niveau client dans un délai d'un jour ouvrable. Les nouveaux clients NetApp seront intégrés conformément aux pratiques commerciales standard, en plus de voir leur compte NSS passer au niveau client. La fourniture de l'ID du système de fichiers permet d'accélérer ce processus. Vous pouvez vérifier l'état de votre compte NSS en vous connectant à mysupport.netapp.com et en accédant à la page d'accueil. Le niveau d'accès de votre compte doit être Accès client.

Utiliser NetApp BlueXP

NetApp BlueXP est un plan de contrôle unifié qui simplifie les expériences de gestion des services de stockage et de données dans les environnements sur site et dans le cloud. BlueXP fournit une interface utilisateur centralisée pour gérer, surveiller et automatiser les déploiements ONTAP

dans AWS et sur site. Pour plus d'informations, consultez la documentation NetApp BlueXP et la documentation NetApp BlueEXP pour Amazon FSx for ONTAP. NetApp

> **Note**
>
> NetApp BlueXPn'est pas pris en charge pour les systèmes de fichiers scale-out.

Utilisation NetApp de System Manager avec BlueXP

Vous pouvez gérer vos systèmes de fichiers Amazon FSx for NetApp ONTAP à l'aide de System Manager directement depuis. BlueXP BlueXPvous permet d'utiliser la même interface System Manager que celle que vous avez l'habitude d'utiliser, afin de gérer votre infrastructure multicloud hybride à partir d'un seul plan de contrôle. Vous avez également accès aux autres fonctionnalités de BlueXP. Pour plus d'informations, consultez la rubrique Intégration de System Manager à BlueXP dans la documentation NetApp ONTAP.

> **Note**
>
> NetApp System Manager n'est pas pris en charge pour les systèmes de fichiers évolutifs.

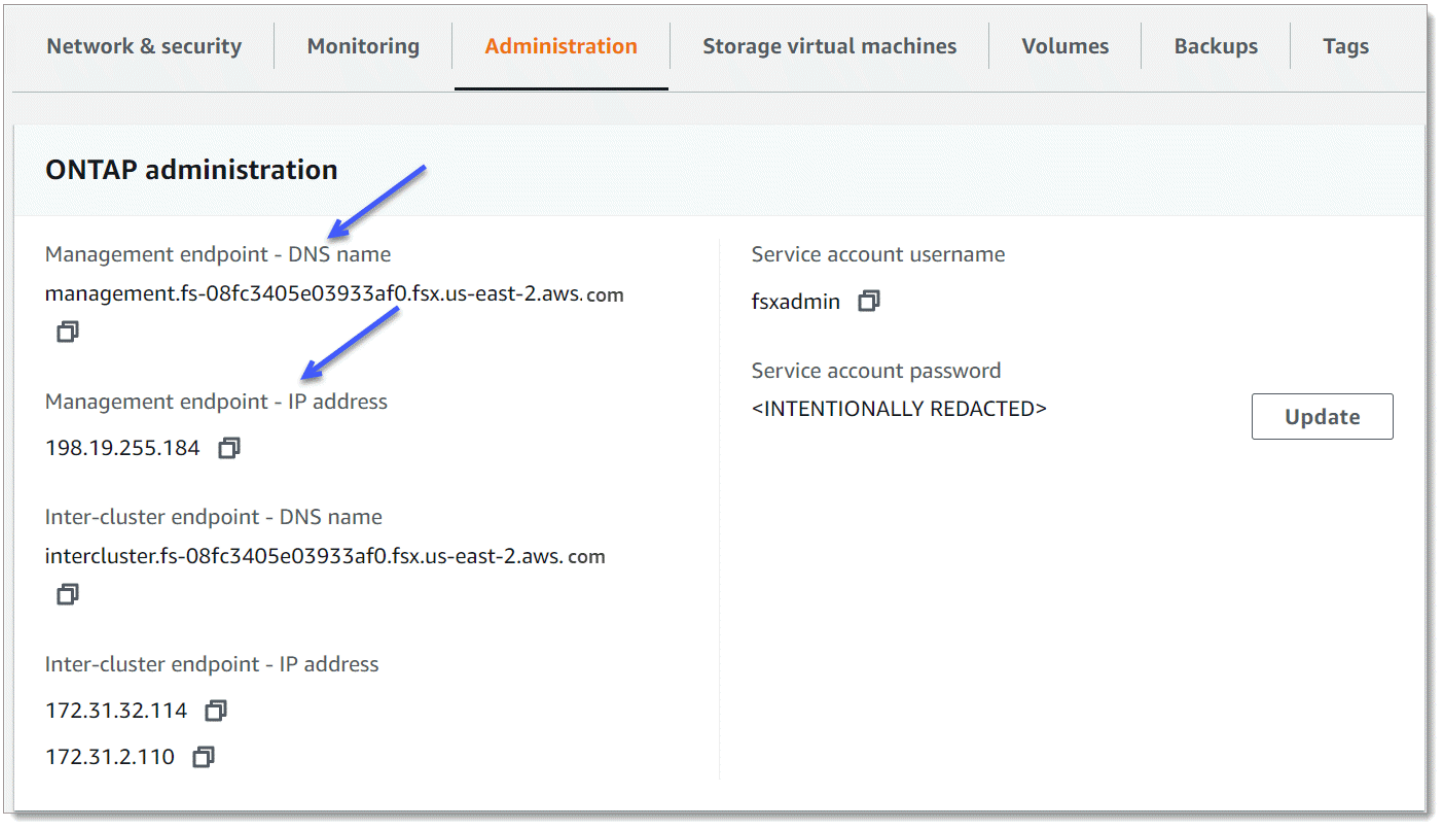
Utilisation de la CLI NetApp ONTAP

Vous pouvez gérer vos ressources Amazon FSx for NetApp ONTAP à l'aide de la CLI. NetApp ONTAP Vous pouvez gérer les ressources au niveau du système de fichiers (analogue au cluster NetApp ONTAP) et au niveau de la SVM.

Gestion des systèmes de fichiers à l'aide de la ONTAP CLI

Vous pouvez exécuter des commandes ONTAP CLI sur votre système de fichiers FSx for ONTAP, comme si vous les exécutiez sur un cluster. NetApp ONTAP Vous accédez à la ONTAP CLI de votre système de fichiers en établissant une connexion Secure Shell (SSH) avec le point de terminaison de gestion du système de fichiers, en vous connectant avec le `fsxadmin` nom d'utilisateur et le mot de passe. Vous avez la possibilité de définir le mot de passe lorsque vous créez un système de fichiers à l'aide du flux de création personnalisé ou à l'aide du AWS CLI. Si vous avez créé le système de fichiers à l'aide de l'option de création rapide, le `fsxadmin` mot de passe n'a pas été défini. Vous devrez donc en définir un pour vous connecter à la CLI ONTAP. Pour plus d’informations, consultez Mettre à jour un système de fichiers. Vous trouverez le nom DNS et l'adresse IP du

point de terminaison de gestion de votre système de fichiers dans la console Amazon FSx, dans l'onglet Administration de la page de détails du système de fichiers FSx for ONTAP, illustrée dans le graphique suivant.



Pour vous connecter au point de terminaison de gestion du système de fichiers via SSH, utilisez l'`fsxadmin`utilisateur et le mot de passe. Vous pouvez accéder par SSH à l'adresse IP ou au nom DNS du point de terminaison de gestion du système de fichiers à partir d'un client qui se trouve dans le même VPC que le système de fichiers, comme dans les exemples suivants.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

La commande SSH avec des exemples de valeurs :

```
ssh fsxadmin@198.51.100.0
```

La commande SSH utilisant le nom DNS du point de terminaison de gestion :

```
ssh fsxadmin@file-system-management-endpoint-dns-name
```

La commande SSH utilisant un exemple de nom DNS :

```
$ ssh fsxadmin@management.fs-0abcdef123456789.fsx.us-east-2.aws.com
  Password: fsxadmin-password

This is your first recorded login.
FsxId0abcdef123456789::>
```

Étendue des commandes ONTAP CLI disponibles pour **`fsxadmin`**

La `fsxadmin` vue administrative se situe au niveau du système de fichiers, qui inclut toutes les SVM et tous les volumes du système de fichiers. Le `fsxadmin` rôle joue le rôle d'administrateur du ONTAP cluster. Les systèmes de fichiers Amazon FSx for NetApp ONTAP étant entièrement gérés, le `fsxadmin` rôle peut exécuter un sous-ensemble des commandes CLI disponibles. ONTAP

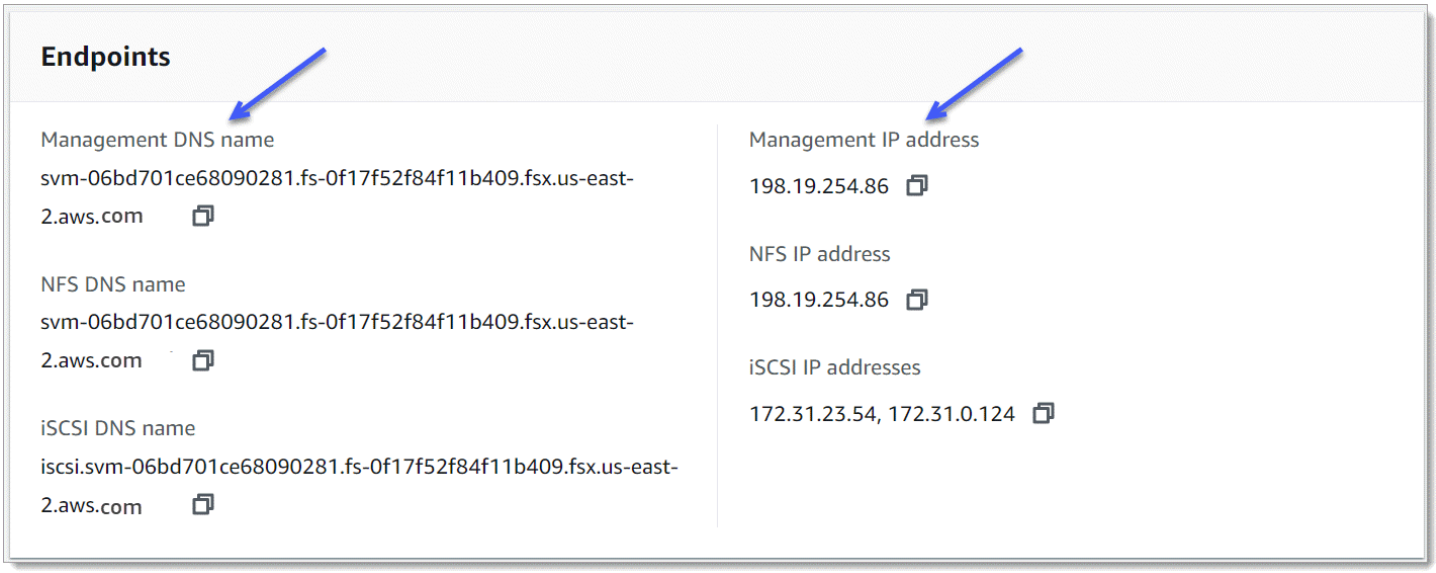
Pour consulter la liste des commandes `fsxadmin` pouvant être exécutées, utilisez la commande [security login role show](ONTAPCLI) suivante :

```
FsxId0abc123def456::> security login role show -role fsxadmin -access !none
           Role          Command/                                    Access
Vserver    Name          Directory                          Query    Level
---------- ------------- --------- ---------------------------------- --------
FsxId0abcdef123456789
           fsxadmin      application                                   all
                         cluster application-record                    all
                         cluster date show                             readonly
                         cluster ha modify                             readonly
                         cluster ha show                               readonly
                         cluster identity modify                       readonly
                         cluster identity show                         readonly
                         cluster log-forwarding           -port !55555 all
                         cluster modify                                readonly
                         cluster peer                                  all
                         cluster show                                  readonly
                         cluster statistics show                       readonly
                         cluster time-service ntp server create        readonly
                         cluster time-service ntp server delete        readonly
                         cluster time-service ntp server modify        readonly
                         cluster time-service ntp server show          readonly
                         debug network tcpdump       -ipspace !Cluster all
                         debug san lun                                 all
                         df         -vserver !FsxId* -vserver !Cluster readonly
                         echo                                          all
                         event catalog show                            readonly
```

```
                          event config                                    all
.
.
.
363 entries were displayed.
```

Gestion des SVM à l'aide de la CLI ONTAP

Vous pouvez accéder à la ONTAP CLI de votre SVM en établissant une connexion Secure Shell (SSH) avec le point de terminaison de gestion de la SVM à l'aide du nom `vsadmin` d'utilisateur `fsxadmin` ou du mot de passe. Le nom DNS et l'adresse IP du point de terminaison de gestion de la SVM se trouvent dans la console Amazon FSx, dans le panneau Endpoints de la page de détails des machines virtuelles de stockage, illustré dans le graphique suivant.



Pour vous connecter au point de gestion de la SVM via SSH, vous pouvez utiliser le nom d'`fsxadmin`utilisateur et le `vsadmin` mot de passe. Si vous n'avez pas défini de mot de passe pour l'`vsadmin`utilisateur lors de la création de la SVM, vous pouvez le `vsadmin` définir à tout moment. Pour plus d'informations, consultez Mise à jour d'une machine virtuelle de stockage. Vous pouvez accéder à la SVM par SSH depuis un client qui se trouve dans le même VPC que le système de fichiers, en utilisant l'adresse IP ou le nom DNS du point de terminaison de gestion.

```
ssh vsadmin@svm-management-endpoint-ip-address
```

La commande avec des exemples de valeurs :

```
ssh vsadmin@198.51.100.10
```

La commande SSH utilisant le nom DNS du point de terminaison de gestion :

```
ssh vsadmin@svm-management-endpoint-dns-name
```

La commande SSH utilisant un exemple de nom DNS :

```
ssh vsadmin@management.svm-abcdef01234567892fs-0abcdef123456789.fsx.us-east-2.aws.com
```

```
Password: vsadmin-password

This is your first recorded login.
FsxId0abcdef123456789::>
```

Amazon FSx for NetApp ONTAP prend en charge les commandes CLINetApp ONTAP.

Pour une référence complète des commandes NetApp ONTAP CLI, reportez-vous à la section Commandes ONTAP : référence de page de manuel.

Utilisation de l'API REST ONTAP

Lorsque vous accédez à votre système de fichiers FSx for ONTAP à l'aide de l'ONTAPAPI REST à l'aide des `fsxadmin` informations d'identification, effectuez l'une des opérations suivantes :

- Désactivez la validation TLS.

  Ou

- Faites confiance aux autorités de AWS certification (CA) : le bundle de certificats pour les autorités de certification de chaque région se trouve aux adresses URL suivantes :
  - https://fsx-aws-certificates.s3.amazonaws.com/bundle - *aws-region .pem* pour le public Régions AWS
  - https://fsx-aws-us-gov-certificates.s3.us-gov-west-1.amazonaws.com/bundle - *aws-region .pem* pour les régions AWS GovCloud
  - https://fsx-aws-cn-certificates.s3.cn-north-1.amazonaws.com.cn/bundle - *aws-region .pem* pour les régions de Chine AWS

Pour une référence complète des commandes de l'NetApp ONTAPAPI REST, consultez la référence en ligne de l'NetApp ONTAPAPI REST.

Sécurité dans Amazon FSx pour ONTAP NetApp

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon FSx for NetApp ONTAP, consultez la section AWS Services concernés par programme de conformitéAWS Services concernés par programme .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'Amazon FSx. Les rubriques suivantes expliquent comment configurer Amazon FSx pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources Amazon FSx.

Rubriques

- Sécurité de l'infrastructure dans Amazon FSx pour ONTAP NetApp
- Utiliser NetApp ONTAP Vscan avec FSx pour ONTAP
- Rôles et utilisateurs dans Amazon FSx pour ONTAP NetApp

Protection des données dans Amazon FSx pour ONTAP NetApp

Le modèle de responsabilité AWS partagée Le modèle s'applique à la protection des données dans Amazon FSx for NetApp ONTAP. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Amazon FSx ou une autre entreprise à Services AWS l'aide de la console, de l'API ou AWS des AWS CLI SDK. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement des données dans FSx pour ONTAP

Amazon FSx for NetApp ONTAP prend en charge le chiffrement des données au repos et le chiffrement des données en transit. Le chiffrement des données au repos est automatiquement activé lors de la création d'un système de fichiers Amazon FSx. Amazon FSx for NetApp ONTAP prend en charge le chiffrement basé sur Kerberos en transit via les protocoles NFS et SMB si vous accédez aux données d'une machine virtuelle de stockage (SVM) connectée à un Active Directory ou à un domaine à l'aide du Lightweight Directory Access Protocol (LDAP).

Quand utiliser le chiffrement ?

Si votre entreprise est soumise à des politiques d'entreprise ou réglementaires qui exigent le chiffrement des données et des métadonnées au repos, vos données sont automatiquement chiffrées au repos. Nous vous recommandons également d'activer le chiffrement des données en transit en installant votre système de fichiers à l'aide du chiffrement des données en transit.

Pour plus d'informations sur le chiffrement des données avec Amazon FSx for NetApp ONTAP, consultez et. Chiffrement de données au repos chiffrement des données en transit

Chiffrement de données au repos

Tous les systèmes de fichiers Amazon FSx for NetApp ONTAP sont chiffrés au repos avec des clés gérées à l'aide AWS Key Management Service de ().AWS KMS Les données sont automatiquement cryptées avant d'être écrites dans le système de fichiers et déchiffrées automatiquement au fur et à mesure de leur lecture. Ces processus sont gérés de manière transparente par Amazon FSx, de sorte que vous n'avez pas à modifier vos applications.

Amazon FSx utilise un algorithme de chiffrement AES-256 conforme aux normes du secteur pour chiffrer les données et métadonnées Amazon FSx au repos. Pour de plus amples informations,

consultez Principes de base du chiffrement dans le Guide du développeur AWS Key Management Service .

> **Note**
>
> L'infrastructure de gestion des AWS clés utilise des algorithmes cryptographiques approuvés par les Federal Information Processing Standards (FIPS) 140-2. Cette infrastructure est conforme aux recommandations NIST (National Institute of Standards and Technology) 800-57.

Comment Amazon FSx utilise AWS KMS

Amazon FSx s'intègre à la gestion AWS KMS des clés. Amazon FSx utilise des clés KMS pour chiffrer votre système de fichiers. Vous choisissez la clé KMS utilisée pour chiffrer et déchiffrer les systèmes de fichiers (données et métadonnées). Vous pouvez activer, désactiver ou révoquer les autorisations sur cette clé KMS. Cette clé KMS peut être de l'un des deux types suivants :

- AWS-clé KMS gérée : il s'agit de la clé KMS par défaut, dont l'utilisation est gratuite.
- Clé KMS gérée par le client : il s'agit de la clé KMS la plus flexible à utiliser, car vous pouvez configurer ses politiques clés et ses autorisations pour plusieurs utilisateurs ou services. Pour plus d'informations sur la création de clés KMS, consultez la section Création de clés dans le guide du AWS Key Management Service développeur.

> **Important**
>
> Amazon FSx accepte uniquement les clés KMS de chiffrement symétriques. Vous ne pouvez pas utiliser de clés KMS asymétriques avec Amazon FSx.

Si vous utilisez une clé KMS gérée par le client comme clé KMS pour le chiffrement et le déchiffrement des données de fichiers, vous pouvez activer la rotation des clés. Lorsque vous activez la rotation des clés, AWS KMS effectue automatiquement une rotation de votre clé une fois par an. En outre, avec une clé KMS gérée par le client, vous pouvez choisir à tout moment à quel moment désactiver, réactiver, supprimer ou révoquer l'accès à votre clé KMS. Pour plus d'informations, voir Rotation, activation AWS KMS keys et désactivation des clés dans le guide du AWS Key Management Service développeur.

Politiques clés d'Amazon FSx pour AWS KMS

Les politiques de clé constituent le principal moyen de contrôler l'accès aux clés KMS. Pour plus d'informations sur les politiques clés, consultez la section Utilisation des politiques clés AWS KMS dans le Guide du AWS Key Management Service développeur.La liste suivante décrit toutes les autorisations AWS KMS associées prises en charge par Amazon FSx pour les systèmes de fichiers chiffrés au repos :

- kms:Encrypt - (Facultatif) Chiffre le texte brut en texte chiffré. Cette autorisation est incluse dans la stratégie de clé par défaut.
- kms:Decrypt - (Obligatoire) Déchiffre le texte chiffré. Le texte chiffré est du texte brut préalablement chiffré. Cette autorisation est incluse dans la stratégie de clé par défaut.
- kms : ReEncrypt — (Facultatif) Chiffre les données côté serveur avec une nouvelle AWS KMS key, sans exposer le texte clair des données côté client. Les données sont d'abord déchiffrées, puis chiffrées à nouveau. Cette autorisation est incluse dans la stratégie de clé par défaut.
- kms : GenerateData KeyWithout Plaintext — (Obligatoire) Renvoie une clé de chiffrement des données chiffrée sous une clé KMS. Cette autorisation est incluse dans la politique de clé par défaut sous kms : GenerateData Key*.
- kms : CreateGrant — (Obligatoire) Ajoute une autorisation à une clé pour spécifier qui peut utiliser la clé et dans quelles conditions. Les octrois sont des mécanismes d'autorisation alternatifs aux stratégies de clé. Pour plus d'informations sur les octrois, consultez Utilisation d'octrois dans le AWS Key Management Service Guide du développeur. Cette autorisation est incluse dans la stratégie de clé par défaut.
- kms : DescribeKey — (Obligatoire) Fournit des informations détaillées sur la clé KMS spécifiée. Cette autorisation est incluse dans la stratégie de clé par défaut.
- kms : ListAliases — (Facultatif) Répertorie tous les alias clés du compte. Lorsque vous utilisez la console pour créer un système de fichiers chiffré, cette autorisation alimente la liste des clés KMS. Nous vous recommandons d'utiliser cette autorisation pour offrir un confort d'utilisation maximal. Cette autorisation est incluse dans la stratégie de clé par défaut.

chiffrement des données en transit

Cette rubrique décrit les différentes options disponibles pour chiffrer les données de vos fichiers lorsqu'elles sont en transit entre un système de fichiers FSx for ONTAP et les clients connectés. Il fournit également des conseils pour vous aider à choisir la méthode de chiffrement la mieux adaptée à votre flux de travail.

Toutes les données circulant Régions AWS sur le réseau AWS mondial sont automatiquement cryptées au niveau de la couche physique avant de quitter les installations AWS sécurisées. L'ensemble du trafic entre les zones de disponibilité est chiffré. Des couches de chiffrement supplémentaires, notamment celles répertoriées dans cette section, fournissent des protections supplémentaires. Pour plus d'informations sur la manière AWS dont les données circulent entre elles Régions AWS, les zones disponibles et les instances, consultez la section Chiffrement en transit dans le guide de l'utilisateur Amazon Elastic Compute Cloud pour les instances Linux.

Amazon FSx for NetApp ONTAP prend en charge les méthodes suivantes pour chiffrer les données en transit entre les systèmes de fichiers FSx for ONTAP et les clients connectés :

- Chiffrement automatique basé sur Nitro sur tous les protocoles et clients pris en charge exécutés sur des types d'instances Amazon EC2 Linux et Windows compatibles.
- Chiffrement basé sur Kerberos via les protocoles NFS et SMB.
- Chiffrement basé sur IPsec sur les protocoles NFS, iSCSI et SMB

Toutes les méthodes prises en charge pour chiffrer les données en transit utilisent des algorithmes cryptographiques conformes à la norme industrielle AES-256 qui fournissent un chiffrement à la pointe de l'entreprise.

Rubriques

- Choix d'une méthode de chiffrement des données en transit
- Chiffrer les données en transit avec AWS Nitro System
- Chiffrement des données en transit grâce au chiffrement basé sur Kerberos
- Chiffrement des données en transit avec le chiffrement IPSec
- Activer le chiffrement des données en transit par les PME
- Configuration d'IPSec à l'aide de l'authentification PSK
- Configuration d'IPSec à l'aide de l'authentification par certificat

Choix d'une méthode de chiffrement des données en transit

Cette section fournit des informations qui peuvent vous aider à choisir le cryptage pris en charge dans les méthodes de transit qui convient le mieux à votre flux de travail. Reportez-vous à cette section pour découvrir les options prises en charge décrites en détail dans les sections suivantes.

Plusieurs facteurs doivent être pris en compte lorsque vous choisissez le mode de chiffrement des données en transit entre votre système de fichiers FSx for ONTAP et les clients connectés. Ces facteurs incluent :

- Le système de fichiers dans Région AWS lequel s'exécute votre système de fichiers FSx for ONTAP.
- Type d'instance sur lequel le client s'exécute.
- Emplacement du client accédant à votre système de fichiers.
- Exigences relatives aux performances du réseau.
- Protocole de données que vous souhaitez chiffrer.
- Si vous utilisez Microsoft Active Directory.

Région AWS

Le système de fichiers dans Région AWS lequel s'exécute votre système de fichiers détermine si vous pouvez ou non utiliser le chiffrement basé sur Amazon Nitro. Le chiffrement basé sur Nitro est disponible dans les versions suivantes : Régions AWS

- USA Est (Virginie du Nord)
- USA Est (Ohio)
- USA Ouest (Oregon)
- Europe (Irlande)

En outre, le chiffrement basé sur Nitro est disponible pour les systèmes de fichiers évolutifs en Asie-Pacifique (Sydney). Région AWS

Type d'instance client

Vous pouvez utiliser le chiffrement basé sur Amazon Nitro si le client accédant à votre système de fichiers s'exécute sur l'un des types d'instance Amazon EC2 Mac, Linux ou Windows pris en charge, et si votre flux de travail répond à toutes les autres exigences relatives à l'utilisation du chiffrement basé sur Nitro. Aucun type d'instance client n'est requis pour utiliser le chiffrement Kerberos ou IPSec.

Emplacement du client

L'emplacement du client accédant aux données par rapport à l'emplacement de votre système de fichiers a une incidence sur les méthodes de chiffrement en transit disponibles. Vous pouvez utiliser l'une des méthodes de chiffrement prises en charge si le client et le système de fichiers

se trouvent dans le même VPC. Il en va de même si le client et le système de fichiers sont situés dans des VPC homologues, à condition que le trafic ne transite pas par un périphérique ou un service réseau virtuel, tel qu'une passerelle de transit. Le chiffrement basé sur Nitro n'est pas une option disponible si le client n'est pas dans le même VPC ou dans un VPC homologue, ou si le trafic passe par un périphérique ou un service réseau virtuel.

Performances réseau

L'utilisation du chiffrement basé sur Amazon Nitro n'a aucun impact sur les performances du réseau. Cela est dû au fait que les instances Amazon EC2 prises en charge utilisent les capacités de déchargement du matériel Nitro System sous-jacent pour chiffrer automatiquement le trafic en transit entre les instances.

L'utilisation du chiffrement Kerberos ou IPSec a un impact sur les performances du réseau. En effet, ces deux méthodes de chiffrement sont basées sur des logiciels, ce qui oblige le client et le serveur à utiliser des ressources informatiques pour chiffrer et déchiffrer le trafic en transit.

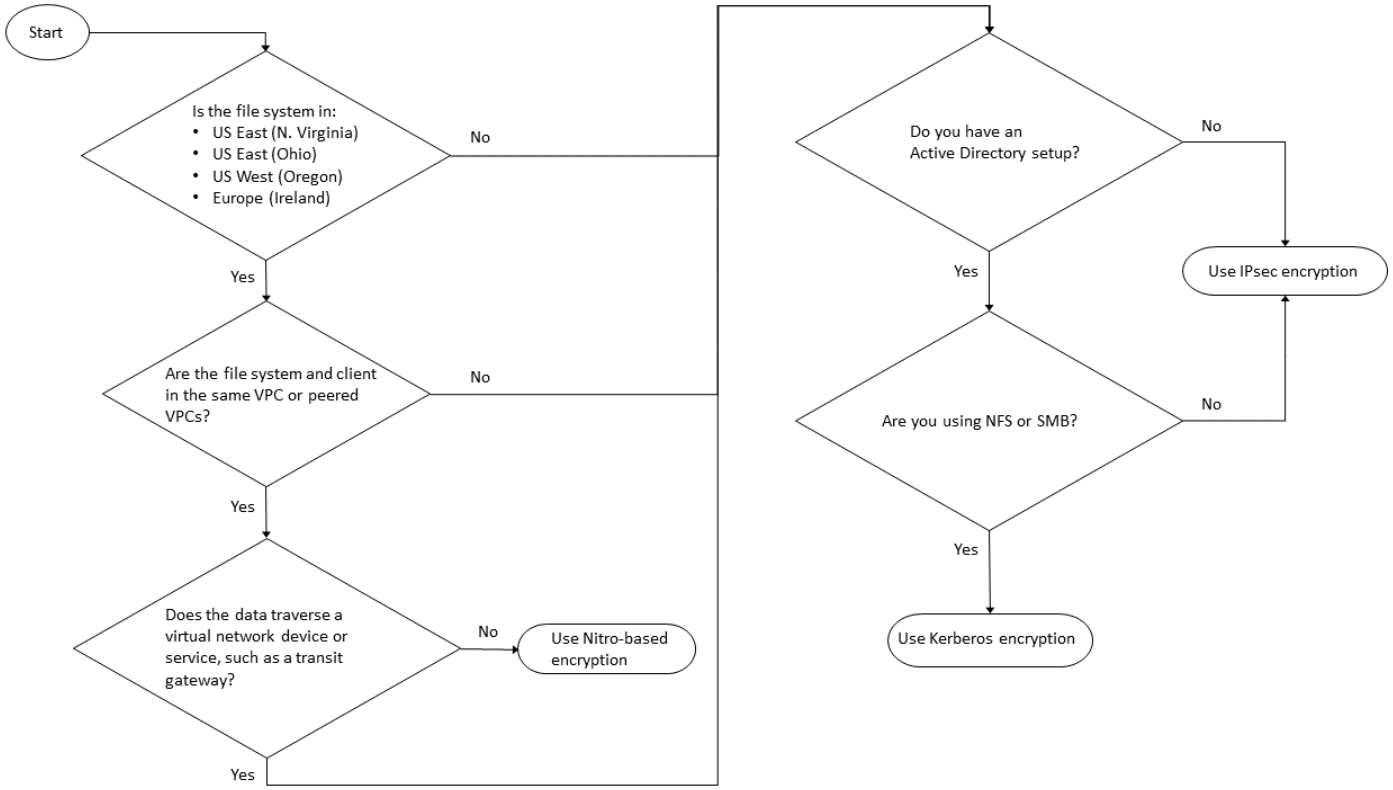
Protocole de données

Vous pouvez utiliser le chiffrement basé sur Amazon Nitro et le chiffrement IPsec avec tous les protocoles pris en charge : NFS, SMB et iSCSI. Vous pouvez utiliser le chiffrement Kerberos avec les protocoles NFS et SMB (avec un Active Directory).

Active Directory

Si vous utilisez Microsoft Active Directory, vous pouvez utiliser le chiffrement Kerberos sur les protocoles NFS et SMB.

Utilisez le schéma suivant pour vous aider à choisir la méthode de chiffrement en transit à utiliser.



Le chiffrement IPsec est la seule option disponible lorsque toutes les conditions suivantes s'appliquent à votre flux de travail :

- Vous utilisez le protocole NFS, SMB ou iSCSI.
- Votre flux de travail ne prend pas en charge l'utilisation du chiffrement basé sur Amazon Nitro.
- Vous n'utilisez pas de domaine Microsoft Active Directory.

Chiffrer les données en transit avec AWS Nitro System

Avec le chiffrement basé sur Nitro, les données en transit sont chiffrées automatiquement lorsque les clients accédant à vos systèmes de fichiers s'exécutent sur des types d'instances Amazon EC2 Linux ou Windows compatibles.

L'utilisation du chiffrement basé sur Amazon Nitro n'a aucun impact sur les performances du réseau. Cela est dû au fait que les instances Amazon EC2 prises en charge utilisent les capacités de déchargement du matériel Nitro System sous-jacent pour chiffrer automatiquement le trafic en transit entre les instances.

Le chiffrement basé sur Nitro est activé automatiquement lorsque les types d'instances clientes pris en charge se trouvent dans le même VPC ou dans un VPC apparenté au VPC du système de fichiers. Région AWS De plus, si le client se trouve dans un VPC apparenté, les données ne peuvent pas traverser un périphérique ou un service réseau virtuel (tel qu'une passerelle de transit) afin que le chiffrement basé sur Nitro soit automatiquement activé. Pour plus d'informations sur le chiffrement basé sur Nitro, consultez la section Chiffrement en transit du Guide de l'utilisateur Amazon EC2 pour les types d'instances Linux ou Windows.

Le chiffrement en transit basé sur Nitro est disponible pour les systèmes de fichiers créés après le 28 novembre 2022 dans les conditions suivantes : Régions AWS

- USA Est (Virginie du Nord)
- USA Est (Ohio)
- USA Ouest (Oregon)
- Europe (Irlande)

En outre, le chiffrement basé sur Nitro est disponible pour les systèmes de fichiers évolutifs en Asie-Pacifique (Sydney). Région AWS

Pour plus d'informations sur les lieux Régions AWS où FSx for ONTAP est disponible, consultez la section Tarification d'Amazon FSx for ONTAP. NetApp

Pour plus d'informations sur les spécifications de performances de FSx pour les systèmes de fichiers ONTAP, consultez. Impact de la capacité de débit sur les performances

Chiffrement des données en transit grâce au chiffrement basé sur Kerberos

Si vous utilisez Microsoft Active Directory, vous pouvez utiliser le chiffrement Kerberos sur les protocoles NFS et SMB pour chiffrer les données en transit pour les volumes enfants de SVM joints à un Microsoft Active Directory.

Chiffrement des données en transit via NFS à l'aide de Kerberos

Le chiffrement des données en transit à l'aide de Kerberos est pris en charge par les protocoles NFSv3 et NFSv4. Pour activer le chiffrement en transit à l'aide de Kerberos pour le protocole NFS, consultez la section Utilisation de Kerberos avec NFS pour une sécurité renforcée dans le Centre de documentation. NetApp ONTAP

Chiffrement des données en transit sur SMB à l'aide de Kerberos

Le chiffrement des données en transit via le protocole SMB est pris en charge sur les partages de fichiers mappés sur une instance de calcul compatible avec le protocole SMB 3.0 ou version ultérieure. Cela inclut toutes les Microsoft Windows versions de Microsoft Windows Server 2012 et versions ultérieures, ainsi que Microsoft Windows 8 et versions ultérieures. Lorsqu'il est activé, FSx for ONTAP chiffre automatiquement les données en transit à l'aide du chiffrement SMB lorsque vous accédez à votre système de fichiers sans avoir à modifier vos applications.

FSx for ONTAP SMB prend en charge le chiffrement 128 et 256 bits, qui est déterminé par la demande de session du client. Pour une description des différents niveaux de chiffrement, consultez la section Définir le niveau de sécurité d'authentification minimal du serveur SMB de la section Gérer les PME avec la CLI dans le Centre de NetApp ONTAP documentation.

> **Note**
>
> Le client détermine l'algorithme de chiffrement. Les authentifications NTLM et Kerberos fonctionnent avec un cryptage à 128 et 256 bits. Le serveur FSx for ONTAP SMB accepte toutes les demandes standard des clients Windows, et les contrôles granulaires sont gérés par la politique de groupe Microsoft ou les paramètres du registre.

La ONTAP CLI permet de gérer le chiffrement dans les paramètres de transit sur FSx pour les SVM et les volumes ONTAP. Pour accéder à la NetApp ONTAP CLI, établissez une session SSH sur la SVM sur laquelle vous effectuez le chiffrement dans les paramètres de transit, comme décrit dans. Gestion des SVM à l'aide de la CLI ONTAP

Pour savoir comment activer le chiffrement SMB sur une SVM ou un volume, reportez-vous à la section. Activer le chiffrement des données en transit par les PME

Chiffrement des données en transit avec le chiffrement IPSec

FSx for ONTAP prend en charge l'utilisation du protocole IPsec en mode transport afin de garantir la sécurité et le chiffrement continus des données pendant leur transit. IPsec permet de end-to-end chiffrer les données en transit entre les clients et les systèmes de fichiers FSx for ONTAP pour tout le trafic IP pris en charge (protocoles NFS, iSCSI et SMB). Avec le chiffrement IPsec, vous établissez un tunnel IPsec entre une SVM FSx for ONTAP configurée avec IPsec activé et un client IPsec exécuté sur le client connecté accédant aux données.

Nous vous recommandons d'utiliser IPsec pour chiffrer les données en transit via les protocoles NFS, SMB et iSCSI lorsque vous accédez à vos données depuis des clients qui ne prennent pas en charge le chiffrement basé sur Nitro, et si votre client et vos SVM ne sont pas associés à un Active Directory, ce qui est requis pour le chiffrement basé sur Kerberos. Le chiffrement IPsec est la seule option disponible pour chiffrer les données en transit pour le trafic iSCSI lorsque votre client iSCSI ne prend pas en charge le chiffrement basé sur Nitro.

Pour l'authentification IPsec, vous pouvez utiliser des clés pré-partagées (PSK) ou des certificats. Si vous utilisez un PSK, le client IPsec que vous utilisez doit prendre en charge Internet Key Exchange version 2 (IKEv2) avec un PSK. Les étapes de haut niveau pour configurer le chiffrement IPsec à la fois sur FSx for ONTAP et sur le client sont les suivantes :

1. Activez et configurez IPSec sur votre système de fichiers.
2. Installez et configurez IPSec sur votre client
3. Configuration d'IPsec pour un accès client multiple

Pour plus d'informations sur la configuration d'IPsec à l'aide de PSK, consultez la section Configuration de la sécurité IP (IPsec) par chiffrement filaire dans le NetApp ONTAP centre de documentation.

Pour plus d'informations sur la configuration d'IPsec à l'aide de certificats, consultezConfiguration d'IPSec à l'aide de l'authentification par certificat.

Activer le chiffrement des données en transit par les PME

Par défaut, lorsque vous créez une SVM, le chiffrement SMB est désactivé. Vous pouvez activer le chiffrement SMB requis sur les partages individuels ou sur une SVM, qui l'active pour tous les partages de cette SVM.

> **Note**
>
> Lorsque le chiffrement SMB requis est activé sur une SVM ou un partage, les clients PME qui ne prennent pas en charge le chiffrement ne peuvent pas se connecter à cette SVM ou à ce partage.

Pour exiger le chiffrement du trafic SMB entrant sur une SVM

Pour exiger le chiffrement SMB d'une SVM à l'aide de la CLINetApp ONTAP, procédez comme suit.

1. Pour vous connecter au point de gestion de la SVM via SSH, utilisez le nom d'utilisateur `vsadmin` et le mot de passe vsadmin que vous avez définis lors de la création de la SVM. Si vous n'avez pas défini de mot de passe vsadmin, utilisez le nom d'utilisateur `fsxadmin` et le mot de passe fsxadmin. Vous pouvez accéder à la SVM par SSH depuis un client qui se trouve dans le même VPC que le système de fichiers, en utilisant l'adresse IP ou le nom DNS du point de terminaison de gestion.

   ```
   ssh vsadmin@svm-management-endpoint-ip-address
   ```

   La commande avec des exemples de valeurs :

   ```
   ssh vsadmin@198.51.100.10
   ```

   La commande SSH utilisant le nom DNS du point de terminaison de gestion :

   ```
   ssh vsadmin@svm-management-endpoint-dns-name
   ```

   La commande SSH utilisant un exemple de nom DNS :

   ```
   ssh vsadmin@management.svm-abcdef01234567892fs-08fc3405e03933af0.fsx.us-
   east-2.aws.com
   ```

   ```
   Password: vsadmin-password

   This is your first recorded login.
   FsxIdabcdef01234567892::>
   ```

2. Utilisez la commande `vserver cifs security modify`NetApp ONTAPCLI pour exiger le chiffrement SMB du trafic SMB entrant dans la SVM.

   ```
   vserver cifs security modify -vserver vserver_name -is-smb-encryption-required true
   ```

3. Pour ne plus exiger le chiffrement SMB pour le trafic SMB entrant, utilisez la commande suivante.

   ```
   vserver cifs security modify -vserver vserver_name -is-smb-encryption-required
    false
   ```

4. Pour voir les `is-smb-encryption-required` paramètres actuels d'une SVM, utilisez la commande `vserver cifs security show`NetApp ONTAPCLI :

```
vserver cifs security show -vserver vs1 -fields is-smb-encryption-required

vserver  is-smb-encryption-required
-------- -------------------------
vs1      true
```

Pour plus d'informations sur la gestion du chiffrement SMB sur une SVM, consultez la section Configuration du chiffrement SMB requis sur les serveurs SMB pour les transferts de données via SMB dans le Centre de documentation. NetApp ONTAP

Pour activer le chiffrement SMB sur un volume

Utilisez la procédure suivante pour activer le chiffrement SMB sur un partage à l'aide de la NetApp ONTAP CLI.

1. Établissez une connexion Secure Shell (SSH) avec le point de terminaison de gestion de la SVM, comme décrit dans. Gestion des SVM à l'aide de la CLI ONTAP
2. Utilisez la commande NetApp ONTAP CLI suivante pour créer un nouveau partage SMB et exiger le chiffrement SMB lors de l'accès à ce partage.

```
vserver cifs share create -vserver vserver_name -share-name share_name -
path share_path -share-properties encrypt-data
```

   Pour plus d'informations, consultez `vserver cifs share create`les pages de manuel des commandes NetApp ONTAP CLI.

3. Pour exiger le chiffrement SMB sur un partage SMB existant, utilisez la commande suivante.

```
vserver cifs share properties add -vserver vserver_name -share-name share_name -
share-properties encrypt-data
```

   Pour plus d'informations, consultez `vserver cifs share create`les pages de manuel des commandes NetApp ONTAP CLI.

4. Pour désactiver le chiffrement SMB sur un partage SMB existant, utilisez la commande suivante.

```
vserver cifs share properties remove -vserver vserver_name -share-name share_name -
share-properties encrypt-data
```

Pour plus d'informations, consultez `vserver cifs share properties remove`les pages de manuel des commandes NetApp ONTAP CLI.

5. Pour voir le `is-smb-encryption-required` paramètre actuel sur un partage SMB, utilisez la commande NetApp ONTAP CLI suivante :

```
vserver cifs share properties show -vserver vserver_name -share-name share_name -
fields share-properties
```

Si l'une des propriétés renvoyées par la commande est la `encrypt-data` propriété, cette propriété indique que le chiffrement SMB doit être utilisé lors de l'accès à ce partage.

Pour plus d'informations, consultez `vserver cifs share properties show`les pages de manuel des commandes NetApp ONTAP CLI.

Configuration d'IPSec à l'aide de l'authentification PSK

Si vous utilisez PSK pour l'authentification, les étapes de configuration du chiffrement IPsec sur FSx for ONTAP et sur le client sont les suivantes :

1. Activez et configurez IPSec sur votre système de fichiers.
2. Installez et configurez IPSec sur votre client
3. Configuration d'IPsec pour un accès client multiple

Pour plus de détails sur la configuration d'IPsec à l'aide de PSK, consultez la section Configuration de la sécurité IP (IPsec) par chiffrement filaire dans le NetApp ONTAP centre de documentation.

Configuration d'IPSec à l'aide de l'authentification par certificat

Les rubriques suivantes fournissent des instructions pour configurer le chiffrement IPsec à l'aide de l'authentification par certificat sur un système de fichiers FSx for ONTAP et un client exécutant Libreswan IPsec. Cette solution utilise AWS Certificate Manager et AWS Private Certificate Authority pour créer une autorité de certification privée et pour générer les certificats.

Les étapes de haut niveau pour configurer le chiffrement IPsec à l'aide de l'authentification par certificat sur FSx pour les systèmes de fichiers ONTAP et les clients connectés sont les suivantes :

1. Mettez en place une autorité de certification pour délivrer les certificats.
2. Générez et exportez des certificats CA pour le système de fichiers et le client.
3. Installez le certificat et configurez IPsec sur l'instance cliente.
4. Installez le certificat et configurez IPsec sur votre système de fichiers.
5. Définissez la base de données des politiques de sécurité (SPD).
6. Configurez IPsec pour un accès client multiple.

Création et installation de certificats CA

Pour l'authentification par certificat, vous devez générer et installer des certificats à partir d'une autorité de certification sur votre système de fichiers FSx for ONTAP et des clients qui accèderont aux données de votre système de fichiers. L'exemple suivant permet AWS Private Certificate Authority de configurer une autorité de certification privée et de générer les certificats à installer sur le système de fichiers et le client. À l'aide de AWS Private Certificate Authority, vous pouvez créer une hiérarchie entièrement AWS hébergée d'autorités de certification (CA) racines et subordonnées à usage interne par votre organisation. Ce processus comporte cinq étapes :

1. Créez une autorité de certification (CA) privée à l'aide de AWS Private CA
2. Émettre et installer le certificat racine sur l'autorité de certification privée
3. Demandez un certificat privé AWS Certificate Manager pour votre système de fichiers et vos clients
4. Exportez le certificat pour le système de fichiers et les clients.

Pour plus d'informations, consultez la section Administration de Private CA dans le Guide de AWS Private Certificate Authority l'utilisateur.

Pour créer l'autorité de certification privée racine

1. Lorsque vous créez une autorité de certification, vous devez spécifier la configuration de l'autorité de certification dans un fichier que vous fournissez. La commande suivante utilise l'éditeur de texte Nano pour créer le `ca_config.txt` fichier, qui spécifie les informations suivantes :

- Le nom de l'algorithme
- L'algorithme de signature utilisé par l'autorité de certification pour signer
- Les informations sur l'objet X.500

```
$ > nano ca_config.txt
```

L'éditeur de texte apparaît.

2. Modifiez le fichier contenant les spécifications de votre autorité de certification.

```
{
   "KeyAlgorithm":"RSA_2048",
   "SigningAlgorithm":"SHA256WITHRSA",
   "Subject":{
      "Country":"US",
      "Organization":"Example Corp",
      "OrganizationalUnit":"Sales",
      "State":"WA",
      "Locality":"Seattle",
      "CommonName":"*.ec2.internal"
   }
}
```

3. Enregistrez et fermez le fichier en quittant l'éditeur de texte. Pour plus d'informations, consultez la section Procédure de création d'une autorité de certification dans le guide de AWS Private Certificate Authority l'utilisateur.
4. Utilisez la commande AWS Private CA CLI create-certificate-authority pour créer une autorité de certification privée.

```
~/home > aws acm-pca create-certificate-authority \
     --certificate-authority-configuration file://ca_config.txt \
     --certificate-authority-type "ROOT" \
     --idempotency-token 01234567 --region aws-region
```

En cas de succès, cette commande affiche l'Amazon Resource Name (ARN) de l'autorité de certification.

```
{
```

```
   "CertificateAuthorityArn": "arn:aws:acm-pca:aws-region:111122223333:certificate-
authority/12345678-1234-1234-1234-123456789012"
}
```

Pour créer et installer un certificat pour votre autorité de certification racine privée (AWS CLI)

1. Générez une demande de signature de certificat (CSR) à l'aide de la commande [get-certificate-authority-csr](#) AWS CLI.

   ```
   $ aws acm-pca get-certificate-authority-csr \
        --certificate-authority-arn arn:aws:acm-pca:aws-
   region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
        --output text \
        --endpoint https://acm-pca.aws-region.amazonaws.com \
        --region eu-west-1 > ca.csr
   ```

   Le fichier obtenu `ca.csr`, un fichier PEM codé au format base64, présente l'aspect suivant.

   ```
   -----BEGIN CERTIFICATE-----
    MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
    VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
    b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
    BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
    MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
    VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
    b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
    YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
    21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
    rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
    Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
    nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
    FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
    NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
    -----END CERTIFICATE-----
   ```

   Pour plus d'informations, consultez la section [Installation d'un certificat CA racine](#) dans le guide de AWS Private Certificate Authority l'utilisateur.

2. Utilisez la [issue-certificate](#) AWS CLI commande pour émettre et installer le certificat racine sur votre autorité de certification privée.

```
$ aws acm-pca issue-certificate \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --csr file://ca.csr \
     --signing-algorithm SHA256WITHRSA \
     --template-arn arn:aws:acm-pca:::template/RootCACertificate/V1 \
     --validity Value=3650,Type=DAYS --region aws-region
```

3. Téléchargez le certificat racine à l'aide de la `get-certificate` AWS CLI commande.

```
$ aws acm-pca get-certificate \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
    --certificate-arn arn:aws:acm-pca:aws-region:486768734100:certificate-
authority/12345678-1234-1234-1234-123456789012/certificate/
abcdef0123456789abcdef0123456789 \
    --output text --region aws-region > rootCA.pem
```

4. Installez le certificat racine sur votre autorité de certification privée à l'aide de la `import-certificate-authority-certificate` AWS CLI commande.

```
$ aws acm-pca import-certificate-authority-certificate \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --certificate file://rootCA.pem --region aws-region
```

Génération et exportation du système de fichiers et du certificat client

1. Utilisez la `request-certificate` AWS CLI commande pour demander un AWS Certificate Manager certificat à utiliser sur votre système de fichiers et vos clients.

```
$ aws acm request-certificate \
    --domain-name *.ec2.internal \
    --idempotency-token 12345 \
    --region aws-region \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012
```

   Si la demande aboutit, l'ARN du certificat émis est renvoyé.

2. Pour des raisons de sécurité, vous devez attribuer un mot de passe à la clé privée lors de son exportation. Créez un mot de passe et stockez-le dans un fichier nommé `passphrase.txt`
3. Utilisez la `export-certificate` AWS CLI commande pour exporter le certificat privé émis précédemment. Le fichier exporté contient le certificat, la chaîne de certificats et la clé RSA privée chiffrée de 2048 bits associée à la clé publique intégrée au certificat. Pour des raisons de sécurité, vous devez attribuer un mot de passe à la clé privée lors de son exportation. L'exemple suivant concerne une instance Linux EC2.

```
$ aws acm export-certificate \
     --certificate-arn arn:aws:acm:aws-
region:111122223333:certificate/12345678-1234-1234-1234-123456789012 \
     --passphrase $(cat passphrase.txt | base64)) --region aws-region >
 exported_cert.json
```

4. Utilisez les `jq` commandes suivantes pour extraire la clé privée et le certificat de la réponse JSON.

```
$ cat exported_cert.json | jq -r .PrivateKey > prv.key

cat exported_cert.json | jq -r .Certificate > cert.pem
openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

5. Utilisez la `openssl` commande suivante pour déchiffrer la clé privée à partir de la réponse JSON. Après avoir saisi la commande, vous êtes invité à saisir le mot de passe.

```
$ openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

Installation et configuration de Libreswan IPsec sur un client Amazon Linux 2

Les sections suivantes fournissent des instructions pour installer et configurer Libreswan IPsec sur une instance Amazon EC2 exécutant Amazon Linux 2.

Pour installer et configurer Libreswan

1. Connectez-vous à votre instance EC2 via SSH. Pour obtenir des instructions spécifiques sur la manière de procéder, consultez Connect to your Linux instance using a SSH in the Amazon Elastic Compute Cloud User Guide for Linux Instances.
2. Exécutez la commande suivante pour installer `libreswan` :

```
$ sudo yum install libreswan
```

3. (Facultatif) Lors de la vérification d'IPsec lors d'une étape ultérieure, ces propriétés peuvent être signalées sans ces paramètres. Nous vous suggérons de tester d'abord votre configuration sans ces paramètres. En cas de problème de connexion, revenez à cette étape et apportez les modifications suivantes.

   Une fois l'installation terminée, utilisez votre éditeur de texte préféré pour ajouter les entrées suivantes au `/etc/sysctl.conf` fichier.

```
net.ipv4.ip_forward=1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.lo.accept_redirects = 0
net.ipv4.conf.lo.send_redirects = 0
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.eth0.rp_filter = 0
```

   Enregistrez les modifications et quittez l'éditeur de texte.

4. Appliquez les modifications.

```
$ sudo sysctl -p
```

5. Vérifiez la configuration IPSec.

```
$ sudo ipsec verify
```

   Vérifiez que la version que `Libreswan` vous avez installée est en cours d'exécution.

6. Initialisez la base de données IPSec NSS.

```
$ sudo ipsec checknss
```

Pour installer le certificat sur le client

1. Copiez le certificat que vous avez généré pour le client dans le répertoire de travail de l'instance EC2. Vous
2. Exportez le certificat généré précédemment dans un format compatible avec`libreswan`.

```
$ openssl pkcs12 -export -in cert.pem -inkey decrypted.key \
    -certfile rootCA.pem -out certkey.p12 -name fsx
```

3. Importez la clé reformatée en fournissant le mot de passe lorsque vous y êtes invité.

```
$ sudo ipsec import certkey.p12
```

4. Créez un fichier de configuration IPsec à l'aide de l'éditeur de texte préféré.

```
$ sudo cat /etc/ipsec.d/nfs.conf
```

Ajoutez les entrées suivantes au fichier de configuration :

```
conn fsxn
    authby=rsasig
    left=172.31.77.6
    right=198.19.254.13
    auto=start
    type=transport
    ikev2=insist
    keyexchange=ike
    ike=aes256-sha2_384;dh20
    esp=aes_gcm_c256
    leftcert=fsx
    leftrsasigkey=%cert
    leftid=%fromcert
    rightid=%fromcert
    rightrsasigkey=%cert
```

Vous démarrerez IPsec sur le client après avoir configuré IPsec sur votre système de fichiers.

Configuration d'IPSec sur votre système de fichiers

Cette section fournit des instructions sur l'installation du certificat sur votre système de fichiers FSx for ONTAP et sur la configuration d'IPsec.

Pour installer le certificat sur votre système de fichiers

1. Copiez les fichiers du certificat racine ()`rootCA.pem`), du certificat client (`cert.pem`) et de la clé déchiffrée (`decrypted.key`) dans votre système de fichiers. Vous devez connaître le mot de passe du certificat.
2. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *`management_endpoint_ip`* par l'adresse IP du port de gestion du système de fichiers.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Pour plus d'informations, consultez Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.
3. catUtilisez-le sur un client (et non sur votre système de fichiers) pour répertorier le `rootCA.pem` contenu des `decrypted.key` fichiers `cert.pem` et ainsi copier le résultat de chaque fichier et le coller lorsque vous y êtes invité dans les étapes suivantes.

   ```
   $ > cat cert.pem
   ```

   Copiez le contenu du certificat.
4. Vous devez installer tous les certificats d'autorité de certification utilisés lors de l'authentification mutuelle, y compris les certificats d'autorité de ONTAP certification côté TAP et côté client, dans la gestion des certificats, sauf s'ils sont déjà installés (comme c'est le cas d'une autorité de certification racine autosignée ONTAP).

   Utilisez la commande `security certificate install` NetApp CLI comme suit pour installer le certificat client :

   ```
   FSxID123:: > security certificate install -vserver dr -type client -cert-name
    ipsec-client-cert
   ```

   ```
   Please enter Certificate: Press <Enter> when done
   ```

Collez le contenu du `cert.pem` fichier que vous avez copié précédemment et appuyez sur Entrée.

```
Please enter Private Key: Press <Enter> when done
```

Collez le contenu du `decrypted.key` fichier et appuyez sur Entrée.

```
Do you want to continue entering root and/or intermediate certificates {y|n}:
```

Entrez n pour terminer la saisie du certificat client.

5. Créez et installez un certificat destiné à être utilisé par la SVM. L'autorité de certification émettrice de ce certificat doit déjà être installée ONTAP et ajoutée à IPsec.

   Utilisez la commande suivante pour installer le certificat racine.

```
FSxID123:: > security certificate install -vserver dr -type server-ca -cert-name
 ipsec-ca-cert
```

```
Please enter Certificate: Press <Enter> when done
```

   Collez le contenu du `rootCA.pem` fichier et appuyez sur Entrée.

6. Pour vous assurer que l'autorité de certification installée se trouve dans le chemin de recherche de l'autorité de certification IPsec lors de l'authentification, ajoutez les autorités de certification de gestion des ONTAP certificats au module IPsec à l'aide de la commande « security ipsec ca-certificate add ».

   Entrez la commande suivante pour ajouter le certificat racine.

```
FSxID123:: > security ipsec ca-certificate add -vserver dr -ca-certs ipsec-ca-cert
```

7. Entrez la commande suivante pour créer la politique IPsec requise dans la base de données des politiques de sécurité (SPD).

```
security ipsec policy create -vserver dr -name policy-name -local-ip-
subnets 198.19.254.13/32 -remote-ip-subnets 172.31.0.0/16 -auth-method PKI -action
 ESP_TRA -cipher-suite SUITEB_GCM256 -cert-name ipsec-client-cert -local-identity
 "CN=*.ec2.internal" -remote-identity "CN=*.ec2.internal"
```

8. Utilisez la commande suivante pour afficher la politique IPSec du système de fichiers à confirmer.

```
FSxID123:: > security ipsec policy show -vserver dr -instance

                                 Vserver: dr
                             Policy Name: promise
                          Local IP Subnets: 198.19.254.13/32
                         Remote IP Subnets: 172.31.0.0/16
                               Local Ports: 0-0
                              Remote Ports: 0-0
                                 Protocols: any
                                    Action: ESP_TRA
                              Cipher Suite: SUITEB_GCM256
        IKE Security Association Lifetime: 86400
      IPsec Security Association Lifetime: 28800
IPsec Security Association Lifetime (bytes): 0
                         Is Policy Enabled: true
                            Local Identity: CN=*.ec2.internal
                           Remote Identity: CN=*.ec2.internal
                    Authentication Method: PKI
           Certificate for Local Identity: ipsec-client-cert
```

Démarrez IPSec sur le client

Maintenant qu'IPsec est configuré à la fois sur le système de fichiers FSx for ONTAP et sur le client, vous pouvez démarrer IPsec sur le client.

1. Connectez-vous à votre système client via SSH.
2. Démarrez IPSec.

```
$ sudo ipsec start
```

3. Vérifiez l'état d'IPSec.

```
$ sudo ipsec status
```

4. Montez un volume sur votre système de fichiers.

```
$ sudo mount -t nfs 198.19.254.13:/benchmark /home/ec2-user/acm/dr
```

5. Vérifiez la configuration IPsec en affichant la connexion cryptée sur votre système de fichiers FSx for ONTAP.

```
FSxID123:: > security ipsec show-ikesa -node FsxId123
FsxId08ac16c7ec2781a58::> security ipsec show-ikesa -node FsxId08ac16c7ec2781a58-01
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ---------------- -----------
dr          policy-name
                   198.19.254.13   172.31.77.6     551c55de57fe8976 ESTABLISHED
fsx         policy-name
                   198.19.254.38   172.31.65.193   4fd3f22c993e60c5 ESTABLISHED
2 entries were displayed.
```

Configuration d'IPsec pour plusieurs clients

Lorsqu'un petit nombre de clients ont besoin de tirer parti d'IPsec, il suffit d'utiliser une seule entrée SPD pour chaque client. Toutefois, lorsque des centaines, voire des milliers de clients ont besoin de tirer parti d'IPsec, nous vous recommandons d'utiliser la configuration de plusieurs clients IPsec.

FSx for ONTAP permet de connecter plusieurs clients sur de nombreux réseaux à une seule adresse IP de SVM avec IPsec activé. Pour ce faire, vous pouvez utiliser la `subnet` configuration ou la `Allow all clients` configuration, qui sont expliquées dans les procédures suivantes :

Pour configurer IPsec pour plusieurs clients à l'aide d'une configuration de sous-réseau

Pour permettre à tous les clients d'un sous-réseau donné (192.168.134.0/24 par exemple) de se connecter à une seule adresse IP de SVM en utilisant une seule entrée de politique SPD, vous devez la spécifier sous forme de sous-réseau. `remote-ip-subnets` En outre, vous devez spécifier le `remote-identity` champ avec l'identité correcte côté client.

> **Important**
>
> Lorsque vous utilisez l'authentification par certificat, chaque client peut utiliser son propre certificat unique ou un certificat partagé pour s'authentifier. FSx for ONTAP IPSec vérifie la validité du certificat en fonction des autorités de certification installées sur son magasin de confiance local. FSx for ONTAP prend également en charge la vérification des listes de révocation de certificats (CRL).

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *`management_endpoint_ip`* par l'adresse IP du port de gestion du système de fichiers.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Pour plus d'informations, consultez Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.

2. Utilisez la commande `security ipsec policy create` NetApp ONTAP CLI comme suit, en remplaçant les valeurs *`d'échantillon`* par vos valeurs spécifiques.

   ```
   FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
     -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 \
     -local-ports 2049 -protocols tcp -auth-method PSK \
     -cert-name my_nfs_server_cert -local-identity ontap_side_identity \
     -remote-identity client_side_identity
   ```

Pour configurer IPsec pour plusieurs clients à l'aide d'une configuration Autoriser tous les clients

Pour permettre à n'importe quel client, quelle que soit son adresse IP source, de se connecter à l'adresse IP compatible IPsec de la SVM, utilisez le caractère générique lorsque vous `0.0.0.0/0` spécifiez le champ. `remote-ip-subnets`

En outre, vous devez spécifier le `remote-identity` champ avec l'identité correcte côté client. Pour l'authentification par certificat, vous pouvez entrer`ANYTHING`.

En outre, lorsque le joker 0.0.0.0/0 est utilisé, vous devez configurer un numéro de port local ou distant spécifique à utiliser. Par exemple, le port NFS 2049.

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *`management_endpoint_ip`* par l'adresse IP du port de gestion du système de fichiers.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Pour plus d'informations, consultez Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.

2. Utilisez la commande `security ipsec policy create` NetApp ONTAP CLI comme suit, en remplaçant les valeurs *d'échantillon* par vos valeurs spécifiques.

```
FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
  -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 0.0.0.0/0 \
  -local-ports 2049 -protocols tcp -auth-method PSK \
  -cert-name my_nfs_server_cert -local-identity ontap_side_identity \
  -local-ports 2049 -remote-identity client_side_identity
```

Gestion des identités et des accès pour Amazon FSx for ONTAP NetApp

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources Amazon FSx. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Amazon FSx.

Utilisateur du service : si vous utilisez le service Amazon FSx pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin.

Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités d'Amazon FSx pour effectuer votre travail, il se peut que vous ayez besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans Amazon FSx, consultez. Résolution des problèmes d'identité et d'accès à Amazon FSx for NetApp ONTAP

Administrateur du service — Si vous êtes responsable des ressources Amazon FSx au sein de votre entreprise, vous avez probablement un accès complet à Amazon FSx. C'est à vous de déterminer les fonctionnalités et les ressources d'Amazon FSx auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec Amazon FSx, consultez. Comment Amazon FSx pour NetApp ONTAP fonctionne avec IAM

Administrateur IAM — Si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Amazon FSx. Pour consulter des exemples de politiques basées sur l'identité Amazon FSx que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité pour Amazon FSx for ONTAP NetApp

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir

d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un

administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d’accès (ACL)

Les listes de contrôle d’accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l’autorisation d’accéder à une ressource. Les listes de contrôle d’accès sont similaires aux politiques basées sur les ressources, bien qu’elles n’utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d’accès, consultez Vue d’ensemble des listes de contrôle d’accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d’autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d’autorisations : une limite d’autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d’autorisations qu’une politique basée sur l’identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d’autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l’identité d’une entité et de ses limites d’autorisation. Les politiques basées sur les ressources qui spécifient l’utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d’autorisations. Un refus explicite dans l’une de ces politiques remplace l’autorisation. Pour plus d’informations sur les limites d’autorisations, consultez Limites d’autorisations pour des entités IAM dans le Guide de l’utilisateur IAM.
- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d’une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l’un ou à l’ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d’informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l’utilisateur AWS Organizations .
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques

basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment Amazon FSx pour NetApp ONTAP fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Amazon FSx, découvrez quelles fonctionnalités IAM peuvent être utilisées avec Amazon FSx.

Fonctionnalités IAM que vous pouvez utiliser avec Amazon NetApp FSx pour ONTAP

Fonction IAM	Assistance Amazon FSx
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition d'une politique	Oui
ACL	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d'identification temporaires	Oui
Transmission des sessions d'accès (FAS)	Oui
Fonctions du service	Non

Fonction IAM	Assistance Amazon FSx
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont Amazon FSx et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez les AWS services compatibles avec IAM dans le guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Amazon FSx

Prend en charge les politiques basées sur l’identité	Oui

Les politiques basées sur l’identité sont des documents de politique d’autorisations JSON que vous pouvez attacher à une identité telle qu’un utilisateur, un groupe d’utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l’identité, consultez Création de politiques IAM dans le Guide de l’utilisateur IAM.

Avec les politiques IAM basées sur l’identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s’applique à l’utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l’utilisateur IAM.

Exemples de politiques basées sur l'identité pour Amazon FSx

Pour consulter des exemples de politiques basées sur l'identité Amazon FSx, consultez. Exemples de politiques basées sur l'identité pour Amazon FSx for ONTAP NetApp

Politiques basées sur les ressources au sein d'Amazon FSx

Prend en charge les politiques basées sur les ressources	Non

Actions politiques pour Amazon FSx

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions Amazon FSx, consultez la section Actions définies par Amazon FSx dans le Service Authorization Reference.

Les actions politiques dans Amazon FSx utilisent le préfixe suivant avant l'action :

```
fsx
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "fsx:action1",
      "fsx:action2"
         ]
```

Pour consulter des exemples de politiques basées sur l'identité Amazon FSx, consultez. Exemples de politiques basées sur l'identité pour Amazon FSx for ONTAP NetApp

Ressources relatives aux politiques pour Amazon FSx

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources Amazon FSx et de leurs ARN, consultez la section Ressources définies par Amazon FSx dans le Service Authorization Reference. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Amazon FSx.

Pour consulter des exemples de politiques basées sur l'identité Amazon FSx, consultez. Exemples de politiques basées sur l'identité pour Amazon FSx for ONTAP NetApp

Clés de conditions de politique pour Amazon FSx

Prend en charge les clés de condition de politique spécifiques au service	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition Amazon FSx, consultez la section Clés de condition pour Amazon FSx dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par Amazon FSx.

Pour consulter des exemples de politiques basées sur l'identité Amazon FSx, consultez. Exemples de politiques basées sur l'identité pour Amazon FSx for ONTAP NetApp

Listes de contrôle d'accès (ACL) dans Amazon FSx

Prend en charge les listes ACL	Non

Contrôle d'accès basé sur les attributs (ABAC) avec Amazon FSx

Prend en charge ABAC (étiquettes dans les politiques)	Oui

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur le balisage des ressources Amazon FSx, consultez. Baliser vos ressources Amazon FSx

Pour visualiser un exemple de politique basée sur l'identité permettant de limiter l'accès à une ressource en fonction des balises de cette ressource, consultez Utilisation de balises pour contrôler l'accès à vos ressources Amazon FSx.

Utilisation d'informations d'identification temporaires avec Amazon FSx

Prend en charge les informations d'identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent

avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Transférer les sessions d'accès pour Amazon FSx

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Rôles de service pour Amazon FSx

Prend en charge les fonctions de service	Non

Rôles liés à un service pour Amazon FSx

Prend en charge les rôles liés à un service.	Oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés aux services Amazon FSx, consultez. Utilisation de rôles liés à un service pour Amazon FSx

Exemples de politiques basées sur l'identité pour Amazon FSx for ONTAP NetApp

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources Amazon FSx. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par Amazon FSx, y compris le format des ARN pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour Amazon FSx dans le Service Authorization Reference.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console Amazon FSx
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources Amazon FSx dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue.

Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console Amazon FSx

Pour accéder à la console Amazon FSx for NetApp ONTAP, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux ressources Amazon FSx présentes dans votre. Compte AWS Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console Amazon FSx, associez également la politique `AmazonFSxConsoleReadOnlyAccess` AWS gérée aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Vous pouvez consulter les politiques de service géré d'Amazon FSx `AmazonFSxConsoleReadOnlyAccess` et les autres dans. AWS politiques gérées pour Amazon FSx

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

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

```
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Résolution des problèmes d'identité et d'accès à Amazon FSx for NetApp ONTAP

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Amazon FSx et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Amazon FSx
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources Amazon FSx

Je ne suis pas autorisé à effectuer une action dans Amazon FSx

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `fsx:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fsx:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `fsx:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Amazon FSx.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Amazon FSx. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources Amazon FSx

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Amazon FSx prend en charge ces fonctionnalités, consultez. Comment Amazon FSx pour NetApp ONTAP fonctionne avec IAM
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès entre comptes, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Utilisation de balises avec Amazon FSx

Vous pouvez utiliser des balises pour contrôler l'accès aux ressources Amazon FSx et pour implémenter le contrôle d'accès basé sur les attributs (ABAC). Pour appliquer des balises aux ressources Amazon FSx lors de la création, les utilisateurs doivent disposer de certaines autorisations AWS Identity and Access Management (IAM).

Accorder l'autorisation de baliser les ressources lors de la création

Avec certaines actions d'API Amazon FSx qui créent des ressources, vous pouvez spécifier des balises lors de la création de la ressource. Vous pouvez utiliser ces balises de ressources pour

implémenter le contrôle d'accès basé sur les attributs (ABAC). Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

Pour que les utilisateurs puissent étiqueter les ressources lors de leur création, ils doivent être autorisés à utiliser l'action qui crée la ressource`fsx:CreateFileSystem`, telle que`fsx:CreateStorageVirtualMachine`, ou`fsx:CreateVolume`. Si des balises sont spécifiées dans l'action de création de ressources, IAM octroie une autorisation supplémentaire à l'`fsx:TagResource`action afin de vérifier si les utilisateurs sont autorisés à créer des balises. Par conséquent, les utilisateurs doivent également avoir des autorisations explicites d'utiliser l'action `fsx:TagResource`.

L'exemple de politique suivant permet aux utilisateurs de créer des systèmes de fichiers et des machines virtuelles de stockage (SVM) et de leur appliquer des balises lors de leur création dans un environnement spécifique Compte AWS.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:CreateStorageVirtualMachine",
         "fsx:TagResource"
      ],
      "Resource": [
         "arn:aws:fsx:region:account-id:file-system/*",
         "arn:aws:fsx:region:account-id:file-system/*/storage-virtual-machine/*"
      ]
    }
  ]
}
```

De même, la politique suivante permet aux utilisateurs de créer des sauvegardes sur un système de fichiers spécifique et d'appliquer des balises à la sauvegarde lors de la création de la sauvegarde.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateBackup"
```

```
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/file-system-id*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*"
    }
  ]
}
```

L'`fsx:TagResource`action est évaluée uniquement si des balises sont appliquées lors de l'action de création de ressources. Par conséquent, un utilisateur autorisé à créer une ressource (en supposant qu'il n'existe aucune condition de balisage) n'a pas besoin d'autorisation pour utiliser l'`fsx:TagResource`action si aucune balise n'est spécifiée dans la demande. Toutefois, si l'utilisateur essaie de créer une ressource avec des balises, la demande échoue s'il n'a pas les autorisations d'utiliser l'action `fsx:TagResource`.

Pour plus d'informations sur le balisage des ressources Amazon FSx, consultez. Baliser vos ressources Amazon FSx Pour plus d'informations sur l'utilisation de balises pour contrôler l'accès aux ressources Amazon FSx, consultez. Utilisation de balises pour contrôler l'accès à vos ressources Amazon FSx

Utilisation de balises pour contrôler l'accès à vos ressources Amazon FSx

Pour contrôler l'accès aux ressources et aux actions Amazon FSx, vous pouvez utiliser des politiques IAM basées sur des balises. Vous pouvez fournir le contrôle de deux manières :

- Vous pouvez contrôler l'accès aux ressources Amazon FSx en fonction des balises associées à ces ressources.
- Vous pouvez contrôler les balises qui peuvent être transmises dans une condition de demande IAM.

Pour plus d'informations sur l'utilisation des balises pour contrôler l'accès aux AWS ressources, consultez la section Contrôle de l'accès à l'aide de balises dans le guide de l'utilisateur IAM. Pour plus d'informations sur le balisage des ressources Amazon FSx lors de leur création, consultez.

Accorder l’autorisation de baliser les ressources lors de la création Pour plus d’informations sur le balisage des ressources, consultez Baliser vos ressources Amazon FSx.

Contrôle de l’accès en fonction des balises sur une ressource

Pour contrôler les actions qu'un utilisateur ou un rôle peut effectuer sur une ressource Amazon FSx, vous pouvez utiliser des balises sur la ressource. Par exemple, vous pouvez autoriser ou refuser des opérations d’API spécifiques sur une ressource de système de fichiers en fonction de la paire clé-valeur de la balise sur la ressource.

Example Exemple de politique — Création d'un système de fichiers uniquement lorsqu'une balise spécifique est utilisée

Cette politique permet à l'utilisateur de créer un système de fichiers uniquement lorsqu'il le balise avec une paire clé-valeur spécifique, dans cet exemple,,`key=Department`. `value=Finance`

```
{
    "Effect": "Allow",
    "Action": [
        "fsx:CreateFileSystem",
        "fsx:TagResource"
    ],
    "Resource": "arn:aws:fsx:region:account-id:file-system/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/Department": "Finance"
        }
    }
}
```

Example Exemple de politique — Création de sauvegardes uniquement d'Amazon FSx pour les volumes NetApp ONTAP dotés d'une balise spécifique

Cette politique permet aux utilisateurs de créer des sauvegardes uniquement de FSx pour les volumes ONTAP marqués avec la paire clé-valeur,. `key=Department` `value=Finance` La sauvegarde est créée avec le tag`Department=Finance`.

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

```
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }

    ]
}
```

Example Exemple de politique — Création d'un volume avec une balise spécifique à partir de sauvegardes dotées d'une balise spécifique

Cette politique permet aux utilisateurs de créer des volumes étiquetés avec `Department=Finance` uniquement à partir de sauvegardes étiquetées avec`Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup",
                "fsx:TagResource"
            ],
```

```
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example Exemple de politique — Supprimer des systèmes de fichiers dotés de balises spécifiques

Cette politique permet à un utilisateur de supprimer uniquement les systèmes de fichiers marqués avec`Department=Finance`. S'ils créent une sauvegarde finale, elle doit être étiquetée avec`Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteFileSystem"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example Exemple de politique — Supprimer un volume avec des balises spécifiques

Cette politique permet à un utilisateur de supprimer uniquement les volumes marqués avec`Department=Finance`. S'ils créent une sauvegarde finale, elle doit être étiquetée avec`Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteVolume"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Utilisation de rôles liés à un service pour Amazon FSx

Amazon FSx utilise des rôles liés à un AWS Identity and Access Management service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à Amazon FSx. Les rôles liés à un service sont prédéfinis par Amazon FSx et incluent toutes les autorisations requises par le service pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration d'Amazon FSx, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Amazon FSx définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul Amazon FSx peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos ressources Amazon FSx, car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez Services AWS fonctionnant avec IAM et recherchez les services où Oui figure dans la colonne Rôle lié à un service. Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour Amazon FSx

Amazon FSx utilise le rôle lié à un service nommé AWSServiceRoleForAmazonFSx— qui exécute certaines actions dans votre compte, comme la création d'interfaces réseau élastiques pour vos systèmes de fichiers dans votre VPC et la publication de statistiques de système de fichiers et de volume dans. CloudWatch

Pour les mises à jour de cette politique, voir Amazon F SxService RolePolicy

Détails de l'autorisation

Détails de l’autorisation

Les autorisations de AWSServiceRoleForAmazonFSx rôle sont définies par la politique SxService RolePolicy AWS gérée d'AmazonF. AWSServiceRoleForAmazonFSx Il dispose des autorisations suivantes :

> **Note**
>
> AWSServiceRoleForAmazonFSx Il est utilisé par tous les types de systèmes de fichiers Amazon FSx ; certaines des autorisations répertoriées ne s'appliquent pas à FSx for ONTAP.

- `ds`— Permet à Amazon FSx d'afficher, d'autoriser et d'annuler les applications de votre annuaire. AWS Directory Service
- `ec2`— Permet à Amazon FSx d'effectuer les opérations suivantes :
  - Affichez, créez et dissociez les interfaces réseau associées à un système de fichiers Amazon FSx.
  - Affichez une ou plusieurs adresses IP élastiques associées à un système de fichiers Amazon FSx.
  - Affichez les VPC, les groupes de sécurité et les sous-réseaux Amazon associés à un système de fichiers Amazon FSx.
  - Fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.
  - Créez une autorisation permettant à un utilisateur AWS autorisé d'effectuer certaines opérations sur une interface réseau.
- `cloudwatch`— Permet à Amazon FSx de publier des points de données métriques dans l'espace de CloudWatch noms AWS/FSx.
- `route53`— Permet à Amazon FSx d'associer un Amazon VPC à une zone hébergée privée.
- `logs`— Permet à Amazon FSx de décrire et d'écrire dans les flux de CloudWatch journaux Logs. Cela permet aux utilisateurs d'envoyer les journaux d'audit d'accès aux fichiers d'un système de fichiers FSx for Windows File Server vers CloudWatch un flux de journaux.
- `firehose`— Permet à Amazon FSx de décrire et d'écrire dans les flux de diffusion Amazon Data Firehose. Cela permet aux utilisateurs de publier les journaux d'audit d'accès aux fichiers d'un système de fichiers Amazon FSx for Windows File Server sur un flux de diffusion Amazon Data Firehose.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateFileSystem",
            "Effect": "Allow",
            "Action": [
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
                "ec2:GetSecurityGroupsForVpc",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PutMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/FSx"
                }
            }
        },

        {
```

```
            "Sid": "TagResourceNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
            "Sid": "ManageNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
        {
            "Sid": "ManageRouteTable",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
```

```
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
        },
        {
            "Sid": "PutCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Sid": "ManageAuditLogs",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
}
```

Toute mise à jour de cette politique est décrite dansAmazon FSx met à jour les politiques gérées AWS.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez la section Autorisations relatives aux rôles liés à un service dans le guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour Amazon FSx

Vous n’avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez un système de fichiers dans l' AWS Management Console interface de ligne de commande IAM ou l'API IAM, Amazon FSx crée le rôle lié au service pour vous.

> **Important**
>
> Ce rôle lié à un service peut apparaître dans votre compte si vous avez effectué une action dans un autre service qui utilise les fonctions prises en charge par ce rôle. Pour de plus amples informations, veuillez consulter Un nouveau rôle est apparu dans mon compte IAM.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez un système de fichiers, Amazon FSx crée à nouveau le rôle lié à un service pour vous.

Modification d'un rôle lié à un service pour Amazon FSx

Amazon FSx ne vous permet pas de modifier le rôle lié au AWSServiceRoleForAmazonFSx service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour Amazon FSx

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Toutefois, vous devez supprimer tous vos systèmes de fichiers et toutes vos sauvegardes avant de pouvoir supprimer manuellement le rôle lié à un service.

> **Note**
>
> Si le service Amazon FSx utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, la CLI IAM ou l'API IAM pour supprimer le rôle lié au AWSServiceRoleForAmazonFSx service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés au service Amazon FSx

Amazon FSx prend en charge l'utilisation de rôles liés à un service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez AWS Régions et points de terminaison.

AWS politiques gérées pour Amazon FSx

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

Amazon F SxService RolePolicy

Permet à Amazon FSx de gérer les AWS ressources en votre nom. Pour en savoir plus, veuillez consulter Utilisation de rôles liés à un service pour Amazon FSx.

AWS politique gérée : AmazonF SxDelete ServiceLinked RoleAccess

Vous ne pouvez pas joindre de `AmazonFSxDeleteServiceLinkedRoleAccess` à vos entités IAM. Cette politique est liée à un service et utilisée uniquement avec le rôle lié au service pour ce service. Vous ne pouvez pas joindre, détacher, modifier ou supprimer cette politique. Pour plus d'informations, consultez Utilisation de rôles liés à un service pour Amazon FSx.

Cette politique accorde des autorisations administratives qui permettent à Amazon FSx de supprimer son rôle lié au service pour l'accès à Amazon S3, utilisé uniquement par Amazon FSx for Lustre.

Détails de l’autorisation

Cette politique inclut des autorisations permettant `iam` à Amazon FSx d'afficher, de supprimer et de visualiser l'état de suppression des rôles liés au service FSx pour l'accès à Amazon S3.

Pour consulter les autorisations associées à cette politique, consultez AmazonF SxDelete ServiceLinked RoleAccess dans le Guide de référence des politiques AWS gérées.

AWS politique gérée : AmazonF Access SxFull

Vous pouvez associer AmazonF SxFullAccess à vos entités IAM. Amazon FSx associe également cette politique à un rôle de service qui permet à Amazon FSx d'effectuer des actions en votre nom.

Fournit un accès complet à Amazon FSx et aux services associés AWS .

Détails de l’autorisation

Cette politique inclut les autorisations suivantes.

- `fsx`— Permet aux principaux un accès complet pour effectuer toutes les actions Amazon FSx, à l'exception de. `BypassSnaplockEnterpriseRetention`
- `ds`— Permet aux directeurs d'accéder aux informations relatives aux AWS Directory Service annuaires.
- `ec2`
  - Permet aux principaux de créer des balises dans les conditions spécifiées.
  - Fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.
- `iam`— Permet aux principes de créer un rôle lié au service Amazon FSx au nom de l'utilisateur. Cela est nécessaire pour qu'Amazon FSx puisse gérer les AWS ressources au nom de l'utilisateur.
- `logs`— Permet aux principaux de créer des groupes de journaux, des flux de journaux et d'écrire des événements dans des flux de journaux. Cela est nécessaire pour que les utilisateurs puissent surveiller l'accès au système de fichiers FSx for Windows File Server en envoyant des journaux d'accès aux audits CloudWatch à Logs.

- `firehose`— Permet aux principaux d'écrire des enregistrements sur un Amazon Data Firehose. Cela est nécessaire pour que les utilisateurs puissent surveiller l'accès au système de fichiers FSx for Windows File Server en envoyant des journaux d'accès aux audits à Firehose.

Pour consulter les autorisations associées à cette politique, consultez AmazonF SxFull Access dans le Guide de référence des politiques AWS gérées.

AWS politique gérée : AmazonF SxConsole FullAccess

Vous pouvez associer la politique `AmazonFSxConsoleFullAccess` à vos identités IAM.

Cette politique accorde des autorisations administratives qui permettent un accès complet à Amazon FSx et l'accès aux AWS services associés via le. AWS Management Console

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `fsx`— Permet aux principaux d'effectuer toutes les actions dans la console de gestion Amazon FSx, à l'exception de. `BypassSnaplockEnterpriseRetention`
- `cloudwatch`— Permet aux principaux de consulter les CloudWatch alarmes et les métriques dans la console de gestion Amazon FSx.
- `ds`— Permet aux principaux de répertorier les informations relatives à un AWS Directory Service répertoire.
- `ec2`
  - Permet aux principaux de créer des balises sur les tables de routage, de répertorier les interfaces réseau, les tables de routage, les groupes de sécurité, les sous-réseaux et le VPC associé à un système de fichiers Amazon FSx.
  - Permet aux principaux de fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.
- `kms`— Permet aux principaux de répertorier les alias des AWS Key Management Service clés.
- `s3`— Permet aux principaux de répertorier certains ou tous les objets d'un compartiment Amazon S3 (jusqu'à 1 000).
- `iam`— Accorde l'autorisation de créer un rôle lié à un service qui permet à Amazon FSx d'effectuer des actions au nom de l'utilisateur.

Pour consulter les autorisations associées à cette politique, consultez AmazonF SxConsole FullAccess dans le Guide de référence des politiques AWS gérées.

AWS politique gérée : AmazonF Access SxConsole ReadOnly

Vous pouvez associer la politique `AmazonFSxConsoleReadOnlyAccess` à vos identités IAM.

Cette politique accorde des autorisations en lecture seule à Amazon FSx et aux AWS services associés afin que les utilisateurs puissent consulter les informations relatives à ces services dans le. AWS Management Console

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `fsx`— Permet aux principaux de consulter les informations relatives aux systèmes de fichiers Amazon FSx, y compris toutes les balises, dans la console de gestion Amazon FSx.
- `cloudwatch`— Permet aux principaux de consulter les CloudWatch alarmes et les métriques dans la console de gestion Amazon FSx.
- `ds`— Permet aux principaux de consulter les informations relatives à un AWS Directory Service répertoire dans la console de gestion Amazon FSx.
- `ec2`
  - Permet aux principaux de visualiser les interfaces réseau, les groupes de sécurité, les sous-réseaux et le VPC associé à un système de fichiers Amazon FSx dans la console de gestion Amazon FSx.
  - Fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.
- `kms`— Permet aux principaux d'afficher les alias des AWS Key Management Service clés dans la console de gestion Amazon FSx.
- `log`— Permet aux principaux de décrire les groupes de CloudWatch journaux Amazon Logs associés au compte à l'origine de la demande. Cela est nécessaire pour que les principaux puissent consulter la configuration d'audit d'accès aux fichiers existante pour un système de fichiers FSx for Windows File Server.
- `firehose`— Permet aux principaux de décrire les flux de diffusion Amazon Data Firehose associés au compte à l'origine de la demande. Cela est nécessaire pour que les principaux puissent consulter la configuration d'audit d'accès aux fichiers existante pour un système de fichiers FSx for Windows File Server.

Pour consulter les autorisations associées à cette politique, consultez AmazonF SxConsole ReadOnly Access dans le Guide de référence des politiques AWS gérées.

AWS politique gérée : AmazonF SxRead OnlyAccess

Vous pouvez associer la politique `AmazonFSxReadOnlyAccess` à vos identités IAM.

Cette politique inclut les autorisations suivantes.

- `fsx`— Permet aux principaux de consulter les informations relatives aux systèmes de fichiers Amazon FSx, y compris toutes les balises, dans la console de gestion Amazon FSx.
- `ec2`— Fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.

Pour consulter les autorisations associées à cette politique, consultez AmazonF SxRead OnlyAccess dans le Guide de référence des politiques AWS gérées.

Amazon FSx met à jour les politiques gérées AWS

Consultez les informations relatives aux mises à jour des politiques AWS gérées pour Amazon FSx depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page Amazon FSxHistorique du document pour Amazon FSx for ONTAP NetApp .

Modification	Description	Date
AmazonF SxService RolePolicy — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `ec2:GetSecurityGroupsForVpc` qui permet aux principaux de fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.	9 janvier 2024

Modification	Description	Date
AmazonF SxRead OnlyAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `ec2:GetSecurityGroupsForVpc` qui permet aux principaux de fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.	9 janvier 2024
AmazonF SxConsole ReadOnly Access — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `ec2:GetSecurityGroupsForVpc` qui permet aux principaux de fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.	9 janvier 2024
Amazon F SxFull Access — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `ec2:GetSecurityGroupsForVpc` qui permet aux principaux de fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.	9 janvier 2024

Modification	Description	Date
AmazonF SxConsole FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `ec2:GetSecurityGroupsForVpc` qui permet aux principaux de fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.	9 janvier 2024
Amazon F SxFull Access — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation pour permettre aux utilisateurs d'effectuer une réplication de données entre régions et entre comptes pour FSx pour les systèmes de fichiers OpenZFS.	20 décembre 2023
AmazonF SxConsole FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation pour permettre aux utilisateurs d'effectuer une réplication de données entre régions et entre comptes pour FSx pour les systèmes de fichiers OpenZFS.	20 décembre 2023

Modification	Description	Date
Amazon F SxFull Access — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation permettant aux utilisateurs d'effectuer une réplication à la demande de volumes pour FSx pour les systèmes de fichiers OpenZFS.	26 novembre 2023
AmazonF SxConsole FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation permettant aux utilisateurs d'effectuer une réplication à la demande de volumes pour FSx pour les systèmes de fichiers OpenZFS.	26 novembre 2023
Amazon F SxFull Access — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux utilisateurs d'afficher, d'activer et de désactiver le support VPC partagé pour FSx pour les systèmes de fichiers ONTAP Multi-AZ.	14 novembre 2023
AmazonF SxConsole FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux utilisateurs d'afficher, d'activer et de désactiver le support VPC partagé pour FSx pour les systèmes de fichiers ONTAP Multi-AZ.	14 novembre 2023

Modification	Description	Date
Amazon F SxFull Access — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre à Amazon FSx de gérer les configurations réseau pour FSx pour les systèmes de fichiers multi-AZ OpenZFS.	9 août 2023
AWS politique gérée : AmazonF SxService RolePolicy — Mise à jour d'une politique existante	Amazon FSx a modifié l'`cloudwatch:PutMetricData` autorisation existante afin qu'Amazon FSx publie les CloudWatch métriques dans l'espace de noms. `AWS/FSx`	24 juillet 2023
Amazon F SxFull Access — Mise à jour d'une politique existante	Amazon FSx a mis à jour la politique afin de supprimer l'`fsx:*`autorisation et d'ajouter des actions spécifiques`fsx`.	13 juillet 2023
AmazonF SxConsole FullAccess — Mise à jour d'une politique existante	Amazon FSx a mis à jour la politique afin de supprimer l'`fsx:*`autorisation et d'ajouter des actions spécifiques`fsx`.	13 juillet 2023

Modification	Description	Date
AmazonF SxConsole ReadOnly Access — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux utilisateurs de consulter les indicateurs de performance améliorés et les actions recommandées pour les systèmes de fichiers FSx for Windows File Server dans la console Amazon FSx.	21 septembre 2022
AmazonF SxConsole FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux utilisateurs de consulter les indicateurs de performance améliorés et les actions recommandées pour les systèmes de fichiers FSx for Windows File Server dans la console Amazon FSx.	21 septembre 2022
AmazonF SxRead OnlyAccess — Politique de suivi lancée	Cette politique accorde un accès en lecture seule à toutes les ressources Amazon FSx et à toutes les balises qui leur sont associées.	4 février 2022
AmazonF SxDelete ServiceLinked RoleAccess — Politique de suivi mise en place	Cette politique accorde des autorisations administratives qui permettent à Amazon FSx de supprimer son rôle lié au service pour l'accès à Amazon S3.	7 janvier 2022

Modification	Description	Date
AmazonF SxService RolePolicy — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre à Amazon FSx de gérer les configurations réseau pour les systèmes de fichiers Amazon FSx for ONTAP. NetApp	2 septembre 2021
Amazon F SxFull Access — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre à Amazon FSx de créer des balises sur les tables de routage EC2 pour les appels délimités.	2 septembre 2021
AmazonF SxConsole FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre à Amazon FSx de créer des systèmes de fichiers multi-AZ Amazon FSx pour ONTAP. NetApp	2 septembre 2021
AmazonF SxConsole FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre à Amazon FSx de créer des balises sur les tables de routage EC2 pour les appels délimités.	2 septembre 2021

Modification	Description	Date
AmazonF SxService RolePolicy — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre à Amazon FSx de décrire et d'écrire dans les flux de journaux Logs. CloudWatch Cela est nécessaire pour que les utilisateurs puissent consulter les journaux d'audit d'accès aux fichiers pour les systèmes de fichiers FSx for Windows File Server à CloudWatch l'aide des journaux.	8 juin 2021
AmazonF SxService RolePolicy — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre à Amazon FSx de décrire et d'écrire dans les flux de diffusion Amazon Data Firehose. Cela est nécessaire pour que les utilisateurs puissent consulter les journaux d'audit d'accès aux fichiers d'un système de fichiers FSx for Windows File Server à l'aide d'Amazon Data Firehose.	8 juin 2021

Modification	Description	Date
Amazon F SxFull Access — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux principaux de décrire et de créer des groupes de CloudWatch journaux, des flux de journaux et d'écrire des événements dans des flux de journaux. Cela est nécessaire pour que les principaux puissent consulter les journaux d'audit d'accès aux fichiers pour les systèmes CloudWatch de fichiers FSx for Windows File Server à l'aide des journaux.	8 juin 2021
Amazon F SxFull Access — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux principaux de décrire et d'écrire des enregistrements dans un Amazon Data Firehose. Cela est nécessaire pour que les utilisateurs puissent consulter les journaux d'audit d'accès aux fichiers d'un système de fichiers FSx for Windows File Server à l'aide d'Amazon Data Firehose.	8 juin 2021

Modification	Description	Date
AmazonF SxConsole FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux principaux de décrire les groupes de CloudWatch journaux Amazon Logs associés au compte à l'origine de la demande. Cela est nécessaire pour que les principaux puissent choisir un groupe de CloudWatch journaux Logs existant lors de la configuration de l'audit d'accès aux fichiers pour un système de fichiers FSx for Windows File Server.	8 juin 2021
AmazonF SxConsole FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux principaux de décrire les flux de diffusion Amazon Data Firehose associés au compte à l'origine de la demande. Cela est nécessaire pour que les principaux puissent choisir un flux de diffusion Firehose existant lors de la configura tion de l'audit d'accès aux fichiers pour un système de fichiers FSx for Windows File Server.	8 juin 2021

Modification	Description	Date
AmazonF SxConsole ReadOnly Access — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux principaux de décrire les groupes de CloudWatch journaux Amazon Logs associés au compte à l'origine de la demande. Cela est nécessaire pour que les principaux puissent consulter la configuration d'audit d'accès aux fichiers existante pour un système de fichiers FSx for Windows File Server.	8 juin 2021
AmazonF SxConsole ReadOnly Access — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux principaux de décrire les flux de diffusion Amazon Data Firehose associés au compte à l'origine de la demande. Cela est nécessaire pour que les principaux puissent consulter la configuration d'audit d'accès aux fichiers existante pour un système de fichiers FSx for Windows File Server.	8 juin 2021

Modification	Description	Date
Amazon FSx a commencé à suivre les modifications	Amazon FSx a commencé à suivre les modifications apportées à ses politiques AWS gérées.	8 juin 2021

Contrôle d'accès au système de fichiers avec Amazon VPC

Vous accédez à vos systèmes de fichiers et SVM Amazon FSx for NetApp ONTAP en utilisant le nom DNS ou l'adresse IP de l'un de leurs points de terminaison, selon le type d'accès. Le nom DNS correspond à l'adresse IP privée de l'interface Elastic network du système de fichiers ou de la SVM dans votre VPC. Seules les ressources du VPC associé, ou les ressources connectées au VPC associé par un VPN, peuvent accéder aux données de votre système de fichiers via les protocoles NFS, SMB AWS Direct Connect ou iSCSI. Pour plus d'informations, consultez Qu'est-ce qu'Amazon VPC ? dans le guide de l'utilisateur Amazon VPC.

> **Warning**
>
> Vous ne devez ni modifier ni supprimer les interfaces elastic network associées à votre système de fichiers. La modification ou la suppression de l'interface réseau peut entraîner une perte permanente de connexion entre votre VPC et votre système de fichiers.

Groupes de sécurité Amazon VPC

Un groupe de sécurité agit comme un pare-feu virtuel pour vos systèmes de fichiers FSx for ONTAP afin de contrôler le trafic entrant et sortant. Les règles entrantes contrôlent le trafic entrant vers votre système de fichiers, tandis que les règles sortantes contrôlent le trafic sortant de votre système de fichiers. Lorsque vous créez un système de fichiers, vous spécifiez le VPC dans lequel il est créé et le groupe de sécurité par défaut pour ce VPC est appliqué. Vous pouvez ajouter à chaque groupe de sécurité des règles qui autorisent le trafic à destination ou en provenance des systèmes de fichiers et des SVM associés. Vous pouvez modifier les règles pour un groupe de sécurité à la fois. Les règles nouvelles et modifiées sont automatiquement appliquées à toutes les ressources associées au groupe de sécurité. Lorsqu'Amazon FSx décide d'autoriser ou non le trafic à atteindre une ressource, il évalue toutes les règles de tous les groupes de sécurité associés à la ressource.

Pour utiliser un groupe de sécurité afin de contrôler l'accès à votre système de fichiers Amazon FSx, ajoutez des règles d'entrée et de sortie. Les règles entrantes contrôlent le trafic entrant, tandis que les règles sortantes contrôlent le trafic sortant de votre système de fichiers. Assurez-vous que vous disposez des bonnes règles de trafic réseau dans votre groupe de sécurité pour mapper le partage de fichiers de votre système de fichiers Amazon FSx à un dossier de votre instance de calcul prise en charge.

Pour plus d'informations sur les règles des groupes de sécurité, consultez la section Règles des groupes de sécurité dans le guide de l'utilisateur Amazon EC2.

Création d'un groupe de sécurité VPC

Pour créer un groupe de sécurité pour Amazon FSx

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Sélectionnez Créer un groupe de sécurité.
4. Attribuez un nom et une description au groupe de sécurité.
5. Pour le VPC, choisissez l'Amazon VPC associé à votre système de fichiers pour créer le groupe de sécurité au sein de ce VPC.
6. Pour les règles de sortie, autorisez tout le trafic sur tous les ports.
7. Ajoutez les règles suivantes aux ports entrants de votre groupe de sécurité. Pour le champ source, vous devez choisir Personnalisé et saisir les groupes de sécurité ou les plages d'adresses IP associés aux instances qui doivent accéder à votre système de fichiers FSx for ONTAP, notamment :

   - Clients Linux, Windows et/ou macOS qui accèdent aux données de votre système de fichiers via NFS, SMB ou iSCSI.
   - Tous les systèmes de fichiers/clusters ONTAP que vous allez associer à votre système de fichiers (par exemple, pour les utiliser SnapMirror ou). SnapVault FlexCache
   - Tous les clients que vous utiliserez pour accéder à l'API ONTAP REST, à la CLI ou aux ZAPI (par exemple, une instance Harvest/Grafana, un connecteur ou BlueXP). NetApp NetApp

Protocole	Ports	Rôle
Tous les ICMP	Tous	Envoyer un ping à l'instance

Protocole	Ports	Rôle
SSH	22	Accès SSH à l'adresse IP du LIF de gestion du cluster ou d'un LIF de gestion des nœuds
TCP	111	Appel de procédure à distance pour NFS
TCP	135	Appel de procédure à distance pour CIFS
TCP	139	Session de service NetBIOS pour CIFS
TCP	161-162	Protocole de gestion réseau simple (SNMP)
TCP	443	Accès par API REST ONTAP à l'adresse IP du LIF de gestion du cluster ou d'un LIF de gestion de la SVM
TCP	445	Microsoft SMB/CIFS sur TCP avec cadrage NetBIOS
TCP	635	Montage NFS
TCP	749	Kerberos
TCP	2049	Démon de serveur NFS
TCP	3260	Accès iSCSI via le LIF de données iSCSI
TCP	4045	Démon de verrouillage NFS
TCP	4046	Moniteur d'état du réseau pour NFS
TCP	10 000	Protocole de gestion des données réseau (NDMP) et communication NetApp SnapMirror entre clusters
TCP	11104	Gestion de la NetApp SnapMirror communication entre clusters
TCP	11105	SnapMirror transfert de données à l'aide de LIFS interclusters
UDP	111	Appel de procédure à distance pour NFS

Protocole	Ports	Rôle
UDP	135	Appel de procédure à distance pour CIFS
UDP	137	Résolution de noms NetBIOS pour CIFS
UDP	139	Session de service NetBIOS pour CIFS
UDP	161-162	Protocole de gestion réseau simple (SNMP)
UDP	635	Montage NFS
UDP	2049	Démon de serveur NFS
UDP	4045	Démon de verrouillage NFS
UDP	4046	Moniteur d'état du réseau pour NFS
UDP	4049	Protocole de quotas NFS

8. Ajoutez le groupe de sécurité à l'interface elastic network du système de fichiers.

Interdire l'accès à un système de fichiers

Pour interdire temporairement à tous les clients l'accès réseau à votre système de fichiers, vous pouvez supprimer tous les groupes de sécurité associés aux interfaces Elastic Network de votre système de fichiers et les remplacer par un groupe dépourvu de règles entrantes/sortantes.

Validation de conformité pour Amazon FSx pour ONTAP NetApp

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et

réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.

- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Amazon FSx pour NetApp ONTAP et points de terminaison VPC d'interface ()AWS PrivateLink

Vous pouvez améliorer le niveau de sécurité de votre VPC en configurant Amazon FSx pour utiliser un point de terminaison VPC d'interface. Les points de terminaison VPC d'interface sont alimentés par AWS PrivateLinkune technologie qui vous permet d'accéder en privé aux API Amazon FSx sans passerelle Internet, périphérique NAT, connexion VPN ou connexion. AWS Direct Connect Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec les API Amazon FSx. Le trafic entre votre VPC et Amazon FSx ne quitte pas le réseau. AWS

Chaque point de terminaison VPC d'interface est représenté par une ou plusieurs interfaces réseau élastiques dans vos sous-réseaux. Une interface réseau fournit une adresse IP privée qui sert de point d'entrée pour le trafic vers l'API Amazon FSx.

Considérations relatives aux points de terminaison VPC de l'interface Amazon FSx

Avant de configurer un point de terminaison VPC d'interface pour Amazon FSx, assurez-vous de consulter les propriétés et les limites du point de terminaison d'interface VPC dans le guide de l'utilisateur Amazon VPC.

Vous pouvez appeler n'importe quelle opération d'API Amazon FSx depuis votre VPC. Par exemple, vous pouvez créer un système de fichiers FSx pour ONTAP en appelant l' CreateFileSystem API depuis votre VPC. Pour obtenir la liste complète des API Amazon FSx, consultez la section Actions du manuel de référence des API Amazon FSx.

Considérations relatives au peering VPC

Vous pouvez connecter d'autres VPC au VPC à l'aide de points de terminaison VPC d'interface à l'aide du peering VPC. L'appairage de VPC est une connexion réseau entre deux VPC. Vous pouvez établir une connexion d'appairage VPC entre vos deux VPC ou avec un VPC dans un autre. Compte AWS Les VPC peuvent également se présenter sous deux formes différentes. Régions AWS

Le trafic entre les VPC pairs reste sur le AWS réseau et ne traverse pas l'Internet public. Une fois les VPC pairs, les ressources telles que les instances Amazon Elastic Compute Cloud (Amazon EC2) présentes dans les deux VPC peuvent accéder à l'API Amazon FSx via les points de terminaison VPC d'interface créés dans l'un des VPC.

Création d'un point de terminaison VPC d'interface pour l'API Amazon FSx

Vous pouvez créer un point de terminaison VPC pour l'API Amazon FSx à l'aide de la console Amazon VPC ou du (). AWS Command Line Interface AWS CLI Pour plus d'informations, consultez Création d'un point de terminaison VPC d'interface dans le guide de l'utilisateur Amazon VPC.

Pour créer un point de terminaison VPC d'interface pour Amazon FSx, utilisez l'une des méthodes suivantes :

- **`com.amazonaws.`*`region`*`.fsx`**— Crée un point de terminaison pour les opérations d'API Amazon FSx.
- **`com.amazonaws.`*`region`*`.fsx-fips`**— Crée un point de terminaison pour l'API Amazon FSx conforme à la norme fédérale de traitement de l'information (FIPS) 140-2.

Pour utiliser l'option DNS privé, vous devez définir les `enableDnsSupport` attributs `enableDnsHostnames` et de votre VPC. Pour plus d'informations, consultez la section Affichage et mise à jour du support DNS pour votre VPC dans le guide de l'utilisateur Amazon VPC.

Sauf Régions AWS en Chine, si vous activez le DNS privé pour le point de terminaison, vous pouvez envoyer des demandes d'API à Amazon FSx avec le point de terminaison VPC en utilisant son nom DNS par défaut pour, par exemple. Région AWS`fsx.us-east-1.amazonaws.com` Pour la Chine (Pékin) et la Chine (Ningxia) Régions AWS, vous pouvez effectuer des demandes d'API avec le point de terminaison VPC `fsx-api.cn-north-1.amazonaws.com.cn` en utilisant `fsx-api.cn-northwest-1.amazonaws.com.cn` et, respectivement.

Pour plus d'informations, consultez la section Accès à un service via un point de terminaison VPC d'interface dans le guide de l'utilisateur Amazon VPC.

Création d'une politique de point de terminaison VPC pour Amazon FSx

Pour contrôler l'accès à l'API Amazon FSx, vous pouvez associer une politique AWS Identity and Access Management (IAM) à votre point de terminaison VPC. La stratégie spécifie les éléments suivants :

- Le principal qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

Pour plus d'informations, consultez Contrôle de l'accès aux services avec points de terminaison d'un VPC dans le Guide de l'utilisateur Amazon VPC.

Résilience dans Amazon FSx pour ONTAP NetApp

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Outre l'infrastructure AWS mondiale, Amazon FSx propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données.

Sauvegarde et restauration

Amazon FSx crée et enregistre des sauvegardes automatisées des volumes de votre système de fichiers Amazon FSx for NetApp ONTAP. Amazon FSx crée des sauvegardes automatisées de vos volumes pendant la fenêtre de sauvegarde de votre système de fichiers Amazon FSx for NetApp ONTAP. Amazon FSx enregistre les sauvegardes automatisées de vos volumes conformément à la période de conservation des sauvegardes que vous spécifiez. Vous pouvez également sauvegarder vos volumes manuellement, en créant une sauvegarde initiée par l'utilisateur. Vous pouvez restaurer une sauvegarde de volume à tout moment en créant un nouveau volume avec la sauvegarde spécifiée comme source.

Pour plus d'informations, consultez Utilisation des sauvegardes.

Instantanés

Amazon FSx crée des copies instantanées des volumes Amazon FSx pour ONTAP. NetApp Les copies instantanées offrent une protection contre la suppression ou la modification accidentelle de fichiers de vos volumes par les utilisateurs finaux. Pour plus d'informations, consultez Utilisation des instantanés.

Zones de disponibilité

Les systèmes de fichiers Amazon FSx for NetApp ONTAP sont conçus pour garantir la disponibilité continue des données, même en cas de panne du serveur. Chaque système de fichiers est alimenté par deux serveurs de fichiers situés dans au moins une zone de disponibilité, chacun disposant de son propre espace de stockage. Amazon FSx réplique automatiquement vos données pour les protéger contre les défaillances des composants, surveille en permanence les défaillances matérielles et remplace automatiquement les composants de l'infrastructure en cas de panne. Les systèmes de fichiers basculent automatiquement selon les besoins (généralement dans les 60 secondes), et les clients basculent automatiquement à plusieurs reprises avec le système de fichiers.

Systèmes de fichiers multi-AZ

Les systèmes de fichiers Amazon FSx for NetApp ONTAP sont hautement disponibles et durables dans toutes les zones de AWS disponibilité, et sont conçus pour garantir une disponibilité continue des données, même en cas d'indisponibilité d'une zone de disponibilité.

Pour plus d'informations, consultez Disponibilité et durabilité.

Systèmes de fichiers mono-AZ

Les systèmes de fichiers Amazon FSx for NetApp ONTAP sont hautement disponibles et durables au sein d'une seule zone de AWS disponibilité, et sont conçus pour garantir une disponibilité continue au sein de cette zone de disponibilité en cas de défaillance d'un serveur de fichiers ou d'un disque individuel.

Pour plus d'informations, consultez Disponibilité et durabilité.

Sécurité de l'infrastructure dans Amazon FSx pour ONTAP NetApp

En tant que service géré, Amazon FSx for NetApp ONTAP est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont

AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à Amazon FSx via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Utiliser NetApp ONTAP Vscan avec FSx pour ONTAP

Vous pouvez utiliser la fonction Vscan d' NetApp ONTAP pour exécuter un logiciel antivirus tiers compatible. Pour plus d'informations, consultez les ressources suivantes pour chacune des solutions prises en charge.

- McAfee — Guide des solutions antivirus pour les données en cluster ONTAP : McAfee
- SentinelOne — Solutions partenaires Vscan et sécurité des données SentinelOne Singularity Cloud
- Solutions partenaires Symantec — Vscan et Symantec Protection Engine
- Trend Micro — Guide des solutions antivirus pour les données en cluster ONTAP : Trend Micro

Rôles et utilisateurs dans Amazon FSx pour ONTAP NetApp

NetApp ONTAPinclut une fonctionnalité de contrôle d'accès basé sur les rôles (RBAC) robuste et extensible. ONTAPles rôles définissent les capacités et les privilèges des utilisateurs lors de l'utilisation de la ONTAP CLI et de l'API REST. Chaque rôle définit un niveau différent de capacités et de privilèges administratifs. Vous attribuez des rôles aux utilisateurs dans le but de contrôler leur accès aux ressources FSx for ONTAP lors de l'utilisation de l'ONTAPAPI REST et de la CLI.

Des ONTAP rôles sont disponibles séparément pour les utilisateurs du système de fichiers FSx for ONTAP et pour les utilisateurs de machines virtuelles de stockage (SVM).

Lorsque vous créez un système de fichiers FSx for ONTAP, un ONTAP utilisateur par défaut est créé au niveau du système de fichiers et au niveau de la SVM. Vous pouvez créer des utilisateurs de systèmes de fichiers et de SVM supplémentaires, ainsi que des rôles de SVM supplémentaires pour répondre aux besoins de votre organisation. Ce chapitre explique ONTAP les utilisateurs et les rôles, et fournit des procédures détaillées pour créer des utilisateurs et des rôles de SVM supplémentaires.

Rôles et utilisateurs de l'administrateur du système de fichiers

L'utilisateur du système de ONTAP fichiers par défaut est`fsxadmin`, à qui le `fsxadmin` rôle est assigné. Vous pouvez attribuer deux rôles prédéfinis aux utilisateurs du système de fichiers, répertoriés comme suit :

- **`fsxadmin`**—Les administrateurs dotés de ce rôle disposent de droits illimités dans le ONTAP système. Ils peuvent configurer toutes les ressources du système de fichiers et de la SVM disponibles sur les systèmes de fichiers FSx for ONTAP.
- **`fsxadmin-readonly`**—Les administrateurs dotés de ce rôle peuvent tout afficher au niveau du système de fichiers, mais ne peuvent apporter aucune modification.

  Ce rôle convient parfaitement aux applications de surveillance, notamment NetApp Harvest parce qu'il dispose d'un accès en lecture seule à toutes les ressources disponibles et à leurs propriétés, mais qu'il ne peut pas y apporter de modifications.

Vous pouvez créer des utilisateurs supplémentaires du système de fichiers et leur attribuer le `fsxadmin-readonly` rôle `fsxadmin` ou. Vous ne pouvez pas créer de nouveaux rôles ni modifier les rôles existants. Pour plus d'informations, consultez Création de nouveaux ONTAP utilisateurs pour l'administration du système de fichiers et des SVM.

Le tableau suivant décrit le niveau d'accès dont disposent les rôles d'administrateur de système de fichiers pour les commandes et les répertoires de commandes de la ONTAP CLI et de l'API REST.

Nom du rôle	Niveau d'accès	Vers les commandes ou répertoires de commandes suivants
`fsxadmin`	Tout	Tous les répertoires de commandes disponibles dans FSx for ONTAP
`fsxadmin-readonly`	Tout	`security login password` Pour gérer le compte utilisateur, le mot de passe local et les informations clés uniquement
	none	`security`
	lecture seule	Tous les autres répertoires de commandes disponibles dans FSx for ONTAP

Rôles et utilisateurs de l'administrateur de la SVM

Chaque SVM possède un domaine d'authentification distinct et peut être gérée indépendamment par ses propres administrateurs. Pour chaque SVM de votre système de fichiers, l'utilisateur par défaut est vsadmin, auquel le `vsadmin` rôle est attribué par défaut. Outre le `vsadmin` rôle, il existe d'autres rôles de SVM prédéfinis qui fournissent des autorisations limitées que vous pouvez attribuer aux utilisateurs de SVM. Vous pouvez également créer des rôles personnalisés qui fournissent le niveau de contrôle d'accès adapté aux besoins de votre organisation.

Les rôles prédéfinis pour les administrateurs de SVM et leurs capacités sont les suivants :

Nom du rôle	Fonctionnalités
`vsadmin`	• Gérez votre compte utilisateur, votre mot de passe local et vos informations clés

Nom du rôle	Fonctionnalités
	• Gérez les volumes, à l'exception des déplacements de volumes • Gérez les quotas, les qtrees, les copies instantanées et les fichiers • Gérer les LUN • Effectuer des SnapLock opérations, à l'exception de la suppression privilégiée • Configuration des protocoles : NFS, SMB et iSCSI • Configuration des services : DNS, LDAP et NIS • Surveillance des tâches • Surveiller les connexions réseau et l'interface réseau • Surveillez l'état de santé de la SVM
`vsadmin-volume`	• Gérez votre compte utilisateur, votre mot de passe local et vos informations clés • Gérez les volumes, y compris les déplacements de volumes • Gérez les quotas, les qtrees, les copies instantanées et les fichiers • Gérer les LUN • Configuration des protocoles : NFS, SMB et iSCSI • Configuration des services : DNS, LDAP et NIS • Surveiller l'interface réseau • Surveillez l'état de santé de la SVM

Nom du rôle	Fonctionnalités
`vsadmin-protocol`	• Gérez votre compte utilisateur, votre mot de passe local et vos informations clés • Gérer les LUN • Configuration des protocoles : NFS, SMB et iSCSI • Configuration des services : DNS, LDAP et NIS • Surveiller l'interface réseau • Surveillez l'état de santé de la SVM
`vsadmin-backup`	• Gérez votre compte utilisateur, votre mot de passe local et vos informations clés • Gestion des opérations NDMP • Lecture et écriture d'un volume restauré • Gérez SnapMirror les relations et les copies instantanées • Afficher les volumes et les informations sur le réseau

Nom du rôle	Fonctionnalités
`vsadmin-snaplock`	• Gérez votre compte utilisateur, votre mot de passe local et vos informations clés • Gérez les volumes, à l'exception des déplacements de volumes • Gérez les quotas, les qtrees, les copies instantanées et les fichiers • Exécuter SnapLock des opérations, y compris la suppression privilégiée • Configuration des protocoles : NFS et SMB • Configuration des services : DNS, LDAP et NIS • Surveillance des tâches • Surveiller les connexions réseau et l'interface réseau
`vsadmin-readonly`	• Gérez votre compte utilisateur, votre mot de passe local et vos informations clés • Surveillez l'état de santé de la SVM • Surveiller l'interface réseau • Afficher les volumes et les LUN • Afficher les services et les protocoles

Pour plus d'informations sur la création d'un nouveau rôle de SVM, consultezCréation d'un nouveau rôle de SVM.

Utilisation d'Active Directory pour authentifier les utilisateurs ONTAP

Vous pouvez authentifier l'accès des utilisateurs du domaine Windows Active Directory à un système de fichiers FSx for ONTAP et à une SVM. Vous devez effectuer les tâches suivantes avant que les comptes Active Directory puissent accéder à votre système de fichiers :

- Vous devez configurer l'accès du contrôleur de domaine Active Directory à la SVM.

La SVM que vous utilisez pour configurer en tant que passerelle ou tunnel pour l'accès au contrôleur de domaine Active Directory doit soit avoir le protocole CIFS activé, soit être jointe à un Active Directory, soit les deux. Si vous n'activez pas le CIFS et que vous joignez uniquement la SVM du tunnel à une instance Active Directory, assurez-vous que la SVM est jointe à votre Active Directory. Pour plus d'informations, consultez Joindre des SVM à un Microsoft Active Directory.

- Vous devez activer un compte utilisateur de domaine Active Directory pour accéder au système de fichiers.

  Vous pouvez utiliser l'authentification par mot de passe ou l'authentification par clé publique SSH pour les utilisateurs du domaine Windows accédant à la ONTAP CLI ou à l'API REST.

Pour les procédures décrivant comment configurer l'authentification Active Directory pour les administrateurs de systèmes de fichiers et de SVM, reportez-vous Configuration de l'authentification Active Directory pour ONTAP les utilisateurs à la section.

Création de nouveaux ONTAP utilisateurs pour l'administration du système de fichiers et des SVM

Chaque ONTAP utilisateur est associé à une SVM ou au système de fichiers. Les utilisateurs du système de fichiers dotés de `fsxadmin` ce rôle peuvent créer de nouveaux rôles et utilisateurs de SVM à l'aide de la commande `security login create`ONTAPCLI.

La `security login create` commande crée une méthode de connexion pour l'utilitaire de gestion. Une méthode de connexion comprend un nom d'utilisateur, une application (méthode d'accès) et une méthode d'authentification. Un nom d'utilisateur peut être associé à plusieurs applications. Il peut éventuellement inclure un nom de rôle de contrôle d'accès. Si un nom de groupe Active Directory, LDAP ou NIS est utilisé, la méthode de connexion donne accès aux utilisateurs appartenant au groupe spécifié. Si l'utilisateur est membre de plusieurs groupes fournis dans la table de connexion de sécurité, il aura accès à une liste combinée des commandes autorisées pour les groupes individuels.

Pour plus d'informations sur la façon de créer un nouvel ONTAP utilisateur, consultezCréation d'un nouvel utilisateur ONTAP.

Rubriques

- Création d'un nouvel utilisateur ONTAP
- Création d'un nouveau rôle de SVM

- Configuration de l'authentification Active Directory pour ONTAP les utilisateurs
- Configuration de l'authentification par clé publique
- Mise à jour des exigences relatives aux mots de passe pour les rôles de système de fichiers et de SVM
- La mise à jour du mot de passe du fsxadmin compte échoue

Création d'un nouvel utilisateur ONTAP

Pour créer un nouvel utilisateur de SVM ou de système de fichiers (ONTAPCLI)

Seuls les utilisateurs du système de fichiers dotés de ce `fsxadmin` rôle peuvent créer de nouveaux utilisateurs de SVM et de systèmes de fichiers.

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *`management_endpoint_ip`* par l'adresse IP du port de gestion du système de fichiers.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Pour plus d'informations, consultez Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.

2. Utilisez la commande `security login create` ONTAP CLI pour créer un nouveau compte utilisateur sur votre système de fichiers FSx for ONTAP ou votre SVM.

   Insérez vos données pour les espaces réservés dans l'exemple afin de définir les propriétés obligatoires suivantes :

   - `-vserver`— Spécifie le nom de la SVM dans laquelle vous souhaitez créer le nouveau rôle ou utilisateur de SVM. Si vous créez un rôle ou un utilisateur dans le système de fichiers, ne spécifiez pas de SVM.
   - `-user-or-group-name`— Spécifie le nom d'utilisateur ou le nom de groupe Active Directory de la méthode de connexion. Le nom du groupe Active Directory ne peut être spécifié qu'avec la méthode `domain` d'authentification et les `ssh` applications `ontapi` et.
   - `-application`— Spécifie l'application de la méthode de connexion. Les valeurs possibles incluent http, ontapi et ssh.

- `-authentication-method`— Spécifie la méthode d'authentification pour la connexion. Les valeurs possibles sont notamment les suivantes :
  - domaine — À utiliser pour l'authentification Active Directory
  - mot de passe — À utiliser pour l'authentification par mot de passe
  - publickey — Utilisateur pour l'authentification par clé publique
- `-role`— Spécifie le nom du rôle de contrôle d'accès pour la méthode de connexion. Au niveau du système de fichiers, le seul rôle qui peut être spécifié est. `fsxadmin`

(Facultatif) Vous pouvez également utiliser un ou plusieurs des paramètres suivants avec la commande :

- `[-comment]`— À utiliser pour inclure une notation ou un commentaire pour le compte utilisateur. Par exemple, **`Guest account`**. La longueur maximale est de 128 caractères.
- `[-second-authentication-method {none|publickey|password|nsswitch}]`— Spécifie la méthode d'authentification à second facteur. Vous pouvez définir les méthodes suivantes :
  - mot de passe — À utiliser pour l'authentification par mot de passe
  - publickey — À utiliser pour l'authentification par clé publique
  - nsswitch — À utiliser pour l'authentification NIS ou LDAP
  - none — La valeur par défaut si vous n'en spécifiez aucune

```
Fsx0123456::> security login create -vserver vserver_name -user-or-group-
name user_or_group_name -application login_application -authentication-
method auth_method -role role_or_account_name
```

La commande suivante crée un nouvel utilisateur du système de fichiers `new_fsxadmin` avec le `fsxadmin-readonly` rôle assigné, en utilisant SSH avec un mot de passe pour se connecter. Lorsque vous y êtes invité, entrez un mot de passe pour l'utilisateur.

```
Fsx0123456::> security login create -user-or-group-name new_fsxadmin -application
 ssh -authentication-method password -role fsxadmin-readonly

Please enter a password for user 'new_fsxadmin':
Please enter it again:
```

```
Fsx0123456::>
```

3. La commande suivante crée `new_vsadmin` sur la SVM un nouvel utilisateur doté du `fsx vsadmin_readonly` rôle, configuré pour utiliser SSH avec un mot de passe pour se connecter. Lorsque vous y êtes invité, entrez un mot de passe pour l'utilisateur.

```
Fsx0123456::> security login create -vserver fsx  -user-or-group-name new_vsadmin -
application ssh -authentication-method password -role vsadmin-readonly

Please enter a password for user 'new_vsadmin':
Please enter it again:

Fsx0123456::>
```

4. La commande suivante crée un nouvel utilisateur du système de fichiers en lecture seule `harvest2-user` qui sera utilisé par l'application NetApp Harvest pour collecter des métriques de performance et de capacité. Pour plus d'informations, consultez Surveillance des systèmes de fichiers FSx pour ONTAP à l'aide de Harvest et Grafana.

```
Fsx0123456::> security login create -user-or-group-name harvest2-user -application
 ssh -role fsxadmin-readonly -authentication-method password
```

Pour consulter les informations relatives à tous les utilisateurs de systèmes de fichiers et de SVM

- Utilisez la commande suivante pour afficher toutes les informations de connexion à votre système de fichiers et à vos SVM.

```
Fsx0123456::> security login show

Vserver: Fsx0123456
                                                                 Second
User/Group                 Authentication                 Acct   Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------ --------------
autosupport    console     password      autosupport      no     none
fsxadmin       http        password      fsxadmin         no     none
fsxadmin       ontapi      password      fsxadmin         no     none
fsxadmin       ssh         password      fsxadmin         no     none
fsxadmin       ssh         publickey     fsxadmin         -      none
new_fsxadmin   ssh         password      fsxadmin-readonly
                                                        no     none
```

```
Vserver: fsx
                                                                  Second
User/Group                Authentication                 Acct   Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------ --------------
new_vsadmin    ssh         password      vsadmin-readonly no     none
vsadmin        http        password      vsadmin          yes    none
vsadmin        ontapi      password      vsadmin          yes    none
vsadmin        ssh         password      vsadmin          yes    none
10 entries were displayed.

Fsx0123456::>
```

Création d'un nouveau rôle de SVM

Chaque SVM que vous créez possède un administrateur de SVM par défaut auquel est attribué le rôle prédéfini`vsadmin`. Outre l'ensemble de rôles de SVM prédéfinis, vous pouvez créer de nouveaux rôles de SVM. Si vous devez créer de nouveaux rôles pour votre SVM, utilisez la commande `security login role create` ONTAP CLI. Cette commande est disponible pour les administrateurs de systèmes de fichiers dotés du `fsxadmin` rôle.

Pour créer un nouveau rôle de SVM (CLI ONTAP)

1. Vous pouvez créer un nouveau rôle de SVM à l'aide de la `security login role create` ONTAP CLI commande suivante :

   ```
   Fsx0123456::> security login role create -role vol_role -cmddirname volume
   ```

2. Spécifiez les paramètres obligatoires suivants dans la commande :

   - `-role`— Le nom du rôle.
   - `-cmddirname`— La commande ou le répertoire de commandes auquel le rôle donne accès. Placez les noms des sous-répertoires de commandes entre guillemets doubles. Par exemple, `"volume snapshot"`. Entrez `DEFAULT` pour spécifier tous les répertoires de commandes.

3. (Facultatif) Vous pouvez également ajouter l'un des paramètres suivants à la commande :

   - `-vserver`— Le nom de la SVM associée au rôle.
   - `-access`— Le niveau d'accès pour le rôle. Pour les répertoires de commandes, cela inclut :

- `none`— Refuse l'accès aux commandes du répertoire des commandes. Il s'agit de la valeur par défaut pour les rôles personnalisés.
- `readonly`— Accorde l'accès aux commandes show dans le répertoire des commandes et ses sous-répertoires.
- `all`— Accorde l'accès à toutes les commandes du répertoire de commandes et de ses sous-répertoires. Pour accorder ou refuser l'accès aux commandes intrinsèques, vous devez spécifier le répertoire des commandes.

Pour les commandes non intrinsèques (commandes qui ne se terminent pas par `create`,`modify`,`delete`, ou`show`) :

- `none`— Refuse l'accès aux commandes du répertoire des commandes. Il s'agit de la valeur par défaut pour les rôles personnalisés.
- `readonly`— Non applicable. N'utilisez pas.
- `all`— Accorde l'accès à la commande.

- `-query`— L'objet de requête utilisé pour filtrer le niveau d'accès, qui est spécifié sous la forme d'une option valide pour la commande ou pour une commande dans le répertoire des commandes. Placez l'objet de la requête entre guillemets doubles.

4. Exécutez la commande `security login role create`.

   La commande suivante crée un rôle de contrôle d'accès nommé « admin » pour le vserver vs1.example.com. Le rôle a tous accès à la commande « volume », mais uniquement au sein de l'agrégat « aggr0 ».

```
Fsx0123456::>security login role create -role admin -cmddirname volume -query "-
aggr aggr0" -access all -vserver vs1.example.com
```

Configuration de l'authentification Active Directory pour ONTAP les utilisateurs

Utilisez la ONTAP CLI pour configurer l'utilisation de l'authentification Active Directory pour les utilisateurs ONTAP du système de fichiers et des SVM.

Vous devez être un administrateur de système de fichiers `fsxadmin` habilité à utiliser les commandes de cette procédure.

Pour configurer l'authentification Active Directory pour les ONTAP utilisateurs (ONTAPCLI)

Les commandes de cette procédure sont accessibles aux utilisateurs du système de fichiers dotés du `fsxadmin` rôle.

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *`management_endpoint_ip`* par l'adresse IP du port de gestion du système de fichiers.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Pour plus d'informations, consultez Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.

2. Utilisez la `security login domain-tunnel create`commande comme indiqué pour établir un tunnel de domaine afin d'authentifier les utilisateurs de Windows Active Directory. Remplacez *`svm_name`* par le nom de la SVM que vous utilisez pour le tunnel de domaine.

   ```
   FsxId0123456::> security login domain-tunnel create -vserver svm_name
   ```

3. Utilisez la `security login create`commande pour créer des comptes utilisateur de domaine Active Directory qui accèderont au système de fichiers.

   Spécifiez les paramètres obligatoires suivants dans la commande :

   - `-vserver`— Le nom de la SVM configurée avec CIFS et jointe à votre Active Directory. Il sera utilisé comme tunnel pour authentifier les utilisateurs du domaine Active Directory auprès du système de fichiers dans lequel le nouveau rôle ou utilisateur sera créé.
   - `-user-or-group-name`— Le nom d'utilisateur ou le nom de groupe Active Directory de la méthode de connexion. Le nom du groupe Active Directory ne peut être spécifié qu'avec la méthode `domain` d'authentification `ontapi` et `ssh` l'application.
   - `-application`— L'application de la méthode de connexion. Les valeurs possibles incluent http, ontapi et ssh.
   - `-authentication-method`— Méthode d'authentification utilisée pour la connexion. Les valeurs possibles sont notamment les suivantes :
     - domaine — pour l'authentification Active Directory
     - mot de passe — pour l'authentification par mot de passe
     - publickey — pour l'authentification par clé publique

- `-role`— Le nom du rôle de contrôle d'accès pour la méthode de connexion. Au niveau du système de fichiers, le seul rôle qui peut être spécifié est. `-role fsxadmin`

L'exemple suivant crée un compte utilisateur de domaine Active Directory `CORP\Admin` pour le système de `filesystem1` fichiers.

```
FSxId012345::> security login create -vserver filesystem1 -username CORP\Admin -
application ssh -authmethod domain -role fsxadmin
```

L'exemple suivant crée le compte `CORP\Admin` utilisateur avec une authentification par clé publique.

```
FsxId0123456ab::> security login create -user-or-group-name "CORP\Admin" -
application ssh -authentication-method publickey -role fsxadmin
Warning: To use public-key authentication, you must create a public key for user
 "CORP\Admin".
```

Créez une clé publique pour l'`CORP\Admin`utilisateur à l'aide de la commande suivante :

```
FsxId0123456ab::> security login publickey create -username "CORP
\Admin" -publickey "ecdsa-sha2-nistp256 SECRET_STRING_HERE_IS_REDACTED=
 cwaltham@b0be837a91bf.ant.amazon.com"
```

Pour vous connecter au système de fichiers à l'aide de SSH avec des informations d'identification Active Directory

- L'exemple suivant montre comment accéder par SSH à votre système de fichiers avec vos informations d'identification Active Directory si vous choisissez `ssh` le `-application` type. Le format `username "domain-name\user-name"` est le nom de domaine et le nom d'utilisateur que vous avez fournis lors de la création du compte, séparés par une barre oblique inverse et entre guillemets.

```
Fsx0123456::> ssh "CORP\user"@management.fs-abcdef01234567892.fsx.us-east-2.aws.com
```

Lorsque vous êtes invité à saisir un mot de passe, utilisez le mot de passe de l'utilisateur Active Directory.

Configuration de l'authentification par clé publique

Pour activer l'authentification par clé publique SSH, vous devez d'abord générer une clé SSH et l'associer à un compte administrateur à l'aide de la `security login publickey create` commande. Cela permet au compte d'accéder à la SVM. La `security login publickey create` commande accepte les paramètres suivants.

Paramètre	Description
`-vserver` (facultatif)	Nom de la SVM à laquelle le compte accède. Si vous configurez l'authentification par clé publique SSH pour les utilisateurs du système de fichiers, ne l'incluez `-versver` pas.
`-username`	Le nom d'utilisateur du compte. La valeur par défaut`admin`, est le nom par défaut de l'administrateur du cluster.
`-index`	Numéro d'index de la clé publique. La valeur par défaut est 0 si la clé est la première clé créée pour le compte. Dans le cas contraire , la valeur par défaut est supérieure d'un au numéro d'index le plus élevé existant pour le compte.
`-publickey`	La clé publique OpenSSH. Placez la clé entre guillemets doubles.
`-role`	Rôle de contrôle d'accès attribué au compte.
`-comment` (facultatif)	Texte descriptif de la clé publique. Placez le texte entre guillemets doubles.

L'exemple suivant associe une clé publique au compte administrateur de `svmadmin` la `svm01` SVM. Un numéro d'index est attribué à la clé publique`5`.

```
Fsx0123456::> security login publickey create -vserver svm01 -username svmadmin
 -index 5 -publickey "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAspH64CYbUsDQCdW22JnK6J/
```

```
vU9upnKzd2zAk9C1f7YaWRUAFNs2Qe5lUmQ3ldi8AD0Vfbr5T6HZPCixNAIzaFciDy7hgnmdj9eNGedGr/
JNrftQbLD1hZybX
+72DpQB0tYWBhe6eDJ1oPLobZBGfMlPXh8VjeU44i7W4+s0hG0E=tsmith@publickey.example.com"
```

> **Important**
>
> Vous devez être administrateur de SVM ou de système de fichiers pour effectuer cette tâche.

Mise à jour des exigences relatives aux mots de passe pour les rôles de système de fichiers et de SVM

Vous pouvez mettre à jour les exigences en matière de mot de passe pour un système de fichiers ou un rôle de SVM à l'aide de la commande `security login role config modify`ONTAPCLI. Cette commande n'est disponible que pour les comptes d'administrateur de système de fichiers dotés du `fsxadmin` rôle. Lors de la modification des exigences relatives au mot de passe, le système avertit si des utilisateurs existants ayant ce rôle seront affectés par la modification.

L'exemple suivant modifie la longueur minimale du mot de passe à 12 caractères pour les utilisateurs ayant le `vsadmin-readonly` rôle sur la `fsx` SVM. Dans cet exemple, certains utilisateurs possèdent déjà ce rôle.

```
FsxId0123456::> security login role config modify -role vsadmin-readonly -vserver fsx -
passwd-minlength 12
```

Le système affiche l'avertissement suivant en raison des utilisateurs existants :

```
Warning: User accounts with this role exist. Modifications to the username/password
 restrictions on this role could result in non-compliant user
        accounts.
Do you want to continue? {y|n}:

FsxId0123456::>
```

La mise à jour du mot de passe du **`fsxadmin`** compte échoue

Lorsque vous mettez à jour le mot de passe de l'`fsxadmin`utilisateur, vous pouvez recevoir un message d'erreur s'il ne répond pas aux exigences de mot de passe définies dans le système de

fichiers. Vous pouvez consulter les exigences relatives au mot de passe à l'aide de la `security login role config show` ONTAP commande CLI ou de l'API REST.

Pour consulter les exigences en matière de mot de passe pour un système de fichiers ou un rôle de SVM

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *`management_endpoint_ip`* par l'adresse IP du port de gestion du système de fichiers.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Pour plus d'informations, consultez Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.

2. La `security login role config show` commande renvoie les exigences en matière de mot de passe pour un rôle de système de fichiers ou de SVM.

   ```
   FsxId0123456::> security login role config show -role fsxadmin -
   fields password_requirement_fields
   ```

   Pour le `-fields` paramètre, spécifiez l'une ou l'ensemble des options suivantes :

   - `passwd-minlength`— La longueur minimale du mot de passe.
   - `passwd-min-special-chars`— Le nombre minimum de caractères spéciaux dans le mot de passe.
   - `passwd-min-lowercase-chars`— Le nombre minimal de caractères minuscules dans le mot de passe.
   - `passwd-min-uppercase-chars`— Le nombre minimal de caractères majuscules dans le mot de passe.
   - `passwd-min-digits`— Le nombre minimum de chiffres dans le mot de passe.
   - `passwd-alphanum`— Informations relatives à l'inclusion ou à l'exclusion de caractères alphanumériques.
   - `passwd-expiry-time`— Le délai d'expiration du mot de passe.
   - `passwd-expiry-warn-time`— L'heure d'avertissement d'expiration du mot de passe.

3. Exécutez la commande suivante pour voir toutes les exigences en matière de mot de passe :

```
FsxId0123456::> security login role config show -role fsxadmin -fields passwd-
minlength, passwd-min-special-chars, passwd-min-lowercase-chars, passwd-min-
digits, passwd-alphanum, passwd-expiry-time, passwd-expiry-warn-time, passwd-min-
uppercase-chars

vserver                role     passwd-minlength passwd-alphanum passwd-min-
special-chars passwd-expiry-time passwd-min-lowercase-chars passwd-min-uppercase-
chars passwd-min-digits passwd-expiry-warn-time
---------------------- -------- ---------------- ---------------
 ------------------------ ------------------ --------------------------
 -------------------------- ----------------- ----------------------
FsxId0123456           fsxadmin 3                enabled         0
       unlimited          0                        0                        0
               unlimited
```

Migration vers Amazon NetApp FSx pour ONTAP

Les sections suivantes fournissent des informations sur la façon de migrer vos systèmes de fichiers NetApp ONTAP existants vers Amazon FSx NetApp for ONTAP.

> **Note**
>
> Si vous envisagez d'utiliser la politique de `All` hiérarchisation pour migrer vos données vers le niveau du pool de capacités, gardez à l'esprit que les métadonnées des fichiers sont toujours stockées sur le niveau SSD et que toutes les nouvelles données utilisateur sont d'abord écrites sur le niveau SSD. Lorsque les données sont écrites sur le niveau SSD, le processus de hiérarchisation en arrière-plan commence à hiérarchiser vos données en fonction de la capacité de stockage du pool, mais le processus de hiérarchisation n'est pas immédiat et consomme les ressources du réseau. Vous devez dimensionner le niveau de votre SSD pour prendre en compte les métadonnées des fichiers (3 à 7 % de la taille des données utilisateur), en tant que tampon pour les données utilisateur avant qu'elles ne soient hiérarchisées en fonction de la capacité de stockage du pool. Nous vous recommandons de ne pas dépasser 80 % d'utilisation de votre niveau SSD.
> Lors de la migration des données, veillez à surveiller le niveau de votre SSD à l'aide des métriques du système de CloudWatch fichiers afin de vous assurer qu'il ne se remplit pas plus rapidement que le processus de hiérarchisation ne peut déplacer les données vers le pool de capacité de stockage.

Rubriques

- Migration vers FSx pour ONTAP à l'aide de NetApp SnapMirror
- Migration vers FSx pour ONTAP à l'aide de AWS DataSync

Migration vers FSx pour ONTAP à l'aide de NetApp SnapMirror

Vous pouvez migrer vos systèmes de fichiers NetApp ONTAP vers Amazon FSx NetApp for ONTAP à l'aide de. NetApp SnapMirror

NetApp SnapMirror utilise la réplication au niveau des blocs entre deux systèmes de fichiers ONTAP, pour répliquer les données d'un volume source spécifié vers un volume de destination. Nous vous

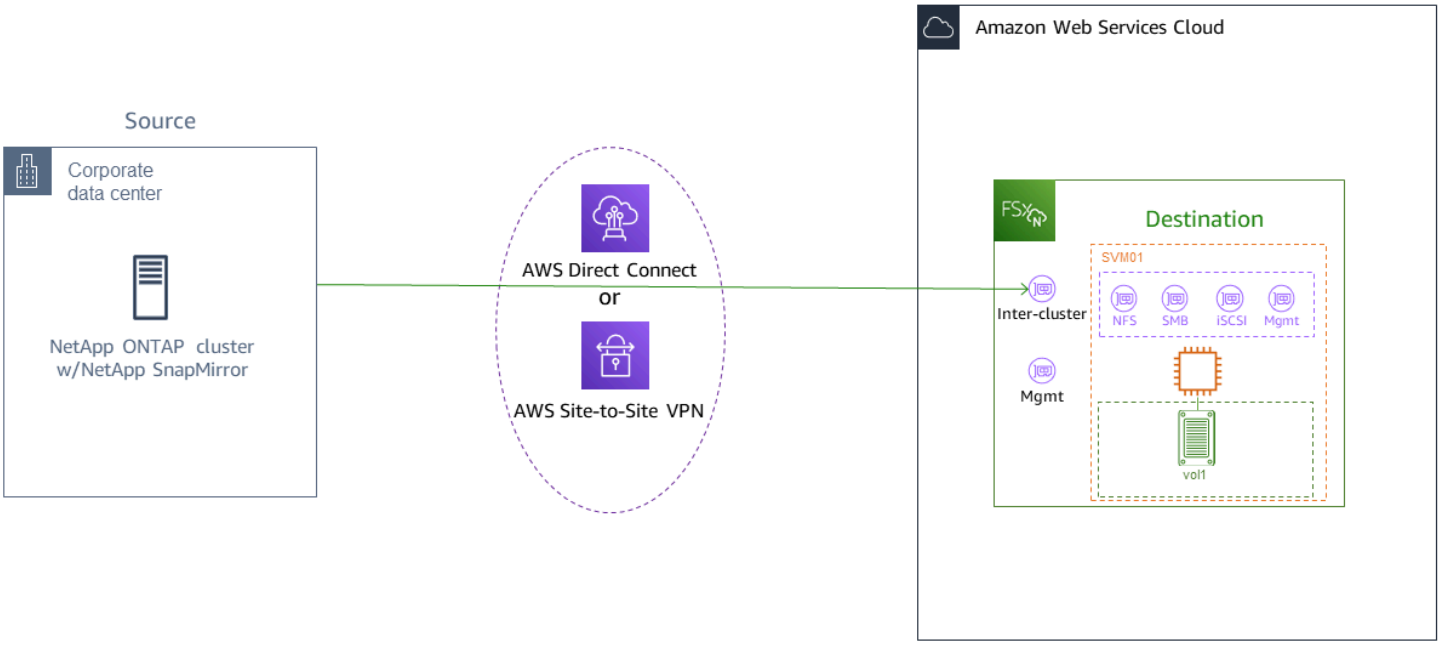
recommandons de l'utiliser SnapMirror pour migrer les systèmes de fichiers NetApp ONTAP sur site vers FSx for ONTAP. NetApp SnapMirrorLa réplication au niveau des blocs est rapide et efficace, même pour les systèmes de fichiers dotés des caractéristiques suivantes :

- Structures de répertoires complexes
- Plus de 50 millions de fichiers
- Fichiers de très petite taille (de l'ordre du kilo-octet)

Lorsque vous migrez SnapMirror vers FSx for ONTAP, les données dédupliquées et compressées restent dans ces états, ce qui réduit les temps de transfert et la quantité de bande passante requise pour la migration. Les instantanés qui existent sur les volumes ONTAP sources sont conservés lors de la migration vers les volumes de destination. La migration de vos systèmes de fichiers NetApp ONTAP locaux vers FSx for ONTAP implique les tâches de haut niveau suivantes :

1. Créez le volume de destination dans Amazon FSx.
2. Rassemblez les interfaces logiques source et de destination (LIF).
3. Établissez un peering de cluster entre les systèmes de fichiers source et de destination.
4. Créez une relation d'appairage avec la SVM.
5. Créez la SnapMirror relation.
6. Maintenez un cluster de destination à jour.
7. Passez à votre système de fichiers FSx for ONTAP.

Le schéma suivant illustre le scénario de migration décrit dans cette section.



Rubriques

- Avant de commencer
- Créez le volume de destination
- Enregistrez les LIF inter-clusters source et de destination
- Établissez le peering du cluster entre la source et la destination
- Création d'une relation de peering avec la SVM
- Créez la SnapMirror relation
- Transférez des données vers votre système de fichiers FSx for ONTAP
- Passage à Amazon FSx

Avant de commencer

Avant de commencer à utiliser les procédures décrites dans les sections suivantes, assurez-vous de remplir les conditions préalables suivantes :

- FSx for ONTAP donne la priorité au trafic client par rapport aux tâches d'arrière-plan, notamment la hiérarchisation des données, l'efficacité du stockage et les sauvegardes. Lors de la migration des données, nous vous recommandons, en règle générale, de surveiller la capacité de votre niveau SSD afin de vous assurer qu'elle ne dépasse pas 80 % d'utilisation. Vous pouvez surveiller

l'utilisation de votre niveau SSD à l'aide des métriques CloudWatch du système de fichiers. Pour plus d'informations, consultez Métriques de volume.

- Si vous définissez la politique de hiérarchisation des données du volume de destination `All` lors de la migration de vos données, toutes les métadonnées des fichiers sont stockées sur le niveau de stockage SSD principal. Les métadonnées des fichiers sont toujours stockées sur le niveau principal basé sur le SSD, quelle que soit la politique de hiérarchisation des données du volume. Nous vous recommandons de prendre un ratio de 1 : 10 pour le niveau principal : capacité de stockage du niveau pool.
- Les systèmes de fichiers source et de destination sont connectés dans le même VPC ou se trouvent dans des réseaux qui sont pairés à l'aide d'Amazon VPC Peering, Transit Gateway ou. AWS Direct Connect AWS VPN Pour plus d'informations, consultez Accès aux données depuis l'intérieur AWS et Qu'est-ce que le peering VPC ? dans le guide de peering Amazon VPC.
- Le groupe de sécurité VPC du système de fichiers FSx for ONTAP possède des règles entrantes et sortantes autorisant les protocoles ICMP et TCP sur les ports 443, 10000, 11104 et 11105 pour vos points de terminaison inter-clusters (LIF).
- Vérifiez que les volumes source et de destination exécutent des versions NetApp ONTAP compatibles avant de créer une relation de protection SnapMirror des données. Pour plus d'informations, consultez la section Versions ONTAP compatibles pour les SnapMirror relations dans NetApp la documentation utilisateur d'ONTAP. Les procédures présentées ici utilisent un système de fichiers NetApp ONTAP sur site pour la source.
- Votre système de fichiers NetApp ONTAP sur site (source) inclut une SnapMirror licence.
- Vous avez créé un système de fichiers FSx pour ONTAP de destination à l'aide d'une SVM, mais vous n'avez pas créé de volume de destination. Pour plus d'informations, consultez Création de FSx pour les systèmes de fichiers ONTAP.

Les commandes de ces procédures utilisent les alias de cluster, de SVM et de volume suivants :

- *`FSx-Dest`*— l'ID du cluster de destination (FSx) (au format F SxIdabcdef 1234567890a).
- *`OnPrem-Source`*— l'ID du cluster source.
- *`DestSVM`*— le nom de la SVM de destination.
- *`SourceSVM`*— le nom de la SVM source.
- Les noms des volumes source et de destination sont`vol1`.

> **Note**
>
> Un système de fichiers FSx for ONTAP est appelé cluster dans toutes les commandes de la CLI ONTAP.

Les procédures décrites dans cette section utilisent les commandes NetApp ONTAP CLI suivantes.

- commande de création de volume
- commandes de cluster
- commandes vserver peer
- commandes snapmirror

Vous utiliserez la CLI NetApp ONTAP pour créer et gérer une SnapMirror configuration sur votre système de fichiers FSx for ONTAP. Pour plus d'informations, consultez Utilisation de la CLI NetApp ONTAP.

Créez le volume de destination

Vous pouvez créer un volume de destination pour la protection des données (DP) à l'aide de la console Amazon FSx, de l'API et de l'API Amazon FSxAWS CLI, en plus de la NetApp CLI ONTAP et de l'API REST. Pour plus d'informations sur la création d'un volume de destination à l'aide de la console Amazon FSxAWS CLI, consultez. Création de volumes

Dans la procédure suivante, vous allez utiliser la CLI NetApp ONTAP pour créer un volume de destination sur votre système de fichiers FSx for ONTAP. Vous aurez besoin du `fsxadmin` mot de passe et de l'adresse IP ou du nom DNS du port de gestion du système de fichiers.

1. Établissez une session SSH avec le système de fichiers de destination à l'aide de l'utilisateur `fsxadmin` et du mot de passe que vous avez définis lors de la création du système de fichiers.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Créez un volume sur le cluster de destination dont la capacité de stockage est au moins égale à la capacité de stockage du volume source. `-type DP`À utiliser pour le désigner comme destination d'une SnapMirror relation.

Si vous envisagez d'utiliser la hiérarchisation des données, nous vous recommandons de le `-tiering-policy` configurer `all` sur. Cela garantit que vos données sont immédiatement transférées vers le stockage en pool de capacité et vous évite de manquer de capacité sur le niveau SSD. Après la migration, vous pouvez passer `-tiering-policy` à`auto`.

> **Note**
>
> Les métadonnées des fichiers sont toujours stockées sur le niveau principal basé sur le SSD, quelle que soit la politique de hiérarchisation des données du volume.

```
FSx-Dest::> vol create -vserver DestSVM -volume vol1 -aggregate aggr1 -size 1g -
type DP -tiering-policy all
```

Enregistrez les LIF inter-clusters source et de destination

SnapMirror utilise des interfaces logiques inter-clusters (LIF), chacune dotée d'une adresse IP unique, pour faciliter le transfert de données entre les clusters source et de destination.

1. Pour le FSx de destination pour les systèmes de fichiers ONTAP, vous pouvez récupérer les adresses IP du point de terminaison inter-clusters depuis la console Amazon FSx en accédant à l'onglet Administration de la page de détails de votre système de fichiers.
2. Pour le cluster NetApp ONTAP source, récupérez les adresses IP LIF inter-clusters à l'aide de la CLI ONTAP. Exécutez la commande suivante :

```
OnPrem-Source::> network interface show -role intercluster

Logical                         Network
Vserver     Interface  Status  Address/Mask
----------- ---------- ------- ------------
FSx-Dest
             inter_1    up/up  10.0.0.36/24
             inter_2    up/up  10.0.1.69/24
```

> **Note**
>
> Pour les systèmes de fichiers évolutifs, il existe deux adresses IP inter-clusters pour chaque paire de haute disponibilité (HA). Enregistrez ces valeurs pour plus tard.

Enregistrez les adresses `inter_2` IP `inter_1` et. Ils sont référencés au `FSx-Dest` fur `dest_inter_1` et à mesure `dest_inter_2` et au `OnPrem-Source` fur `source_inter_1` et à mesure`source_inter_2`.

Établissez le peering du cluster entre la source et la destination

Établissez une relation entre pairs du cluster sur le cluster de destination en fournissant les adresses IP inter-clusters. Vous devrez également créer une phrase secrète que vous devrez saisir lorsque vous établirez le peering de cluster sur le cluster source.

1. Configurez le peering sur le cluster de destination à l'aide de la commande suivante. Pour les systèmes de fichiers évolutifs, vous devez fournir chaque adresse IP inter-clusters.

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-
addrs source_inter_1,source_inter_2

Enter the passphrase:
Confirm the passphrase:
Notice: Now use the same passphrase in the "cluster peer create" command in the
 other cluster.
```

2. Ensuite, établissez la relation entre pairs du cluster sur le cluster source. Vous devrez saisir le mot de passe que vous avez créé ci-dessus pour vous authentifier. Pour les systèmes de fichiers évolutifs, vous devez fournir chaque adresse IP inter-clusters.

```
OnPrem-Source::> cluster peer create -address-family ipv4 -peer-
addrs dest_inter_1,dest_inter_2

Enter the passphrase:
Confirm the passphrase:
```

3. Vérifiez que le peering a réussi à l'aide de la commande suivante sur le cluster source. Dans la sortie, `Availability` doit être défini sur`Available`.

```
OnPrem-Source::> cluster peer show

Peer Cluster Name  Availability   Authentication
-----------------  -------------- --------------
FSx-Dest           Available      ok
```

Création d'une relation de peering avec la SVM

Une fois le peering en cluster établi, l'étape suivante consiste à appairer les SVM. Créez une relation d'appairage de la SVM sur le cluster de destination (FSX-DEST) à l'aide de la commande. `vserver peer` Les alias supplémentaires utilisés dans les commandes suivantes sont les suivants :

- `DestLocalName`— c'est le nom utilisé pour identifier la SVM de destination lors de la configuration de l'appairage de la SVM sur la SVM source.
- `SourceLocalName`— c'est le nom utilisé pour identifier la SVM source lors de la configuration de l'appairage de la SVM sur la SVM de destination.

1. Utilisez la commande suivante pour créer une relation d'appairage entre les SVM source et de destination.

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver SourceSVM -peer-
cluster OnPrem-Source -applications snapmirror -local-name SourceLocalName

 Info: [Job 207] 'vserver peer create' job queued
```

2. Acceptez la relation d'appairage sur le cluster source :

```
OnPrem-Source::> vserver peer accept -vserver SourceSVM -peer-vserver DestSVM -
local-name DestLocalName

 Info: [Job 211] 'vserver peer accept' job queued
```

3. Vérifiez l'état d'appairage de la SVM à l'aide de la commande suivante ; `Peer State` il doit être défini sur `peered` dans la réponse.

```
OnPrem-Source::> vserver peer show

Peer    Peer     Peer   Peering  Remote
```

```
vserver Vserver  State  Cluster  Applications  Vserver
------- -------- ------ -------- ------------ ---------
svm01   destsvm1 peered FSx-Dest snapmirror    svm01
```

Créez la SnapMirror relation

Maintenant que vous avez examiné les SVM source et de destination, les étapes suivantes consistent à créer et à initialiser la SnapMirror relation sur le cluster de destination.

> **Note**
>
> Une fois que vous avez créé et initialisé une SnapMirror relation, les volumes de destination sont en lecture seule jusqu'à ce que la relation soit rompue.

- Utilisez la `snapmirror create` commande pour créer la SnapMirror relation sur le cluster de destination. La `snapmirror create` commande doit être utilisée depuis la SVM de destination.

  Vous pouvez éventuellement l'utiliser `-throttle` pour définir la bande passante maximale (en Kbit/s) pour la SnapMirror relation.

  ```
  FSx-Dest::> snapmirror create -source-path SourceLocalName:vol1 -destination-
  path DestSVM:vol1 -vserver DestSVM -throttle unlimited

   Operation succeeded: snapmirror create for the relationship with destination
   "DestSVM:vol1".
  ```

Transférez des données vers votre système de fichiers FSx for ONTAP

Maintenant que vous avez créé la SnapMirror relation, vous pouvez transférer les données vers le système de fichiers de destination.

1. Vous pouvez transférer des données vers le système de fichiers de destination en exécutant la commande suivante sur le système de fichiers de destination.

> **Note**
>
> Une fois que vous avez exécuté cette commande, le transfert des instantanés des données du volume source vers le volume de destination SnapMirror commence.

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:vol1 -source-
path SourceLocalName:vol1
```

2. Si vous migrez des données utilisées activement, vous devez mettre à jour votre cluster de destination afin qu'il reste synchronisé avec votre cluster source. Pour effectuer une mise à jour unique du cluster de destination, exécutez la commande suivante.

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

3. Vous pouvez également planifier des mises à jour horaires ou quotidiennes avant de terminer la migration et de transférer vos clients vers FSx for ONTAP. Vous pouvez établir un calendrier de SnapMirror mise à jour à l'aide de la `snapmirror modify`commande.

```
FSx-Dest::> snapmirror modify -destination-path DestSVM:vol1 -schedule hourly
```

Passage à Amazon FSx

Pour préparer le transfert vers votre système de fichiers FSx for ONTAP, procédez comme suit :

- Déconnectez tous les clients qui écrivent sur le cluster source.
- Effectuez un dernier SnapMirror transfert pour éviter toute perte de données lors du découpage.
- Brisez la SnapMirror relation.
- Connectez tous les clients à votre système de fichiers FSx for ONTAP.

1. Pour vous assurer que toutes les données du cluster source sont transférées vers le système de fichiers FSx for ONTAP, effectuez un dernier transfert Snapmirror.

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

2. Assurez-vous que la migration des données est terminée en vérifiant que ce paramètre `Mirror State` est défini sur et `Relationship Status` est défini sur`Idle`. `Snapmirrored` Vous devez également vous assurer que la `Last Transfer End Timestamp` date correspond à vos attentes, car elle indique la date du dernier transfert vers le volume de destination.
3. Exécutez la commande suivante pour afficher l' SnapMirror état.

```
FSx-Dest::> snapmirror show -fields state,status,last-transfer-end-timestamp

Source     Destination   Mirror        Relationship Last Transfer End
Path       Path          State         Status       Timestamp
---------- -----------   ----------    -------      --------------
Svm01:vol1 svm02:DestVol Snapmirrored  Idle         09/02 09:02:21
```

4. Désactivez tous SnapMirror les futurs transferts à l'aide de la `snapmirror quiesce` commande.

```
FSx-Dest::> snapmirror quiesce -destination-path DestSVM:vol1
```

5. Vérifiez que le `Relationship Status` est passé à `Quiesced` l'utilisation`snapmirror show`.

```
FSx-Dest::> snapmirror show

Source            Destination   Mirror        Relationship
Path              Path          State         Status
-----------       ------------  ------------- --------
sourcesvm1:vol1   svm01:DestVol Snapmirrored  Quiesced
```

6. Pendant la migration, le volume de destination est en lecture seule. Pour activer la lecture/écriture, vous devez rompre la SnapMirror relation et passer à votre système de fichiers FSx for ONTAP. Rompez la SnapMirror relation à l'aide de la commande suivante.

```
FSx-Dest::> snapmirror break -destination-path DestSVM:vol1

Operation succeeded: snapmirror break for destination "DestSVM:vol1".
```

7. Une fois la SnapMirror réplication terminée et la SnapMirror relation rompue, vous pouvez monter le volume pour rendre les données disponibles.

```
FSx-Dest::> vol mount -vserver fsx -volume vol1 -junction-path /vol1
```

Le volume est désormais disponible avec les données du volume source entièrement migrées vers le volume de destination. Les clients peuvent également y lire et écrire sur le volume. Si vous avez précédemment défini ce volume sur`all`, vous pouvez le `tiering-policy` remplacer par `auto` ou `snapshot-only` et vos données passeront automatiquement d'un niveau de stockage à un autre en fonction des modèles d'accès. Pour rendre ces données accessibles aux clients et aux applications, voirAccès aux données .

Migration vers FSx pour ONTAP à l'aide de AWS DataSync

Nous vous recommandons de l'utiliser AWS DataSync pour transférer des données entre les systèmes de fichiers FSx pour ONTAP et les systèmes de fichiers non-ONTAP, notamment FSx for Lustre, FSx pour OpenZFS, FSx pour Windows File Server, Amazon EFS, Amazon S3 et les filers sur site. Si vous transférez des fichiers entre FSx for ONTAP et NetApp ONTAP, nous vous recommandons d'utiliser. NetApp SnapMirror AWS DataSyncest un service de transfert de données qui simplifie, automatise et accélère le déplacement et la réplication des données entre des systèmes de stockage autogérés et des services AWS de stockage via Internet ou. AWS Direct Connect DataSync peut transférer les données et les métadonnées de votre système de fichiers, telles que la propriété, les horodatages et les autorisations d'accès.

Vous pouvez l'utiliser DataSync pour transférer des fichiers entre deux systèmes de fichiers FSx for ONTAP, ainsi que pour déplacer des données vers un système de fichiers appartenant à un autre Région AWS compte OR. AWS Vous pouvez également l'utiliser DataSync avec les systèmes de fichiers FSx for ONTAP pour d'autres tâches. Par exemple, vous pouvez effectuer des migrations de données ponctuelles, ingérer régulièrement des données pour des charges de travail distribuées et planifier la réplication à des fins de protection et de restauration des données.

Dans DataSync, un emplacement est le point de terminaison d'un système de fichiers FSx for ONTAP. Pour plus d'informations sur des scénarios de transfert spécifiques, consultez la section Utilisation des emplacements dans le guide de AWS DataSync l'utilisateur.

> **Note**
>
> Si vous envisagez d'utiliser la politique de `All` hiérarchisation pour migrer vos données vers le niveau du pool de capacités, gardez à l'esprit que les métadonnées des fichiers sont toujours stockées sur le niveau SSD et que toutes les nouvelles données utilisateur sont d'abord écrites sur le niveau SSD. Lorsque les données sont écrites sur le niveau SSD, le processus de hiérarchisation en arrière-plan commence à hiérarchiser vos données en fonction de la capacité de stockage du pool, mais le processus de hiérarchisation n'est pas

immédiat et consomme les ressources du réseau. Vous devez dimensionner le niveau de votre SSD pour prendre en compte les métadonnées des fichiers (3 à 7 % de la taille des données utilisateur), en tant que tampon pour les données utilisateur avant qu'elles ne soient hiérarchisées en fonction de la capacité de stockage du pool. Nous vous recommandons de ne pas dépasser 80 % d'utilisation du SSD.
Lors de la migration des données, veillez à surveiller le niveau de votre SSD à l'aide des métriques du système de CloudWatch fichiers afin de vous assurer qu'il ne se remplit pas plus rapidement que le processus de hiérarchisation ne peut déplacer les données vers le pool de capacité de stockage. Vous pouvez également limiter les DataSync transferts à un taux inférieur à celui de la hiérarchisation afin de garantir que le niveau d'utilisation de votre SSD ne dépasse pas 80 %. Par exemple, pour les systèmes de fichiers dotés d'une capacité de débit d'au moins 512 Mo/s, une limitation de 200 Mo/s permet généralement d'équilibrer les taux de transfert de données et de hiérarchisation des données.

Prérequis

Pour migrer des données vers votre configuration FSx for ONTAP, vous avez besoin d'un serveur et d'un réseau répondant aux exigences. DataSync Pour en savoir plus, consultez la section Exigences DataSync du guide de AWS DataSync l'utilisateur.

Étapes de base pour la migration de fichiers à l'aide de DataSync

Le transfert de fichiers d'une source vers une destination DataSync implique les étapes de base suivantes :

- Téléchargez et déployez un agent dans votre environnement, puis activez-le (inutile en cas de transfert entre deuxServices AWS).
- Créez un emplacement source et un emplacement de destination.
- Créez une tâche.
- Exécutez la tâche pour transférer les fichiers depuis la source vers la destination.

Pour plus d'informations, consultez les rubriques suivantes dans le AWS DataSyncGuide de l'utilisateur :

- Transfert de données entre le stockage autogéré et AWS
- Création d'un emplacement pour Amazon FSx for ONTAP NetApp

Surveillance d'Amazon FSx pour ONTAP NetApp

Vous pouvez utiliser les services et outils suivants pour surveiller l'utilisation et l'activité d'Amazon FSx for NetApp ONTAP :

- Amazon CloudWatch — Vous pouvez surveiller les systèmes de fichiers à l'aide d'Amazon CloudWatch, qui collecte et traite automatiquement les données brutes de FSx for ONTAP pour en faire des métriques lisibles. Ces statistiques sont conservées pendant une période de 15 mois afin que vous puissiez accéder aux informations historiques et voir comment fonctionne votre système de fichiers. Vous pouvez également définir des alarmes en fonction de vos mesures sur une période donnée et effectuer une ou plusieurs actions en fonction de la valeur des mesures par rapport aux seuils que vous spécifiez.
- Événements ONTAP EMS — Vous pouvez surveiller votre système de fichiers FSx for ONTAP en utilisant les événements générés par le système de gestion des événements (EMS) d'ONTAP. Les événements EMS sont des notifications d'événements survenus dans votre système de fichiers, tels que la création de LUN iSCSI ou le dimensionnement automatique des volumes.
- NetApp Cloud Insights : vous pouvez surveiller les indicateurs de configuration, de capacité et de performance de vos systèmes de fichiers FSx for ONTAP à l'aide du service NetApp Cloud Insights. Vous pouvez également créer des alertes en fonction des conditions métriques.
- NetApp Harvest et NetApp Grafana — Vous pouvez surveiller votre système de fichiers FSx for ONTAP en utilisant Harvest et Grafana. NetApp NetApp NetApp Harvest surveille les systèmes de fichiers ONTAP en collectant des indicateurs de performance, de capacité et de matériel à partir de FSx pour les systèmes de fichiers ONTAP. Grafana fournit un tableau de bord où les statistiques de récolte collectées peuvent être affichées.
- AWS CloudTrail— Vous pouvez l'utiliser AWS CloudTrail pour capturer tous les appels d'API pour Amazon FSx sous forme d'événements. Ces événements fournissent un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Amazon FSx.

Rubriques

- Enregistrement de FSx pour les appels d'API ONTAP avecAWS CloudTrail

Surveillance avec Amazon CloudWatch

Vous pouvez surveiller les systèmes de fichiers à l'aide d'Amazon CloudWatch, qui collecte et traite les données brutes d'Amazon FSx for NetApp ONTAP pour en faire des métriques lisibles en temps quasi réel. Ces statistiques sont conservées pendant une période de 15 mois, afin que vous puissiez accéder aux informations historiques afin de déterminer les performances de votre système de fichiers. Les données métriques de FSx for ONTAP sont automatiquement envoyées par défaut à des CloudWatch intervalles d'une minute. Pour plus d'informations CloudWatch, consultez Qu'est-ce qu'Amazon CloudWatch ? dans le guide de CloudWatch l'utilisateur Amazon.

> **Note**
>
> Par défaut, FSx for ONTAP envoie des données métriques à des intervalles d'une minute, CloudWatch à l'exception des métriques suivantes qui sont envoyées à intervalles de 5 minutes :
>
> - `FileServerDiskThroughputBalance`
> - `FileServerDiskIopsBalance`

CloudWatch les métriques pour FSx for ONTAP sont organisées en quatre catégories, définies par les dimensions utilisées pour interroger chaque métrique. Pour plus d'informations sur les dimensions, consultez la section Dimensions du guide de CloudWatch l'utilisateur Amazon.

- Mesures du système de fichiers : mesures des ile-system-level performances et de la capacité de stockage F.
- Mesures détaillées du système de fichiers : F métriques ile-system-level de stockage par niveau de stockage (SSD et pool de capacité).
- Mesures de volume : mesures de performance et de capacité de stockage par volume.
- Mesures de volume détaillées : mesures de capacité de stockage par volume par niveau de stockage ou par type de données (utilisateur, instantané ou autre).

Toutes les CloudWatch métriques de FSx for ONTAP sont publiées dans l'espace de noms dans`AWS/FSx`. CloudWatch

Rubriques

Comment utiliser FSx pour les métriques ONTAP CloudWatch

Les CloudWatch métriques rapportées par Amazon FSx fournissent des informations précieuses sur vos systèmes de fichiers et volumes FSx for ONTAP.

Rubriques

Surveillance des métriques du système de fichiers dans la console Amazon FSx

Vous pouvez utiliser le panneau Surveillance et performance du tableau de bord de votre système de fichiers dans la console Amazon FSx pour consulter les métriques décrites dans le tableau suivant. Pour plus d'informations, consultez Accès aux CloudWatch métriques.

Surveillance et performance	Comment puis-je...	Diagramme	Métriques pertinentes
Récapitulatif	... déterminer la capacité de stockage disponible sur mon système de fichiers ?	Capacité de stockage principal disponible (octets)	`StorageCapacity {SSD} - StorageUsed {SSD}`

Surveillance et performance	Comment puis-je...	Diagramme	Métriques pertinentes
	... déterminer le débit client total de mon système de fichiers ?	Débit client total (octets/s)	SOMME (`DataReadBytes +DataWriteBytes`) /PÉRIODE (en secondes)
	... déterminer le nombre total d'IOPS des clients de mon système de fichiers ?	Nombre total d'IOPS par seconde du client (opérations/s)	SOMME (`DataReadOperations + DataWriteOperations +MetadataOperations`) /PÉRIODE (en secondes)
	... déterminer la latence moyenne pour les opérations de lecture, d'écriture et de métadonnées de mon système de fichiers ?	Latence moyenne (ms/opération)	Latence de lecture moyenne : `DataReadOperationTime * 1000/DataReadOperations` Latence d'écriture moyenne : `DataWriteOperationTime * 1000/DataWriteOperations` Latence moyenne des métadonnées : `MetadataOperationTime * 1000/MetadataOperations`

Surveillance et performance	Comment puis-je...	Diagramme	Métriques pertinentes
	... déterminer la répartition de la capacité de stockage utilisée et gratuite sur mon système de fichiers ?	Distribution du stockage	Niveau principal disponible : `StorageCapacity {SSD} - StorageUsed {SSD}` Niveau principal utilisé : `StorageUsed {SSD}` Pool de capacités utilisé : `StorageUsed {StandardCapacityPool }`
	... déterminer les économies réalisées grâce à l'efficacité du stockage (compression, déduplication et compactage) ?	Économies d'efficacité du stockage	`StorageEfficiencySavings`
	... déterminer la quantité de stockage principal disponible ?	Capacité de stockage principal disponible (octets)	`StorageCapacity {SSD} - StorageUsed {SSD}`
Stockag	... déterminer le pourcentage de stockage principal utilisé pour mon système de fichiers ?	Taux d'utilisation de la capacité de stockage principal (pourcentage)	`StorageUsed {SSD} * 100/ StorageCapacity {} SSD`

Surveillance et performance	Comment puis-je...	Diagramme	Métriques pertinentes
Performances du serveur de fichiers	... déterminer si mon système de fichiers approche de sa limite de débit réseau ?	Débit du réseau — utilisation (pourcentage)	`NetworkThroughputUtilization`
	... déterminer si mon système de fichiers approche de sa limite de débit de disque ?	Débit du disque : utilisation (pourcentage)	`FileServerDiskThroughputUtilization`
	... déterminer si mon système de fichiers a épuisé ses crédits de rafale autorisés pour le débit du disque ?	Débit du disque — solde de rafale (pourcentage)	`FileServerDiskThroughputBalance`
	... déterminer si mon système de fichiers approche la limite d'IOPS SSD de ses serveurs de fichiers ?	IOPS sur disque : taux d'utilisation (pourcentage)	`FileServerDiskIopsUtilization`

Surveillance et performance	Comment puis-je...	Diagramme	Métriques pertinentes
	... déterminer si mon système de fichiers a épuisé les crédits de rafale autorisés par ses serveurs de fichiers pour les IOPS sur disque SSD ?	Nombre d'E/S par seconde sur le disque : équilibre des rafales (pourcentage)	`FileServerDiskIopsBalance`
	... déterminer l'utilisation moyenne du processeur du système de fichiers ?	Utilisation du processeur (pourcentage)	`CPUUtilization`
	... déterminer si ma charge de travail utilise efficacement la RAM et les caches de lecture NVMe de mon système de fichiers ?	Taux de réussite du cache (pourcentage)	`FileServerCacheHitRatio`
Performances disque	... déterminer si mon système de fichiers est proche de sa capacité d'IOPS SSD actuellement allouée ?	IOPS du disque : utilisation (SSD) (pourcentage)	`DiskIopsUtilization`

> **Note**
>
> Nous vous recommandons de maintenir une utilisation moyenne de la capacité de débit pour toutes les dimensions liées aux performances telles que l'utilisation du réseau, l'utilisation du processeur et l'utilisation des IOPS sur SSD à moins de 50 %. Cela garantit que vous disposez d'une capacité de débit inutilisée suffisante pour faire face aux pics inattendus de votre charge de travail, ainsi que pour toutes les opérations de stockage en arrière-plan (telles que la synchronisation du stockage, la hiérarchisation des données ou les sauvegardes).

Surveillance des métriques de volume dans la console Amazon FSx

Vous pouvez consulter le panneau de surveillance sur le tableau de bord de votre volume dans la console Amazon FSx pour consulter des indicateurs de performance supplémentaires. Pour plus d'informations, consultez Accès aux CloudWatch métriques.

Surveillance	Comment puis-je...	Diagramme	Métriques pertinentes
	... déterminer la capacité de stockage disponible de mon volume ?	Capacité de stockage disponible	`StorageCapacity`
	... déterminer le débit client total de mon volume ?	Débit client total (octets/s)	SOMME (`DataReadBytes +DataWriteBytes`) /PÉRIODE (en secondes)
	... déterminer le nombre total d'IOPS par client de mon volume ?	Nombre total d'IOPS par seconde du client	SOMME (`DataRead0perations + DataWrite0perations +Metadata0perations`) /PÉRIODE (en secondes)

Surveillance	Comment puis-je...	Diagramme	Métriques pertinentes
		(opérations/s)	
	... déterminer le nombre d'opérations de lecture et d'écriture provenant ou destinées au niveau du pool de capacités ?	Nombre d'IOPS du pool de capacités (opérations/sec)	Opérations de lecture : `CapacityPoolReadOperations` Opérations d'écriture : `CapacityPoolWriteOperations`
	... déterminer la latence moyenne pour les opérations de lecture, d'écriture et de métadonnées de mon volume ?	Latence moyenne (ms/opération)	Latence de lecture moyenne : `DataReadOperationTime * 1000/DataReadOperations` Latence d'écriture moyenne : `DataWriteOperationTime * 1000/DataWriteOperations` Latence moyenne des métadonnées : `MetadataOperationTime * 1000/MetadataOperations`
	... déterminer le nombre de fichiers ou d'inodes disponibles sur mon volume ?	Fichiers disponibles (inodes)	`FilesCapacity - FilesUsed`
	... déterminer la répartition de la capacité de stockage utilisée et gratuite sur mon volume ?	Distribution du stockage	`StorageCapacity - StorageUsed`

Accès aux CloudWatch métriques

Vous pouvez consulter les CloudWatch métriques Amazon pour Amazon FSx de la manière suivante :

- La console Amazon FSx
- La CloudWatch console Amazon
- Le AWS Command Line Interface (AWS CLI) pour CloudWatch
- L' CloudWatch API

La procédure suivante explique comment consulter les CloudWatch métriques de votre système de fichiers avec la console Amazon FSx.

Pour consulter CloudWatch les métriques de votre système de fichiers à l'aide de la console Amazon FSx

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation de gauche, choisissez Systèmes de fichiers, puis choisissez le système de fichiers dont vous souhaitez consulter les métriques.
3. Sur la page Résumé, choisissez Surveillance et performances dans le deuxième panneau pour afficher les graphiques des métriques de votre système de fichiers.

Le panneau Surveillance et performance comporte quatre onglets.

- Choisissez Résumé (onglet par défaut) pour afficher les avertissements, les CloudWatch alarmes et les graphiques actifs relatifs à l'activité du système de fichiers.
- Choisissez Stockage pour afficher la capacité de stockage et les indicateurs d'utilisation.
- Choisissez Performances pour consulter les indicateurs de performance du serveur de fichiers et du stockage.
- Choisissez les CloudWatch alarmes pour afficher les graphiques de toutes les alarmes configurées pour votre système de fichiers.

La procédure suivante explique comment consulter les CloudWatch métriques de votre volume avec la console Amazon FSx

Pour consulter CloudWatch les métriques de votre volume à l'aide de la console Amazon FSx

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation de gauche, choisissez Volumes, puis le volume dont vous souhaitez consulter les métriques.
3. Sur la page Résumé, choisissez Surveillance (onglet par défaut) dans le deuxième panneau pour afficher les graphiques des indicateurs de votre volume.

La procédure suivante explique comment consulter les CloudWatch métriques de votre système de fichiers avec la CloudWatch console Amazon.

Pour consulter les métriques à l'aide de la CloudWatch console Amazon

1. Sur la page Résumé de votre système de fichiers, choisissez Surveillance et performances dans le deuxième panneau pour afficher les graphiques des métriques de votre système de fichiers.
2. Choisissez Afficher dans les métriques dans le menu des actions en haut à droite du graphique que vous souhaitez afficher dans la CloudWatch console Amazon. Cela ouvre la page Metrics dans la CloudWatch console Amazon.

La procédure suivante explique comment ajouter les métriques du système de fichiers FSx for ONTAP à un tableau de bord dans la console Amazon. CloudWatch

Pour ajouter des métriques à une CloudWatch console Amazon

1. Choisissez l'ensemble de mesures (résumé, stockage ou performances) dans le panneau Monitoring & performance de la console Amazon FSx.
2. Choisissez Ajouter au tableau de bord dans le coin supérieur droit du panneau. Cela ouvre la CloudWatch console Amazon.
3. Sélectionnez un CloudWatch tableau de bord existant dans la liste ou créez-en un nouveau. Pour plus d'informations, consultez la section Utilisation CloudWatch des tableaux de bord Amazon dans le guide de CloudWatch l'utilisateur Amazon.

La procédure suivante explique comment accéder aux métriques de votre système de fichiers à l'aide du AWS CLI.

Pour accéder aux métriques depuis le AWS CLI

- Utilisez la commande CloudWatch list-metrics CLI avec le `--namespace "AWS/FSx"` paramètre. Pour plus d'informations, consultez la référence de la commande AWS CLI.

La procédure suivante explique comment accéder aux métriques de votre système de fichiers avec l' CloudWatch API.

Pour accéder aux métriques depuis l' CloudWatch API

- Appelez l'opération GetMetricStatistics API. Pour plus d'informations, consultez le Amazon CloudWatch API Reference.

Métriques du système de fichiers

Vos métriques de système de fichiers Amazon FSx for NetApp ONTAP sont classées en métriques de système de fichiers ou en métriques de système de fichiers détaillées.

- Les métriques du système de fichiers sont des mesures de performance et de stockage agrégées pour un système de fichiers unique qui prennent une seule dimension,`FileSystemId`. Ces indicateurs mesurent les performances du réseau et l'utilisation de la capacité de stockage de votre système de fichiers.
- Les indicateurs détaillés du système de fichiers mesurent la capacité de stockage de votre système de fichiers et le stockage utilisé à chaque niveau de stockage (par exemple, le stockage SSD et le stockage en pool de capacité). Chaque métrique inclut une `DataType` dimension `FileSystemIdStorageTier`, et.

Notez ce qui suit concernant le moment où Amazon FSx publie des points de données pour ces métriques afin de : CloudWatch

- Pour les métriques d'utilisation (toute métrique dont le nom se termine par Utilization, par exemple`NetworkThroughputUtilization`), un point de données est émis à chaque période pour chaque serveur de fichiers ou agrégat actif. Par exemple, Amazon FSx émet une métrique en minutes par serveur de fichiers actif pour`FileServerDiskIopsUtilization`, et une métrique en minutes par agrégat pour. `DiskIopsUtilization`
- Pour toutes les autres mesures, un seul point de données est émis par période, correspondant à la valeur totale de la métrique sur tous vos serveurs de fichiers actifs (comme `DataReadBytes` pour

les métriques de serveur de fichiers) ou sur tous vos agrégats (comme `DiskReadBytes` pour les métriques de stockage).

Rubriques

Métriques d'E/S réseau

Toutes ces mesures ont une seule dimension,`FileSystemId`.

Métrique	Description
`NetworkThroughputUtilization`	Pourcentage d'utilisation du débit réseau pour le système de fichiers. La `Average` statistique représente l'utilisa tion moyenne du débit réseau du système de fichiers sur une période spécifiée. La `Minimum` statistique représente le taux d'utilisation du débit réseau le plus faible du système de fichiers sur une période spécifiée. La `Maximum` statistique représente le taux d'utilisation du débit réseau le plus élevé du système de fichiers sur une période spécifiée. Unités : pourcentage Statistiques valides : `Average`,`Minimum`, et `Maximum`

Métrique	Description
`NetworkSentBytes`	Nombre d'octets (E/S réseau) envoyés par le système de fichiers. La `Sum` statistique est le nombre total d'octets envoyés par le système de fichiers sur une période spécifiée. Pour calculer le débit envoyé (octets par seconde) pour n'importe quelle statistique, divisez la statistique par les secondes pendant la période spécifiée. Unités : octets Statistiques valides : `Sum`
`NetworkReceivedBytes`	Nombre d'octets (E/S réseau) reçus par le système de fichiers. La `Sum` statistique représente le nombre total d'octets reçus par le système de fichiers au cours d'une période spécifiée. Pour calculer le débit reçu (octets par seconde) pour n'importe quelle statistique, divisez la statistique par les secondes pendant la période spécifiée. Unités : octets Statistiques valides : `Sum`

Métrique	Description
`DataReadBytes`	Nombre d'octets (E/S réseau) entre les lectures effectuées par les clients et le système de fichiers. La `Sum` statistique représente le nombre total d'octets associés aux opérations de lecture pendant la période spécifiée. Pour calculer le débit moyen (octets par seconde) pour une période, divisez la `Sum` statistique par le nombre de secondes pendant la période spécifiée. Unités : octets Statistiques valides : `Sum`
`DataWriteBytes`	Nombre d'octets (E/S réseau) provenant des écritures effectuées par les clients sur le système de fichiers. La `Sum` statistique représente le nombre total d'octets associés aux opérations d'écriture pendant la période spécifiée. Pour calculer le débit moyen (octets par seconde) pour une période, divisez la `Sum` statistique par le nombre de secondes pendant la période spécifiée. Unités : octets Statistiques valides : `Sum`

Métrique	Description
`DataReadOperations`	Nombre d'opérations de lecture (E/S réseau) entre les lectures effectuées par les clients et le système de fichiers. La `Sum` statistique représente le nombre total d'opérations d'E/S survenues au cours d'une période spécifiée. Pour calculer le nombre moyen d'opérations de lecture par seconde pendant une période, divisez la `Sum` statistique par le nombre de secondes pendant la période spécifiée. Unités : nombre Statistiques valides : `Sum`
`DataWriteOperations`	Nombre d'opérations d'écriture (E/S réseau) effectuées à partir des écritures effectuées par les clients dans le système de fichiers. La `Sum` statistique représente le nombre total d'opérations d'E/S survenues au cours d'une période spécifiée. Pour calculer la moyenne des opérations d'écriture par seconde pendant une période, divisez la `Sum` statistique par le nombre de secondes pendant la période spécifiée. Unités : nombre Statistiques valides : `Sum`

Métrique	Description
`MetadataOperations`	Nombre d'opérations de métadonnées (E/S réseau) effectuées par les clients sur le système de fichiers. La `Sum` statistique représente le nombre total d'opérations d'E/S survenues au cours d'une période spécifiée. Pour calculer le nombre moyen d'opérations de métadonnées par seconde pendant une période, divisez la `Sum` statistique par le nombre de secondes pendant la période spécifiée. Unités : nombre Statistiques valides : `Sum`
`DataReadOperationTime`	Somme du temps total passé dans le système de fichiers pour les opérations de lecture (E/S réseau) par les clients accédant aux données du système de fichiers. La `Sum` statistique représente le nombre total de secondes consacrées aux opérations de lecture pendant la période spécifiée. Pour calculer la latence de lecture moyenne pour une période, divisez la `Sum` statistique par le chiffre `Sum` de la `DataReadOperations` métrique sur la même période. Unités : secondes Statistiques valides : `Sum`

Métrique	Description
`DataWriteOperationTime`	Somme du temps total passé dans le système de fichiers pour effectuer les opérations d'écriture (E/S réseau) des clients accédant aux données du système de fichiers. La `Sum` statistique représente le nombre total de secondes consacrées aux opérations d'écriture pendant la période spécifiée. Pour calculer la latence d'écriture moyenne pour une période, divisez la `Sum` statistique par `Sum` la `DataWriteOperations` métrique sur la même période. Unités : secondes Statistiques valides : `Sum`
`CapacityPoolReadBytes`	Nombre d'octets lus (E/S réseau) depuis le niveau du pool de capacités du système de fichiers. Pour garantir l'intégrité des données, ONTAP effectue une opération de lecture sur le pool de capacités immédiatement après avoir effectué une opération d'écriture. La `Sum` statistique représente le nombre total d'octets lus depuis le niveau du pool de capacités du système de fichiers sur une période spécifiée. Pour calculer le pool de capacité en octets par seconde, divisez la `Sum` statistique par les secondes au cours d'une période spécifiée. Unités : octets Statistiques valides : `Sum`

Métrique	Description
`CapacityPoolReadOperations`	Nombre d'opérations de lecture (E/S réseau) depuis le niveau du pool de capacités du système de fichiers. Cela se traduit par une demande de lecture du pool de capacités. Pour garantir l'intégrité des données, ONTAP effectue une opération de lecture sur le pool de capacités immédiatement après avoir effectué une opération d'écriture. La `Sum` statistique représente le nombre total d'opérations de lecture depuis le niveau du pool de capacités du système de fichiers sur une période spécifiée. Pour calculer le pool de demandes par seconde, divisez la `Sum` statistiq ue par les secondes sur une période spécifiée. Unités : nombre Statistiques valides : `Sum`

Métrique	Description
`CapacityPoolWriteBytes`	Nombre d'octets écrits (E/S réseau) dans le niveau du pool de capacités du système de fichiers. Pour garantir l'intégrité des données, ONTAP effectue une opération de lecture sur le pool de capacités immédiatement après avoir effectué une opération d'écriture. La `Sum` statistique représente le nombre total d'octets écrits dans le niveau du pool de capacité du système de fichiers sur une période spécifiée. Pour calculer le pool de capacité en octets par seconde, divisez la `Sum` statistiq ue par les secondes au cours d'une période spécifiée. Unités : octets Statistiques valides : `Sum`

Métrique	Description
`CapacityPoolWriteOperations`	Nombre d'opérations d'écriture (E/S réseau) sur le système de fichiers depuis le niveau du pool de capacités. Cela se traduit par une demande écrite. Pour garantir l'intégrité des données, ONTAP effectue une opération de lecture sur le pool de capacités immédiatement après avoir effectué une opération d'écriture. La `Sum` statistique représente le nombre total d'opérations d'écriture sur le niveau du pool de capacités du système de fichiers sur une période spécifiée. Pour calculer le pool de demandes par seconde, divisez la `Sum` statistiq ue par les secondes sur une période spécifiée. Unités : nombre Statistiques valides : `Sum`

Métriques du serveur de fichiers

Toutes ces mesures ont une seule dimension,`FileSystemId`.

Métrique	Description
`CPUUtilization`	Pourcentage d'utilisation des ressources du processeur du système de fichiers. La `Average` statistique représente l'utilisation moyenne du processeur du système de fichiers sur une période spécifiée.

Métrique	Description
	La `Minimum` statistique représente le taux d'utilisation du processeur le plus faible du système de fichiers sur une période donnée. La `Maximum` statistique représente le taux d'utilisation du processeur le plus élevé du système de fichiers sur une période donnée. Unités : pourcentage Statistiques valides : `AverageMinimum`, et `Maximum`
`FileServerDiskThroughputUtilization`	Débit du disque entre votre serveur de fichiers et le niveau principal, en pourcentage de la limite allouée déterminée par la capacité de débit. La `Average` statistique représente le pourcentage moyen d'utilisation du débit de disque des serveurs de fichiers sur une période donnée. La `Minimum` statistique représente le pourcentage le plus faible d'utilisation du débit de disque des serveurs de fichiers sur une période donnée. La `Maximum` statistique représente le taux d'utilisation le plus élevé du débit de disque des serveurs de fichiers sur une période donnée. Unités : pourcentage Statistiques valides : `AverageMinimum`, et `Maximum`

Métrique	Description
`FileServerDiskThroughputBalance`	Pourcentage de crédits de rafale disponibles pour le débit du disque entre votre serveur de fichiers et le niveau principal. Cela est valable pour les systèmes de fichiers configurés avec une capacité de débit inférieure ou égale à 512 Mo/s. La `Average` statistique est le solde de rafale moyen disponible sur une période spécifiée. La `Minimum` statistique est le solde de rafale minimum disponible sur une période spécifiée. La `Maximum` statistique représente le solde de rafale maximal disponible sur une période spécifiée. Unités : pourcentage Statistiques valides : `Average`, `Minimum`, et `Maximum`

Métrique	Description
`FileServerDiskIopsBalance`	Pourcentage de crédits en rafale disponibles pour les IOPS de disque entre votre serveur de fichiers et le niveau principal. Cela est valable pour les systèmes de fichiers configurés avec une capacité de débit inférieure ou égale à 512 Mo/s. La `Average` statistique est le solde de rafale moyen disponible sur une période spécifiée. La `Minimum` statistique est le solde de rafale minimum disponible sur une période spécifiée. La `Maximum` statistique représente le solde de rafale maximal disponible sur une période spécifiée. Unités : pourcentage Statistiques valides : `Average`, `Minimum`, et `Maximum`

Métrique	Description
`FileServerDiskIopsUtilization`	Pourcentage d'utilisation des IOPS par rapport à la capacité d'IOPS du disque disponible pour votre serveur de fichiers. La `Average` statistique représente l'utilisa tion moyenne des IOPS sur le disque par le système de fichiers sur une période donnée. La `Minimum` statistique représente l'utilisation minimale d'IOPS sur le disque du système de fichiers sur une période spécifiée. La `Maximum` statistique représente l'utilisation maximale d'IOPS sur le disque par le système de fichiers sur une période spécifiée. Unités : pourcentage Statistiques valides : `AverageMinimum`, et `Maximum`

Métrique	Description
`FileServerCacheHitRatio`	Pourcentage de toutes les demandes de lecture traitées par des données contenues dans la RAM et les caches NVMe du système de fichiers. Un pourcentage plus élevé signifie que davantage de lectures sont effectuées par les caches de lecture du système de fichiers. Unités : pourcentage La `Average` statistique représente le pourcentage moyen d'accès au cache pour le système de fichiers sur une période donnée. La `Minimum` statistique représente le plus faible pourcentage d'accès au cache du système de fichiers sur une période donnée. `Maximum`Cette statistique représente le pourcentage d'accès au cache le plus élevé pour le système de fichiers sur une période donnée. Statistiques valides : `Average`, `Minimum`, et `Maximum`

Métriques d'E/S sur disque

Toutes ces mesures ont une seule dimension,`FileSystemId`.

Métrique	Description
`DiskReadBytes`	Le nombre d'octets (E/S de disque) d'un disque lu vers le niveau principal du système de fichiers.

Métrique	Description
	La `Sum` statistique est le nombre total d'octets lus depuis le système de fichiers sur une période spécifiée. Pour calculer le débit du disque de lecture (octets par seconde) pour n'importe quelle statistique, divisez la `Sum` statistique par les secondes pendant la période spécifiée. Unités : octets Statistiques valides : `Sum`
`DiskWriteBytes`	Le nombre d'octets (E/S de disque) d'un disque écrit sur le niveau principal du système de fichiers. La `Sum` statistique est le nombre total d'octets écrits depuis le système de fichiers sur une période spécifiée. Pour calculer le débit du disque d'écriture (octets par seconde) pour n'importe quelle statistique, divisez `Sum` la statistique par les secondes pendant la période spécifiée. Unités : octets Statistiques valides : `Sum`

Métrique	Description
`DiskIopsUtilization`	Le nombre d'IOPS sur le disque entre votre serveur de fichiers et les volumes de stockage, exprimé en pourcentage de la limite d'IOPS du disque allouée aux niveaux principaux. La `Average` statistique représente l'utilisa tion moyenne des IOPS sur le disque par le système de fichiers sur une période donnée. La `Minimum` statistique représente l'utilisation minimale d'IOPS sur le disque du système de fichiers sur une période spécifiée. La `Maximum` statistique représente l'utilisation maximale d'IOPS sur le disque par le système de fichiers sur une période spécifiée. Unités : pourcentage Statistiques valides : `Average`, `Minimum`, et `Maximum`
`DiskReadOperations`	Nombre d'opérations de lecture (E/S sur disque) depuis le niveau principal du système de fichiers. La `Sum` statistique représente le nombre total d'opérations de lecture depuis le niveau principal sur une période spécifiée. Unités : nombre Statistiques valides : `Sum`

Métrique	Description
`DiskWriteOperations`	Nombre d'opérations d'écriture (E/S de disque) sur le niveau principal du système de fichiers. La `Sum` statistique représente le nombre total d'opérations d'écriture sur le niveau principal au cours d'une période spécifiée. Unités : nombre Statistiques valides : `Sum`

Indicateurs de capacité de stockage

Toutes ces mesures ont une seule dimension,`FileSystemId`.

Métrique	Description
`StorageEfficiencySavings`	Les octets économisés grâce aux fonctionn alités d'efficacité du stockage (compression, déduplication et compactage). La `Average` statistique représente les économies moyennes d'efficacité du stockage sur une période donnée. Pour calculer les économies d'efficacité du stockage en pourcentage de toutes les données stockées, sur une période d'une minute, divisez `StorageEfficiencySavings` par la somme de `StorageEfficiencySavings` et la métrique du système de `StorageUs ed` fichiers, à l'aide de la `Sum` statistique pour`StorageUsed` . La `Minimum` statistique représente les économies minimales en termes d'efficacité du stockage sur une période donnée.

Métrique	Description
	La `Maximum` statistique représente les économies maximales en termes d'efficacité du stockage sur une période donnée. Unités : octets Statistiques valides : `AverageMinimum`, et `Maximum`
`StorageUsed`	La quantité totale de données physiques stockées sur le système de fichiers, à la fois au niveau principal (SSD) et au niveau du pool de capacités. Cet indicateur inclut les économies réalisées grâce aux fonctionnalités d'efficacité du stockage, telles que la compression et la déduplication des données. Unités : octets Statistiques valides : `AverageMinimum`, et `Maximum`

Métrique	Description
`LogicalDataStored`	La quantité totale de données logiques stockées sur le système de fichiers, en tenant compte à la fois du niveau SSD et du niveau du pool de capacités. Cette métrique inclut la taille logique totale des instantanés FlexClones, mais n'inclut pas les économies d'efficacité du stockage réalisées grâce à la compression, au compactage et à la déduplication. Pour calculer les économies d'efficacité du stockage en octets, prenez le nombre `Average` de `StorageUsed` sur une période donnée et soustrayez-le du nombre de sur la `Average` même `LogicalDataStored` période. Pour calculer les économies d'efficacité du stockage en pourcentage de la taille logique totale des données, prenez le chiffre `Average` de `StorageUsed` sur une période donnée et soustrayez-le du chiffre de `LogicalDataStored` sur la `Average` même période. Divisez ensuite la différence par le `Average` de `LogicalDataStored` sur la même période. Unités : octets Statistiques valides : `AverageMinimum`, et `Maximum`

Mesures détaillées du système de fichiers

Les métriques détaillées du système de fichiers sont des mesures détaillées d'utilisation du stockage pour chacun de vos niveaux de stockage. Les métriques détaillées du système de fichiers ont toutes les dimensions `FileSystemIdStorageTier`, et`DataType`.

- La `StorageTier` dimension indique le niveau de stockage mesuré par la métrique, avec des valeurs possibles de `SSD` et`StandardCapacityPool`.
- La `DataType` dimension indique le type de données que la métrique mesure, avec la valeur possible`All`.

Il existe une ligne pour chaque combinaison unique d'une métrique donnée et de paires clé-valeur dimensionnelle, avec une description de ce que mesure cette combinaison.

Métrique	Description
`StorageCapacityUtilization`	L'utilisation de la capacité de stockage pour chacun des agrégats de votre système de fichiers. Une métrique est émise chaque minute pour chacun des agrégats de votre système de fichiers. La `Average` statistique représente le taux moyen d'utilisation de la capacité de stockage pour le niveau de performance de votre système de fichiers au cours de la période spécifiée. `Minimum`Cette statistique représente le niveau le plus faible d'utilisation de la capacité de stockage pour le niveau de performance de votre système de fichiers au cours de la période spécifiée. `Maximum`Cette statistique représente le taux d'utilisation de la capacité de stockage le plus élevé pour le niveau de performance de votre système de fichiers au cours de la période spécifiée. Unités : pourcentage

Métrique	Description
	Statistiques valides : `AverageMinimum`, et `Maximum`
`StorageCapacity`	Capacité de stockage totale du niveau principal (SSD). Unités : octets Statistiques valides : `Maximum`

Métrique	Description
`StorageUsed`	Capacité de stockage physique utilisée en octets, spécifique au niveau de stockage. Cette valeur inclut les économies réalisées grâce aux fonctionnalités d'efficacité du stockage, telles que la compression et la déduplication des données. Les valeurs de dimension valides pour `StorageTier` sont `SSD` et`StandardCapacityPool` , correspondant au niveau de stockage mesuré par cette métrique. Cette métrique nécessite également la `DataType` dimension avec la valeur`All`. Les `Maximum` statistiques`Average`,`Minimum`, et sont la consommation de stockage par niveau en octets pour la période donnée. Pour calculer l'utilisation de la capacité de stockage de votre niveau de stockage principal (SSD), divisez l'une de ces statistiques par le `Maximum` `StorageCapacity` chiffre correspondant à la même période, avec `StorageTier` une dimension égale à`SSD`. Pour calculer la capacité de stockage disponible de votre niveau de stockage principal (SSD) en octets, soustrayez l'une de ces statistiques de la `Maximum` `StorageCapacity` même période, avec une dimension `StorageTier` égale à`SSD`. Unités : octets Statistiques valides : `Average``Minimum`, et `Maximum`

Mesures du système de fichiers évolutives

Les métriques suivantes sont fournies pour FSx pour les systèmes de fichiers ONTAP dotés d'au moins deux paires de haute disponibilité (HA). Pour les métriques, un point de données est émis pour chaque paire HA et pour chaque agrégat (pour les métriques d'utilisation du stockage).

> **Note**
>
> Si votre système de fichiers comporte plusieurs paires HA, vous pouvez également utiliser les métriques de système de fichiers à paire HA unique et les métriques de volume.

Rubriques

Métriques d'E/S réseau

Toutes ces mesures prennent deux dimensions, `FileSystemId` et`FileServer`.

- `FileSystemId`— L'ID de AWS ressource de votre système de fichiers.
- `FileServer`— Le nom d'un serveur de fichiers (ou d'un nœud) dans ONTAP (par exemple,`FsxId01234567890abcdef-01`). Les serveurs de fichiers impairs sont des serveurs de fichiers préférés (c'est-à-dire qu'ils gèrent le trafic sauf si le système de fichiers est passé au serveur de fichiers secondaire), tandis que les serveurs de fichiers pairs sont des serveurs de fichiers secondaires (c'est-à-dire qu'ils ne desservent le trafic que lorsque leur partenaire n'est pas disponible). De ce fait, les serveurs de fichiers secondaires sont généralement moins utilisés que les serveurs de fichiers préférés.

Métrique	Description
`NetworkThroughputUtilization`	Utilisation du débit réseau en pourcentage du débit réseau disponible pour votre système de fichiers. Cette métrique est équivalente à la

Métrique	Description
	capacité maximale `NetworkSentBytes` et `NetworkReceivedBytes` en pourcentage de la capacité de débit réseau d'une paire HA pour votre système de fichiers. L'ensemble du trafic est pris en compte dans cette métrique, y compris les tâches en arrière-plan (telles que SnapMirror la hiérarchisation et les sauvegard es). Une métrique est émise chaque minute pour chacun des serveurs de fichiers de votre système de fichiers. La `Average` statistique représente l'utilisation moyenne du débit réseau pour le serveur de fichiers donné au cours de la période spécifiée. La `Minimum` statistique représente l'utilisation du débit réseau la plus faible pour le serveur de fichiers donné sur une minute, pendant la période spécifiée. La `Maximum` statistique représente le taux d'utilisation du débit réseau le plus élevé pour un serveur de fichiers donné sur une minute, pendant la période spécifiée. Unités : pourcentage Statistiques valides : `Average`, `Minimum`, et `Maximum`

Métrique	Description
`NetworkSentBytes`	Le nombre d'octets (E/S réseau) envoyés par votre système de fichiers. L'ensemble du trafic est pris en compte dans cette métrique, y compris les tâches en arrière-plan (telles que SnapMirror la hiérarchisation et les sauvegard es). Une métrique est émise chaque minute pour chacun des serveurs de fichiers de votre système de fichiers. La `Sum` statistique est le nombre total d'octets envoyés sur le réseau par le serveur de fichiers donné au cours de la période spécifiée. La `Average` statistique est le nombre moyen d'octets envoyés sur le réseau par le serveur de fichiers donné au cours de la période spécifiée. La `Minimum` statistique est le plus petit nombre d'octets envoyés sur le réseau par le serveur de fichiers donné au cours de la période spécifiée. La `Maximum` statistique représente le plus grand nombre d'octets envoyés sur le réseau par le serveur de fichiers donné au cours de la période spécifiée. Pour calculer le débit envoyé (octets par seconde) pour n'importe quelle statistique, divisez la statistique par les secondes pendant la période spécifiée. Unités : octets

Métrique	Description
	Statistiques valides : `Sum`,`Average`,`Minimum`, et `Maximum`

Métrique	Description
`NetworkReceivedBytes`	Nombre d'octets (E/S réseau) reçus par votre système de fichiers. L'ensemble du trafic est pris en compte dans cette métrique, y compris les tâches en arrière-plan (telles que SnapMirro r la hiérarchisation et les sauvegardes). Une métrique est émise chaque minute pour chacun des serveurs de fichiers de votre système de fichiers. La `Sum` statistique est le nombre total d'octets reçus sur le réseau par le serveur de fichiers donné au cours de la période spécifiée. La `Average` statistique est le nombre moyen d'octets reçus sur le réseau par le serveur de fichiers donné chaque minute au cours de la période spécifiée. La `Minimum` statistique est le plus petit nombre d'octets reçus sur le réseau par le serveur de fichiers donné chaque minute au cours de la période spécifiée. La `Maximum` statistique représente le plus grand nombre d'octets reçus sur le réseau par le serveur de fichiers donné chaque minute au cours de la période spécifiée. Pour calculer le débit reçu (octets par seconde) pour n'importe quelle statistique, divisez la statistique par les secondes de la période. Unités : octets Statistiques valides : `Sum`,`Average`,`Minimum`, et `Maximum`

Métriques du serveur de fichiers

Toutes ces mesures prennent deux dimensions, `FileSystemId` et`FileServer`.

Métrique	Description
`CPUUtilization`	Pourcentage d'utilisation des ressources du processeur du système de fichiers. Une métrique est émise chaque minute pour chacun des serveurs de fichiers de votre système de fichiers. La `Average` statistique représente l'utilisation moyenne du processeur du système de fichiers sur une période spécifiée. La `Minimum` statistique représente le taux d'utilisation du processeur le plus faible pour le serveur de fichiers donné au cours de la période spécifiée. La `Maximum` statistique représente le taux d'utilisation du processeur le plus élevé pour le serveur de fichiers donné au cours de la période spécifiée. Unités : pourcentage Statistiques valides : `Average`, `Minimum`, et `Maximum`
`FileServerDiskThroughputUtilization`	Débit du disque entre votre serveur de fichiers et l'agrégat, en pourcentage de la limite allouée déterminée par la capacité de débit. L'ensemble du trafic est pris en compte dans cette métrique, y compris les tâches en arrière-plan (telles que SnapMirror la hiérarchisation et les sauvegardes). Cette métrique est équivalente à la somme `DiskReadBytes` et `DiskWrite`

Métrique	Description
	`Bytes` en pourcentage de la capacité de débit de disque du serveur de fichiers d'une paire HA pour votre système de fichiers. Une métrique est émise chaque minute pour chacun des serveurs de fichiers de votre système de fichiers. La `Average` statistique représente l'utilisation moyenne du débit de disque du serveur de fichiers pour le serveur de fichiers donné au cours de la période spécifiée. La `Minimum` statistique représente l'utilisation la plus faible du débit de disque du serveur de fichiers pour le serveur de fichiers donné au cours de la période spécifiée. La `Maximum` statistique représente le taux d'utilisation du débit de disque le plus élevé du serveur de fichiers pour le serveur de fichiers donné au cours de la période spécifiée. Unités : pourcentage Statistiques valides : `Average`, `Minimum`, et `Maximum`

Métrique	Description
`FileServerDiskIopsUtilization`	Utilisation par IOPS de la capacité d'IOPS du disque disponible pour votre serveur de fichiers, en pourcentage de sa limite d'IOPS sur le disque. Cela se distingue `DiskIopsUtilization` par le fait que l'utilisation des IOPS sur le disque dépasse le maximum que votre serveur de fichiers peut gérer, par opposition aux IOPS sur disque que vous avez provisionnées. L'ensemble du trafic est pris en compte dans cette métrique, y compris les tâches en arrière-plan (telles que SnapMirror la hiérarchisation et les sauvegardes). Une métrique est émise chaque minute pour chacun des serveurs de fichiers de votre système de fichiers. La `Average` statistique représente l'utilisation moyenne des IOPS sur le disque pour le serveur de fichiers donné au cours de la période spécifiée. La `Minimum` statistique représente le taux d'utilisation IOPS le plus faible du disque pour le serveur de fichiers donné au cours de la période spécifiée. La `Maximum` statistique représente le taux d'utilisation IOPS le plus élevé du disque pour le serveur de fichiers donné au cours de la période spécifiée. Unités : pourcentage Statistiques valides : `Average`, `Minimum`, et `Maximum`

Métrique	Description
`FileServerCacheHitRatio`	Le pourcentage de toutes les demandes de lecture traitées par des données résidant dans la RAM ou dans les caches NVMe de votre système de fichiers pour chacune de vos paires HA (par exemple, le serveur de fichiers actif dans une paire HA). Un pourcentage plus élevé indique un ratio plus élevé de lectures mises en cache par rapport au nombre total de lectures. Toutes les E/S sont prises en compte, y compris les tâches en arrière-plan (telles que SnapMirror la hiérarchisation et les sauvegard es). Une métrique est émise chaque minute pour chacun des serveurs de fichiers de votre système de fichiers. Unités : pourcentage La `Average` statistique représente le taux de réussite moyen du cache pour l'une des paires HA de votre système de fichiers au cours de la période spécifiée. `Minimum`Cette statistique représente le taux de réussite du cache le plus faible pour l'une des paires HA de votre système de fichiers au cours de la période spécifiée. `Maximum`Cette statistique représente le taux de réussite du cache le plus élevé pour l'une des paires HA de votre système de fichiers au cours de la période spécifiée. Statistiques valides : `Average``Minimum`, et `Maximum`

Métriques d'E/S sur disque

Toutes ces mesures prennent deux dimensions, `FileSystemId` et`Aggregate`.

- `FileSystemId`— L'ID de AWS ressource de votre système de fichiers.
- `Aggregate`— Le niveau de performance de votre système de fichiers se compose de plusieurs pools de stockage appelés agrégats. Il existe un agrégat pour chaque paire HA. Par exemple, `aggr1` des mappages agrégés vers le serveur de fichiers `FsxId01234567890abcdef-01` (le serveur de fichiers actif) et le serveur de fichiers `FsxId01234567890abcdef-02` (le serveur de fichiers secondaire) dans une paire HA.

Métrique	Description
`DiskReadBytes`	Le nombre d'octets (E/S de disque) de n'importe quel disque est lu à partir de cet agrégat. L'ensemble du trafic est pris en compte dans cette métrique, y compris les tâches en arrière-plan (telles que SnapMirro r la hiérarchisation et les sauvegardes). Une métrique est émise chaque minute pour chacun des agrégats de votre système de fichiers. La `Sum` statistique est le nombre total d'octets lus chaque minute à partir de l'agrégat donné au cours de la période spécifiée. La `Average` statistique est le nombre moyen d'octets lus par minute à partir de l'agrégat donné sur la période spécifiée. La `Minimum` statistique représente le plus petit nombre d'octets lus par minute à partir de l'agrégat donné au cours de la période spécifiée. La `Maximum` statistique représente le plus grand nombre d'octets lus par minute à partir

Métrique	Description
	de l'agrégat donné au cours de la période spécifiée. Pour calculer le débit du disque de lecture (octets par seconde) pour n'importe quelle statistique, divisez la statistique par les secondes de la période. Unités : octets Statistiques valides : `SumAverage`,`Minimum`, et `Maximum`

Métrique	Description
`DiskWriteBytes`	Le nombre d'octets (E/S de disque) d'un disque écrit sur cet agrégat. L'ensemble du trafic est pris en compte dans cette métrique, y compris les tâches en arrière-plan (telles que SnapMirro r la hiérarchisation et les sauvegardes). Une métrique est émise chaque minute pour chacun des agrégats de votre système de fichiers. La `Sum` statistique est le nombre total d'octets écrits dans l'agrégat donné au cours de la période spécifiée. La `Average` statistique est le nombre moyen d'octets écrits sur l'agrégat donné chaque minute au cours de la période spécifiée. La `Minimum` statistique est le plus petit nombre d'octets écrits dans l'agrégat donné chaque minute au cours de la période spécifiée. La `Maximum` statistique représente le plus grand nombre d'octets écrits dans l'agrégat donné chaque minute au cours de la période spécifiée. Pour calculer le débit du disque d'écriture (octets par seconde) pour n'importe quelle statistique, divisez la statistique par les secondes pendant la période spécifiée. Unités : octets Statistiques valides : `Sum`,`Average`,`Minimum`, et `Maximum`

Métrique	Description
`DiskIopsUtilization`	Utilisation des IOPS sur le disque par un agrégat, en pourcentage de la limite d'IOPS du disque de l'agrégat (c'est-à-dire le nombre total d'IOPS du système de fichiers divisé par le nombre de paires HA de votre système de fichiers). Cela diffère du `FileServerDiskIopsUtilization` fait qu'il s'agit de l'utilisation des IOPS de disque allouées par rapport à votre limite d'IOPS allouées, par opposition au nombre maximal d'IOPS sur disque pris en charge par le serveur de fichiers (c'est-à-dire dicté par votre capacité de débit configurée par paire HA). L'ensemble du trafic est pris en compte dans cette métrique, y compris les tâches en arrière-plan (telles que SnapMirror la hiérarchisation et les sauvegardes). Une métrique est émise chaque minute pour chacun des agrégats de votre système de fichiers. La `Average` statistique représente l'utilisation moyenne des IOPS du disque pour l'agrégat donné sur la période spécifiée. La `Minimum` statistique représente le taux d'utilisation IOPS le plus faible du disque pour l'agrégat donné au cours de la période spécifiée. La `Maximum` statistique est le taux d'utilisation IOPS le plus élevé du disque pour un agrégat donné au cours de la période spécifiée. Unités : pourcentage

Métrique	Description
	Statistiques valides : `AverageMinimum`, et `Maximum`

Métrique	Description
`DiskReadOperations`	Nombre d'opérations de lecture (E/S sur disque) sur cet agrégat. L'ensemble du trafic est pris en compte dans cette métrique, y compris les tâches en arrière-plan (telles que SnapMirror la hiérarchisation et les sauvegard es). Une métrique est émise chaque minute pour chacun des agrégats de votre système de fichiers. La `Sum` statistique est le nombre total d'opérati ons de lecture effectuées par l'agrégat donné au cours de la période spécifiée. La `Average` statistique est le nombre moyen d'opérations de lecture effectuées chaque minute par l'agrégat donné au cours de la période spécifiée. La `Minimum` statistique représente le plus petit nombre d'opérations de lecture effectuée s chaque minute par l'agrégat donné sur la période spécifiée. La `Maximum` statistique représente le plus grand nombre d'opérations de lecture effectuée s chaque minute par l'agrégat donné au cours de la période spécifiée. Pour calculer le nombre moyen d'IOPS sur le disque au cours de la période, utilisez la `Average` statistique et divisez le résultat par 60 (secondes). Unités : nombre

Métrique	Description
	Statistiques valides : `Sum`,`Average`,`Minimum`, et `Maximum`
`DiskWriteOperations`	Nombre d'opérations d'écriture (E/S sur disque) sur cet agrégat. L'ensemble du trafic est pris en compte dans cette métrique, y compris les tâches en arrière-plan (telles que SnapMirro r la hiérarchisation et les sauvegardes). Une métrique est émise chaque minute pour chacun des agrégats de votre système de fichiers. La `Sum` statistique est le nombre total d'opérati ons d'écriture effectuées par l'agrégat donné au cours de la période spécifiée. La `Average` statistique est le nombre moyen d'opérations d'écriture effectuées chaque minute par l'agrégat donné au cours de la période spécifiée. Pour calculer le nombre moyen d'IOPS sur le disque au cours de la période, utilisez la `Average` statistique et divisez le résultat par 60 (secondes). Unités : nombre Statistiques valides : `Sum` et `Average`

Mesures détaillées du système de fichiers

Les métriques détaillées du système de fichiers sont des mesures détaillées d'utilisation du stockage pour chacun de vos niveaux de stockage. Les métriques détaillées du système de fichiers ont soit les `FileSystemId` `DataType` dimensions,,, soit les `FileSystemId` `Aggregate` dimensions `StorageTierDataType`,, et. `StorageTier`

- Lorsque la `Aggregate` dimension n'est pas fournie, les métriques concernent l'ensemble de votre système de fichiers. Les `StorageCapacity` métriques `StorageUsed` et ont un point de données unique par minute correspondant au stockage total consommé par le système de fichiers (par niveau de stockage) et à la capacité de stockage totale (pour le niveau SSD). Pendant ce temps, la `StorageCapacityUtilization` métrique émet une métrique par minute pour chaque agrégat.
- Lorsque la `Aggregate` dimension est fournie, les métriques concernent chaque agrégat.

La signification des dimensions est la suivante :

- `FileSystemId`— L'ID de AWS ressource de votre système de fichiers.
- `Aggregate`— Le niveau de performance de votre système de fichiers se compose de plusieurs pools de stockage appelés agrégats. Il existe un agrégat pour chaque paire HA. Par exemple, `aggr1` des mappages agrégés vers le serveur de fichiers `FsxId01234567890abcdef-01` (le serveur de fichiers actif) et le serveur de fichiers `FsxId01234567890abcdef-02` (le serveur de fichiers secondaire) dans une paire HA.
- `StorageTier`— Indique le niveau de stockage mesuré par la métrique, avec des valeurs possibles de `SSD` et`StandardCapacityPool`.
- `DataType`— Indique le type de données mesuré par la métrique, avec la valeur possible`All`.

Il existe une ligne pour chaque combinaison unique d'une métrique donnée et de paires clé-valeur dimensionnelle, avec une description de ce que mesure cette combinaison.

Métrique	Description
`StorageCapacityUtilization`	Utilisation de la capacité de stockage pour un agrégat de système de fichiers donné. Une métrique est émise chaque minute pour chacun des agrégats de votre système de fichiers. La `Average` statistique représente le taux moyen d'utilisation de la capacité de stockage pour un agrégat donné au cours de la période spécifiée. La `Minimum` statistique représente le niveau minimum d'utilisation de la capacité de

Métrique	Description
	stockage pour un agrégat donné au cours de la période spécifiée. La `Maximum` statistique représente le niveau maximal d'utilisation de la capacité de stockage pour un agrégat donné au cours de la période spécifiée. Unités : pourcentage Statistiques valides : `AverageMinimum`, et `Maximum`
`StorageCapacity`	Capacité de stockage pour un agrégat de système de fichiers donné. Une métrique est émise chaque minute pour chacun des agrégats de votre système de fichiers. La `Average` statistique représente la capacité de stockage moyenne pour un agrégat donné sur la période spécifiée. La `Minimum` statistique représente la quantité minimale de capacité de stockage pour un agrégat donné sur la période spécifiée. La `Maximum` statistique représente la capacité de stockage maximale pour un agrégat donné sur la période spécifiée. Unités : octets Statistiques valides : `AverageMinimum`, et `Maximum`

Métrique	Description
`StorageUsed`	Capacité de stockage physique utilisée en octets, spécifique au niveau de stockage. Cette valeur inclut les économies réalisées grâce aux fonctionnalités d'efficacité du stockage, telles que la compression et la déduplication des données. Les valeurs de dimension valides pour `StorageTier` sont `SSD` et`StandardCapacityPool` , correspondant au niveau de stockage mesuré par cette métrique. Une métrique est émise chaque minute pour chacun des agrégats de votre système de fichiers. La `Average` statistique est la quantité moyenne de capacité de stockage physique consommée sur le niveau de stockage donné par l'agrégat donné au cours de la période spécifiée. La `Minimum` statistique représente la quantité minimale de capacité de stockage physique consommée sur le niveau de stockage donné par l'agrégat donné au cours de la période spécifiée. La `Maximum` statistique représente la quantité maximale de capacité de stockage physique consommée sur le niveau de stockage donné par l'agrégat donné au cours de la période spécifiée. Unités : octets Statistiques valides : `Average``Minimum`, et `Maximum`

Métriques de volume

Votre système de fichiers Amazon FSx for NetApp ONTAP peut comporter un ou plusieurs volumes qui stockent vos données. Chacun de ces volumes possède un ensemble de mesures, classées en métriques de volume ou en métriques de volume détaillées.

- Les mesures de volume sont des mesures de performance et de stockage par volume qui prennent deux dimensions, `FileSystemId` et`VolumeId`. `FileSystemId`correspond au système de fichiers auquel appartient le volume.
- Les mesures de volume détaillées sont per-storage-tier des mesures qui mesurent la consommation de stockage par niveau avec la `StorageTier` dimension (avec les valeurs possibles de `SSD` et`StandardCapacityPool`) et par type de données avec la `DataType` dimension (avec les valeurs possibles de `UserSnapshot`, et`Other`). Ces mesures ont les `DataType` dimensions `FileSystemId` `VolumeId``StorageTier`,, et.

Rubriques

Métriques d'E/S réseau

Toutes ces mesures prennent deux dimensions, `FileSystemId` et`VolumeId`.

Métrique	Description
`DataReadBytes`	Nombre d'octets (E/S réseau) lus depuis le volume par les clients. La `Sum` statistique représente le nombre total d'octets associés aux opérations de lecture pendant la période spécifiée. Pour calculer le débit moyen (octets par seconde) pour une période, divisez la `Sum` statistique par le nombre de secondes pendant la période spécifiée.

Métrique	Description
	Unités : octets Statistiques valides : `Sum`
`DataWriteBytes`	Nombre d'octets (E/S réseau) écrits sur le volume par les clients. La `Sum` statistique représente le nombre total d'octets associés aux opérations d'écriture pendant la période spécifiée. Pour calculer le débit moyen (octets par seconde) pour une période, divisez la `Sum` statistique par le nombre de secondes pendant la période spécifiée. Unités : octets Statistiques valides : `Sum`
`DataReadOperations`	Nombre d'opérations de lecture (E/S réseau) effectuées sur le volume par les clients. La `Sum` statistique représente le nombre total d'opérations de lecture au cours de la période spécifiée. Pour calculer le nombre moyen d'opérations de lecture par seconde pendant une période, divisez la `Sum` statistique par le nombre de secondes pendant la période spécifiée. Unités : nombre Statistiques valides : `Sum`

Métrique	Description
`DataWriteOperations`	Nombre d'opérations d'écriture (E/S réseau) effectuées par les clients sur le volume. La `Sum` statistique représente le nombre total d'opérations d'écriture au cours de la période spécifiée. Pour calculer la moyenne des opérations d'écriture par seconde pendant une période, divisez la `Sum` statistique par le nombre de secondes pendant la période spécifiée. Unités : nombre Statistiques valides : `Sum`
`MetadataOperations`	Nombre d'opérations d'E/S (E/S réseau) entre les activités de métadonnées des clients et le volume. La `Sum` statistique représente le nombre total d'opérations de métadonnées au cours de la période spécifiée. Pour calculer le nombre moyen d'opérations de métadonnées par seconde pendant une période, divisez la `Sum` statistique par le nombre de secondes pendant la période spécifiée. Unités : nombre Statistiques valides : `Sum`

Métrique	Description
`DataReadOperationTime`	Somme du temps total passé dans le volume pour les opérations de lecture (E/S réseau) par les clients accédant aux données du volume. La `Sum` statistique représente le nombre total de secondes consacrées aux opérations de lecture pendant la période spécifiée. Pour calculer la latence de lecture moyenne pour une période, divisez la `Sum` statistique par le chiffre `Sum` de la `DataReadOperations` métrique sur la même période. Unités : secondes Statistiques valides : `Sum`
`DataWriteOperationTime`	Somme du temps total passé dans le volume pour effectuer les opérations d'écriture (E/S réseau) des clients accédant aux données du volume. La `Sum` statistique représente le nombre total de secondes consacrées aux opérations d'écriture pendant la période spécifiée. Pour calculer la latence d'écriture moyenne pour une période, divisez la `Sum` statistique par `Sum` la `DataWriteOperations` métrique sur la même période. Unités : secondes Statistiques valides : `Sum`

Métrique	Description
`MetadataOperationTime`	Somme du temps total passé dans le volume pour exécuter les opérations de métadonnées (E/S réseau) des clients accédant aux données du volume. La `Sum` statistique représente le nombre total de secondes consacrées aux opérations de lecture pendant la période spécifiée. Pour calculer la latence moyenne pour une période, divisez la `Sum` statistique par le `Sum` nombre de `MetadataOperations` sur la même période. Unités : secondes Statistiques valides : `Sum`
`CapacityPoolReadBytes`	Nombre d'octets lus (E/S réseau) depuis le niveau du pool de capacité du volume. Pour garantir l'intégrité des données, ONTAP effectue une opération de lecture sur le pool de capacités immédiatement après avoir effectué une opération d'écriture. La `Sum` statistique représente le nombre total d'octets lus depuis le niveau du pool de capacité du volume sur une période spécifiée . Pour calculer le pool de capacité en octets par seconde, divisez la `Sum` statistique par les secondes au cours d'une période spécifiée. Unités : octets Statistiques valides : `Sum`

Métrique	Description
`CapacityPoolReadOperations`	Nombre d'opérations de lecture (E/S réseau) depuis le niveau du pool de capacités du volume. Cela se traduit par une demande de lecture du pool de capacités. Pour garantir l'intégrité des données, ONTAP effectue une opération de lecture sur le pool de capacités immédiatement après avoir effectué une opération d'écriture. La `Sum` statistique représente le nombre total d'opérations de lecture depuis le niveau du pool de capacités du volume sur une période spécifiée. Pour calculer le pool de demandes par seconde, divisez la `Sum` statistique par les secondes sur une période spécifiée. Unités : nombre Statistiques valides : `Sum`

Métrique	Description
`CapacityPoolWriteBytes`	Nombre d'octets écrits (E/S réseau) dans le niveau du pool de capacités du volume. Pour garantir l'intégrité des données, ONTAP effectue une opération de lecture sur le pool de capacités immédiatement après avoir effectué une opération d'écriture. La `Sum` statistique représente le nombre total d'octets écrits dans le niveau du pool de capacité du volume sur une période spécifiée . Pour calculer le pool de capacité en octets par seconde, divisez la `Sum` statistique par les secondes au cours d'une période spécifiée. Unités : octets Statistiques valides : `Sum`

Métrique	Description
`CapacityPoolWriteOperations`	Nombre d'opérations d'écriture (E/S réseau) sur le volume depuis le niveau du pool de capacités. Cela se traduit par une demande écrite. Pour garantir l'intégrité des données, ONTAP effectue une opération de lecture sur le pool de capacités immédiatement après avoir effectué une opération d'écriture. La `Sum` statistique représente le nombre total d'opérations d'écriture sur le niveau du pool de capacité du volume sur une période spécifiée. Pour calculer le pool de demandes par seconde, divisez la `Sum` statistique par les secondes sur une période spécifiée. Unités : nombre Statistiques valides : `Sum`

Indicateurs de capacité de stockage

Toutes ces mesures prennent deux dimensions, `FileSystemId` et`VolumeId`.

Métrique	Description
`StorageCapacity`	Taille du volume en octets. Unités : octets Statistiques valides : `Maximum`
`StorageUsed`	Capacité de stockage logique utilisée par le volume. Unités : octets

Métrique	Description
	Statistiques valides : `AverageMinimum`, et `Maximum`
`StorageCapacityUtilization`	Utilisation de la capacité de stockage du volume. Unités : pourcentage Statistiques valides : `Average`
`FilesUsed`	Les fichiers utilisés (nombre de fichiers ou d'inodes) sur le volume. Unités : nombre Statistiques valides : `AverageMinimum`, et `Maximum`
`FilesCapacity`	Nombre total d'inodes pouvant être créés sur le volume. Unités : nombre Statistiques valides : `Maximum`

Mesures de volume détaillées

Les mesures de volume détaillées prennent plus de dimensions que les mesures de volume, ce qui permet de mesurer vos données de manière plus précise. Toutes les mesures de volume détaillées ont les dimensions `FileSystemIdVolumeId`,`StorageTier`, et`DataType`.

- La `StorageTier` dimension indique le niveau de stockage mesuré par la métrique, avec les valeurs possibles de `AllSSD`, et`StandardCapacityPool`.
- La `DataType` dimension indique le type de données que la métrique mesure, avec les valeurs possibles de `AllUser`,`Snapshot`, et`Other`.

Le tableau suivant définit ce que `StorageUsed` mesure la métrique pour les dimensions répertoriées.

Métrique	Description
`StorageUsed`	Quantité d'espace logique utilisée, en octets. Cette métrique mesure différents types de consommation d'espace en fonction des dimensions utilisées avec cette métrique. Lorsque vous définissez `StorageTier` SSD ou`StandardCapacityPool` , et que vous définissez `DataType` sur`All`, cette métrique mesure l'utilisation de l'espace logique pour ce volume pour les niveaux de votre SSD et de votre pool de capacité, respectiv ement. Lorsque vous définissez la `DataType` dimension sur `User` `SnapshotOther`, ou et sur`All`, cette métrique mesure l'utilisation de l'espace logique pour chaque type de données respectif. `StorageTier` La consommation de `Snapshot` données inclut la réserve d'instant anés, qui représente 5 % de la taille du volume par défaut. Unités : octets Statistiques valides : `Average`, `Minimum`, et `Maximum`
`StorageCapacityUtilization`	Pourcentage d'espace disque physique utilisé par le volume. Unités : pourcentage Statistiques valides : `Maximum`

Avertissements et recommandations en matière de performances

FSx for ONTAP affiche un avertissement pour les CloudWatch métriques chaque fois que l'une de ces métriques approche ou dépasse un seuil prédéterminé pour plusieurs points de données consécutifs. Ces avertissements vous fournissent des recommandations pratiques que vous pouvez utiliser pour optimiser les performances de votre système de fichiers.

Les avertissements sont accessibles dans plusieurs zones du tableau de bord de surveillance et de performance. Tous les avertissements de performance actifs ou récents d'Amazon FSx et toutes les CloudWatch alarmes configurées pour le système de fichiers présentant un état ALARM apparaissent dans le panneau Surveillance et performances de la section Résumé. L'avertissement apparaît également dans la section du tableau de bord où le graphique métrique est affiché.

Vous pouvez créer des CloudWatch alarmes pour toutes les métriques Amazon FSx. Pour plus d'informations, consultez Création d' CloudWatch alarmes Amazon pour surveiller Amazon FSx.

Utiliser des avertissements relatifs aux performances pour améliorer les performances du système de fichiers

Amazon FSx fournit des recommandations pratiques que vous pouvez utiliser pour optimiser les performances de votre système de fichiers. Ces recommandations décrivent la manière dont vous pouvez remédier à un éventuel goulot d'étranglement en matière de performances. Vous pouvez prendre les mesures recommandées si vous pensez que l'activité se poursuivra ou si elle a un impact sur les performances de votre système de fichiers. Selon la métrique qui a déclenché un avertissement, vous pouvez le résoudre en augmentant la capacité de débit ou de stockage du système de fichiers, comme décrit dans le tableau suivant.

Section du tableau de bord	S'il existe un avertissement pour cette métrique	Faites ceci
Stockage	Utilisation de la capacité de stockage principale	Augmentez la capacité de stockage principale de votre système de fichiers si celui-ci n'atteint pas déjà la capacité de stockage SSD maximale. Pour plus d'informations, consultez Modification de la capacité de stockage SSD et des IOPS provisionnées. Si votre système de fichiers comporte plusieurs paires HA et que l'utilisation de votre capacité de stockage

Section du tableau de bord	S'il existe un avertissement pour cette métrique	Faites ceci
		principale n'est supérieure que pour un sous-ensemble des agrégats de votre système de fichiers (les pools de stockage qui constituent votre niveau de stockage principal), vous pouvez également rééquilibrer votre charge de travail afin que l'utilisation de votre capacité de stockage principale soit répartie de manière plus uniforme sur l'ensemble de votre système de fichiers. Pour plus d'informations sur le rééquilibrage de vos charges de travail, consultez. Surveillance de FSx pour équilibrer la charge de travail ONTAP
Performances du serveur de fichiers	Débit réseau Débit du disque IOPS sur disque Utilisation de l'UC	Augmentez la capacité de débit de votre système de fichiers si celui-ci n'atteint pas déjà sa capacité de débit maximale. Pour plus d'informations sur la mise à jour de la capacité de débit, consultezComment modifier la capacité de débit. Si votre système de fichiers comporte plusieurs paires HA et que l'utilisation n'est élevée que pour un sous-ensemble de serveurs de fichiers, vous pouvez également rééquilibrer votre charge de travail afin qu'elle utilise de manière plus uniforme les capacités de performance de chacune des paires HA de votre système de fichiers. Pour plus d'informations sur le rééquilibrage de vos charges de travail, consultez. Surveillance de FSx pour équilibrer la charge de travail ONTAP

Section du tableau de bord	S'il existe un avertissement pour cette métrique	Faites ceci
Performances disque	IOPS sur disque	Augmentez le nombre d'IOPS SSD si votre système de fichiers n'atteint pas déjà le maximum d'IOPS SSD correspondant à la capacité de débit actuelle de votre système de fichiers. Pour plus d'informations sur la mise à jour des IOPS provisionnées de votre système de fichiers, consultez. Modification de la capacité de stockage SSD et des IOPS provisionnées Si votre système de fichiers comporte plusieurs paires HA et que l'utilisation des IOPS de votre disque n'est plus élevée que pour un sous-ensemble des agrégats de votre système de fichiers (les pools de stockage qui constituent votre niveau de stockage principal), vous pouvez également rééquilibrer votre charge de travail afin que vos IOPS de disque soient utilisées de manière plus uniforme dans l'ensemble de votre système de fichiers. Pour plus d'informations sur le rééquilibrage de vos charges de travail, consultez. Surveillance de FSx pour équilibrer la charge de travail ONTAP

Pour plus d'informations sur les performances du système de fichiers, consultezAmazon FSx pour NetApp les performances d'ONTAP.

Création d' CloudWatch alarmes Amazon pour surveiller Amazon FSx

Vous pouvez créer une CloudWatch alarme qui envoie un message Amazon Simple Notification Service (Amazon SNS) lorsque l'état de l'alarme change. Une alarme surveille une seule métrique pendant la période que vous spécifiez. Si nécessaire, l'alarme exécute ensuite une ou plusieurs actions en fonction de la valeur de la métrique par rapport à un seuil donné sur un certain nombre de périodes. L'action est une notification envoyée à une rubrique Amazon SNS ou à une stratégie Auto Scaling.

Les alarmes déclenchent des actions uniquement pour les changements d'état prolongés. CloudWatch les alarmes n'appellent pas d'actions uniquement parce qu'elles sont dans un état particulier ; l'état doit avoir changé et être maintenu pendant un certain nombre de périodes. Vous pouvez créer une alarme à partir de la console Amazon FSx ou de la console Amazon CloudWatch .

Les procédures suivantes décrivent comment créer des alarmes à l'aide de la console Amazon FSx, AWS Command Line Interface (AWS CLI) et de l'API.

Pour définir des alarmes à l'aide de la console Amazon FSx

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation de gauche, choisissez Systèmes de fichiers, puis choisissez le système de fichiers pour lequel vous souhaitez créer l'alarme.
3. Sur la page Résumé, choisissez Surveillance et performances dans le deuxième panneau.
4. Choisissez l'onglet CloudWatch Alarmes.
5. Choisissez Créer une CloudWatch alarme. Vous êtes ensuite redirigé vers la console CloudWatch.
6. Choisissez Select metric (Sélectionner une métrique).
7. Dans la section Metrics, choisissez FSx.
8. Choisissez une catégorie de mesures :
   - Métriques du système de fichiers
   - Métriques détaillées du système de fichiers
   - Métriques de volume
   - Mesures de volume détaillées
9. Choisissez la métrique pour laquelle vous souhaitez définir l'alarme, puis sélectionnez Sélectionner une métrique.
10. Dans la section Conditions, choisissez les conditions que vous souhaitez pour l'alarme, puis cliquez sur Suivant.

> **Note**
>
> Les métriques peuvent ne pas être publiées pendant la maintenance du système de fichiers. Pour éviter toute modification inutile et trompeuse des conditions d'alarme et pour configurer vos alarmes de manière à ce qu'elles résistent aux points de données

manquants, consultez la section Configuration du traitement des données manquantes par les CloudWatch alarmes dans le guide de CloudWatch l'utilisateur Amazon.

11. Si vous souhaitez vous CloudWatch envoyer un e-mail ou une notification Amazon SNS lorsque l'état d'alarme déclenche l'action, choisissez un état d'alarme pour Alarm state trigger.

    Pour Envoyer une notification à la rubrique SNS suivante, choisissez une option. Si vous choisissez Créer une rubrique, vous pouvez définir le nom d'une nouvelle liste d'abonnement par e-mail et les adresses e-mail pour cette liste. La liste est enregistrée et s'affiche dans le champ des alarmes futures. Choisissez Suivant.

    > **Note**
    >
    > Si vous utilisez Créer la rubrique pour créer une nouvelle rubrique Amazon SNS, les adresses e-mail doivent être vérifiées avant de pouvoir recevoir des notifications.
    > Les e-mails sont envoyés uniquement lorsque l'alarme passe à un état défini. Si ce changement d'état de l'alarme se produit avant la vérification des adresses e-mail, ces dernières ne reçoivent pas de notification.

12. Renseignez les champs Nom de l'alarme et Description de l'alarme, puis choisissez Suivant.
13. Sur la page Aperçu et création, passez en revue l'alarme que vous êtes sur le point de créer, puis choisissez Créer une alarme.

Pour définir des alarmes à l'aide de la CloudWatch console

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Choisissez Créer une alarme pour démarrer l'assistant de création d'alarme.
3. Suivez la procédure décrite dans Pour configurer les alarmes à l'aide de la console Amazon FSx, en commençant par l'étape 6.

Pour régler une alarme à l'aide du AWS CLI

- Appelez la commande CLI put-metric-alarm. Pour plus d'informations, consultez la référence de la commande AWS CLI.

Pour configurer une alarme à l'aide de l' CloudWatch API

- Appelez l'opération PutMetricAlarm API. Pour plus d'informations, consultez le Amazon CloudWatch API Reference.

Surveillance de FSx pour équilibrer la charge de travail ONTAP

Si votre système de fichiers comporte plusieurs paires HA, ses performances et son débit sont répartis sur chacune de vos paires HA. FSx for ONTAP équilibre automatiquement vos fichiers au fur et à mesure qu'ils sont écrits dans votre système de fichiers, mais dans de rares cas, il est possible que les données de votre charge de travail ou vos E/S soient déséquilibrées entre les paires HA, ce qui peut avoir un impact sur les performances globales de votre charge de travail. Vous pouvez surveiller votre charge de travail pour vous assurer qu'elle reste équilibrée entre chacune des paires HA de votre système de fichiers (ainsi que les serveurs de fichiers et les agrégats correspondants, c'est-à-dire les pools de stockage qui constituent votre niveau de stockage principal).

Rubriques

- Équilibre d'utilisation du stockage principal
- Déséquilibre d'utilisation des performances du serveur de fichiers et du disque
- Mappage des CloudWatch dimensions aux ressources de la CLI ONTAP et de l'API REST
- Rééquilibrage des clients à fort trafic
- Rééquilibrage des volumes très utilisés

Équilibre d'utilisation du stockage principal

La capacité de stockage principale de votre système de fichiers est répartie de manière égale entre chacune de vos paires HA dans des pools de stockage appelés agrégats. Chaque paire HA possède un agrégat. Nous vous recommandons de maintenir un taux d'utilisation moyen ne dépassant pas 80 % pour votre niveau de stockage principal sur une base continue. Pour les systèmes de fichiers comportant plusieurs paires HA, nous vous recommandons de maintenir une utilisation moyenne maximale de 80 % pour chaque agrégat.

Le maintien d'un taux d'utilisation de 80 % garantit qu'il y a de l'espace libre pour les nouvelles données entrantes et permet de réduire les frais généraux liés aux opérations de maintenance, qui peuvent temporairement demander de l'espace libre sur vos agrégats.

Si vous remarquez un déséquilibre entre vos agrégats, vous pouvez soit augmenter la capacité de stockage principale de votre système de fichiers (en augmentant proportionnellement la capacité de stockage de chaque agrégat), soit déplacer vos volumes entre les agrégats à l'aide de la commande volume move de la CLI ONTAP.

Déséquilibre d'utilisation des performances du serveur de fichiers et du disque

Les capacités de performance totales de votre système de fichiers (telles que le débit réseau, le débit entre le serveur de fichiers et les IOPS, et les IOPS sur le disque) sont réparties de manière égale entre les paires HA de votre système de fichiers. Nous vous recommandons de maintenir un taux d'utilisation moyen inférieur à 50 % (et un pic d'utilisation maximal inférieur à 80 %) pour toutes les limites de performances sur une base continue. Cela vaut à la fois pour l'utilisation globale des ressources du serveur de fichiers de votre système de fichiers sur toutes les paires HA, ainsi que pour chaque serveur de fichiers.

Si vous remarquez que l'utilisation des performances de votre serveur de fichiers est déséquilibrée (et que les serveurs de fichiers sur lesquels votre charge de travail est déséquilibrée ont une utilisation continue de plus de 80 %), vous pouvez utiliser la CLI ONTAP et l'API REST pour mieux diagnostiquer la cause du déséquilibre des performances et y remédier. Vous trouverez ci-dessous un tableau des indicateurs de déséquilibre possibles et des prochaines étapes pour un diagnostic plus approfondi.

Si votre système de fichiers est...	Alors...
Le débit du disque du serveur de fichiers ou les IOPS du disque du serveur de fichiers sont déséquilibrés	Vous êtes peut-être confronté à un hotspot d'E/S sur un sous-ensemble de paires HA (un sous-ensemble de vos volumes contenant une quantité énorme de données consultées), ce qui peut limiter les performances globales de votre charge de travail car elle est bloquée par rapport à un sous-ensemble de paires HA. Pour chaque serveur de fichiers très utilisé, vérifiez les volumes les plus utilisés afin de déterminer quels volumes sont les plus actifs au sein d'un agrégat. Pour plus d'informa tions sur cette procédure, consultez Rééquilibrage des volumes très utilisés.
Le débit du réseau est déséquilibré, mais	Vos données sont réparties uniformément entre les paires HA, mais pas vos clients. Pour les serveurs de fichiers dont l'utilisation du débit réseau

Si votre système de fichiers est...	Alors...
le débit du disque de votre serveur de fichiers, le nombre d'IOPS du disque du serveur de fichiers ou le nombre d'IOPS du disque ne sont pas déséquilibrés	est supérieure à celle des autres, vérifiez les principaux clients pour chaque serveur de fichiers, puis rééquilibrez ces clients en démontant les volumes de ces clients et en les remontant à l'aide d'un point de terminaison différent sur une paire HA différente. Pour plus d'informations sur cette procédure, consultez Rééquilibrage des clients à fort trafic.

Mappage des CloudWatch dimensions aux ressources de la CLI ONTAP et de l'API REST

Votre système de fichiers scale-out contient des CloudWatch métriques Amazon avec la dimension `FileServer` or`Aggregate`. Afin de mieux diagnostiquer les cas de déséquilibre, vous devez mapper ces valeurs de dimension à des serveurs de fichiers (ou nœuds) et à des agrégats spécifiques dans la CLI ONTAP ou l'API REST.

- Pour les serveurs de fichiers, chaque nom de serveur de fichiers est mappé à un nom de serveur de fichiers (ou de nœud) dans ONTAP (par exemple,`FsxId01234567890abcdef-01`). Les serveurs de fichiers impairs sont des serveurs de fichiers préférés (c'est-à-dire qu'ils gèrent le trafic sauf si le système de fichiers est passé au serveur de fichiers secondaire), tandis que les serveurs de fichiers pairs sont des serveurs de fichiers secondaires (c'est-à-dire qu'ils ne desservent le trafic que lorsque leur partenaire n'est pas disponible). De ce fait, les serveurs de fichiers secondaires sont généralement moins utilisés que les serveurs de fichiers préférés.
- Pour les agrégats, chaque nom d'agrégat correspond à un agrégat dans ONTAP (par exemple,`aggr1`). Il existe un agrégat pour chaque paire HA, ce qui signifie que l'agrégat `aggr1` est partagé par les serveurs de fichiers `FsxId01234567890abcdef-01` (le serveur de fichiers actif) et `FsxId01234567890abcdef-02` (le serveur de fichiers secondaire) dans une paire HA, l'agrégat `aggr2` est partagé par `FsxId01234567890abcdef-03` les serveurs de fichiers`FsxId01234567890abcdef-04`, etc.

Vous pouvez consulter les mappages entre tous les agrégats et les serveurs de fichiers à l'aide de la CLI ONTAP.

1. Pour accéder en SSH à la NetApp CLI ONTAP de votre système de fichiers, suivez les étapes décrites dans la Utilisation de la CLI NetApp ONTAP section du guide de l'utilisateur d'Amazon FSx for NetApp ONTAP.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Utilisez la commande storage aggregate show en spécifiant le `-fields node` paramètre.

   ```
   ::> storage aggregate show -fields node
   aggregate                     node
   ----------------------------- ------------------------
   aggr1                         FsxId01234567890abcdef-01
   aggr2                         FsxId01234567890abcdef-03
   aggr3                         FsxId01234567890abcdef-05
   aggr4                         FsxId01234567890abcdef-07
   aggr5                         FsxId01234567890abcdef-09
   aggr6                         FsxId01234567890abcdef-11
   6 entries were displayed.
   ```

Rééquilibrage des clients à fort trafic

Si vous rencontrez un déséquilibre des E/S sur les serveurs de fichiers (en particulier en ce qui concerne l'utilisation du débit réseau), cela peut être dû à un nombre élevé de clients d'E/S. Pour identifier les clients à fort trafic, utilisez la CLI ONTAP.

1. Pour accéder en SSH à la NetApp CLI ONTAP de votre système de fichiers, suivez les étapes décrites dans la Utilisation de la CLI NetApp ONTAP section du guide de l'utilisateur d'Amazon FSx for NetApp ONTAP.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Pour afficher les clients les plus fréquentés, utilisez la commande statistics top client show ONTAP CLI. Vous pouvez éventuellement spécifier le `-node` paramètre pour afficher uniquement les principaux clients d'un serveur de fichiers spécifique. Si vous diagnostiquez le déséquilibre d'un serveur de fichiers spécifique, utilisez le `-node` paramètre en le `node_name` remplaçant par le nom du serveur de fichiers (par exemple,`FsxId01234567890abcdef-01`).

   Vous pouvez éventuellement ajouter le `-interval` paramètre, en fournissant l'intervalle sur lequel mesurer (en secondes) avant la sortie de chaque rapport. L'augmentation de l'intervalle

(par exemple, jusqu'à 300 secondes au maximum) fournit un échantillon à plus long terme du volume de trafic acheminé vers chaque volume. La valeur par défaut est 5 (secondes).

```
::> statistics top client show -node FsxId01234567890abcdef-01 [-interval [5,300]]
```

Dans le résultat, les principaux clients sont indiqués par leur adresse IP et leur port.

```
                                                    *Total     Total
            Client   Vserver          Node              Ops     (Bps)
------------------ --------- ------------------------ ------ ---------
 172.17.236.53:938 svm01     FsxId01234567890abcdef-01   2143 140443648
172.17.236.160:898 svm02     FsxId01234567890abcdef-01    812  53215232
```

3. Vous pouvez rééquilibrer un sous-ensemble des clients à fort trafic répertoriés vers d'autres serveurs de fichiers. Pour ce faire, démontez le volume du client et remontez-le en utilisant le nom DNS du point de terminaison NFS/SMB de la SVM. Cela renvoie un point de terminaison aléatoire correspondant à une paire HA aléatoire.

   Nous vous recommandons de réutiliser le nom DNS, mais vous avez la possibilité de choisir explicitement la paire HA montée par un client donné. Pour garantir que vous montez un client sur un point de terminaison différent, vous pouvez spécifier une adresse IP de point de terminaison différente de celle correspondant au nœud soumis à un trafic élevé. Vous pouvez le faire en exécutant la commande suivante :

```
::> network interface show -vserver svm_name -lif nfs_smb_management* -fields
 address,curr-node
vserver   lif                  address      curr-node
--------- -------------------- ------------ ------------------------
svm01 nfs_smb_management_1 172.31.15.89 FsxId01234567890abcdef-01
svm01 nfs_smb_management_3 172.31.8.112 FsxId01234567890abcdef-03
2 entries were displayed.
```

   Selon l'exemple de sortie de la `statistics top client show` commande, le client `172.17.236.53` génère un trafic élevé vers`FsxId01234567890abcdef-01`. La sortie de la `network interface show` commande indique qu'il s'agit de l'adresse`172.31.15.89`. Pour effectuer le montage sur un autre point de terminaison, sélectionnez une autre adresse (dans cet exemple, la seule autre adresse est`172.31.8.112`, correspondant à`FsxId01234567890abcdef-03`).

Rééquilibrage des volumes très utilisés

Si vous rencontrez un déséquilibre d'E/S entre vos volumes ou agrégats, vous pouvez rééquilibrer les volumes afin de redistribuer votre trafic d'E/S entre vos volumes.

> **Note**
>
> Si vous constatez un déséquilibre d'utilisation du stockage entre vos agrégats, il n'y a généralement aucun impact sur les performances, sauf si le taux d'utilisation élevé est associé à un déséquilibre des E/S. Bien que vous puissiez déplacer des volumes entre des agrégats pour équilibrer l'utilisation du stockage, nous vous recommandons de ne déplacer des volumes que si vous constatez un impact sur les performances, car le déplacement de volumes peut avoir un impact négatif sur les performances si vous ne tenez pas également compte des E/S acheminées vers chaque volume que vous envisagez de déplacer.

1. Pour accéder en SSH à la NetApp CLI ONTAP de votre système de fichiers, suivez les étapes décrites dans la Utilisation de la CLI NetApp ONTAP section du guide de l'utilisateur d'Amazon FSx for NetApp ONTAP.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Utilisez la commande statistics volume show ONTAP CLI pour afficher les volumes de trafic les plus élevés pour un agrégat donné, avec les modifications suivantes :

   - Remplacez *`aggregate_name`* par le nom de l'agrégat (par exemple,). `aggr1`
   - Vous pouvez éventuellement ajouter le `-interval` paramètre, en fournissant l'intervalle sur lequel mesurer (en secondes) avant la sortie de chaque rapport. L'augmentation de l'intervalle (par exemple, jusqu'à 300 secondes au maximum) fournit un échantillon à plus long terme du volume de trafic acheminé vers chaque volume. La valeur par défaut est 5 (secondes).

   ```
   ::> statistics volume show -aggregate aggregate_name -sort-key total_ops [-interval
    [5,300]]
   ```

   Selon l'intervalle que vous avez choisi, l'affichage des données peut prendre jusqu'à 5 minutes. La commande affiche tous les volumes de l'agrégat, ainsi que le volume de trafic acheminé vers chaque agrégat.

```
                          *Total Read Write Other      Read Write Latency
    Volume Vserver Aggregate    Ops  Ops   Ops   Ops     (Bps) (Bps)    (us)
---------- ------- --------- ------ ---- ----- ----- --------- ----- -------
vol1__0007    svm1     aggr1   4078 4078     0     0 267255808     0    1092
vol1__0005    svm1     aggr1   4078 4078     0     0 267255808     0    1086
vol1__0003    svm1     aggr1   4077 4077     0     0 267223040     0    1086
vol1__0001    svm1     aggr1   4077 4077     0     0 267239424     0    1087
vol1__0008    svm1     aggr2   2314 2314     0     0 151650304     0    1112
vol1__0006    svm1     aggr2   2144 2144     0     0 140509184     0    1104
vol1__0002    svm1     aggr2   2183 2183     0     0 143065088     0    1106
vol1__0004    svm1     aggr2   2183 2183     0     0 143065088     0    1103
```

Les statistiques de volume sont affichées par constituant (par exemple, `vol1__0015` il s'agit du 15e constituant pour FlexGroup`vol1`). Vous pouvez voir dans l'exemple de sortie que les composants de `aggr1` sont plus utilisés que les composants de. `aggr2` Pour équilibrer le trafic entre les agrégats, vous pouvez déplacer les volumes constitutifs entre les agrégats afin de répartir le trafic de manière plus uniforme.

3. Pour déplacer un volume entre des agrégats, utilisez la commande volume move start ONTAP CLI, en remplaçant les valeurs suivantes :

   - Remplacez *`svm_name`* par le nom de la SVM hébergeant le volume que vous déplacez.
   - Remplacez *`volume_name`* par le nom du composant du volume (par exemple,`vol1__0001`).
   - Remplacez *`aggregate_name`* par le nom de l'agrégat de destination pour le volume.

   > **Important**
   >
   > Le déplacement de volumes consomme les ressources du réseau et du disque pour les serveurs de fichiers source et de destination. Par conséquent, les performances de votre charge de travail peuvent être affectées par tout déplacement de volume en cours. En outre, il existe une phase de coupure du processus de déplacement du volume qui interrompt temporairement les E/S pour tout trafic vers le volume.

```
::> volume move start -vserver svm_name -volume volume_name -
destination aggregate_name -foreground false
[Job 1] Job is queued: Move "vol1__0001" in Vserver "svm01" to aggregate "aggr1".
```

```
Use the "volume move show -vserver svm01 -volume vol1__0001" command to view the
 status of this operation.
```

Pour vérifier l'état de l'opération de déplacement du volume, utilisez la commande `volume move show` ONTAP CLI.

```
::> volume move show -vserver svm_name -volume volume_name
                          Vserver Name: svm01
                           Volume Name: vol1__0001
                  Actual Completion Time: -
                         Bytes Remaining: 1.00TB
             Specified Action For Cutover: retry_on_failure
           Specified Cutover Time Window: 30
                  Destination Aggregate: aggr2
                       Destination Node: FsxId01234567890abcdef-03
                        Detailed Status: Transferring data: 12.23GB sent.
                    Percentage Complete: 1%
                             Move Phase: replicating
                Prior Issues Encountered: -
            Estimated Remaining Duration: 00:40:25
                  Replication Throughput: 434.3MB/s
                       Duration of Move: 00:00:27
                       Source Aggregate: aggr2
                            Source Node: FsxId01234567890abcdef-01
                             Move State: healthy
```

Cette commande indique le temps estimé pour terminer le déplacement, dans l'un des champs d'information. Lorsque l'opération est terminée, la même commande indique que le `Move Phase` champ est rempli.

Vous devez vous assurer que chacun FlexGroup est uniformément réparti entre vos agrégats, idéalement avec les 8 constituants recommandés par agrégat. Si vous déplacez un volume constitutif vers un autre agrégat pour un autre volume équilibréFlexGroup, vous devez à son tour déplacer un autre volume constitutif (moins utilisé) vers l'agrégat source afin de maintenir l'équilibre.

Surveillance des événements FSx pour ONTAP EMS

Vous pouvez surveiller les événements du système de fichiers FSx for ONTAP à l'aide du système de gestion des événements (EMS) natif de NetApp ONTAP. Vous pouvez consulter ces événements à l'aide de la CLI NetApp ONTAP.

Rubriques

Vue d'ensemble des événements EMS

Les événements EMS sont des notifications générées automatiquement qui vous alertent lorsqu'une condition prédéfinie se produit dans votre système de fichiers FSx for ONTAP. Ces notifications vous tiennent informés afin que vous puissiez prévenir ou corriger les problèmes susceptibles d'entraîner des problèmes plus importants, tels que les problèmes d'authentification des machines virtuelles de stockage (SVM) ou les volumes complets.

Par défaut, les événements sont enregistrés dans le journal du système de gestion des événements. À l'aide d'EMS, vous pouvez surveiller des événements tels que les changements de mot de passe utilisateur, un composant FlexGroup dont la capacité est presque maximale, un numéro d'unité logique (LUN) mis en ligne ou hors ligne manuellement ou le redimensionnement automatique d'un volume.

Pour plus d'informations sur les événements ONTAP EMS, consultez le document de référence ONTAP EMS dans le centre de documentation NetApp ONTAP. Pour afficher les catégories d'événements, utilisez le volet de navigation de gauche du document.

> **Note**
>
> Seuls certains messages ONTAP EMS sont disponibles pour FSx pour les systèmes de fichiers ONTAP. Pour afficher la liste des messages ONTAP EMS disponibles, utilisez la NetApp commande ONTAP CLI event catalog show.

Les descriptions des événements EMS contiennent les noms des événements, leur gravité, leurs causes possibles, les messages de journal et les actions correctives qui peuvent vous aider à décider comment réagir. Par exemple, un événement wafl.vol.autosize.Fail se produit lorsque le dimensionnement automatique d'un volume échoue. Selon la description de l'événement, l'action corrective consiste à augmenter la taille maximale du volume lors du réglage du dimensionnement automatique.

Affichage des événements EMS

Utilisez la commande NetApp ONTAP CLI event log show pour afficher le contenu du journal des événements. Cette commande est disponible si vous détenez le `fsxadmin` rôle dans votre système de fichiers. La syntaxe de la commande est la suivante :

```
event log show [event_options]
```

Les événements les plus récents sont listés en premier. Par défaut, cette commande affiche `EMERGENCYALERT`, et les événements de `ERROR` niveau de gravité avec les informations suivantes :

- Heure : heure de l'événement.
- Nœud : nœud sur lequel l'événement s'est produit.
- Gravité : niveau de gravité de l'événement. Pour afficher `NOTICE` des événements ou `INFORMATIONAL` des événements de `DEBUG` niveau de gravité, utilisez l'`-severity`option.
- Événement : nom et message de l'événement.

Pour afficher des informations détaillées sur les événements, utilisez une ou plusieurs des options d'événements répertoriées dans le tableau suivant.

Option d'événement	Description
`-detail`	Affiche des informations supplémentaires sur les événements.
`-detailtime`	Affiche des informations détaillées sur les événement s dans l'ordre chronologique inverse.
`-instance`	Affiche des informations détaillées sur tous les champs.
`-node` *`nodename`*`|local`	Affiche la liste des événement s pour le nœud que vous spécifiez. Utilisez cette option

Option d'événement	Description
	`-seqnum` pour afficher des informations détaillées.
`-seqnum` *`sequence_number`*	Sélectionne les événements correspondant à ce numéro dans la séquence. Utilisez avec `-node` pour afficher des informations détaillées.

Option d'événement	Description

`-time` *`MM/DD/YYYY HH:MM:SS`*	Sélectionne les événements survenus à ce moment précis. Utilisez le format : MM/DD/YYYY HH:MM:SS [+- HH:MM]. Vous pouvez spécifier une plage de temps en utilisant l'`..`opérateur entre deux instructions temporelles.
	`event log show -time "04/17/2023 05:55:00".."04/17/2023 06:10:00"`
	Les valeurs temporelles comparatives sont relatives à l'heure actuelle à laquelle vous exécutez la commande. L'exemple suivant montre comment afficher uniquement les événements survenus au cours de la dernière minute :
	`event log show -time >1m`
	Les champs de mois et de date de cette option ne sont pas remplis à zéro. Ces champs peuvent être composés d'un seul chiffre ; par exemple,`4/1/2023 06:45:00`.

Option d'événement	Description
`-severity sev_level`	Sélectionne les événement s correspondant à la valeur *sev_level* , qui doit être l'une des suivantes : • EMERGENCY — Perturbat ion • ALERT— Point de défaillan ce unique • ERROR— Dégradation • NOTICE— Informations • INFORMATIONAL — Informations • DEBUG— Informations de débogage Pour afficher tous les événements, spécifiez leur gravité comme suit : `event log show -severity <=DEBUG`

Option d'événement	Description
`-ems-severity` *ems_sev_level*	Sélectionne les événement s correspondant à la valeur *ems_sev_level* , qui doit être l'une des suivantes : • `NODE_FAULT` — Une corruption des données est détectée ou le nœud n'est pas en mesure de fournir un service client. • `SVC_FAULT` — Une perte de service temporaire, généralement une défaillan ce logicielle transitoire, est détectée. • `NODE_ERROR` — Une erreur matérielle qui n'est pas immédiatement fatale est détectée. • `SVC_ERROR` — Une erreur logicielle qui n'est pas immédiatement fatale est détectée. • `WARNING`— Un message hautement prioritaire qui n'indique aucun défaut. • `NOTICE`— Un message de priorité normale qui n'indique aucun défaut. • `INFO`— Un message de faible priorité qui n'indique aucun défaut.

Option d'événement	Description
	• DEBUG— Un message de débogage. • VAR— Un message de gravité variable, sélectionné lors de l'exécution. Pour afficher tous les événements, spécifiez leur gravité comme suit : `event log show -ems-severity <=DEBUG`
`-source` *text*	Sélectionne les événements correspondant à la valeur *du texte*. La source est généralement un module logiciel.
`-message-name` *message_name*	Sélectionne les événements correspondant à la valeur *message_name* . Les noms des messages étant descriptifs, le filtrage de la sortie par nom de message permet d'afficher les messages d'un type spécifique.
`-event` *text*	Sélectionne les événements correspondant à la valeur *du texte*. Le `event` champ contient le texte intégral de l'événement, y compris les paramètres éventuels.

Option d'événement	Description
`-kernel-generation-num` *integer*	Sélectionne les événement s correspondant à la valeur *entière*. Seuls les événements qui proviennent du noyau ont des numéros de génération du noyau.
`-kernel-sequence-num` *integer*	Sélectionne les événement s correspondant à la valeur *entière*. Seuls les événements qui proviennent du noyau ont des numéros de séquence du noyau.
`-action` *text*	Sélectionne les événement s correspondant à la valeur *du texte*. Le `action` champ décrit les mesures correctiv es que vous devez prendre, le cas échéant, pour remédier à la situation.
`-description` *text*	Sélectionne les événement s correspondant à la valeur *du texte*. Le `descripti on` champ décrit pourquoi l'événement s'est produit et ce que cela signifie.
`-filter-name` *filter_name*	Sélectionne les événement s correspondant à la valeur *filter_name* . Seuls les événements inclus par les filtres existants qui correspon dent à cette valeur s'affichent.

Option d'événement	Description
`-fields` *`fieldname ,...`*	Indique que la sortie de commande inclut également le ou les champs spécifiés. Vous pouvez l'`-fields ?`utiliser pour sélectionner les champs que vous souhaitez spécifier.

Pour consulter les événements EMS

1. Pour accéder en SSH à la NetApp CLI ONTAP de votre système de fichiers, suivez les étapes décrites dans la Utilisation de la CLI NetApp ONTAP section du guide de l'utilisateur d'Amazon FSx for NetApp ONTAP.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Utilisez la `event log show` commande pour afficher le contenu du journal des événements.

   ```
   ::> event log show
   Time                Node          Severity      Event
   ------------------- ------------- ------------- ------------------------
   6/30/2023 13:54:19  node1         NOTICE        vifmgr.portup: A link up event was
    received on node node1, port e0a.
   6/30/2023 13:54:19  node1         NOTICE        vifmgr.portup: A link up event was
    received on node node1, port e0d.
   ```

Pour plus d'informations sur les événements EMS renvoyés par la `event log show` commande, reportez-vous à la référence ONTAP EMS dans le centre de documentation NetApp ONTAP.

Transfert d'événements EMS vers un serveur Syslog

Vous pouvez configurer les événements EMS pour transférer les notifications à un serveur Syslog. Le transfert d'événements EMS est utilisé pour surveiller en temps réel votre système de fichiers afin de déterminer et d'isoler les causes profondes d'un large éventail de problèmes. Si votre environnement ne contient pas encore de serveur Syslog pour les notifications d'événements, vous devez d'abord en créer un. Le DNS doit être configuré sur le système de fichiers pour résoudre le nom du serveur Syslog.

Pour configurer les événements EMS afin de transférer les notifications à un serveur Syslog

1. Pour accéder en SSH à la NetApp CLI ONTAP de votre système de fichiers, suivez les étapes décrites dans la Utilisation de la CLI NetApp ONTAP section du guide de l'utilisateur d'Amazon FSx for NetApp ONTAP.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Utilisez la commande event notification destination create pour créer une destination de notification d'événement de typesyslog, en spécifiant les attributs suivants :

   - *dest_name*— Le nom de la destination de notification à créer (par exemple,syslog-ems). Le nom de destination d'une notification d'événement doit comporter de 2 à 64 caractères. Les caractères valides sont les caractères ASCII suivants : A-Z, a-z, 0-9, « _ » et « - ». Le nom doit commencer et se terminer par : A-Z, a-z ou 0-9.
   - *syslog_name*— Le nom d'hôte ou l'adresse IP du serveur Syslog auxquels les messages Syslog sont envoyés.
   - *transport_protocol*— Le protocole utilisé pour envoyer les événements :
     - udp-unencrypted— Protocole de datagramme utilisateur sans aucune sécurité. Il s'agit du protocole par défaut.
     - tcp-unencrypted— Protocole de contrôle de transmission sans sécurité.
     - tcp-encrypted— Protocole de contrôle de transmission avec sécurité de la couche de transport (TLS). Lorsque cette option est spécifiée, FSx for ONTAP vérifie l'identité de l'hôte de destination en validant son certificat.
   - *port_number*— Le port du serveur Syslog auquel les messages Syslog sont envoyés. Le syslog-port paramètre de valeur par défaut dépend du réglage du syslog-transport paramètre. S'il syslog-transport est défini surtcp-encrypted, la valeur syslog-port par défaut est6514. Si syslog-transport est défini surtcp-unencrypted, syslog-port possède la valeur par défaut601. Dans le cas contraire, le port par défaut est défini sur514.

   ```
   ::> event notification destination create -name dest_name -syslog syslog_name -
   syslog-transport transport_protocol -syslog-port port_number
   ```

3. Utilisez la commande event notification create pour créer une nouvelle notification d'un ensemble d'événements défini par un filtre d'événements vers la destination de notification créée à l'étape précédente, en spécifiant les attributs suivants :

- *node_name*— Nom du filtre d'événements. Les événements inclus dans le filtre d'événements sont transférés vers les destinations spécifiées dans le `-destinations` paramètre.
- *dest_name*— Nom de la destination de notification existante à laquelle les notifications d'événements sont envoyées.

```
::> event notification create -filter-name filter_name -destinations dest_name
```

4. Utilisez la `event notification destination check` commande pour générer un message de test et vérifier que votre configuration fonctionne. Spécifiez les attributs suivants à l'aide de la commande :

- *node_name*— Le nom du nœud (par exemple,`FsxId07353f551e6b557b4-01`).
- *dest_name*— Nom de la destination de notification existante à laquelle les notifications d'événements sont envoyées.

```
::> set diag
::*> event notification destination check -node node_name -destination-
name dest_name
```

Surveillance avec Cloud Insights

NetApp Cloud Insights est un NetApp service que vous pouvez utiliser pour surveiller vos systèmes de fichiers Amazon FSx for NetApp ONTAP parallèlement à vos autres NetApp solutions de stockage. Avec Cloud Insights, vous pouvez surveiller les indicateurs de configuration, de capacité et de performance au fil du temps afin de comprendre les tendances de votre charge de travail et de planifier les performances futures et les besoins en capacité de stockage. Vous pouvez également créer des alertes basées sur des conditions métriques qui peuvent s'intégrer à vos flux de travail et outils de productivité existants.

> **Note**
>
> Cloud Insights n'est pas pris en charge pour les systèmes de fichiers évolutifs.

Cloud Insights fournit :

- Un large éventail de mesures et de journaux : collectez des indicateurs de configuration, de capacité et de performance. Découvrez l'évolution de votre charge de travail grâce à des tableaux de bord, des alertes et des rapports prédéfinis.
- Analyse des utilisateurs et protection contre les ransomwares : avec les instantanés Cloud Secure et ONTAP, vous pouvez auditer, détecter, arrêter et réparer les incidents liés aux erreurs des utilisateurs et aux ransomwares.
- SnapMirror création de rapports — Comprenez vos SnapMirror relations et définissez des alertes en cas de problèmes de réplication.
- Planification des capacités : comprenez les besoins en ressources des charges de travail sur site afin de vous aider à migrer votre charge de travail vers une configuration FSx for ONTAP plus efficace. Vous pouvez également utiliser ces informations pour planifier le moment où des performances ou des capacités supplémentaires seront nécessaires pour votre déploiement de FSx for ONTAP.

Pour plus d'informations sur Cloud Insights, consultez NetApp Cloud Insights sur NetApp Cloud Central.

Surveillance des systèmes de fichiers FSx pour ONTAP à l'aide de Harvest et Grafana

NetApp Harvest est un outil open source permettant de recueillir des mesures de performance et de capacité à partir des systèmes ONTAP. Il est compatible avec FSx for ONTAP. Vous pouvez utiliser Harvest avec Grafana pour une solution de surveillance open source.

Commencer à utiliser Harvest et Grafana

La section suivante explique comment configurer Harvest et Grafana pour mesurer les performances et l'utilisation de la capacité de stockage de votre système de fichiers FSx for ONTAP.

Vous pouvez surveiller votre système de fichiers Amazon FSx for NetApp ONTAP à l'aide de Harvest et Grafana. NetApp Harvest surveille les centres de données ONTAP en collectant des indicateurs de performance, de capacité et de matériel à partir de FSx pour les systèmes de fichiers ONTAP. Grafana fournit un tableau de bord où les métriques de récolte collectées peuvent être affichées.

Tableaux de bord Harvest pris en charge

Amazon FSx for NetApp ONTAP présente un ensemble de mesures différent de celui d'ONTAP sur site. NetApp Par conséquent, seuls les tableaux de bord out-of-the-box Harvest suivants marqués avec le tag `fsx` sont actuellement pris en charge pour une utilisation avec FSx for ONTAP. Certains panneaux de ces tableaux de bord peuvent ne pas contenir des informations qui ne sont pas prises en charge.

- ONTAP : Conformité
- ONTAP : Instantanés de protection des données
- ONTAP : Sécurité
- POINT DE CONTACT : SVM
- ONTAP : Volume

AWS CloudFormation modèle

Pour commencer, vous pouvez déployer un AWS CloudFormation modèle qui lance automatiquement une instance Amazon EC2 exécutant Harvest et Grafana. En entrée du AWS CloudFormation modèle, vous spécifiez l'`fsxadmin`utilisateur et le point de terminaison de gestion Amazon FSx pour le système de fichiers qui sera ajouté dans le cadre de ce déploiement. Une fois le déploiement terminé, vous pouvez vous connecter au tableau de bord Grafana pour surveiller votre système de fichiers.

Cette solution permet AWS CloudFormation d'automatiser le déploiement de la solution Harvest et Grafana. Le modèle crée une instance Linux Amazon EC2 et installe les logiciels Harvest et Grafana. Pour utiliser cette solution, téléchargez le modèle AWS CloudFormation fsx-ontap-harvest-grafana.template.

> **Note**
>
> La mise en œuvre de cette solution entraîne la facturation des AWS services associés. Pour plus d'informations, consultez les pages de détail des tarifs de ces services.

Types d'instances Amazon EC2

Lors de la configuration du modèle, vous indiquez le type d'instance Amazon EC2. NetAppLa recommandation concernant la taille de l'instance dépend du nombre de systèmes de fichiers que vous surveillez et du nombre de métriques que vous choisissez de collecter. Avec la configuration par défaut, pour chaque 10 systèmes de fichiers que vous surveillez, NetApp recommande :

- Processeur : 2 cœurs
- Mémoire : 1 Go
- Disque : 500 Mo (principalement utilisé par les fichiers journaux)

Voici quelques exemples de configurations et le type d'`t3`instance que vous pouvez choisir.

Systèmes de fichiers	CPU	Disk	Type d'instance
Moins de 10 ans	2 noyaux	500 Mo	`t3.micro`
10 à 40	4 cœurs	1000 MO	`t3.xlarge`
40 ans et plus	8 noyaux	2000 MO	`t3.2xlarge`

Pour plus d'informations sur les types d'instances Amazon EC2, consultez la section Instances à usage général dans le guide de l'utilisateur Amazon EC2.

Règles relatives aux ports d'instance

Lorsque vous configurez votre instance Amazon EC2, assurez-vous que les ports 3000 et 9090 sont ouverts au trafic entrant pour le groupe de sécurité auquel appartient l'instance Amazon EC2 Harvest et Grafana. Étant donné que l'instance lancée se connecte à un point de terminaison via HTTPS, elle doit résoudre le point de terminaison, qui a besoin du port 53 TCP/UDP pour le DNS. De plus, pour atteindre le point de terminaison, il a besoin du port 443 TCP pour HTTPS et Internet Access.

Procédure de déploiement

La procédure suivante configure et déploie la solution Harvest/Grafana. Le déploiement prend environ cinq minutes. Avant de commencer, vous devez disposer d'un système de fichiers FSx for ONTAP exécuté dans un Amazon Virtual Private Cloud (Amazon VPC) sur votre AWS compte, ainsi

que des informations sur les paramètres du modèle répertoriées ci-dessous. Pour plus d'informations sur la création d'un système de fichiers, consultezCréation de FSx pour les systèmes de fichiers ONTAP.

Pour lancer la suite de solutions Harvest/Grafana

1. Téléchargez le modèle AWS CloudFormation fsx-ontap-harvest-grafana.template. Pour plus d'informations sur la création d'une AWS CloudFormation pile, consultez la section Création d'une pile sur la AWS CloudFormation console dans le Guide de AWS CloudFormation l'utilisateur.

   > **Note**
   >
   > Par défaut, ce modèle est lancé dans la AWS région USA Est (Virginie du Nord). Vous devez lancer cette solution Région AWS là où Amazon FSx est disponible. Pour plus d'informations, consultez la section Points de terminaison et quotas Amazon FSx dans le.Références générales AWS

2. Pour les paramètres, passez en revue les paramètres du modèle et modifiez-les en fonction des besoins de votre système de fichiers. Cette solution utilise les valeurs par défaut suivantes.

Paramètre	Par défaut	Description
InstanceType	`t3.micro`	Type d'instance Amazon EC2. Voici les types d'`t3`instances. • `t3.micro` • `t3.small` • `t3.medium` • `t3.large` • `t3.xlarge` • `t3.2xlarge` Pour obtenir la liste complète des valeurs de type d'instanc

Paramètre	Par défaut	Description
		e Amazon EC2 autorisées pour ce paramètre, consultez le fsx-ontap-harvest-grafana fichier .template.
KeyPair	Aucune valeur par défaut	La paire de clés utilisée pour accéder à l'instance Amazon EC2.
SecurityGroup	Aucune valeur par défaut	L'ID du groupe de sécurité pour l'instance Harvest/G rafana. Assurez-vous que les ports entrants 3000 et 9090, en plus des ports 53 et 443, sont ouverts depuis les clients que vous souhaitez utiliser pour accéder à votre tableau de bord Grafana.
Type de sous-réseau	Aucune valeur par défaut	Spécifiez le type de sous-réseau, `public` soit`private`. Utilisez un `public` sous-réseau pour les ressources qui doivent être connectées à Internet et un sous-réseau privé pour les ressources qui ne seront pas connectées à Internet. Pour plus d'informations, consultez la section Types de sous-réseaux dans le guide de l'utilisateur Amazon VPC.

Paramètre	Par défaut	Description
Sous-réseau	Aucune valeur par défaut	Spécifiez le même sous-réseau que le sous-réseau préféré de votre système de fichiers Amazon FSx NetApp for ONTAP. Vous pouvez trouver l'ID de sous-réseau préféré du système de fichiers dans la console Amazon FSx, dans l'onglet Réseau et sécurité de la page de détails du système de fichiers FSx for ONTAP
LatestLinuxAmiId	`/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2`	La dernière version de l'AMI Amazon Linux 2 est une donnée Région AWS.
SxEndPoint F	Aucune valeur par défaut	Adresse IP du point de terminaison de gestion du système de fichiers. Vous trouverez l'adresse IP du point de terminaison de gestion du système de fichiers dans la console Amazon FSx, dans l'onglet Administration de la page de détails du système de fichiers FSx for ONTAP.

Paramètre	Par défaut	Description
SecretName	Aucune valeur par défaut	AWS Secrets Manager nom secret contenant le mot de passe de l'`fsxadmin`utilisateur du système de fichiers. Il s'agit du mot de passe que vous avez fourni lors de la création du système de fichiers.

3. Choisissez Suivant.
4. Pour Options, choisissez Next.
5. Pour la révision, vérifiez et confirmez les paramètres. Vous devez cocher la case reconnaissant que le modèle crée des ressources IAM.
6. Choisissez Créer pour déployer la pile.

Vous pouvez consulter l'état de la pile dans la AWS CloudFormation console dans la colonne État. Vous devriez voir le statut CREATE_COMPLETE dans environ cinq minutes.

Connexion à Grafana

Une fois le déploiement terminé, utilisez votre navigateur pour vous connecter au tableau de bord Grafana à l'adresse IP et au port 3000 de l'instance Amazon EC2 :

```
http://EC2_instance_IP:3000
```

Lorsque vous y êtes invité, utilisez le nom d'utilisateur par défaut (`admin`) et le mot de passe (`pass`) de Grafana. Nous vous recommandons de modifier votre mot de passe dès que vous vous connectez.

Pour plus d'informations, consultez la page NetApp Récolte sur GitHub.

Résolution des problèmes liés à Harvest et Grafana

Si vous rencontrez des données manquantes mentionnées dans les tableaux de bord Harvest et Grafana ou si vous rencontrez des difficultés pour configurer Harvest et Grafana avec FSx pour ONTAP, consultez les rubriques suivantes pour trouver une solution potentielle.

Rubriques

Les tableaux de bord des SVM et des volumes sont vides

Si la AWS CloudFormation pile a été déployée avec succès et peut contacter Grafana mais que les tableaux de bord de la SVM et des volumes sont vides, suivez la procédure ci-dessous pour dépanner votre environnement. Vous aurez besoin d'un accès SSH à l'instance Amazon EC2 sur laquelle Harvest and Grafana est déployé.

1. Connectez-vous par SSH à l'instance Amazon EC2 sur laquelle vos clients Harvest et Grafana s'exécutent.

   ```
   [~]$ ssh ec2-user@ec2_ip_address
   ```

2. Utilisez la commande suivante pour ouvrir le `harvest.yml` fichier et :

   - Vérifiez qu'une entrée a été créée pour votre instance FSx for ONTAP en tant que. `Cluster-2`
   - Vérifiez que les entrées du nom d'utilisateur et du mot de passe correspondent à vos `fsxadmin` informations d'identification.

   ```
   [ec2-user@ip-ec2_ip_address ~]$ sudo cat /home/ec2-user/harvest_install/harvest/
   harvest.yml
   ```

3. Si le champ du mot de passe est vide, ouvrez le fichier dans un éditeur et mettez-le à jour avec le `fsxadmin` mot de passe, comme suit :

   ```
   [ec2-user@ip-ec2_ip_address ~]$ sudo vi /home/ec2-user/harvest_install/harvest/
   harvest.yml
   ```

4. Assurez-vous que les informations `fsxadmin` d'identification de l'utilisateur sont stockées dans Secrets Manager au format suivant pour tout futur déploiement, en les *`fsxadmin_password`* remplaçant par votre mot de passe.

   ```
   {"username" : "fsxadmin", "password" : "fsxadmin_password"}
   ```

CloudFormation pile annulée après expiration du délai

Si vous ne parvenez pas à déployer la CloudFormation pile avec succès et qu'elle est annulée avec des erreurs, suivez la procédure ci-dessous pour résoudre le problème. Vous aurez besoin d'un accès SSH à l'instance EC2 déployée par la CloudFormation pile.

1. Redéployez la CloudFormation pile en vous assurant que la restauration automatique est désactivée.
2. Connectez-vous par SSH à l'instance Amazon EC2 sur laquelle vos clients Harvest et Grafana s'exécutent.

```
[~]$ ssh ec2-user@ec2_ip_address
```

3. Vérifiez que les conteneurs docker ont bien été démarrés à l'aide de la commande suivante.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo docker ps
```

Dans la réponse, vous devriez voir cinq conteneurs comme suit :

```
CONTAINER ID   IMAGE                    COMMAND                  CREATED
 STATUS                          PORTS                     NAMES
6b9b3f2085ef   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago
 Restarting (1) 20 seconds ago                             harvest_cluster-2
3cf3e3623fde   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago   Up
 About a minute                                            harvest_cluster-1
708f3b7ef6f8   grafana/grafana         "/run.sh"                8 minutes ago   Up
 8 minutes                   0.0.0.0:3000->3000/tcp   harvest_grafana
0febee61cab7   prom/alertmanager       "/bin/alertmanager -…"   8
 minutes ago   Up 8 minutes                    0.0.0.0:9093->9093/tcp
 harvest_prometheus_alertmanager
1706d8cd5a0c   prom/prometheus         "/bin/prometheus --c…"   8 minutes ago   Up
 8 minutes                   0.0.0.0:9090->9090/tcp   harvest_prometheus
```

4. Si les conteneurs docker ne sont pas en cours d'exécution, vérifiez les défaillances dans le `/var/log/cloud-init-output.log` fichier comme suit.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo cat /var/log/cloud-init-output.log
     PLAY [Manage Harvest]
 ***************************************************

TASK [Gathering Facts] *********************************************************
```

```
ok: [localhost]

TASK [Verify images] ************************************************************
failed: [localhost] (item=prom/prometheus) => {"ansible_loop_var": "item",
 "changed": false, "item": "prom/prometheus",
"msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}
failed: [localhost] (item=prom/alertmanager) => {"ansible_loop_var": "item",
 "changed": false, "item": "prom/alertmanage
r", "msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104,
'Connection reset by peer'))"}
failed: [localhost] (item=rahulguptajss/harvest) => {"ansible_loop_var": "item",
 "changed": false, "item": "rahulguptajs
s/harvest", "msg": "Error connecting: Error while fetching server API version:
 ('Connection aborted.', ConnectionResetEr
ror(104, 'Connection reset by peer'))"}
failed: [localhost] (item=grafana/grafana) => {"ansible_loop_var": "item",
 "changed": false, "item": "grafana/grafana",
"msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}

PLAY RECAP **********************************************************************
localhost                  : ok=1    changed=0    unreachable=0    failed=1
 skipped=0    rescued=0    ignored=0
```

5. En cas d'échec, exécutez les commandes suivantes pour déployer les conteneurs Harvest et Grafana.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo su
     [ec2-user@ip-ec2_ip_address ~]$ cd /home/ec2-user/harvest_install
     [ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
 manage_harvest.yml
     [ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
 manage_harvest.yml --tags api
```

6. Validez les conteneurs démarrés avec succès en exécutant sudo docker ps et en vous connectant à votre URL Harvest et Grafana.

Enregistrement de FSx pour les appels d'API ONTAP avecAWS CloudTrail

Amazon FSx est intégré àAWS CloudTrail, un service qui enregistre les actions effectuées par un utilisateur, un rôle ou unAWSservice dans Amazon FSx. CloudTrail capture tous les appels Amazon FSx API pour Amazon FSx pour NetApp ONTAP en tant qu'événements. Les appels capturés incluent les appels de la console Amazon FSx et les appels de code vers les opérations d'API Amazon FSx.

Si vous créez un journal de suivi, vous pouvez diffuser en continu les fichiers de suivi CloudTrail événements dans un compartiment Amazon S3, y compris les événements pour Amazon FSx. Si vous ne configurez pas de journal de suivi, vous pouvez toujours afficher les événements les plus récents dans le journal de suivi CloudTrail console dansHistorique des événements historiques. Grâce aux informations collectées par CloudTrail, vous pouvez déterminer quelle demande a été faite à Amazon FSx. Vous pouvez aussi déterminer l'adresse IP à partir de laquelle la demande a été faite, qui a effectué la demande, quand elle a eu lieu et autres informations supplémentaires.

Pour en savoir plus sur CloudTrail, consultez le Guide de l'utilisateur AWS CloudTrail.

Informations relatives à Amazon FSx dans CloudTrail

CloudTrail est activé dans votre compte AWS lors de la création de ce dernier. Lorsqu'une activité d'API se produit dans Amazon FSx, elle est enregistrée dans un CloudTrail événement avec d'autresAWSévénements de service dansHistorique des événements historiques. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre AWS compte. Pour de plus amples informations, veuillez consulterAffichage d'événements avec CloudTrail Historique des événements historiques.

Pour un registre continu des événements dans votreAWScompte, y compris les événements pour Amazon FSx, créez un journal d'activité. UNsentierpermet CloudTrail pour livrer des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions AWS. Le journal d'activité consigne les événements de toutes les Régions dans la partition AWSAWS et transfère les fichiers journaux dans le compartiment Amazon S3 de votre choix. De plus, vous pouvez configurer d'autres fichiersAWSservices pour analyser plus en profondeur les données d'événement collectées dans CloudTrail bûches. Pour plus d'informations, consultez les rubriques suivantes dans le AWS CloudTrailGuide de l'utilisateur :

- Création d'un journal d'activité pour votre Compte AWS

- AWSIntégrations de services avec CloudTrail Journaux
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception CloudTrail fichiers journaux de plusieurs régionsetRéception de fichiers journaux CloudTrail de plusieurs comptes

Tous les Amazon FSxAPI calls (Appels d'API)sont enregistrés par CloudTrail. Par exemple, les appels aux`CreateFileSystem`et`TagResource`les opérations génèrent des entrées dans le CloudTrail fichiers journaux

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre service AWS.

Pour plus d'informations, consultez le .CloudTrail userIdentity element.dans leAWS CloudTrailGuide de l'utilisateur .

Présentation des entrées des fichiers journaux Amazon FSx

UNsentierest une configuration qui permet la remise d'événements sous forme de fichiers journaux vers un compartiment Amazon S3 que vous spécifiez. CloudTrail Les fichiers journaux contiennent une ou plusieurs entrées de journal. Unévénementreprésente une demande individuelle émise à partir d'une source quelconque et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail Les fichiers journaux ne constituent pas une série ordonnée retraçant les appels d'API publics. Ils ne suivent aucun ordre précis.

L'exemple suivant montre un CloudTrail entrée de journal qui illustre l'action`TagResource`opération quand une balise pour un système de fichiers est créée depuis la console.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
```

```
        "principalId": “111122223333”,
        "arn": "arn:aws:sts::111122223333:root”,
        "accountId": “111122223333”,
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE”,
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T22:36:07Z"
            }
        }
    },
    "eventTime": "2018-11-14T22:36:07Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": “192.0.2.0”,
    "userAgent": “console.amazonaws.com”,
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789”
    },
    "responseElements": null,
    "requestID": “aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51”,
    "eventID": “bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p”,
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": “111122223333”
}
```

L'exemple suivant montre un CloudTrail entrée de journal qui illustre l'action`UntagResource`action quand une balise pour un système de fichiers est supprimée depuis la console.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": "111122223333",
        "arn": "arn:aws:sts::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
```

```
                "creationDate": "2018-11-14T23:40:54Z"
            }
        }
    },
    "eventTime": "2018-11-14T23:40:54Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "UntagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
    },
    "responseElements": null,
    "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
    "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": "111122223333"
}
```

Quotas

Vous trouverez ci-dessous des informations sur les quotas lorsque vous travaillez avec Amazon FSx pour NetApp ONTAP.

Rubriques

Les quotas que vous pouvez augmenter

Vous trouverez ci-dessous les quotas d'Amazon FSx for NetApp ONTAP que vous pouvez augmenter pour chacun Compte AWS Région AWS d'entre eux.

Ressource	Par défaut	Description
Systèmes de fichiers ONTAP	100	Le nombre maximum de systèmes de fichiers Amazon FSx for NetApp ONTAP que vous pouvez créer dans ce compte.
ONTAPCapacité de stockage SSD	524 288	Capacité maximale de stockage SSD (en GiB) pour tous les systèmes de fichiers Amazon FSx for NetApp ONTAP que vous pouvez avoir sur ce compte.
ONTAPcapacité de débit	10 240	Capacité de débit maximale (en Mo/s) pour tous les systèmes de fichiers Amazon FSx NetApp for ONTAP que vous pouvez avoir sur ce compte.

Ressource	Par défaut	Description
ONTAPE/S PAR SECONDE SUR SSD	1 000 000	Le nombre maximal d'IOPS SSD pour tous les systèmes de fichiers Amazon FSx NetApp for ONTAP que vous pouvez avoir sur ce compte.
ONTAPsauvegardes par système de fichiers	10 000	Nombre maximal de sauvegardes de volumes initiées par l'utilisateur pour tous les systèmes de fichiers Amazon FSx NetApp for ONTAP que vous pouvez avoir dans ce compte.

Pour demander une augmentation de quota

1. Ouvrez la page AWS Support, connectez-vous (si nécessaire), puis choisissez Create case (Créer une demande de support).
2. Pour Créer un dossier, choisissez Compte et assistance à la facturation.
3. Dans le panneau Détails du dossier, saisissez les informations suivantes :
   - Pour Type, choisissez Compte.
   - Pour la catégorie, choisissez Autres problèmes liés au compte.
   - Dans le champ Objet, entrez**`Amazon FSx for NetApp ONTAP service limit increase request`**.
   - Fournissez une description détaillée de votre demande, y compris :
     - Le quota FSx que vous souhaitez augmenter et la valeur à laquelle vous souhaitez qu'il soit augmenté, s'ils sont connus.
     - La raison pour laquelle vous demandez l'augmentation du quota.
     - L'ID du système de fichiers et la région de chaque système de fichiers pour lequel vous demandez une augmentation.
4. Fournissez votre Contact options (Options de contact) préférées et choisissez Submit (Envoyer).

Quotas de ressources pour chaque système de fichiers

Le tableau suivant répertorie les quotas sur Amazon FSx pour les ressources NetApp ONTAP pour chaque système de fichiers d'un. Région AWS

Ressource	Limite par système de fichiers
Capacité de stockage SSD minimale	1 024 GiB par paire de haute disponibilité (HA)
Capacité de stockage SSD maximale	• Scale-out : 512 TiB par paire HA, jusqu'à 1 PiB • Mise à l'échelle : 192 TiB
Nombre maximal d'IOPS sur SSD	Scale-out : • 200 000 par paire HA (jusqu'à 12 paires) Mise à l'échelle : • 160 000 dans les régions USA Est (Ohio), USA Est (Virginie du Nord), USA Ouest (Oregon) et Europe (Irlande) • 80 000 dans tous les autres pays Régions AWS où FSx for ONTAP est disponible
Capacité de débit minimale	• Scale-out : 3 072 Mbits/s par paire HA • Mise à l'échelle : 128 Mbits/s
Capacité de débit maximale	Scale-out : • 73 728 Mo/s 1 Mise à l'échelle :

Ressource	Limite par système de fichiers
	• 4 096 Mb/s [2] dans les régions USA Est (Ohio), USA Est (Virginie du Nord), USA Ouest (Oregon) et Europe (Irlande) • 2 048 Mbits/s dans tous les autres pays Régions AWS où FSx for ONTAP est disponible
Nombre maximum de volumes	• Scale-out : 1 000 • Mise à l'échelle : 500
Nombre maximum d'instantanés	1 023 par volume 3
Nombre maximum de sauvegardes	4 091 par volume 4
Nombre maximum de SVM	Scale-out : • 5 Mise à l'échelle : • 6 (capacité de débit de 128 Mbits/s) • 6 (capacité de débit de 256 Mbits/s) • 14 (capacité de débit de 512 Mbits/s) • 14 (capacité de débit de 1 024 Mbits/s) • 24 (capacité de débit de 2 048 Mbits/s) • 24 (capacité de débit de 4 096 Mbits/s)
Nombre maximum de tags	50

Ressource	Limite par système de fichiers
Durée de conservation maximale pour les sauvegardes automatisées	90 jours
Durée de conservation maximale pour les sauvegardes initiées par l'utilisateur	Aucune limite de rétention
Nombre maximum de routes prises en charge par système de fichiers	50 [5]

Note

[1] Sur un système de fichiers évolutif comportant 12 paires HA (6 144 Mbits/s par paire HA). Pour plus d'informations, consultez Paires à haute disponibilité (HA).

[2] Pour fournir une capacité de débit de 4 Gbit/s, votre système de fichiers d'extension FSx for ONTAP nécessite une configuration du maximum d'IOPS sur SSD (160 000) et un minimum de 5 120 Go de capacité de stockage SSD dans un support compatible. Région AWS Pour plus d'informations sur ceux qui Régions AWS prennent en charge une capacité de débit de 4 096 Mbits/s, consultez. Impact de la capacité de débit sur les performances

[3] Vous pouvez stocker jusqu'à 1 023 instantanés par volume à tout moment. Une fois cette limite atteinte, vous devez supprimer un instantané existant avant de pouvoir créer un nouvel instantané de votre volume.

[4] Vous pouvez stocker jusqu'à 4 091 sauvegardes par volume à tout moment. Une fois cette limite atteinte, vous devez supprimer une sauvegarde existante avant de pouvoir créer une nouvelle sauvegarde de votre volume.

[5] Vous pouvez configurer jusqu'à 50 itinéraires par système de fichiers à tout moment. Une fois cette limite atteinte, vous devez supprimer un itinéraire existant avant de pouvoir en configurer un nouveau. Le nombre de routes de votre système de fichiers est déterminé par le nombre de SVM qu'il possède et par le nombre de tables de routage qui lui sont associées. Vous pouvez déterminer le nombre de routes existantes vers un système de fichiers à l'aide de l'équation suivante : (1 + nombre de SVM dans le système de fichiers) * (tables de routage associées au système de fichiers).

Résolution des problèmes liés à Amazon FSx pour ONTAP NetApp

Utilisez les sections suivantes pour résoudre les problèmes que vous rencontrez avec FSx for ONTAP.

Rubriques

Mon système de fichiers Multi-AZ est dans un état `MISCONFIGURED`

L'`MISCONFIGURED`état d'un système de fichiers peut avoir plusieurs causes, chacune ayant sa propre résolution, comme suit.

Rubriques

Le compte propriétaire du VPC a désactivé le partage VPC multi-AZ

Les systèmes de fichiers multi-AZ créés par un participant Compte AWS dans un sous-réseau VPC partagé passeront à `MISCONFIGURED` un état pour l'une des raisons suivantes :

- Le compte propriétaire qui partageait le sous-réseau VPC a désactivé la prise en charge du partage VPC multi-AZ pour les systèmes de fichiers FSx for ONTAP.

- Le compte propriétaire a annulé le partage du sous-réseau VPC.

Si le compte propriétaire a annulé le partage du sous-réseau VPC, le message suivant s'affichera dans la console pour ce système de fichiers :

```
The vpc ID vpc-012345abcde does not exist
```

Vous devez contacter le compte propriétaire qui a partagé le sous-réseau VPC avec vous pour résoudre le problème. Pour plus d'informations, voir Création de systèmes de fichiers FSx pour ONTAP dans des sous-réseaux partagés pour plus d'informations.

Impossible de créer une nouvelle SVM sur un système de fichiers multi-AZ

Pour les systèmes de fichiers multi-AZ créés par un participant Compte AWS à un VPC partagé, vous ne pourrez pas créer de nouvelle SVM pour l'une des raisons suivantes :

- Le compte propriétaire qui partageait le sous-réseau VPC a désactivé la prise en charge du partage VPC multi-AZ pour les systèmes de fichiers FSx for ONTAP.
- Le compte propriétaire a annulé le partage du sous-réseau VPC.

Vous devez contacter le compte propriétaire qui a partagé le sous-réseau VPC avec vous pour résoudre le problème. Pour plus d'informations, voir Création de systèmes de fichiers FSx pour ONTAP dans des sous-réseaux partagés pour plus d'informations.

Vous ne pouvez pas accéder à votre système de fichiers

L'impossibilité d'accéder à votre système de fichiers peut avoir plusieurs causes, chacune ayant sa propre résolution, comme suit.

Rubriques

- Amazon FSx ne peut pas mettre à jour la table de routage pour les systèmes de fichiers multi-AZ créés à l'aide de AWS CloudFormation
- Impossible d'accéder à un système de fichiers via iSCSI à partir d'un client d'un autre VPC
- Le compte propriétaire a annulé le partage du sous-réseau VPC
- Impossible d'accéder à un système de fichiers via NFS, SMB, la CLI ONTAP ou l'API REST ONTAP depuis un client dans un autre VPC ou sur site

L'interface Elastic Network du système de fichiers a été modifiée ou supprimée

Vous ne devez ni modifier ni supprimer aucune des interfaces réseau élastiques du système de fichiers. La modification ou la suppression d'une interface réseau peut entraîner une perte permanente de connexion entre votre cloud privé virtuel (VPC) et votre système de fichiers. Créez un nouveau système de fichiers et ne modifiez ni ne supprimez l'interface réseau Amazon FSx. Pour plus d’informations, consultez Contrôle d'accès au système de fichiers avec Amazon VPC.

L'adresse IP Elastic attachée à l'interface Elastic Network du système de fichiers a été supprimée

Amazon FSx ne prend pas en charge l'accès aux systèmes de fichiers depuis l'Internet public. Amazon FSx détache automatiquement toute adresse IP élastique qui est une adresse IP publique accessible depuis Internet et attachée à l'interface réseau élastique d'un système de fichiers. Pour plus d’informations, consultez Clients pris en charge.

Le groupe de sécurité VPC du système de fichiers ne dispose pas des règles entrantes requises

Passez en revue les règles entrantes spécifiées dans Groupes de sécurité Amazon VPC et assurez-vous que le groupe de sécurité associé à votre système de fichiers possède les règles entrantes correspondantes.

Le groupe de sécurité VPC de l'instance de calcul ne dispose pas des règles de sortie requises

Passez en revue les règles sortantes spécifiées dans Groupes de sécurité Amazon VPC et assurez-vous que le groupe de sécurité associé à votre instance de calcul possède les règles sortantes correspondantes.

Le sous-réseau de l'instance de calcul n'utilise aucune des tables de routage associées à votre système de fichiers

FSx for ONTAP crée des points de terminaison permettant d'accéder à votre système de fichiers dans une table de routage VPC. Nous vous recommandons de configurer votre système de fichiers pour utiliser toutes les tables de routage VPC associées aux sous-réseaux dans lesquels se trouvent vos clients. Par défaut, Amazon FSx utilise la table de routage principale de votre VPC. Vous pouvez éventuellement spécifier une ou plusieurs tables de routage à utiliser par Amazon FSx lors de la création de votre système de fichiers.

Si vous pouvez envoyer un ping au point de terminaison intercluster de votre système de fichiers, mais pas au point de terminaison de gestion de votre système de fichiers (voir Ressources du système de fichiers pour plus d'informations), votre client ne se trouve probablement pas dans un sous-réseau associé à l'une des tables de routage de votre système de fichiers. Pour accéder à votre système de fichiers, associez l'une des tables de routage de votre système de fichiers au sous-réseau de votre client. Pour plus d'informations sur la mise à jour des tables de routage Amazon VPC de votre système de fichiers, consultez. Mettre à jour un système de fichiers

Amazon FSx ne peut pas mettre à jour la table de routage pour les systèmes de fichiers multi-AZ créés à l'aide de AWS CloudFormation

Amazon FSx gère les tables de routage VPC pour les systèmes de fichiers multi-AZ à l'aide d'une authentification basée sur des balises. Ces tables de routage sont étiquetées avec`Key: AmazonFSx; Value: ManagedByAmazonFSx`. Lors de la création ou de la mise à jour de FSx pour les systèmes de fichiers ONTAP Multi-AZ, AWS CloudFormation nous vous recommandons d'ajouter la balise manuellement. `Key: AmazonFSx; Value: ManagedByAmazonFSx`

Si vous ne parvenez pas à accéder à votre système de fichiers multi-AZ, vérifiez si les tables de routage VPC associées au système de fichiers sont étiquetées avec. `Key: AmazonFSx; Value: ManagedByAmazonFSx` Dans le cas contraire, Amazon FSx ne peut pas mettre à jour ces tables de

routage pour acheminer les adresses IP flottantes des ports de gestion et de données vers le serveur de fichiers actif en cas de basculement. Pour plus d'informations sur la mise à jour des tables de routage Amazon VPC de votre système de fichiers, consultez. Mettre à jour un système de fichiers

Impossible d'accéder à un système de fichiers via iSCSI à partir d'un client d'un autre VPC

Pour accéder à un système de fichiers via le protocole iSCSI (Internet Small Computer Systems Interface) depuis un client d'un autre VPC, vous pouvez configurer le peering Amazon VPC ou entre AWS Transit Gateway le VPC associé à votre système de fichiers et le VPC dans lequel réside votre client. Pour plus d'informations, consultez la section Créer et accepter des connexions de peering VPC dans le guide Amazon Virtual Private Cloud.

Le compte propriétaire a annulé le partage du sous-réseau VPC

Si vous avez créé votre système de fichiers dans un sous-réseau VPC qui a été partagé avec vous, le compte propriétaire a peut-être annulé le partage du sous-réseau VPC.

Si le compte propriétaire a annulé le partage du sous-réseau VPC, le message suivant s'affichera dans la console pour ce système de fichiers :

```
The vpc ID vpc-012345abcde does not exist
```

Vous devrez contacter le compte propriétaire afin qu'il puisse partager à nouveau le sous-réseau avec vous.

Impossible d'accéder à un système de fichiers via NFS, SMB, la CLI ONTAP ou l'API REST ONTAP depuis un client dans un autre VPC ou sur site

Pour accéder à un système de fichiers via le système de fichiers réseau (NFS), le bloc de messages serveur (SMB) ou la CLI NetApp ONTAP et l'API REST depuis un client dans un autre VPC ou sur site, vous devez configurer le routage AWS Transit Gateway entre le VPC associé à votre système de fichiers et le réseau sur lequel réside votre client. Pour plus d'informations, consultez Accès aux données .

Impossible de joindre une machine virtuelle de stockage (SVM) à Active Directory

Si vous ne parvenez pas à joindre une SVM à un Active Directory (AD), vérifiez Joindre des SVM à un Microsoft Active Directory d'abord. Les problèmes courants qui empêchent une SVM de se joindre à votre Active Directory sont répertoriés dans les sections suivantes, y compris les messages d'erreur générés pour chaque situation.

Rubriques

Le nom NetBIOS de la SVM est le même que le nom NetBIOS du domaine d'origine.

La connexion d'une SVM à votre Active Directory autogéré échoue avec le message d'erreur suivant :

Amazon FSx ne parvient pas à établir de connexion avec votre Active Directory. Cela est dû au fait que le nom du serveur que vous avez spécifié est le nom NetBIOS du domaine d'origine. Pour résoudre ce problème, choisissez un nom NetBIOS pour votre SVM différent du nom NetBIOS du domaine d'origine. Réessayez ensuite de joindre votre SVM à votre Active Directory.

Pour résoudre ce problème, suivez la procédure décrite dans la section Joindre une SVM à un Active Directory à l'aide de AWS Management Console l'API AWS CLI et pour réessayer de joindre votre SVM à votre AD. Assurez-vous d'utiliser un nom NetBIOS pour votre SVM différent du nom NetBIOS du domaine d'origine d'Active Directory.

La SVM est déjà jointe à un autre Active Directory

L'association d'une SVM à un Active Directory échoue avec le message d'erreur suivant :

Amazon FSx ne parvient pas à établir de connexion à votre Active Directory. Cela est dû au fait que la SVM est déjà jointe à un domaine. Pour associer cette SVM à un autre domaine, vous pouvez utiliser la CLI ONTAP ou l'API REST pour dissocier cette SVM d'Active Directory. Réessayez ensuite de joindre votre SVM à un autre Active Directory.

Pour résoudre le problème, procédez comme suit :

1. Utilisez la CLI NetApp ONTAP pour dissocier la SVM de son Active Directory actuel. Pour plus d'informations, consultez Dissocier un Active Directory de votre SVM à l'aide de la NetApp CLI ONTAP.
2. Suivez la procédure décrite dans la section Joindre une SVM à un Active Directory à l'aide de AWS Management Console l'API AWS CLI et pour réessayer de joindre votre SVM au nouvel AD.

Amazon FSx ne peut pas se connecter à vos contrôleurs de domaine Active Directory car le nom NetBIOS de la SVM est déjà utilisé

La création d'une SVM associée à votre AD autogéré échoue avec le message d'erreur suivant :

Amazon FSx ne parvient pas à établir de connexion avec votre Active Directory. Cela est dû au fait que le nom NetBIOS (ordinateur) que vous avez spécifié est déjà utilisé dans votre Active Directory. Pour résoudre ce problème, choisissez un nom NetBIOS pour votre SVM qui n'est pas utilisé dans votre Active Directory. Spécifiez un NetBIOS (ordinateur). Réessayez ensuite de joindre votre SVM à votre Active Directory.

Pour résoudre ce problème, suivez la procédure décrite dans la section Joindre une SVM à un Active Directory à l'aide de AWS Management Console l'API AWS CLI et pour réessayer de joindre votre SVM à votre AD. Assurez-vous d'utiliser un nom NetBIOS unique pour votre SVM qui n'est pas déjà utilisé dans votre Active Directory.

Amazon FSx ne peut pas communiquer avec vos contrôleurs de domaine Active Directory

L'association d'une SVM à votre Active Directory autogérée échoue avec le message d'erreur suivant :

Amazon FSx ne parvient pas à communiquer avec votre Active Directory. Pour résoudre ce problème, assurez-vous que le trafic réseau est autorisé entre Amazon FSx et vos contrôleurs de domaine. Réessayez ensuite de joindre votre SVM à votre Active Directory.

Pour résoudre ce problème, procédez comme suit :

1. Passez en revue les exigences décrites dans Exigences en matière de configuration du réseau et apportez les modifications nécessaires pour permettre les communications réseau entre Amazon FSx et votre AD.
2. Une fois qu'Amazon FSx est en mesure de communiquer avec votre AD, suivez la procédure décrite dans Joindre une SVM à un Active Directory à l'aide de AWS Management Console l'API AWS CLI et et réessayez de joindre votre SVM à votre AD.

Amazon FSx ne peut pas se connecter à votre Active Directory en raison d'exigences de port ou d'autorisations de compte de service non satisfaites

L'association d'une SVM à votre Active Directory autogérée échoue avec le message d'erreur suivant :

Amazon FSx ne parvient pas à établir de connexion avec votre Active Directory. Cela est dû soit au fait que les exigences en matière de port pour votre Active Directory ne sont pas respectées, soit au fait que le compte de service fourni n'était pas autorisé à associer la machine virtuelle de stockage au domaine avec l'unité organisationnelle spécifiée. Pour résoudre ce problème, mettez à jour la configuration Active Directory de votre machine virtuelle de stockage après avoir résolu tous les problèmes d'autorisation liés aux ports et aux comptes de service, comme recommandé dans le guide de l'utilisateur d'Amazon FSx.

Pour résoudre ce problème, procédez comme suit :

1. Passez en revue les exigences décrites dansExigences en matière de configuration du réseau, apportez les modifications nécessaires pour répondre aux exigences du réseau et assurez-vous que les communications sont activées sur les ports requis
2. Consultez les exigences relatives aux comptes de service décrites dansExigences relatives aux comptes de service Active Directory. Assurez-vous que le compte de service dispose des autorisations déléguées nécessaires pour associer votre SVM au domaine AD en utilisant l'unité organisationnelle spécifiée.
3. Une fois que vous avez modifié les autorisations de port ou le compte de service, suivez la procédure décrite dans Joindre une SVM à un Active Directory à l'aide de AWS Management Console l'API AWS CLI et et réessayez de joindre votre SVM à votre AD.

Amazon FSx ne peut pas se connecter à vos contrôleurs de domaine Active Directory car les informations d'identification du compte de service ne sont pas valides

La connexion d'une SVM à votre Active Directory autogéré échoue avec le message d'erreur suivant :

Amazon FSx ne parvient pas à établir de connexion avec vos contrôleurs de domaine Active Directory car les informations d'identification du compte de service fournies ne sont pas valides. Pour résoudre ce problème, mettez à jour la configuration Active Directory de votre machine virtuelle de stockage avec un compte de service valide.

Pour résoudre ce problème, suivez la procédure décrite dans la section Mettre à jour la configuration Active Directory d'une SVM existante à l'aide de l' AWS Management ConsoleAPI AWS CLI,, et pour mettre à jour les informations d'identification du compte de service de la SVM. Lorsque vous entrez le nom d'utilisateur du compte de service, veillez à n'inclure que le nom d'utilisateur (par exemple,`ServiceAcct`) et à ne pas inclure de préfixe de domaine (par exemple,`corp.com\ServiceAcct`) ou de suffixe de domaine (par exemple,`ServiceAcct@corp.com`). N'utilisez pas le nom distinctif (DN) lorsque vous entrez le nom d'utilisateur du compte de service (par exemple,`CN=ServiceAcct,OU=example,DC=corp,DC=com`).

Amazon FSx ne peut pas se connecter à vos contrôleurs de domaine Active Directory en raison d'informations d'identification de compte de service insuffisantes

La connexion d'une SVM à votre Active Directory autogéré échoue avec le message d'erreur suivant :

Amazon FSx ne parvient pas à établir de connexion avec vos contrôleurs de domaine Active Directory. Cela est dû au fait que les exigences en matière de port pour Active Directory n'ont pas été respectées ou que le compte de service fourni n'est pas autorisé à joindre la machine virtuelle de stockage au domaine avec l'unité organisationnelle spécifiée.

Pour résoudre ce problème, assurez-vous d'avoir délégué les autorisations requises au compte de service que vous avez fourni. Le compte de service doit être en mesure de créer et de supprimer des objets informatiques dans l'unité d'organisation du domaine auquel vous joignez le système de fichiers. Le compte de service doit également, au minimum, être autorisé à effectuer les opérations suivantes :

- Réinitialisation des mots de passe
- Empêcher les comptes de lire et d'écrire des données
- Capacité validée d'écrire sur le nom d'hôte DNS
- Capacité validée d'écrire dans le nom du principal de service
- Possibilité de créer et de supprimer des objets informatiques
- Aptitude validée à lire et à écrire les restrictions du compte

Pour plus d'informations sur la création d'un compte de service doté des autorisations appropriées, consultez Exigences relatives aux comptes de service Active Directory etDélégation d'autorisations à votre compte de service Amazon FSx.

Amazon FSx ne peut pas communiquer avec vos serveurs DNS ou contrôleurs de domaine Active Directory

La connexion d'une SVM à votre Active Directory autogéré échoue avec le message d'erreur suivant :

Amazon FSx ne parvient pas à communiquer avec votre Active Directory. Cela est dû au fait qu'Amazon FSx ne peut pas accéder aux serveurs DNS ou aux contrôleurs de domaine fournis pour votre domaine. Pour résoudre ce problème, mettez à jour la configuration Active Directory de votre

machine virtuelle de stockage avec des serveurs DNS valides et une configuration réseau permettant au trafic de circuler de la machine virtuelle de stockage vers le contrôleur de domaine.

Pour résoudre ce problème, suivez la procédure suivante :

1. Si seuls certains contrôleurs de domaine de votre Active Directory sont accessibles, par exemple en raison de limitations géographiques ou de pare-feux, vous pouvez ajouter des contrôleurs de domaine préférés. À l'aide de cette option, Amazon FSx tente de contacter les contrôleurs de domaine préférés. Ajoutez des contrôleurs de domaine préférés à l'aide de la commande `vserver cifs domain preferred-dc add` NetApp ONTAP CLI, comme suit :

   a. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *`management_endpoint_ip`* par l'adresse IP du port de gestion du système de fichiers.

      ```
      [~]$ ssh fsxadmin@management_endpoint_ip
      ```

      Pour plus d'informations, consultez Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.

   b. Entrez la commande suivante, où :

      - `-vserver vserver_name`indique le nom de la machine virtuelle de stockage (SVM).
      - `-domain domain_name`spécifie le nom Active Directory complet (FQDN) du domaine auquel appartiennent les contrôleurs de domaine spécifiés.
      - `-preferred-dc IP_address,…` spécifie une ou plusieurs adresses IP des contrôleurs de domaine préférés, sous forme de liste séparée par des virgules, par ordre de préférence.

      ```
      FsxId123456789::> vserver cifs domain preferred-dc add -vserver vserver_name -
      domain domain_name -preferred-dc IP_address, …+
      ```

      La commande suivante ajoute les contrôleurs de domaine 172.17.102.25 et 172.17.102.24 à la liste des contrôleurs de domaine préférés utilisés par le serveur SMB sur SVM vs1 pour gérer l'accès externe au domaine cifs.lab.example.com.

```
FsxId123456789::> vserver cifs domain preferred-dc add -vserver vs1 -domain
 cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

2. Vérifiez si votre contrôleur de domaine peut être résolu avec le DNS. Utilisez la commande `vserver services access-check dns forward-lookup` NetApp ONTAP CLI pour renvoyer l'adresse IP d'un nom d'hôte en fonction de la recherche sur le serveur DNS spécifié ou de la configuration DNS du serveur virtuel.

   a. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx pour NetApp ONTAP en exécutant la commande suivante. Remplacez *`management_endpoint_ip`* par l'adresse IP du port de gestion du système de fichiers.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Pour plus d'informations, consultez Gestion des systèmes de fichiers à l'aide de la ONTAP CLI.

   b. Entrez dans le mode avancé ONTAP CLI à l'aide de la commande suivante.

   ```
   FsxId123456789::> set adv
   ```

   c. Entrez la commande suivante, où :

   - `-vserver vserver_name`indique le nom de la machine virtuelle de stockage (SVM).
   - `-hostname host_name`indique le nom d'hôte à rechercher sur le serveur DNS.
   - `-node node_name` indique le nom du nœud sur lequel la commande est exécutée.
   - `-lookup-type`spécifie le type d'adresse IP à rechercher sur le serveur DNS, la valeur par défaut est`all`.

   ```
   FsxId123456789::> vserver services access-check dns forward-lookup \
   -vserver vserver_name -node node_name \
   -domains domain_name -name-servers dns_server_ip_address \
   -hostname host_name
   ```

3. Consultez les informations dont vous avez besoin pour joindre une SVM à un AD.
4. Vérifiez les exigences en matière de mise en réseau lorsque vous associez une SVM à un AD.

5. Suivez la procédure décrite dans la section Exigences en matière de configuration du réseau pour mettre à jour la configuration AD de votre SVM en utilisant les adresses IP correctes pour vos serveurs DNS AD.

Amazon FSx ne peut pas communiquer avec votre Active Directory en raison d'un nom de domaine Active Directory non valide.

La connexion d'une SVM à votre Active Directory autogéré échoue avec le message d'erreur suivant :

Amazon FSx a détecté que le nom de domaine complet fourni n'est pas valide. Pour résoudre ce problème, mettez à jour la configuration Active Directory de votre machine virtuelle de stockage avec un nom de domaine complet conforme aux exigences de configuration.

Pour résoudre ce problème, suivez la procédure suivante :

1. Passez en revue les exigences relatives aux noms de domaine Active Directory sur site décrites dans Informations nécessaires pour joindre une SVM à un Active Directory Assurez-vous que l'AD que vous essayez de rejoindre répond à ces exigences.
2. Suivez la procédure décrite dans Joindre une SVM à un Active Directory à l'aide de AWS Management Console l'API AWS CLI et et réessayez de joindre votre SVM à un AD. Assurez-vous d'utiliser le format correct pour le FQDN du domaine AD.

Le compte de service ne peut pas accéder au groupe d'administrateurs spécifié dans la configuration Active Directory de la SVM

La connexion d'une SVM à votre Active Directory autogéré échoue avec le message d'erreur suivant :

Amazon FSx n'est pas en mesure d'appliquer votre configuration Active Directory. Cela est dû au fait que le groupe d'administrateurs que vous avez fourni n'existe pas ou n'est pas accessible au compte de service que vous avez fourni. Pour résoudre ce problème, assurez-vous que votre configuration réseau autorise le trafic entre la SVM et les contrôleurs de domaine et les serveurs DNS de votre Active Directory. Mettez ensuite à jour la configuration Active Directory de votre SVM, en fournissant les serveurs DNS de votre SVM et en spécifiant un groupe d'administrateurs dans le domaine accessible au compte de service fourni.

Pour résoudre ce problème, procédez comme suit :

1. Consultez les informations relatives à la fourniture d'un groupe de domaines pour effectuer des actions administratives sur votre SVM. Assurez-vous que vous utilisez le nom correct du groupe d'administrateurs de domaine AD.
2. Suivez la procédure décrite dans Joindre une SVM à un Active Directory à l'aide de AWS Management Console l'API AWS CLI et et réessayez de joindre votre SVM à un AD.

Amazon FSx ne peut pas se connecter aux contrôleurs de domaine Active Directory car l'unité organisationnelle spécifiée n'existe pas ou n'est pas accessible

La connexion d'une SVM à votre Active Directory autogéré échoue avec le message d'erreur suivant :

Amazon FSx ne parvient pas à établir de connexion avec votre Active Directory. Cela est dû au fait que l'unité organisationnelle que vous avez spécifiée n'existe pas ou n'est pas accessible au compte de service fourni. Pour résoudre ce problème, mettez à jour la configuration Active Directory de votre machine virtuelle de stockage, en spécifiant une unité organisationnelle à laquelle le compte de service est autorisé à se joindre.

Pour résoudre ce problème, procédez comme suit :

1. Passez en revue les conditions requises pour joindre une SVM à un AD.
2. Consultez les informations dont vous avez besoin pour joindre une SVM à un AD.
3. Réessayez de joindre la SVM à l'AD en utilisant cette procédure avec l'unité organisationnelle appropriée.

Impossible de supprimer une machine virtuelle ou un volume de stockage

Chaque système de fichiers FSx for ONTAP peut contenir une ou plusieurs machines virtuelles de stockage (SVM), et chaque SVM peut contenir un ou plusieurs volumes. Lorsque vous supprimez une ressource, vous devez d'abord vous assurer que tous ses enfants ont été supprimés. Par exemple, avant de supprimer une SVM, vous devez d'abord supprimer tous les volumes non root de la SVM.

> **Important**
>
> Vous ne pouvez supprimer des machines virtuelles de stockage qu'à l'aide de la console, de l'API et de la CLI Amazon FSx. Vous ne pouvez supprimer des volumes à l'aide de la console, de l'API ou de la CLI Amazon FSx que si les sauvegardes Amazon FSx sont activées sur le volume.

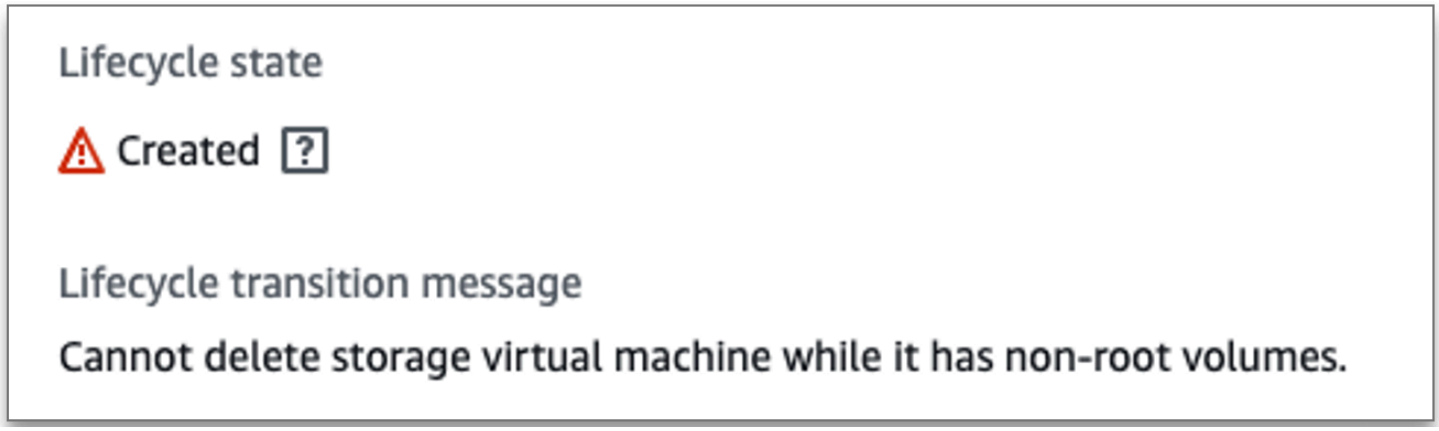
Pour protéger vos données et votre configuration, Amazon FSx empêche la suppression des SVM et des volumes dans certaines circonstances. Si vous tentez de supprimer une SVM ou un volume et que votre demande de suppression n'aboutit pas, Amazon FSx vous fournit des informations dans AWS la console AWS Command Line Interface AWS CLI() et dans l'API expliquant pourquoi la ressource n'a pas été supprimée. Après avoir résolu la cause de l'échec de suppression, vous pouvez réessayer la demande de suppression.

Rubriques

Identification des suppressions échouées

Lorsque vous supprimez une SVM ou un volume Amazon FSx, l'`Lifecycle`état de la ressource passe généralement jusqu'à `DELETING` quelques minutes avant qu'elle ne disparaisse de la console, de la CLI et de l'API Amazon FSx.

Si vous tentez de supprimer une ressource et que son `Lifecycle` état passe de à `DELETING` puis de nouveau à`CREATED`, ce comportement indique que la ressource n'a pas été correctement supprimée. Dans ce cas, Amazon FSx signale une icône d'alerte dans la console à côté de l'état du `CREATED` cycle de vie. Le choix de l'icône d'alerte affiche la raison de l'échec de la suppression, comme illustré dans l'exemple suivant.



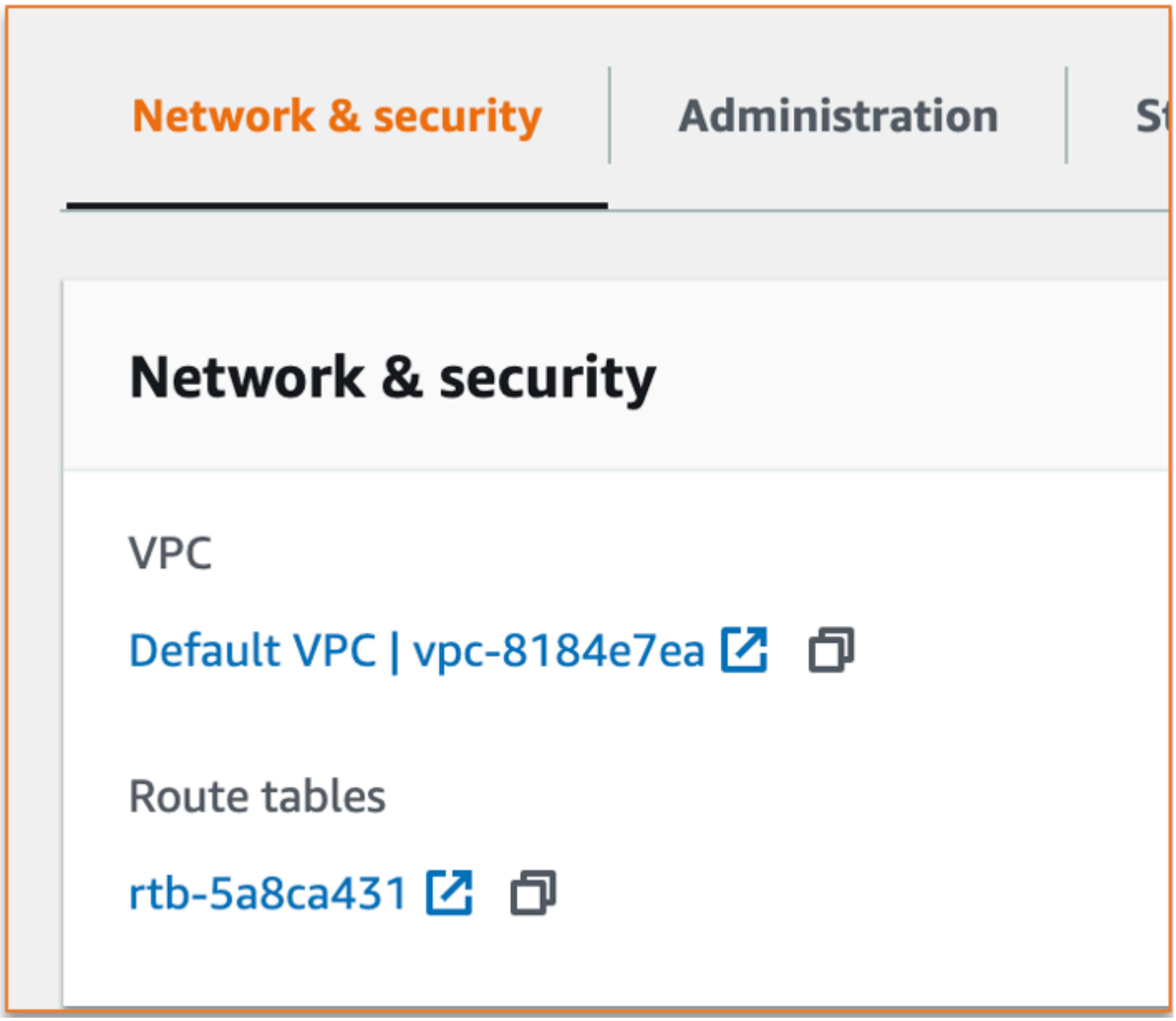
Les raisons les plus courantes pour lesquelles Amazon FSx empêche la suppression de SVM et de volumes sont indiquées dans les sections suivantes, avec des step-by-step instructions sur la manière de résoudre ces problèmes.

Suppression de la SVM : les tables de routage sont inaccessibles

Chaque système de fichiers FSx for ONTAP crée une ou plusieurs entrées de table de routage pour permettre un basculement et un retour en arrière automatiques entre les zones de disponibilité. Par défaut, ces entrées de table de routage sont créées dans la table de routage par défaut de votre VPC. Vous pouvez éventuellement spécifier une ou plusieurs tables de routage autres que celles par défaut dans lesquelles les interfaces FSx pour ONTAP peuvent être créées. Amazon FSx étiquette chaque table de routage associée à un système de fichiers avec une `AmazonFSx` balise, et si cette balise est supprimée, cela peut empêcher Amazon FSx de supprimer des ressources. Dans ce cas, vous pouvez voir ce qui suit `LifecycleTransitionReason` :

```
Amazon FSx is unable to complete the requested storage virtual machine
operation because of an inability to access one or more of the route tables
associated with your file system. Please contact AWS Support.
```

Vous pouvez trouver les tables de routage de votre système de fichiers dans la console Amazon FSx en accédant à la page de résumé du système de fichiers, sous l'onglet Réseau et sécurité :



En choisissant le lien des tables de routage, vous accédez à vos tables de routage. Vérifiez ensuite que chacune des tables de routage associées à votre système de fichiers est étiquetée avec cette paire clé-valeur :

```
Key: AmazonFSx
Value: ManagedByAmazonFSx
```

Si cette balise n'est pas présente, recréez-la, puis réessayez de supprimer la SVM.

Suppression de la SVM : relation avec les pairs

Si vous essayez de supprimer une SVM ou un volume faisant partie d'une relation d'homologue, vous devez d'abord supprimer la relation d'homologue avant de supprimer la SVM ou le volume. Cette exigence permet d'éviter que les SVM homologues ne deviennent insalubres. Si votre SVM ne peut pas être supprimée en raison d'une relation entre pairs, vous pouvez voir ce qui suit : `LifecycleTransitionReason`

Amazon FSx n'est pas en mesure de supprimer la machine virtuelle de stockage car elle fait partie d'une relation d'homologue de SVM ou d'homologue de transition. Supprimez la relation et réessayez.

Vous pouvez supprimer les relations entre homologues de la SVM via la CLI ONTAP. Pour accéder à la CLI ONTAP, suivez les étapes décrites dansGestion des systèmes de fichiers à l'aide de la ONTAP CLI. À l'aide de la CLI ONTAP, procédez comme suit.

1. Vérifiez les relations entre homologues de la SVM à l'aide de la commande suivante. *svm_name*Remplacez-le par le nom de votre SVM.

   ```
   FsxId123456789::> vserver peer show -vserver svm_name
   ```

   Si cette commande aboutit, vous obtiendrez un résultat similaire à ce qui suit :

   ```
               Peer        Peer                          Peering        Remote
   Vserver     Vserver     State        Peer Cluster     Applications   Vserver
   ----------- ----------- ------------ ----------------- -------------- ---------
   svm_name    test2       peered       FsxId02d81fef0d84734b6
                                                          snapmirror     fsxDest
   ```

```
svm_name    test3       peered       FsxId02d81fef0d84734b6
                                                  snapmirror     fsxDest
2 entries were displayed.
```

2. Supprimez chaque relation homologue de la SVM à l'aide de la commande suivante. Remplacez*svm_name*, et *remote_svm_name* par vos valeurs réelles.

```
FsxId123456789abcdef::> vserver peer delete -vserver svm_name -peer-
vserver remote_svm_name
```

Si cette commande aboutit, vous verrez le résultat suivant :

```
Info: 'vserver peer delete' command is successful.
```

Suppression d'une SVM ou d'un volume : SnapMirror

Tout comme il est impossible de supprimer une SVM ayant une relation entre pairs sans supprimer au préalable cette relation (voirSuppression de la SVM : relation avec les pairs), vous ne pouvez pas supprimer une SVM qui a une SnapMirror relation sans la supprimer au SnapMirror préalable. Pour supprimer la SnapMirror relation, utilisez la CLI ONTAP pour effectuer les étapes suivantes sur le système de fichiers qui est la destination de la SnapMirror relation. Pour accéder à la CLI ONTAP, suivez les étapes décrites dansGestion des systèmes de fichiers à l'aide de la ONTAP CLI.

> **Note**
>
> Les sauvegardes Amazon FSx permettent de SnapMirror créer point-in-time des sauvegardes incrémentielles des volumes de votre système de fichiers. Vous ne pouvez pas supprimer cette SnapMirror relation pour vos sauvegardes dans la CLI ONTAP. Toutefois, cette relation est automatiquement supprimée lorsque vous supprimez un volume par le biais de la AWS CLI, de l'API ou de la console.

1. Répertoriez vos SnapMirror relations sur le système de fichiers de destination à l'aide de la commande suivante. *svm_name*Remplacez-le par le nom de votre SVM.

```
FsxId123456789abcdef::> snapmirror show -vserver svm_name
```

Si cette commande aboutit, vous obtiendrez un résultat similaire à ce qui suit :

```
Source            Destination    Mirror  Relationship   Total             Last
Path        Type  Path           State   Status         Progress  Healthy Updated
----------- ---- ------------    ------- -------------- --------- ------- --------
sourceSvm:sourceVol
            XDP  destSvm:destVol Snapmirrored
                                       Idle           -         true    -
```

2. Supprimez votre SnapMirror relation en exécutant la commande suivante sur le système de fichiers de destination.

```
FsxId123456789abcdef::> snapmirror release -destination-path destSvm:destVol -
source-path sourceSvm:sourceVol -force true
```

Suppression de la SVM : LIF compatible avec Kerberos

Si vous essayez de supprimer une SVM dotée d'une interface logique (LIF) avec Kerberos activé, vous devez d'abord désactiver Kerberos sur cette SVM avant de supprimer la SVM.

Vous pouvez désactiver Kerberos sur un LIF via la CLI ONTAP. Pour accéder à la CLI ONTAP, suivez les étapes décrites dansGestion des systèmes de fichiers à l'aide de la ONTAP CLI.

1. Entrez en mode diagnostic dans la CLI ONTAP à l'aide de la commande suivante.

```
FsxId123456789abcdef::> set diag
```

Lorsque vous êtes invité à continuer, entrez**y**.

```
Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y
```

2. Vérifiez les interfaces sur lesquelles Kerberos est activé. *svm_name*Remplacez-le par le nom de votre SVM.

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

Si cette commande aboutit, vous obtiendrez un résultat similaire à ce qui suit :

```
(vserver nfs kerberos interface show)
```

```
               Logical
Vserver        Interface     Address         Kerberos SPN
-------------- ------------ --------------- -------- ----------------------
svm_name       nfs_smb_management_1
                            10.19.153.48    enabled
5 entries were displayed.
```

3. Désactivez le LIF Kerberos à l'aide de la commande suivante. *svm_name*Remplacez-le par le nom de votre SVM. Vous devez fournir le nom d'utilisateur et le mot de passe Active Directory que vous avez utilisés pour associer cette SVM à votre Active Directory.

```
FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
 nfs_smb_management_1
```

Si cette commande aboutit, vous verrez le résultat suivant. Indiquez le nom d'utilisateur et le mot de passe Active Directory que vous avez utilisés pour associer cette SVM à votre Active Directory. Lorsque vous êtes invité à continuer, entrez**y**.

```
(vserver nfs kerberos interface disable)
Username: admin
Password: *************

Warning: This command deletes the service principal name from the machine account
 on the KDC.
Do you want to continue? {y|n}: y

Disabled Kerberos on LIF "nfs_smb_management_1" in Vserver "svm_name".
```

4. Vérifiez que Kerberos est désactivé sur la SVM à l'aide de la commande suivante. *svm_name*Remplacez-le par le nom de votre SVM.

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

Si cette commande aboutit, vous obtiendrez un résultat similaire à ce qui suit :

```
(vserver nfs kerberos interface show)
               Logical
Vserver        Interface     Address         Kerberos SPN
-------------- ------------ --------------- -------- ----------------------
svm_name       nfs_smb_management_1
                            10.19.153.48    disabled
```

```
5 entries were displayed.
```

5. Si l'interface est affichée`disabled`, essayez à nouveau de supprimer la SVM par le biais de la AWS CLI, de l'API ou de la console.

   Si vous n'avez pas pu supprimer le LIF à l'aide des commandes précédentes, vous pouvez forcer la suppression du LIF Kerberos à l'aide de la commande suivante. *`svm_name`*Remplacez-le par le nom de votre SVM.

   > **Important**
   >
   > La commande suivante peut transférer l'objet informatique de votre SVM sur votre Active Directory.

   ```
   FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
    nfs_smb_management_1 -force true
   ```

   Si cette commande aboutit, vous obtiendrez un résultat similaire à ce qui suit. Lorsque vous êtes invité à continuer, entrez**y**.

   ```
   (vserver nfs kerberos interface disable)

   Warning: Kerberos configuration for LIF "nfs_smb_management_1" in Vserver
    "svm_name" will be deleted.
   The corresponding account on the KDC will not be deleted. Do you want to continue?
    {y|n}: y
   ```

Suppression de la SVM : autre raison

Les SVM FSx for ONTAP créent un objet informatique dans votre Active Directory lorsqu'elles rejoignent ce dernier. Dans certains cas, vous souhaiterez peut-être dissocier manuellement une SVM de votre Active Directory à l'aide de la CLI ONTAP. Pour accéder à la CLI ONTAP, suivez les étapes décritesGestion des systèmes de fichiers à l'aide de la ONTAP CLI, en vous connectant à la CLI ONTAP au niveau du système de fichiers avec `fsxadmin` des informations d'identification. À l'aide de la CLI ONTAP, procédez comme suit pour dissocier une SVM de votre Active Directory.

> **Important**
>
> Cette procédure peut transférer l'objet informatique de votre SVM sur votre Active Directory.

1. Passez en mode avancé dans la CLI ONTAP à l'aide de la commande suivante.

```
FsxId123456789abcdef::> set adv
```

   Après avoir exécuté cette commande, vous verrez ce résultat. Entrez **y** pour continuer.

```
Warning: These advanced commands are potentially dangerous; use them only when
      directed to do so by NetApp personnel.
      Do you want to continue? {y|n}: y
```

2. Supprimez le DNS de votre Active Directory à l'aide de la commande suivante. *svm_name*Remplacez-le par le nom de votre SVM.

```
FsxId123456789abcdef::> vserver services name-service dns dynamic-update record
 delete -vserver svm_name -lif nfs_smb_management_1
```

   > **Note**
   >
   > Si l'enregistrement DNS a déjà été supprimé ou si le serveur DNS est inaccessible, cette commande échoue. Dans ce cas, passez à l'étape suivante.

3. Désactivez le DNS à l'aide de la commande suivante. *svm_name*Remplacez-le par le nom de votre SVM.

```
FsxId123456789abcdef::> vserver services name-service dns dynamic-update modify -
vserver svm_name -is-enabled false -use-secure false
```

   Si cette commande aboutit, vous verrez le résultat suivant :

```
Warning: DNS updates for Vserver "svm_name" are now disabled.
     Any LIFs that are subsequently modified or deleted
     can result in a stale DNS entry on the DNS server,
     even when DNS updates are enabled again.
```

4. Dissociez l'appareil d'Active Directory. *svm_name*Remplacez-le par le nom de votre SVM.

```
FsxId123456789abcdef::> vserver cifs delete -vserver svm_name
```

Après avoir exécuté cette commande, vous verrez le résultat suivant, où *CORP.EXAMPLE.COM* est remplacé par le nom de votre domaine. Lorsque vous y êtes invité, entrez votre nom d'utilisateur et votre mot de passe. Lorsqu'on vous demande si vous souhaitez supprimer le serveur, entrez**y**.

```
In order to delete an Active Directory machine account for the CIFS server,
you must supply the name and password of a Windows account with sufficient
privileges to remove computers from the "CORP.EXAMPLE.COM" domain.
Enter the user name: admin
Enter the password:
Warning: There are one or more shares associated with this CIFS server
     Do you really want to delete this CIFS server and all its shares? {y|n}: y
Warning: Unable to delete the Active Directory computer account for this CIFS
 server.
     Do you want to continue with CIFS server deletion anyway? {y|n}: y
```

Suppression d'un volume : FlexCache relation

Vous ne pouvez pas supprimer les volumes qui sont les volumes d'origine d'une FlexCache relation, sauf si vous supprimez d'abord la relation de cache. Pour déterminer quels volumes ont une FlexCache relation, vous pouvez utiliser la CLI ONTAP. Pour accéder à la CLI ONTAP, suivez les étapes décrites dansGestion des systèmes de fichiers à l'aide de la ONTAP CLI.

1. Vérifiez les FlexCache relations à l'aide de la commande suivante.

```
FsxId123456789abcdef::> volume flexcache origin show-caches
```

2. Supprimez toute relation de cache à l'aide de la commande suivante. Remplacez*dest_svm_name*, et *dest_vol_name* par vos valeurs réelles.

```
FsxId123456789abcdef::> volume flexcache delete -vserver dest_svm_name -
volume dest_vol_name
```

3. Après avoir supprimé la relation de cache, essayez à nouveau de supprimer votre SVM par le biais de la AWS CLI, de l'API ou de la console.

Les sauvegardes quotidiennes automatiques échouent en raison d'une capacité de volume insuffisante

Les sauvegardes quotidiennes automatiques de votre volume échouent avec le message suivant :

```
Amazon FSx could not create a backup of your volume because the backup snapshot was
 deleted.
```

Les sauvegardes quotidiennes automatiques échouent car la capacité de stockage disponible sur le volume est insuffisante. Pour pallier ce problème, vous devez libérer de la capacité de stockage sur le volume. Pour ce faire, vous pouvez utiliser une ou plusieurs des options suivantes, en fonction de votre situation :

- Augmenter la capacité de stockage du volume
- Augmenter la réserve d'instantanés du volume
- Désactiver la suppression automatique des instantanés
- Ne supprimez pas l'instantané de sauvegarde à l'aide de la CLI ONTAP

Votre capacité de volume est insuffisante

Si vous manquez d'espace sur vos volumes, vous pouvez utiliser les procédures présentées ici pour diagnostiquer et résoudre le problème.

Rubriques

- Déterminez comment votre capacité de stockage en volume est utilisée
- Augmenter la capacité de stockage d'un volume
- Utilisation du dimensionnement automatique du volume
- Le stockage principal de votre système de fichiers est plein
- Suppression d’instantanés
- Augmenter la capacité maximale de fichiers d'un volume

Déterminez comment votre capacité de stockage en volume est utilisée

Vous pouvez voir comment la capacité de stockage de votre volume est consommée à l'aide de la commande `volume show-space` NetApp ONTAP CLI. Ces informations peuvent vous aider

à prendre des décisions sur la manière de récupérer ou de conserver la capacité de stockage en volume. Pour plus d'informations, consultez Pour surveiller la capacité de stockage d'un volume (console).

Augmenter la capacité de stockage d'un volume

Vous pouvez augmenter la capacité de stockage d'un volume à l'aide de la console Amazon FSx et de l' AWS CLI API Amazon FSx. Pour plus d'informations sur la mise à jour d'un volume avec une capacité accrue, consultezMettre à jour un volume.

Vous pouvez également augmenter la capacité de stockage d'un volume à l'aide de la commande `volume modify` NetApp ONTAP CLI. Pour plus d'informations, consultez Pour modifier la capacité de stockage d'un volume (console).

Utilisation du dimensionnement automatique du volume

Vous pouvez utiliser le dimensionnement automatique des volumes pour qu'un volume augmente automatiquement d'une quantité spécifiée, ou pour atteindre une taille spécifiée lorsqu'il atteint un seuil d'espace utilisé. Vous pouvez le faire pour les types de FlexVol volume, qui est le type de volume par défaut pour FSx for ONTAP, à l'aide de la commande ONTAP `volume autosize` NetApp CLI. Pour plus d'informations, consultez Activation du dimensionnement automatique du volume.

Le stockage principal de votre système de fichiers est plein

Si le stockage principal de votre système de fichiers FSx for ONTAP est plein, vous ne pouvez pas ajouter de données supplémentaires aux volumes de votre système de fichiers, même si un volume indique qu'il dispose d'une capacité de stockage disponible suffisante. Vous pouvez consulter la quantité de capacité de stockage principal disponible dans l'onglet Surveillance et performances de la page de détails du système de fichiers de la console Amazon FSx. Pour plus d'informations, consultez Surveillance de l'utilisation du stockage SSD.

Pour résoudre ce problème, vous pouvez augmenter la taille du niveau de stockage principal de votre système de fichiers. Pour plus d'informations, consultez Mise à jour du système de fichiers, du stockage SSD et des IOPS.

Suppression d’instantanés

Les instantanés sont activés par défaut sur vos volumes, selon la politique de capture par défaut. Les instantanés sont stockés dans le `.snapshot` répertoire situé à la racine d'un volume. Vous pouvez gérer la capacité de stockage en volume par rapport aux instantanés de la manière suivante :

- Suppression manuelle des instantanés : récupérez de la capacité de stockage en supprimant les instantanés manuellement.
- Créez une politique de suppression automatique des instantanés : créez une politique qui supprime les instantanés de manière plus agressive que la politique de capture d'écran par défaut.
- Désactiver les instantanés automatiques : économisez la capacité de stockage en désactivant les instantanés automatiques.

Pour plus d'informations sur la suppression des instantanés et la gestion des politiques relatives aux instantanés afin de préserver la capacité de stockage, consultezSuppression d’instantanés.

Augmenter la capacité maximale de fichiers d'un volume

Un volume FSx for ONTAP peut manquer de capacité de fichier lorsque le nombre d'inodes ou de pointeurs de fichiers disponibles est épuisé. Par défaut, le nombre d'inodes disponibles sur un volume est de 1 pour 32 Ko de taille de volume. Pour plus d’informations, consultez Capacité du fichier de volume.

Le nombre d'inodes dans un volume augmente proportionnellement à la capacité de stockage du volume, jusqu'à un seuil de 648 GiB. Par défaut, les volumes dont la capacité de stockage est supérieure ou égale à 648 GiB ont tous le même nombre d'inodes, soit 21 251 126. Pour consulter la capacité maximale de fichiers d'un volume, consultezAffichage de la capacité de fichier d'un volume.

Si vous créez un volume supérieur à 648 GiB et que vous souhaitez avoir plus de 21 251 126 inodes, vous devez augmenter manuellement le nombre maximum de fichiers sur le volume. Si la capacité de stockage de votre volume est insuffisante, vous pouvez vérifier sa capacité maximale de fichiers. S'il approche de sa capacité de fichier, vous pouvez l'augmenter manuellement. Pour plus d’informations, consultez Pour augmenter le nombre maximum de fichiers sur un volume (ONTAPCLI).

Résolution des problèmes de réseau

Si vous rencontrez des problèmes de réseau, vous pouvez utiliser les procédures indiquées ici pour diagnostiquer le problème.

Vous souhaitez capturer une trace de paquet

Le suivi des paquets est le processus qui consiste à vérifier le chemin d'un paquet à travers les couches jusqu'à sa destination. Vous contrôlez le processus de suivi des paquets à l'aide des commandes NetApp ONTAP CLI suivantes :

- network tcpdump start— Démarre le suivi des paquets
- network tcpdump show— Affiche les traces des paquets en cours d'exécution
- network tcpdump stop— Arrête le traçage d'un paquet en cours

Ces commandes sont accessibles aux utilisateurs qui ont le `fsxadmin` rôle dans votre système de fichiers.

Pour capturer la trace d'un paquet à partir de votre système de fichiers

1. Pour accéder en SSH à la NetApp CLI ONTAP de votre système de fichiers, suivez les étapes décrites dans la Utilisation de la CLI NetApp ONTAP section du guide de l'utilisateur d'Amazon FSx for NetApp ONTAP.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Entrez le niveau de privilège de diagnostic dans la CLI ONTAP à l'aide de la commande suivante.

   ```
   ::> set diag
   ```

   Lorsque vous êtes invité à continuer, entrezy.

   ```
   Warning: These diagnostic commands are for use by NetApp personnel only.
   Do you want to continue? {y|n}: y
   ```

3. Identifiez l'emplacement de votre système de fichiers où vous souhaitez enregistrer la trace de votre paquet. Le volume doit être en ligne et monté dans l'espace de noms avec un chemin de jonction valide. Utilisez la commande suivante pour vérifier les volumes qui répondent à ces critères :

   ```
   ::*> volume show -junction-path !- -fields junction-path
   vserver volume    junction-path
   ------- --------- -------------
   ```

```
fsx     test_vol1 /test_vol1
fsx     test_vol2 /test_vol2
fsx     test_vol2 /test_vol3
```

4. Démarrez le traçage avec le minimum d'arguments requis. Remplacez les éléments suivants :

   - Remplacez *node_name* par le nom du nœud (par exemple,). `FsxId01234567890abcdef-01`
   - Remplacez *svm_name* par le nom de votre machine virtuelle de stockage (par exemple,). `fsx`
   - Remplacez *junction_path_name par le nom* du volume (par exemple,). `test-vol1`

```
::*> debug network tcpdump start -node node_name -ipspace Default -pass-through "-i
 e0e -w /clus/svm_name/junction_path_name"
Info: Started network trace on interface "e0e"
Warning: Snapshots should be disabled on the tcpdump destination volume while
 packet traces are occurring. Use the
"volume modify -snapshot-policy none -vserver fsx -volume test_vol1" command to
 disable Snapshots on the
tcpdump destination volume.
```

> **Important**
>
> Les traces de paquets ne peuvent être capturées que sur l'`e0e`interface et dans l'espace `Default` IP. Dans FSx for ONTAP, tout le trafic réseau utilise l'interface. `e0e`

Lorsque vous utilisez le suivi des paquets, gardez à l'esprit les points suivants :

- *Lorsque vous démarrez un suivi de paquets, vous devez inclure le chemin d'accès à l'endroit où vous souhaitez stocker les fichiers de trace, au format suivant : /clus/ svm_name/junction-path-name*
- Indiquez éventuellement le nom de fichier pour le suivi du paquet. *Si le nom du filtre n'est pas spécifié, il est automatiquement généré sous la forme suivante : nom-de-nœud _ nom_port _ yyyymmdd_hhmmss .trc*
- Si des traces de roulement sont spécifiées, le nom du filtre est suffixé par un chiffre indiquant la position dans la séquence de rotation.
- La CLI ONTAP accepte également les -pass-through arguments facultatifs suivants :

```
-B, --buffer-size=<KiB>
-c <number_of_packets>
-C <file_size-mB>
-F <filter_expression_filename>
-G <rotate_seconds>
--time-stamp-precision {micro|nano}
-Q, --direction {in|out|inout}
-s, --snapshot-length=<bytes>
-U, --packet-buffered
-W <rotate_file_count>
<filter-expression>
```

- Pour plus d'informations sur les expressions de filtre, consultez la page de manuel pcap-filter (7).

5. Consultez les traces en cours :

```
::*> debug network tcpdump show
Node                     IPspace  Port     Filename
-----------------------  -------- -------- --------
FsxId123456789abcdef-01  Default  e0e      /clus/fsx/test_vol1/
FsxId123456789abcdef-01_e0e_20230605_181451.trc
```

6. Arrêtez le traçage :

```
::*> debug network tcpdump stop -node FsxId123456789abcdef-01 -ipspace Default -
port e0e
Info: Stopped network trace on interface "e0e"
```

7. Revenez au niveau de privilège d'administrateur :

```
::*> set -priv admin
::>
```

8. Accédez aux traces des paquets.

   Les traces de vos paquets sont stockées dans le volume que vous avez spécifié à l'aide de la debug network tcpdump start commande et sont accessibles via l'exportation NFS ou un partage SMB correspondant à ce volume.

Pour plus d'informations sur la capture de traces de paquets, consultez la section Comment utiliser le tcpdump du réseau de débogage dans ONTAP 9.10+ dans la base de connaissances. NetApp

Historique du document pour Amazon FSx for ONTAP NetApp

- Version de l'API : 01/03/2018
- Dernière mise à jour de la documentation : 30 avril 2024

Le tableau suivant décrit les modifications importantes apportées au guide de l'utilisateur d'Amazon FSx NetApp ONTAP. Pour recevoir des notifications en cas de mise à jour de cette documentation, abonnez-vous au flux RSS.

Modification	Description	Date
Support ajouté pour le `fsxadmin-readonly` rôle des utilisateurs administratifs du système de fichiers	Le `fsxadmin-readonly` rôle est désormais disponible pour les utilisateurs administr atifs du système de ONTAP fichiers et peut être utilisé pour les applications de surveillance du système de fichiers telles queNetApp Harvest. Pour plus d'informa tions, consultez la section Rôles et utilisateurs des administrateurs de systèmes de fichiers.	30 avril 2024
Support ajouté pour l'authent ification par clé publique SSH pour les utilisateurs administr atifs du domaine Windows	Vous pouvez désormais utiliser l'authentification par clé publique SSH avec les utilisateurs du système de fichiers de domaine Active Directory et des SVM. Pour plus d’informations, consultez https://docs.aws.amazon.com/	30 avril 2024

	fsx/latest/ONTAPGuide/set-up-ad-auth.html.	
Support ajouté pour 12 paires HA dans les systèmes de fichiers évolutifs	Amazon FSx for NetApp ONTAP a ajouté la prise en charge de 12 paires HA dans les systèmes de fichiers évolutifs. Les systèmes de fichiers dotés de 12 paires HA peuvent fournir une capacité de débit allant jusqu'à 72 Gbit/s et 2 400 000 IOPS sur SSD sur 12 paires haute disponibilité (HA). Pour plus d'informations, consultez les paires à haute disponibilité (HA) et Amazon FSx NetApp pour les performances ONTAP.	4 mars 2024
Support ajouté pour le mode d'écriture dans le cloud	Amazon FSx for NetApp ONTAP a ajouté la prise en charge du mode d'écriture dans le cloud pour les volumes. Pour plus d'informations, consultez la section Activation du mode d'écriture dans le cloud sur un volume.	6 février 2024
Support ajouté pour la sauvegarde de FlexGroup volumes avec AWS Backup	Vous pouvez désormais l'utiliser AWS Backup pour sauvegarder et restaurer des FlexGroup volumes sur vos systèmes de fichiers FSx for ONTAP. Pour plus d'informations, consultez Utilisation AWS Backup avec Amazon FSx.	11 janvier 2024

Amazon FSx a mis à jour les politiques gérées Amazon F, AmazonFSx FullAccess, AmazonFSx ConsoleFullAccess, AmazonF SxReadOnlyAccess et SxConsoleReadOnlyAccess AmazonF SxServiceRolePolicy AWS	Amazon FSx a mis à jour les politiques AmazonFSx FullAccess, AmazonF, AmazonFSxConsoleFullAccess, AmazonF SxReadOnlyAccess et SxServiceRolePolicy AmazonF pour SxConsole ReadOnlyAccess ajouter l'autorisation. `ec2:GetSecurityGroupsForVpc` Pour plus d'informations, consultez les mises à jour des politiques AWS gérées par Amazon FSx.	9 janvier 2024
Amazon FSx a mis à jour les politiques gérées par Amazon F SxFullAccess et Amazon F SxConsoleFullAccess AWS	Amazon FSx a mis à jour les SxConsoleFullAccess politiques d'AmazonF SxFullAccess et d'AmazonF pour ajouter cette action. `ManageCrossAccountDataReplication` Pour plus d'informations, consultez les mises à jour des politiques AWS gérées par Amazon FSx.	20 décembre 2023
Support ajouté pour les métriques de scale-out	FSx for ONTAP fournit désormais des CloudWatch métriques Amazon pour les systèmes de fichiers comportant plusieurs paires HA. Pour plus d'informations, consultez la section Mesures du système de fichiers Scale-out.	26 novembre 2023

Support ajouté pour les systèmes de fichiers évolutifs	Amazon FSx for NetApp ONTAP a ajouté la prise en charge des systèmes de fichiers évolutifs capables de fournir une capacité de débit allant jusqu'à 36 Gbit/s et 1 200 000 IOPS sur SSD sur six paires de haute disponibilité (HA). Pour plus d'informations, consultez les paires à haute disponibilité (HA) et Amazon FSx NetApp pour les performances ONTAP.	26 novembre 2023
Support ajouté pour les FlexGroup volumes	Amazon FSx for NetApp ONTAP a ajouté la prise en charge des volumes. FlexGroup Pour plus d'informations, consultez la section Styles de volume.	26 novembre 2023
Ajout du support VPC partagé pour les systèmes de fichiers multi-AZ	Les comptes participants peuvent désormais créer des systèmes de fichiers multi-AZ dans un VPC partagé avec eux. Les comptes propriétaires peuvent gérer cette fonctionnalité dans la console, la CLI et l'API Amazon FSx. Pour plus d'informations, voir Création de FSx pour les systèmes de fichiers ONTAP dans des sous-réseaux partagés	26 novembre 2023

Amazon FSx a mis à jour les politiques gérées par Amazon F SxFullAccess et Amazon F SxConsoleFullAccess AWS	Amazon FSx a mis à jour les SxConsoleFullAccess politique s d'AmazonF SxFullAccess et d'AmazonF pour ajouter l'autorisation. `fsx:CopyS napshotAndUpdateVo lume` Pour plus d'informa tions, consultez les mises à jour des politiques AWS gérées par Amazon FSx.	26 novembre 2023
Amazon FSx a mis à jour les politiques gérées par Amazon F SxFullAccess et Amazon F SxConsoleFullAccess AWS	Amazon FSx a mis à jour les SxConsoleFullAccess politique s d'AmazonF SxFullAccess et d'AmazonF pour ajouter les autorisations et. `fsx:Descr ibeSharedVPCConfig uration` `fsx:Updat eSharedVPCConfigur ation` Pour plus d'informa tions, consultez les mises à jour des politiques AWS gérées par Amazon FSx.	14 novembre 2023

Support ajouté pour la création de rôles et d'utilisateurs ONTAP supplémentaires	Amazon FSx for NetApp ONTAP prend désormais en charge la création de rôles et d'utilisateurs ONTAP supplémentaires afin de définir les capacités et les privilège s des utilisateurs lors de l'utilisation de la CLI ONTAP et de l'API REST. Pour plus d'informations, consultez la section Rôles et utilisateurs dans Amazon FSx for NetApp ONTAP.	6 septembre 2023
Support ajouté pour des CloudWatch mesures supplémentaires et un tableau de bord de surveillance amélioré	FSx for ONTAP fournit désormais des indicateurs de performance supplémen taires et un tableau de bord de surveillance amélioré pour une meilleure visibilité de l'activité du système de fichiers. Pour plus d'informations, consultez la section Surveillance avec CloudWatch.	17 août 2023
Amazon FSx a mis à jour la politique gérée par Amazon SxServiceRolePolicy AWS FSx	Amazon FSx a mis à jour l'`cloudwatch:PutMetr icData` autorisation dans AmazonF. SxServiceRolePolic y Pour plus d'informations, consultez les mises à jour des politiques AWS gérées par Amazon FSx.	24 juillet 2023

Support ajouté pour l'utilisation directe de NetApp System Manager	Vous pouvez gérer vos systèmes de fichiers FSx for ONTAP directement depuis. System Manager NetApp BlueXP Pour plus d'informations, consultez la section Utilisation NetApp du gestionnaire de système avec BlueXP.	13 juillet 2023
Support ajouté pour la surveillance des événements EMS	Vous pouvez surveiller les événements du système de fichiers FSx for ONTAP à l'aide du logiciel natif de NetApp ONTAP. Events Management System (EMS) Vous pouvez consulter les événements EMS à l'aide de la CLI NetApp ONTAP. Pour plus d'informations, consultez la section Surveillance de FSx pour les événements ONTAP EMS.	13 juillet 2023

Support ajouté pour SnapLock	FSx for ONTAP prend désormais en charge les volumes. SnapLock SnapLockvous permet de protéger vos fichiers en les faisant passer à l'état WORM (Write Once, Read Many), qui empêche toute modificat ion ou suppression pendant une période de conservation spécifiée. FSx for ONTAP prend en charge les modes de conformité et de rétention d'entreprise avec. SnapLock Pour plus d'informations, consultez la section Travailler avec SnapLock.	13 juillet 2023
Support ajouté pour le chiffrement IPsec des données en transit	FSx for ONTAP prend désormais en charge l'utilisa tion du chiffrement IPsec pour chiffrer les données en transit entre les systèmes de fichiers et les clients connectés. Pour plus d'informations, consultez Configuration d'IPsec à l'aide de l'authentification PSK et Configuration d'IPsec à l'aide de l'authentification par certificat.	13 juillet 2023

La taille maximale du volume a augmenté	FSx for ONTAP a mis à jour la taille maximale d'un volume de 100 To à 300 To. Pour plus d'informations, voir Activer le dimensionnement automatique du volume.	13 juillet 2023
Amazon FSx a mis à jour la politique gérée par Amazon SxFullAccess AWS FSx	Amazon FSx a mis à jour la SxFullAccess politique d'AmazonF afin de supprimer l'`fsx:*`autorisation et d'ajouter des actions spécifiqu es. `fsx` Pour plus d'informa tions, consultez la SxFullAcc ess politique d'AmazonF.	13 juillet 2023
Amazon FSx a mis à jour la politique gérée par Amazon SxConsoleFullAccess AWS FSx	Amazon FSx a mis à jour la SxConsoleFullAccess politique d'AmazonF afin de supprimer l'`fsx:*`autorisat ion et d'ajouter des actions spécifiques. `fsx` Pour plus d'informations, consultez la SxConsoleFullAccess politique d'AmazonF.	13 juillet 2023
Support ajouté pour joindre des machines virtuelles de stockage existantes à un Active Directory	Vous pouvez joindre des machines virtuelles de stockage existantes à un Active Directory à l'aide de l' AWS Management Console API AWS CLI et. Pour plus d'informations, voir Joindre une SVM à un Active Directory .	13 juin 2023

Support du cache de lecture NVMe ajouté pour les systèmes de fichiers mono-AZ	Le cache de lecture NVMe est désormais pris en charge pour les systèmes de fichiers mono-AZ créés après le 28 novembre 2022 avec une capacité de débit d'au moins 2 Gbit/s dans les régions USA Est (Ohio), USA Est (Virginie du Nord), USA Ouest (Oregon) et Europe (Irlande). Pour plus d'informations, consultez la section Impact du type de déploiement sur les performances.	28 novembre 2022
Support ajouté pour l'utilisation de plages d'adresses IP intégrées au VPC pour créer des systèmes de fichiers multi-AZ	Vous pouvez désormais créer des FSx multi-AZ pour les systèmes de fichiers ONTAP en spécifiant des points de terminaison situés dans la plage d'adresses IP de votre VPC. Pour plus d'informations, voir Création de FSx pour les systèmes de fichiers ONTAP.	28 novembre 2022

Support ajouté pour la mise à jour des tables de routage VPC sur les systèmes de fichiers multi-AZ	Vous pouvez désormais associer (ajouter) une nouvelle table de routage VPC à un système de fichiers FSx pour ONTAP existant ou dissocier (supprimer) une table de routage VPC existante d'un système de fichiers FSx pour ONTAP multi-AZ existant. Pour plus d'informations, consultez la section Mise à jour d'un système de fichiers.	28 novembre 2022
Support ajouté pour le chiffrement des données en transit avec AWS Nitro System	Les données en transit sont chiffrées automatiquement lorsqu'elles sont accessibles à partir d'instances Amazon EC2 prises en charge dans les régions USA Est (Ohio), USA Est (Virginie du Nord), USA Ouest (Oregon) et Europe (Irlande). Pour plus d'informa tions, consultez la section Chiffrement des données en transit avec AWS Nitro System.	28 novembre 2022

Support ajouté pour la création de volumes DP	Vous pouvez désormais créer des volumes DP (protection des données) à l'aide de la console Amazon FSx ou de l' AWS CLI API Amazon FSx. Vous pouvez utiliser les volumes DP comme destination d'une SnapVault relation NetApp SnapMirror or lorsque vous souhaitez migrer ou protéger les données d'un seul volume. Pour plus d'informations, consultez la section Types de volumes.	28 novembre 2022
Support ajouté pour la copie de balises de volume vers des sauvegardes	Vous pouvez désormais activer `CopyTagsToBackups` l'API AWS CLI ou Amazon FSx pour copier automatiquement les balises de vos volumes vers les sauvegardes. Pour plus d'informations, consultez la section Copie de balises dans des sauvegardes.	28 novembre 2022

Support ajouté pour le choix d'une politique de capture instantanée	Vous pouvez désormais choisir entre trois politiques de capture d'écran intégrées lors de la création ou de la mise à jour d'un volume à l'aide de la console Amazon FSx ou de l' AWS CLI API Amazon FSx. Vous pouvez également sélectionner une politique de capture d'écran personnalisée que vous avez définie dans la CLI ONTAP ou l'API REST. Pour plus d'informations, consultez la section Politiques relatives aux snapshots.	28 novembre 2022
Support ajouté pour une option de capacité de débit supplémentaire du système de fichiers	FSx for ONTAP prend désormais en charge une capacité de débit de 4 096 Mbit/s pour les systèmes de fichiers créés après le 28 novembre 2022 dans les régions USA Est (Ohio), USA Est (Virginie du Nord), USA Ouest (Oregon) et Europe (Irlande). Pour plus d'informa tions, consultez la section Impact de la capacité de débit sur les performances.	28 novembre 2022

Support ajouté pour les IOPS SSD supplémentaires	FSx for ONTAP prend désormais en charge 160 000 IOPS sur SSD pour les systèmes de fichiers créés après le 28 novembre 2022 dans les régions USA Est (Ohio), USA Est (Virginie du Nord), USA Ouest (Oregon) et Europe (Irlande). Pour plus d'informations, consultez la section Impact de la capacité de débit sur les performances.	28 novembre 2022
Support ajouté pour l'utilisation de FSx for ONTAP en tant que banque de données externe pour VMware Cloud on AWS	Vous pouvez utiliser FSx for ONTAP comme banque de données externe pour VMware Cloud sur des centres de données AWS définis par logiciel (SDDC). Cette prise en charge supplémentaire offre la flexibilité nécessaire pour augmenter ou diminuer le stockage indépendamment des ressources de calcul de VMware Cloud sur les AWS charges de travail. Pour plus d'informations, consultez la section Utilisation de VMware Cloud avec FSx pour ONTAP.	30 août 2022

Augmenter automatiquement la capacité de stockage d'un système de fichiers	Utilisez un AWS CloudFormation modèle personnalisable AWS développé pour augmenter automatiquement la capacité de stockage de votre système de fichiers lorsque la capacité de stockage SSD utilisée dépasse un seuil que vous spécifiez. Pour plus d'informations, consultez la section Augmenter dynamiquement la capacité de stockage SSD.	3 juin 2022
Amazon FSx est désormais intégré à AWS Backup	Vous pouvez désormais les utiliser AWS Backup pour sauvegarder et restaurer vos systèmes de fichiers FSx en plus d'utiliser les sauvegardes natives d'Amazon FSx. Pour plus d'informations, consultez Utilisation AWS Backup avec Amazon FSx.	18 mai 2022
Support ajouté pour les déploiements de systèmes de fichiers ONTAP dans une seule zone de disponibilité	Vous pouvez créer des FSx mono-AZ pour les systèmes de fichiers ONTAP, conçus pour fournir une disponibilité et une durabilité élevées au sein d'une seule zone de disponibilité (AZ). Pour plus d'informations, consultez la section Choix du déploiement du système de fichiers.	13 avril 2022

Support ajouté pour les points de AWS PrivateLink terminaison on VPC d'interface	Vous pouvez désormais utiliser les points de terminaison on VPC d'interface pour accéder à l'API Amazon FSx depuis votre VPC sans envoyer de trafic sur Internet. Pour plus d'informations, consultez Amazon FSx et les points de terminaison VPC d'interface.	5 avril 2022
Support ajouté pour modifier la capacité de débit des systèmes de fichiers ONTAP existants	Vous pouvez désormais modifier la capacité de débit disponible pour vos systèmes de fichiers ONTAP existants . Pour plus d'informations, consultez la section Gestion de la capacité de débit.	30 mars 2022
Support ajouté pour la capacité de stockage SSD et la mise à l'échelle des IOPS provisionnées	Vous pouvez désormais augmenter la capacité de stockage SSD et les IOPS provisionnées pour les systèmes de fichiers FSx for ONTAP existants au fur et à mesure de l'évolution de vos besoins en matière de stockage et d'IOPS. Pour plus d'informations, consultez la section Gestion de la capacité de stockage et des IOPS provisionnées.	25 janvier 2022

Support ajouté pour les CloudWatch métriques Amazon	Vous pouvez surveiller votre système de fichiers à l'aide d'Amazon CloudWatch, qui collecte et traite les données brutes de FSx for ONTAP pour en faire des indicateurs lisibles en temps quasi réel. Pour plus d'informations, consultez la section Surveillance avec Amazon CloudWatch.	19 janvier 2022
Support ajouté pour des options de débit supplémentaires du système de fichiers	FSx for ONTAP prend désormais en charge les options de 128 Mo/s et 256 Mo/s pour le débit du système de fichiers. Pour plus d'informations, consultez la section Impact de la capacité de débit sur les performances.	30 novembre 2021
Amazon FSx pour NetApp ONTAP est désormais disponible pour tous	FSx for ONTAP est un service entièrement géré qui fournit un stockage de fichiers hautement fiable, évolutif, performant et riche en fonctionnalités basé sur NetApp le système de fichiers ONTAP. Il fournit les fonctionnalités, les performances, les capacités et les API habituelles des systèmes de NetApp fichiers avec l'agilité, l'évolutivité et la simplicité d'un AWS service entièrement géré.	2 septembre 2021

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.