



Guide de l'utilisateur ONTAP

FSx pour ONTAP



FSx pour ONTAP: Guide de l'utilisateur ONTAP

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d'Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d'une manière susceptible d'entraîner une confusion chez les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est-ce qu'Amazon FSx for NetApp ONTAP ?	1
Caractéristiques de FSx for ONTAP	2
Sécurité et protection des données	3
Outils de surveillance	4
Tarification FSx pour ONTAP	4
FSx pour ONTAP sur AWS re:Post	4
Utilisez-vous Amazon pour la première fois FSx ?	4
Comment ça marche	6
Systèmes de fichiers	6
Machines virtuelles de stockage	6
Volumes	7
Niveaux de stockage	7
Mise à niveau des données	8
Efficacité du stockage	8
Accès à vos données	8
Gestion FSx des ressources ONTAP	9
Premiers pas	10
Configuration	10
Inscrivez-vous pour un Compte AWS	10
Création d'un utilisateur doté d'un accès administratif	11
Étape suivante	12
Créez votre système FSx de fichiers for ONTAP	13
Montage de votre système de fichiers	16
Nettoyage des ressources	17
Régions AWS	19
Accès à vos données	23
Clients pris en charge	24
Utilisation de protocoles de stockage par blocs	25
Accès aux données depuis le AWS Cloud	26
Accès aux données depuis le même VPC	26
Accès aux données depuis un autre VPC	27
Accès aux données sur site	31
Accès à NFS, SMB, ONTAP CLI et API sur site	31
Accès aux points de terminaison entre clusters depuis un environnement local	32

Configurez le routage pour accéder aux systèmes de fichiers multi-AZ depuis l'extérieur de votre VPC	33
Configurer le routage pour accéder aux systèmes de fichiers multi-AZ sur site	34
Montage sur des clients Linux	35
Utilisation de /etc/fstab pour le montage automatique lors du redémarrage de l'instance	37
Montage sur des clients Windows	39
Prérequis	39
Montage sur des clients macOS	40
Provisionnement iSCSI pour Linux	43
Avant de commencer	43
Installation et configuration de l'iSCSI sur l'hôte Linux	46
Configuration de l'iSCSI sur le système de fichiers FSx for ONTAP	47
Montez un LUN iSCSI sur votre client Linux	50
Provisionnement iSCSI pour Windows	56
Configuration de l'iSCSI sur le client Windows	57
Configuration de l'iSCSI sur le système de fichiers FSx for ONTAP	58
Monter un LUN iSCSI sur le client Windows	60
Validation de votre configuration iSCSI	64
Provisionnement de NVMe /TCP pour Linux	65
Avant de commencer	66
Installation et configuration NVMe sur l'hôte Linux	67
Configuration NVMe sur le système de fichiers FSx for ONTAP	67
Monter un NVMe appareil sur votre client Linux	70
Provisionnement NVMe/TCP pour Windows	76
Accès aux données via d'autres AWS services	76
Utilisation d'Amazon WorkSpaces	76
Utilisation d'Amazon ECS	82
Utilisation d'Amazon EVS	86
Utilisation du VMware cloud	86
Disponibilité, durabilité et options de déploiement	87
Choix d'un type de déploiement de système de fichiers	87
Types de déploiement mono-AZ	87
Types de déploiements multi-AZ	89
Choix d'une génération de système de fichiers	90
Processus de basculement FSx pour ONTAP	92
Test du basculement sur un système de fichiers	93

Ressources du réseau	93
Sous-réseaux	93
Interfaces réseau élastiques pour systèmes de fichiers	94
Performances	96
Mesurer les performances	96
Latence	96
Débit et IOPS	96
Support pour SMB, multicanal et NFS nconnect	97
Détails des performances	97
Impact du type de déploiement sur les performances	99
Impact de la capacité de stockage sur les performances	102
Impact de la capacité de débit sur les performances	102
Exemple : capacité de stockage et capacité de débit	109
Administration des ressources	111
Gestion de la capacité de stockage	111
Niveaux de stockage	112
Choix de la capacité de stockage du système de fichiers	113
Capacité de stockage et IOPS du système de fichiers	118
Capacité de stockage en volume	139
Gestion des systèmes de fichiers	165
Ressources du système de fichiers	166
Création de systèmes de fichiers	169
Mise à jour des systèmes de fichiers	184
Gestion des paires HA	187
Gestion du NVMe cache	196
Surveillance des détails du système de fichiers	197
Suppression de systèmes de fichiers	199
Gérer SVMs	199
Nombre maximum de systèmes de fichiers SVMs par système de fichiers	200
Création SVMs	201
Mise à jour SVMs	207
Audit de l'accès aux fichiers	209
Configuration de groupes de travail	222
Surveillance des détails de la SVM	229
Suppression SVMs	229
Gestion des volumes	230

Styles de volume	232
Types de volume	234
Style de sécurité des volumes	235
Création de volumes	236
Mise à jour des volumes	241
Volumes en mouvement	245
Volumes de surveillance	250
Supprimer des volumes	252
Création d'un LUN iSCSI	254
Étapes suivantes	256
Mise à jour des fenêtres de maintenance	256
Gestion de la capacité de débit	258
Quand modifier la capacité de débit	259
Comment les demandes simultanées sont traitées	259
Mise à jour de la capacité de débit	260
Surveillance des variations de capacité de débit	261
Gestion des actions des PME	264
Gérer avec NetApp applications	266
S'inscrire à un NetApp compte	266
Utilisation NetApp BlueXP	267
Utilisation de NetApp ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)	268
Utilisation de ONTAP API REST	272
Balisage de ressources	272
Principes de base des étiquettes	273
Balisage de vos ressources	274
Copier des balises dans les sauvegardes	275
Restrictions liées aux étiquettes	276
Autorisations et balisage	277
Protection de vos données	278
Sauvegarde de volumes	278
Comment fonctionnent les sauvegardes	280
Besoins de stockage	281
Sauvegardes quotidiennes automatiques	281
Sauvegardes initiées par l'utilisateur	282
Copier des balises dans les sauvegardes	282
En utilisant AWS Backup	283

Restauration des sauvegardes	284
Performances de sauvegarde	286
Sauvegarde de SnapLock volumes	287
Création de sauvegardes initiées par l'utilisateur	287
Restauration des sauvegardes	288
Restauration d'un sous-ensemble de données	292
Surveillance de la progression de la restauration des volumes	293
Suppression de sauvegardes	295
Utilisation de captures d'écran de volume	297
Règles relatives aux snapshots	298
Restaurer des fichiers à partir de snapshots	299
Affichage de l'instantané commun	300
Mettre à jour l'espace réservé aux instantanés	301
Désactivation des instantanés automatiques	301
Suppression d'instantanés	303
Suppression d'instantanés	304
Réserve d'instantanés	306
Protection des données grâce à une protection autonome contre les ransomwares	307
Comment fonctionne l'ARP	307
Ce que recherche ARP	308
Comment répondre à une attaque présumée avec l'ARP	308
Activation de l'ARP	309
Répondre aux alertes ARP	312
Comprendre les alertes EMS pour l'ARP	314
Protéger les données avec SnapLock	315
Comment ? SnapLock fonctionnement	316
Compréhension SnapLock Conformité d'	321
Compréhension SnapLock Enterprise	322
Comprendre le SnapLock période de conservation	323
Valider des fichiers dans WORM	326
Répliquer vos données avec FlexCache	331
Fonctionnement d'FlexCache	332
FlexCachemodes d'écriture	332
FlexCacheaperçu de la création de volumes	333
Création d'un FlexCache	333
Utilisation SnapMirror pour une réplication planifiée	339

Utilisation NetApp BlueXP pour planifier la réplication	340
Utilisation de ONTAP CLI pour planifier la réplication	340
Rapports d'utilisation et de facturation	341
FSx pour le rapport de facturation ONTAP	341
FSx pour le rapport d'utilisation d'ONTAP	345
Surveillance des systèmes de fichiers	350
Surveillance avec CloudWatch	351
Accès aux CloudWatch métriques	352
Surveillance dans la FSx console Amazon	354
Métriques du système de fichiers	367
Métriques du système de fichiers de deuxième génération	390
Métriques de volume	409
Surveillance des événements EMS	419
Vue d'ensemble des événements EMS	419
Affichage des événements EMS	420
Transfert d'événements EMS vers un serveur Syslog	427
Surveillance à l'aide d'informations sur l'infrastructure de données	429
Surveillance avec Harvest et Grafana	430
Commencer à utiliser Harvest et Grafana	431
Tableaux de bord Harvest pris en charge	431
Non pris en charge Harvest tableaux de bord	432
AWS CloudFormation modèle	432
Types d' EC2 instances Amazon	433
Procédure de déploiement	434
Connexion à Grafana	437
Résolution des problèmes liés à Harvest et Grafana	438
Surveillance avec AWS CloudTrail	441
FSx Informations Amazon dans CloudTrail	441
Comprendre les entrées du fichier FSx journal Amazon	443
Utilisation d'Active Directory	445
Conditions préalables à l'autogestion d'Active Directory	446
Exigences relatives à l'autogestion d'Active Directory	446
Exigences en matière de configuration du réseau	446
Exigences relatives aux comptes de service Active Directory	448
Meilleures pratiques d'autogestion d'Active Directory	450
Délégation d'autorisations à votre compte de FSx service Amazon	450

Maintenir une configuration AD à jour	451
Limiter le trafic au sein d'un VPC avec des groupes de sécurité	452
Création de règles de groupes de sécurité sortants	452
Comment fonctionne SVMs l'adhésion à Active Directory	452
Informations Active Directory nécessaires	453
Gestion des configurations Active Directory des SVM	455
SVMs Adhérer à Active Directory	455
Mise à jour des configurations Active Directory	458
Mise à jour des configurations Active Directory avec la NetApp CLI	460
Migration vers Amazon FSx	466
Migration à l'aide de SnapMirror	466
Avant de commencer	468
Créez le volume de destination	470
Enregistrez l'inter-cluster source et de destination LIFs	471
Établissez le peering du cluster entre la source et la destination	472
Création d'une relation de peering avec la SVM	473
Créez la SnapMirror relation	474
Transférez des données vers votre FSx système de fichiers for ONTAP	475
Passons à Amazon FSx	475
Migration de fichiers avec AWS DataSync	477
Prérequis	478
DataSync étapes de base de la migration	478
Sécurité	480
Protection des données	481
Chiffrement des données dans FSx ONTAP	482
Chiffrement au repos	482
chiffrement des données en transit	485
Gestion des identités et des accès	507
Public ciblé	508
Authentification par des identités	508
Gestion des accès à l'aide de politiques	512
FSx pour ONTAP et IAM	515
Exemples de politiques basées sur l'identité	522
Dépannage IAM	525
Utilisation des rôles liés à un service	527
Utiliser des tags avec Amazon FSx	532

AWS politiques gérées	539
Amazon FSx ServiceRolePolicy	539
Amazon FSx DeleteServiceLinkedRoleAccess	539
Amazon FSx FullAccess	540
Amazon FSx ConsoleFullAccess	541
Amazon FSx ConsoleReadOnlyAccess	542
Amazon FSx ReadOnlyAccess	543
Mises à jour des politiques	543
Contrôle d'accès au système de fichiers avec Amazon VPC	556
Groupes de sécurité Amazon VPC	556
Validation de la conformité	559
Points de terminaison de VPC d'Interface	561
Considérations relatives aux points de terminaison FSx VPC de l'interface Amazon	561
Création d'un point de terminaison VPC d'interface pour Amazon API FSx	562
Création d'une politique de point de terminaison VPC pour Amazon FSx	562
Résilience	563
Sauvegarde et restauration	563
Instantanés	563
Zones de disponibilité	564
Sécurité de l'infrastructure	564
Utilisation d'un logiciel antivirus	565
ONTAP rôles et utilisateurs	566
Rôles et utilisateurs de l'administrateur du système de fichiers	566
Rôles et utilisateurs de l'administrateur de la SVM	567
Authentification des ONTAP utilisateurs avec Active Directory	570
Création de nouveaux ONTAP utilisateurs pour l'administration du système de fichiers et des SVM	571
Création d'utilisateurs ONTAP	572
Création de rôles de SVM	575
Configuration de l'authentification Active Directory pour ONTAP les utilisateurs	576
Configuration de l'authentification par clé publique	579
Mise à jour des exigences en matière	580
La mise à jour du mot de passe du fsxadmin compte échoue	581
Quotas	583
Les quotas que vous pouvez augmenter	583
Quotas de ressources pour chaque système de fichiers	585

Résolution des problèmes	591
Systèmes de fichiers mal configurés	591
Partage VPC désactivé	591
Impossible de créer un système de fichiers multi-AZ	592
Niveau SSD plein à plus de 90 %	592
Vous ne pouvez pas accéder à votre système de fichiers	593
Balises de table de routage manquantes	594
Trop de routes	594
Routes manquantes vers les serveurs	594
ENI modifié ou supprimé	595
ENI supprimée	595
Règles de trafic entrant manquantes	595
Règles sortantes manquantes	595
Le sous-réseau de l'instance de calcul n'utilise aucune des tables de routage associées à votre système de fichiers	596
Impossible de mettre à jour la table de routage multi-AZ	596
Impossible d'accéder à iSCSI	597
Sous-réseau VPC non partagé	597
NFS, SMB, ONTAP CLI et API inaccessibles depuis différents VPC et sur site	597
SVM mal configurée	597
Votre SVM possède un volume hors ligne	598
Votre SVM possède un volume hors ligne doté d'un LUN iSCSI ou d'un espace de noms / TCP NVMe	598
Impossible de joindre SVM à AD	598
Nom NetBIOS de la SVM identique à celui du domaine d'origine	599
La SVM est jointe à un autre AD	600
Nom NetBIOS de la SVM déjà utilisé	600
FSx Impossible d'atteindre les contrôleurs de domaine AD	601
Configuration de port ou autorisations de compte de service insuffisantes	601
Informations d'identification du compte de service non valides	602
Amazon ne FSx peut pas se connecter à vos contrôleurs de domaine Active Directory en raison d'identifiants de compte de service insuffisants	602
Impossible d'atteindre les serveurs DNS ou les contrôleurs de domaine AD	603
Nom de domaine AD non valide	605
Le compte de service ne peut pas accéder au groupe d'administrateurs AD	606
L'unité d'organisation spécifiée n'est pas valide	607

Impossible de supprimer la SVM ou le volume	607
Identification des suppressions échouées	608
Suppression de la SVM : les tables de routage sont inaccessibles	609
Suppression de la SVM : relation avec les pairs	611
Suppression d'une SVM ou d'un volume : SnapMirror	612
Suppression de la SVM : LIF compatible avec Kerberos	613
Suppression de la SVM : autre raison	615
Suppression d'un volume : FlexCache relation	617
Volume mal configuré	618
Volume plein à plus de 98 %	618
Le volume de stockage par blocs est hors ligne	618
Hors connexion FlexCache volume d'origine	619
Volume hors ligne avec SnapMirror relation	619
Le volume de stockage par blocs est limité	620
Volume FlexCache d'origine restreint	620
Volume restreint avec SnapMirror relation	621
Le volume dispose d'un espace de stockage insuffisant	621
Déterminez comment votre capacité de stockage en volume est utilisée	622
Augmenter la capacité de stockage d'un volume	622
Utilisation du dimensionnement automatique du volume	622
Le stockage principal de votre système de fichiers est plein	622
Suppression d'instantanés	623
Augmenter la capacité maximale de fichiers d'un volume	623
Sauvegardes de volumes échouées	624
Résolution des problèmes de réseau	624
Vous souhaitez capturer une trace de paquet	624
Historique de la documentation	628
.....	dclii

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 extrêmement 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 AWS ou sur site. 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 des niveaux de performance 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 durable et hautement disponible 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, ONTAP est la solution idéale FSx pour migrer, sauvegarder ou transférer en rafale vos applications basées sur des fichiers depuis le site 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 développement d'un stockage de fichiers partagé fiable, performant et sécurisé dans le cloud. Avec FSx 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) WorkSpaces, Amazon, AWS Key Management Service (AWS KMS) et. AWS CloudTrail

Rubriques

- [Caractéristiques de FSx for ONTAP](#)
- [Sécurité et protection des données](#)
- [Outils de surveillance](#)
- [Tarification FSx pour ONTAP](#)
- [FSx pour ONTAP sur AWS re:Post](#)
- [Utilisez-vous Amazon pour la première fois FSx ?](#)

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 (GBps) de [débit](#) par système de fichiers
- [Accès multiprotocole aux données à l'aide des](#) protocoles NFS (Network File System), SMB (Server Message Block), iSCSI (Internet Small Computer Systems Interface) et Non-Volatile Memory Express (NVMe)
- 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
- Prise en charge de NetApp's [SnapMirror](#) fonction de réplication

- Prise en charge de NetApp solutions de mise en cache sur site : NetApp Global File Cache et FlexCache
- Support pour l'accès et la gestion en mode natif AWS ou NetApp outils et opérations d'API
 - AWS Management Console, AWS Command Line Interface (AWS CLI), et SDKs
 - [NetApp CLI ONTAP, API REST et BlueXP](#)

Sécurité et protection des données

Le modèle de responsabilité partagée est utilisé en ce qui concerne [Sécurité dans Amazon FSx pour NetApp ONTAP](#). Amazon FSx fournit plusieurs niveaux de sécurité et de [conformité](#) pour faciliter la protection de vos données.

FSx for ONTAP prend en charge les fonctionnalités de protection des données, de sécurité et de contrôle d'accès suivantes :

- [Chiffrement des données au repos](#) pour les données du système de fichiers et les sauvegardes à l'aide de AWS KMS keys
- Chiffrer les données en transit à l'aide de :
 - [Kerberos pour PME](#)
 - [IPSEC](#)
 - [Chiffrement basé sur Nitro](#)
- [Analyse antivirus](#) à la demande
- Authentification et autorisation à l'aide de [Microsoft Active Directory](#)
- [Audit d'accès aux fichiers](#)
- [NetApp SnapLock](#) WORM avec modes de conformité et de rétention d'entreprise

Pour plus d'informations, consultez [Protection des données dans Amazon FSx pour NetApp ONTAP](#) et [Protection de vos données](#).

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 de plus amples informations, veuillez consulter [Protection de vos données](#).

Outils de surveillance

Les outils de surveillance incluent [CloudWatchCloudTrail](#), [ONTAP événements EMS](#), [NetApp Informations sur l'infrastructure de données](#), et [NetApp Récolte](#).

Tarification FSx pour 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 [] -mois) MBps
- 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 les prix et les frais associés à ce service, consultez la page de [tarification Amazon FSx for NetApp ONTAP](#).

FSx pour ONTAP sur AWS re:Post

Si vous rencontrez des problèmes lors de l'utilisation d'Amazon FSx, [AWS re:Post](#)utilisez-le pour obtenir des réponses à vos questions FSx pour ONTAP.

Utilisez-vous Amazon pour la première fois FSx ?

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

1. Si vous êtes nouveau dans le AWS domaine, [Configuration d' FSx ONTAP](#) voir pour configurer un Compte AWS.
2. Si vous êtes prêt à créer votre premier système de FSx fichiers Amazon, suivez les instructions figurant dans[Commencer à utiliser Amazon FSx pour NetApp ONTAP](#).
3. Pour plus d'informations sur les performances, consultez [Amazon FSx pour les performances d' NetApp ONTAP](#).

4. Pour plus d'informations sur FSx la sécurité d'Amazon, consultez [Sécurité dans Amazon FSx pour NetApp ONTAP](#).
5. Pour plus d'informations sur l' FSx API Amazon, consultez le manuel [Amazon FSx API Reference](#).

Comment fonctionne Amazon FSx pour NetApp ONTAP

Cette rubrique présente les principales fonctionnalités des systèmes de fichiers Amazon FSx pour NetApp ONTAP et leur fonctionnement, avec des liens vers des sections contenant des descriptions détaillées, des informations importantes sur la mise en œuvre et des procédures step-by-step de configuration.

Rubriques

- [FSx pour les systèmes de fichiers ONTAP](#)
- [Machines virtuelles de stockage](#)
- [Volumes](#)
- [Niveaux de stockage](#)
- [Efficacité du stockage](#)
- [Accès aux données stockées dans les FSx systèmes de fichiers ONTAP](#)
- [Gestion FSx des ressources ONTAP](#)

FSx pour les systèmes de fichiers ONTAP

Un système de fichiers est la ressource principale 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 de plus amples informations, veuillez consulter [Gestion des FSx 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 ONTAP de première génération FSx et les systèmes de fichiers multi-AZ de deuxième génération prennent en charge une paire HA. Les systèmes de fichiers mono-AZ de deuxième génération prennent en charge jusqu'à 12 paires HA. Pour de plus amples informations, veuillez consulter [Gestion des paires de 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 de plus amples informations, veuillez consulter [Gérer SVMs](#).

Vous pouvez vous connecter SVMs à un Microsoft Active Directory pour l'authentification et l'autorisation d'accès aux fichiers. Pour de plus amples informations, veuillez consulter [Utilisation de Microsoft Active Directory dans FSx ONTAP](#).

Volumes

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

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 .

FSx pour ONTAP, les volumes 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 de plus amples informations, veuillez consulter [Gestion FSx des volumes ONTAP](#).

Niveaux de stockage

Un système de fichiers FSx pour ONTAP possède deux niveaux de stockage : le stockage principal et le stockage en 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 de plus amples informations, veuillez consulter [FSx pour les niveaux de stockage ONTAP](#).

Mise à niveau des données

La hiérarchisation des données est le processus par lequel Amazon FSx for NetApp 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 de plus amples informations, veuillez consulter [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 de plus amples informations, veuillez consulter [Efficacité du stockage](#).

Accès aux données stockées dans les FSx systèmes de fichiers ONTAP

Vous pouvez accéder à vos données sur FSx des volumes 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 de bloc Non-Volatile Memory Express (NVMe) et iSCSI (Internet Small Computer Systems Interface). Pour de plus amples informations, veuillez consulter [Accès à vos données FSx for ONTAP](#).

Gestion FSx des ressources 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 pour ONTAP en utilisant à la fois les outils de gestion ONTAP AWS et les outils de gestion NetApp ONTAP :

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

Pour de plus amples informations, veuillez consulter [Administration des ressources](#).

Commencer à utiliser Amazon FSx pour NetApp ONTAP

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

1. Inscrivez-vous Compte AWS et créez un utilisateur administratif dans le compte.
2. Créez un système de fichiers Amazon FSx for NetApp ONTAP à l'aide de la FSx console Amazon.
3. Montez votre système de fichiers à partir d'une instance Amazon EC2 Linux.
4. Nettoyez les ressources que vous avez créées.

Rubriques

- [Configuration d' FSx ONTAP](#)
- [Création d'un système de fichiers Amazon FSx for NetApp ONTAP](#)
- [Montage de votre système de fichiers à partir d'une instance Amazon EC2 Linux](#)
- [Nettoyage des ressources](#)

Configuration d' FSx 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](#)
- [Création d'un utilisateur doté d'un accès administratif](#)
- [Étape suivante](#)

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 l'<https://portal.aws.amazon.com/billing/inscription>.
2. Suivez les instructions en ligne.

Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique ou un SMS 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 AWS est créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les [tâches nécessitant un accès utilisateur racine](#).

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

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif 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 Console](#) tant 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, voir [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, octroyez 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.

Connexion en tant qu'utilisateur doté 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.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

Pour obtenir des instructions, consultez [Création d'un ensemble d'autorisations](#) dans le Guide de l'utilisateur AWS IAM Identity Center .

2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

Pour obtenir des instructions, consultez [Ajout de groupes](#) dans le Guide de l'utilisateur AWS IAM Identity Center .

Étape suivante

Pour commencer à utiliser FSx for ONTAP, consultez les instructions [Commencer à utiliser Amazon FSx pour NetApp ONTAP](#) pour créer vos FSx ressources Amazon.

Création d'un système de fichiers Amazon FSx for NetApp ONTAP

La FSx console Amazon 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 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 SVMs des volumes supplémentaires selon vos besoins, notamment une SVM associée à un Active Directory pour autoriser l'accès des clients Windows et macOS via le protocole SMB (Server Message Block). Vous pouvez également ajouter des paires de haute disponibilité (HA) supplémentaires en fonction du type de déploiement que vous choisissez et du nombre de paires HA que vous ajoutez lors de la création.

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, consultez [Création de systèmes de fichiers](#).

Pour créer votre système de fichiers .

1. Ouvrez la FSx console Amazon 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 for 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 de plus amples informations, veuillez consulter [Disponibilité, durabilité et options de déploiement](#).

 Note

La dernière génération FSx de système de fichiers ONTAP disponible pour vous Région AWS est sélectionnée par défaut. Vous pouvez spécifier la génération de votre système de fichiers (si disponible Régions AWS) avec l'option de création standard. Pour de plus amples informations, veuillez consulter [Création de systèmes de fichiers](#).

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 1 048 576. Pour de plus amples informations, veuillez consulter [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 de plus amples informations, veuillez consulter [Gestion de la capacité de stockage](#).

8. Pour ce qui est de la capacité de débit, Amazon fournit FSx 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 73 728 MBps selon le type de déploiement et le nombre de paires HA).
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' FSx Amazon 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 adresses IP SVMs 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. 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 et qu'elle n'est pas déjà utilisée par un autre système de fichiers avec le même VPC et les mêmes tables de routage. Nous vous recommandons d'utiliser une plage comprise dans la plage d'adresses IP du VPC.

 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 [Mise à jour des systèmes de fichiers](#)

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 composé d'une SVM (nommée `fsx`) et d'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.

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

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 EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Créez ou sélectionnez une EC2 instance Amazon exécutant Amazon Linux 2 qui se trouve 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 EC2 l'utilisateur Amazon.
3. Connectez-vous à votre instance Amazon EC2 Linux. Pour plus d'informations, consultez [Connect to your Linux instance](#) dans le guide de EC2 l'utilisateur Amazon.
4. Ouvrez un terminal sur votre EC2 instance Amazon à l'aide du protocole Secure Shell (SSH) et connectez-vous avec les informations d'identification appropriées.
5. Créez un répertoire sur votre EC2 instance Amazon 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 car 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 FSx console Amazon 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.
- *volume-junction-path*— Le chemin de jonction du volume que vous montez. Vous pouvez trouver le chemin de jonction d'un volume dans la FSx console Amazon dans le panneau Résumé de la page des détails du volume.
- *mount-point*— Le nom du répertoire que vous avez créé sur votre EC2 instance 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 EC2 instance Amazon (tels que l'expiration du délai de connexion), consultez la section [Résolution des problèmes liés aux EC2 instances](#) dans le guide de l'EC2 utilisateur Amazon.

Nettoyage des 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 EC2 console Amazon, mettez fin à votre instance. Pour plus d'informations, consultez [Résilier votre instance](#) dans le guide de EC2 l'utilisateur Amazon.
2. Ouvrez la FSx console Amazon à l'adresse <https://console.aws.amazon.com/fsx/>.

3. Sur la FSx console Amazon, supprimez tous les volumes FSx for ONTAP qui ne sont pas les volumes racine de votre SVM. Pour de plus amples informations, veuillez consulter [Supprimer des volumes](#).
4. Supprimez tous vos fichiers FSx pour ONTAP SVMs. Pour de plus amples informations, veuillez consulter [Suppression de machines virtuelles de stockage \(SVM\)](#).
5. Sur la FSx console Amazon, 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 passe à 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. Maintenez la case à cocher sélectionnée pour les IDs sauvegardes que vous souhaitez supprimer, puis choisissez Supprimer les sauvegardes.

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

Disponibilité par Région AWS

Les systèmes de fichiers Amazon FSx pour NetApp ONTAP sont disponibles dans les versions suivantes Régions AWS, avec une prise en charge des types de déploiement indiquée pour chaque région :

Région AWS	Mono-AZ 1	Multi-AZ 1	Mono-AZ 2	Multi-AZ 2		
USA Est (Virginie du Nord)	✓	✓	✓	✓		
USA Est (Ohio)	✓	✓	✓	✓		
USA Ouest (Californie du Nord)	✓	✓	✓	✓		
US West (Oregon)	✓	✓	✓	✓		
AWS GovCloud (USA Est)	✓	✓				
AWS GovCloud (US-Ouest)	✓	✓				
Afrique (Le Cap)	✓	✓				
Asie-Pacifique (Hong Kong)	✓	✓				

Région AWS	Mono-AZ 1	Multi-AZ 1	Mono-AZ 2	Multi-AZ 2		
Asie-Pacifique (Tokyo)	✓	✓	✓	✓		
Asie-Pacifique (Séoul)	✓	✓				
Asie-Pacifique (Osaka)	✓	✓				
Asie-Pacifique (Mumbai)	✓	✓	✓	✓		
Asie-Pacifique (Hyderabad)	✓	✓				
Asie-Pacifique (Singapour)	✓	✓	✓	✓		
Asie-Pacifique (Sydney)	✓	✓	✓	✓		
Asie-Pacifique (Jakarta)	✓	✓				

Région AWS	Mono-AZ 1	Multi-AZ 1	Mono-AZ 2	Multi-AZ 2		
Asie-Pacifique (Melbourne)	✓	✓				
Asie-Pacifique (Malaisie)	✓	✓				
Asie-Pacifique (Thaïlande)	✓	✓				
Canada (Centre)	✓	✓				
Canada-Ouest (Calgary)	✓	✓				
Europe (Francfort)	✓	✓	✓	✓		
Europe (Zurich)	✓	✓				
Europe (Stockholm)	✓	✓	✓	✓		
Europe (Milan)	✓	✓				
Europe (Espagne)	✓	✓				

Région AWS	Mono-AZ 1	Multi-AZ 1	Mono-AZ 2	Multi-AZ 2		
Europe (Irlande)	✓	✓	✓	✓		
Europe (Londres)	✓	✓				
Europe (Paris)	✓	✓				
Israël (Tel Aviv)	✓	✓				
Mexique (centre)	✓	✓				
Moyen-Orient (EAU)	✓	✓				
Moyen-Orient (Bahreïn)	✓	✓				
Amérique du Sud (São Paulo)	✓	✓				

Accès à vos données FSx for ONTAP

Vous pouvez accéder à vos systèmes de FSx fichiers Amazon à l'aide de divers clients et méthodes pris en charge, à la fois dans l'environnement 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 la prise en charge du stockage par blocs partagé.
- **Nvme**— Pour la connexion à l'aide du Non-Volatile Memory Express (NVMe) TCP/IP pour la prise en charge du stockage par blocs partagé.
- **Management**— Pour la gestion à SVMs l'aide de la CLI ou de l'API NetApp ONTAP, ou NetApp de BlueXP

Note

Le protocole iSCSI est disponible sur tous les systèmes de fichiers dotés de 6 [paires de haute disponibilité \(HA\)](#) ou moins. Le NVMe/TCP protocole est disponible sur les systèmes de fichiers de deuxième génération comportant 6 paires HA ou moins.

Rubriques

- [Clients pris en charge](#)
- [Utilisation de protocoles de stockage par blocs](#)
- [Accès aux données depuis le AWS Cloud](#)
- [Accès aux données sur site](#)
- [Configurez le routage pour accéder aux systèmes de fichiers multi-AZ depuis l'extérieur de votre VPC](#)
- [Configurer le routage pour accéder aux systèmes de fichiers multi-AZ sur site](#)
- [Montage de volumes sur des clients Linux](#)

- [Montage de volumes sur les clients Microsoft Windows](#)
- [Montage de volumes sur des clients macOS](#)
- [Provisionnement iSCSI pour Linux](#)
- [Provisionnement iSCSI pour Windows](#)
- [Provisionnement de NVMe /TCP pour Linux](#)
- [Provisionnement NVMe/TCP pour Windows](#)
- [Accès aux données via d'autres AWS services](#)

Clients pris en charge

FSx pour que les systèmes de fichiers ONTAP prennent en charge l'accès 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 détache FSx automatiquement toute adresse IP élastique qui est une adresse IP publique accessible depuis Internet et qui est attachée à l'interface Elastic Network d'un système de fichiers.

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

- Instances Amazon Elastic Compute Cloud (Amazon EC2) exécutant Linux avec prise en charge NFS ou SMB, Microsoft Windows et macOS. Pour plus d'informations [Montage de volumes sur des clients Linux](#)[Montage de volumes sur les clients Microsoft Windows](#), voir et [Montage de volumes sur des clients macOS](#).
- Conteneurs Docker Amazon Elastic Container Service (Amazon ECS) sur les instances EC2 Amazon Windows et Linux. Pour de plus amples informations, veuillez consulter [Utilisation d'Amazon Elastic Container Service avec FSx for ONTAP](#).
- Amazon Elastic Kubernetes Service — Pour en savoir plus, consultez le pilote Amazon [NetApp for ONTAP CSI dans le guide de l'utilisateur FSx 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 de plus amples informations, veuillez consulter [Utiliser Amazon WorkSpaces avec FSx for 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 (VMs) exécutées dans le 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 d'Amazon pour ONTAP sur le VMware cloud AWS avec Amazon FSx pour NetApp ONTAP](#).

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

Utilisation de protocoles de stockage par blocs

Amazon FSx for NetApp ONTAP prend en charge l'interface iSCSI (Internet Small Computer Systems Interface) et Non-Volatile Memory Express NVMe () via TCP NVMe/TCP) block storage protocols. In Storage Area Network (SAN) environments, storage systems are targets that have storage target devices. For iSCSI, the storage target devices are referred to as logical units (LUNs). For NVMe/TCP (les périphériques de stockage cibles sont appelés espaces de noms).

Vous utilisez l'interface logique iSCSI (LIF) d'une SVM pour vous connecter à la fois au stockage par blocs iSCSI NVMe et au stockage par blocs iSCSI.

Vous configurez le stockage en créant LUNs pour iSCSI et en créant des espaces de noms pour. NVMe LUNs et les espaces de noms sont ensuite accessibles aux hôtes à l'aide des protocoles iSCSI ou TCP.

Pour plus d'informations sur la configuration de l'iSCSI et du stockage par NVMe/TCP blocs, consultez :

- [Provisionnement iSCSI pour Linux](#)

- [Provisionnement iSCSI pour Windows](#)
- [Provisionnement de NVMe /TCP pour Linux](#)
- [Provisionnement NVMe/TCP pour Windows](#)

 Note

Le provisionnement NVMe/TCP pour Windows nécessite l'utilisation d'un NVMe initiateur tiers.

Accès aux données depuis le AWS Cloud

Chaque système de FSx fichiers Amazon 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 à partir d'autres VPCs AWS comptes ou Régions AWS. Outre les exigences décrites dans les sections suivantes concernant l'accès FSx aux ressources 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, consultez [Groupes de sécurité Amazon VPC](#).

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. Tous SVMs les volumes associés au système de fichiers Amazon FSx for NetApp 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.

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 FSx console Amazon, choisissez 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 FSx d'un système de fichiers ONTAP à partir d' 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

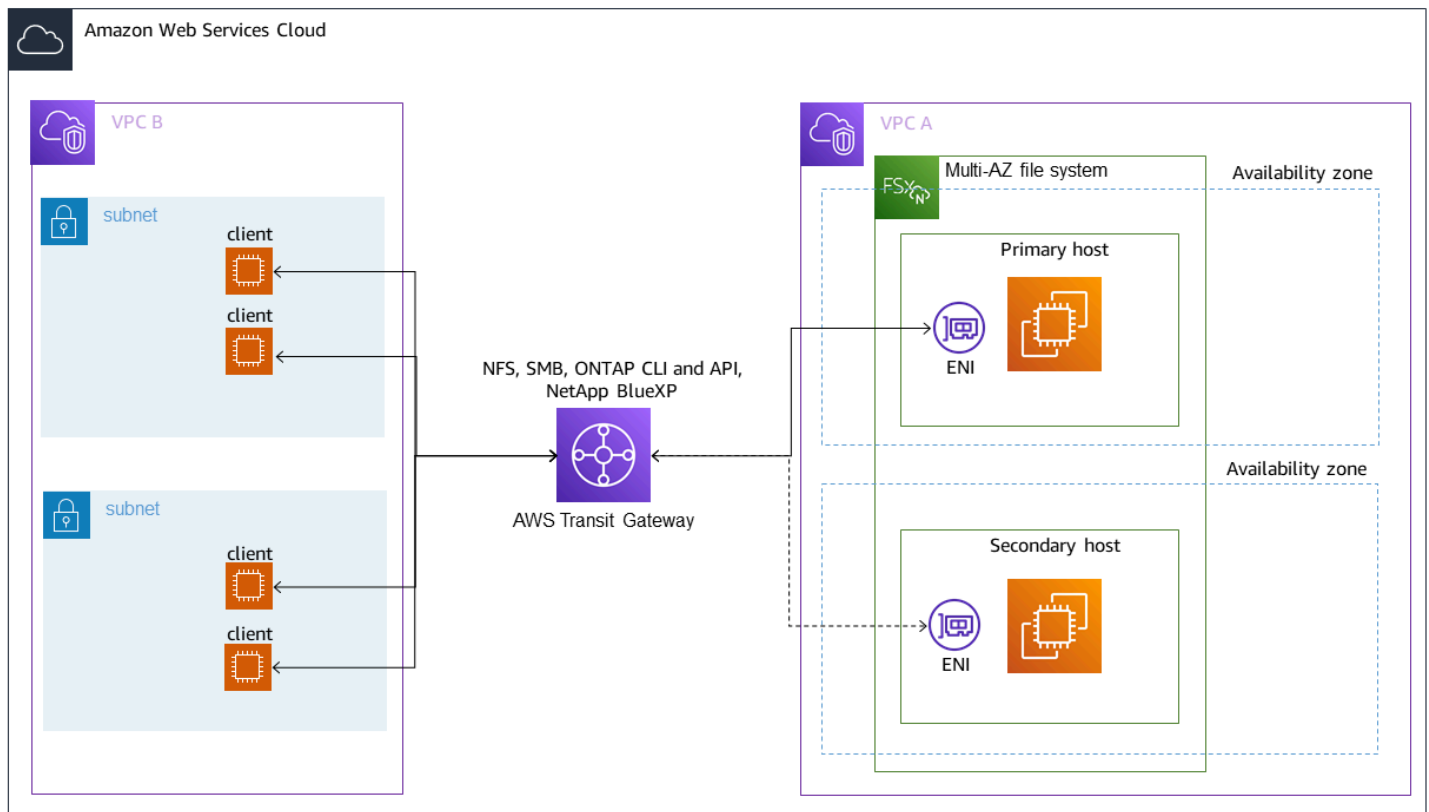
Les points de terminaison de gestion NFS, SMB et ONTAP sur FSx Amazon NetApp pour les systèmes de fichiers ONTAP Multi-AZ utilisent des adresses IP flottantes afin que les clients connectés puissent effectuer une transition fluide entre les serveurs de fichiers préférés et de secours lors d'un incident de basculement. Pour plus d'informations sur les basculements, consultez [Processus de basculement FSx pour 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 FSx console Amazon utilisent par défaut les 64 dernières adresses IP de la plage CIDR principale du VPC pour le système de `EndpointIpAddressRange` fichiers.
- Les systèmes de fichiers multi-AZ créés à l'aide de l' FSx API Amazon AWS CLI ou de l'API Amazon utilisent `EndpointIpAddressRange` par défaut une plage d'`198.19.0.0/16` adresses IP comprise dans le bloc d'adresses.
- Vous pouvez également spécifier votre propre plage d'adresses IP lorsque vous utilisez l'option de création standard. 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 et qu'elle n'est pas déjà utilisée par un autre système de fichiers avec le même VPC et les mêmes tables de routage. Pour cette option, nous recommandons d'utiliser une plage comprise dans la plage d'adresses IP du VPC.

Ne [AWS Transit Gateway](#) prend 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 [Mise à jour des systèmes de fichiers](#)

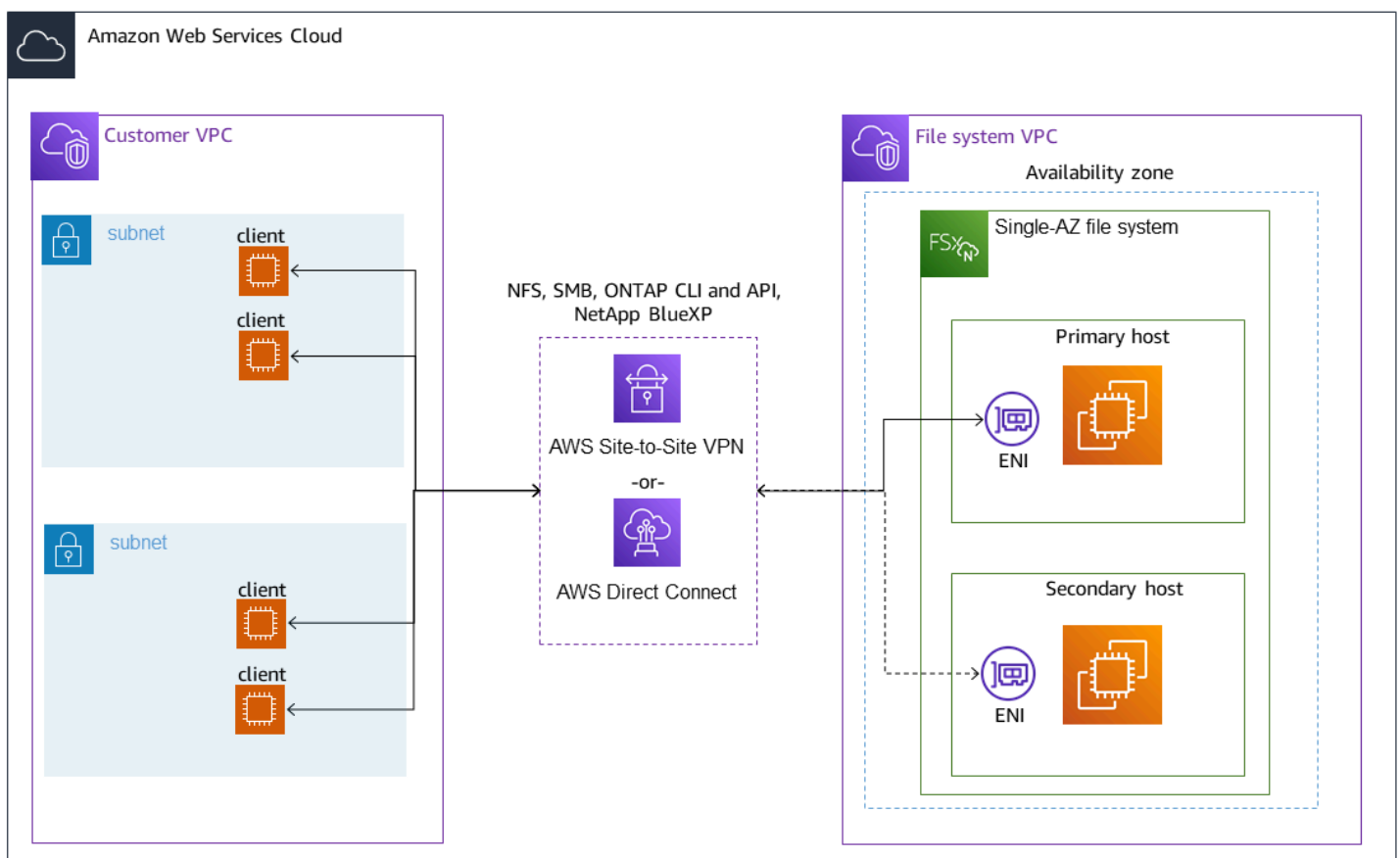
Pour savoir dans quels cas vous devez utiliser Transit Gateway FSx pour accéder à votre système de fichiers ONTAP, consultez [Quand est-ce que Transit Gateway est requis ?](#).

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 FSx des systèmes de fichiers ONTAP Multi-AZ, AWS CloudFormation nous vous recommandons d'ajouter la `Key: AmazonFSx; Value: ManagedByAmazonFSx` balise manuellement.

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 FSx pour accéder aux 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'appariage 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 FSx via NFS, SMB ou l'API REST NetApp ONTAP, CLI ou BlueXP	Uniquement si : • Accès depuis un réseau pair (sur site, par exemple), et • Vous n'y accédez pas FSx par le biais d'une instance NetApp FlexCache ou d'une instance de Global File Cache
Accès aux données via iSCSI	Non
Accès aux données via NVMe	Non
Joindre une SVM à un Active Directory	Non
SnapMirror	Non
FlexCache Mise en cache	Non
Cache de fichiers global	Non

Accès NVMe, points de terminaison iSCSI et inter-clusters en dehors du VPC de déploiement

Vous pouvez utiliser le peering VPC ou accéder AWS Transit Gateway aux points de terminaison de votre système de fichiers, NVMe iSCSI et inter-clusters depuis l'extérieur du VPC de déploiement du système de fichiers. Vous pouvez utiliser le peering VPC pour acheminer le trafic NVMe iSCSI et entre les clusters. VPCs Une connexion d'appairage VPC est une connexion réseau entre deux personnes VPCs, utilisée pour acheminer le trafic entre elles à l'aide d'adresses privées. IPv4 Vous pouvez utiliser le peering VPC pour vous connecter au VPCs sein d'un même système Région AWS 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 VPN](#)et [AWS Direct Connect](#); des instructions d'utilisation plus spécifiques sont disponibles dans les sections suivantes. Outre les exigences répertoriées ci-dessous pour accéder aux différentes FSx ressources ONTAP depuis les locaux, 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 de la CLI et de l'API REST NFS, SMB et ONTAP à partir de locaux

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

Accès aux systèmes de fichiers multi-AZ sur site

Amazon FSx exige que vous utilisiez AWS Transit Gateway ou configuriez le NetApp Global File Cache à distance 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 de disponibilité 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 Gateway](#) conjointement 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. `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 FSx console Amazon utilisent par défaut les 64 dernières adresses IP de la plage CIDR principale du VPC pour le système de `EndpointIpAddressRange` fichiers.
- Les systèmes de fichiers multi-AZ créés à l'aide de l' FSx API Amazon AWS CLI ou de l'API Amazon utilisent `EndpointIpAddressRange` par défaut une plage d'`198.19.0.0/16` adresses IP comprise dans le bloc d'adresses.

- Vous pouvez également spécifier votre propre plage d'adresses IP lorsque vous utilisez l'option de création standard dans la FSx console Amazon. La plage d'adresses IP que vous choisissez peut se situer à l'intérieur ou à l'extérieur de la plage d'adresses IP du VPC, à condition qu'elle ne chevauche aucun sous-réseau et qu'elle n'est pas déjà utilisée par un autre système de fichiers avec le même VPC et les mêmes tables de routage. Pour cette option, nous recommandons d'utiliser une plage comprise dans la plage d'adresses IP du VPC.

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 de plus amples informations, veuillez consulter [Processus de basculement FSx pour 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.

Pour de plus amples informations, veuillez consulter [Configurer le routage pour accéder aux systèmes de fichiers multi-AZ sur site](#).

Accès aux systèmes de fichiers mono-AZ depuis un système sur site

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 entre clusters depuis un environnement local

FSx pour ONTAP, les points de terminaison inter-clusters sont dédiés au trafic de réplication entre les systèmes de fichiers NetApp ONTAP, y compris entre les déploiements sur site et pour NetApp ONTAP. FSx Le trafic de réplication inclut SnapMirror FlexCache, et FlexClone les relations entre les machines virtuelles de stockage (SVMs) et les volumes de différents systèmes de fichiers, ainsi que

le cache de fichiers NetApp global. 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 pour 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.

Pour de plus amples informations, veuillez consulter [Configurer le routage pour accéder aux systèmes de fichiers multi-AZ sur site](#).

Configurez le routage pour accéder aux systèmes de fichiers multi-AZ 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 IP de votre VPC, vous devez configurer un routage supplémentaire pour accéder à votre système de fichiers AWS Transit Gateway à partir de réseaux homologues 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 FSx console Amazon à l'adresse <https://console.aws.amazon.com/fsx/>.

2. Choisissez le FSx système de fichiers 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, consultez [Mise à jour des systèmes 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.

Configurer le routage pour accéder aux systèmes de fichiers multi-AZ sur site

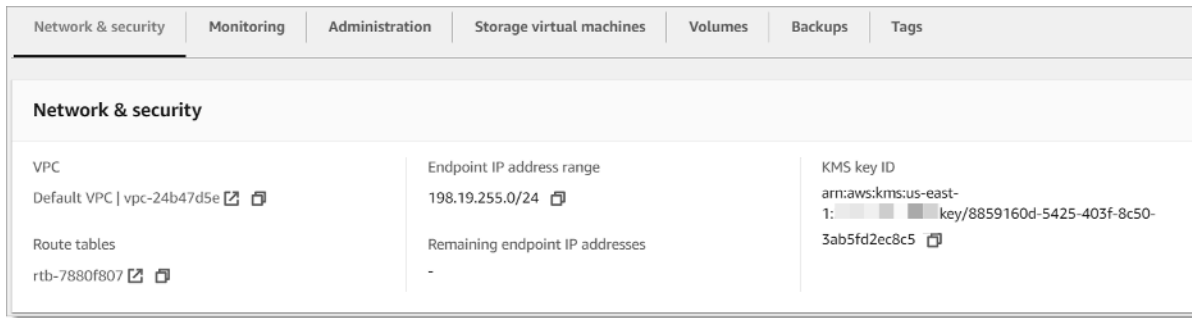
AWS Transit Gateway Pour configurer l'accès aux systèmes de fichiers multi-AZ sur site

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 homologues 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 FSx console Amazon à l'adresse <https://console.aws.amazon.com/fsx/>.
2. Choisissez le FSx système de fichiers 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. Lorsque vous disposez de sous-réseaux de pièces jointes Transit Gateway distincts, vous devez également associer les tables de routage de ces sous-réseaux à Amazon FSx afin qu'elles soient mises à jour avec les adresses des points de FSx terminaison Amazon.

Pour ajouter une table de routage à votre système de fichiers, consultez [Mise à jour des systèmes de fichiers](#).

Montage de volumes sur des clients Linux

Nous recommandons que le style de sécurité des volumes que vous souhaitez monter avec des clients Linux soit défini sur UNIX oumixed. Pour de plus amples informations, veuillez consulter [Gestion FSx des volumes ONTAP](#).

 Note

Par défaut, FSx pour ONTAP, les montages 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 EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Créez ou sélectionnez une EC2 instance Amazon 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 EC2 Linux, consultez [Étape 1 : Lancer une instance](#) dans le guide de EC2 l'utilisateur Amazon.

3. Connectez-vous à votre instance Amazon EC2 Linux. Pour plus d'informations, consultez [Connect to your Linux instance](#) dans le guide de EC2 l'utilisateur Amazon.
4. Ouvrez un terminal sur votre EC2 instance à l'aide du protocole Secure Shell (SSH) et connectez-vous avec les informations d'identification appropriées.
5. Créez un répertoire sur l' EC2 instance pour le montage du 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-01234567890abcdef0.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 de deuxième génération, 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 de deuxième génération, le protocole NFS parallèle (pNFS) est activé par défaut et est utilisé par défaut pour tous les clients qui montent des volumes avec NFS v4.1 ou une 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 Amazon EC2 Linux 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

FSx pour les systèmes de fichiers ONTAP, le montage automatique à l'aide `/etc/fstab` d'instances Amazon EC2 Mac n'est pas pris en charge.

Note

Avant de mettre à jour le `/etc/fstab` fichier de votre EC2 instance, assurez-vous que vous avez déjà créé votre système de fichiers FSx pour ONTAP. Pour de plus amples informations, veuillez consulter [Création de systèmes de fichiers](#).

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

1. Connectez-vous à votre EC2 instance :

- 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 du guide de EC2 l'utilisateur Amazon :

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

Montage de volumes 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 de plus amples informations, veuillez consulter [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, consultez [Gestion FSx des machines virtuelles de stockage ONTAP](#). Pour plus d'informations sur l'utilisation des groupes de travail, consultez [Configuration d'un serveur SMB dans un groupe de travail](#).
- Le volume que vous connectez possède un paramètre de style de sécurité égal à NTFS oumixed. Pour de plus amples informations, veuillez consulter [Style de sécurité des volumes](#).

Pour monter un volume sur un client Windows à l'aide de SMB et d'Active Directory

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Créez ou sélectionnez une EC2 instance Amazon 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 EC2 l'utilisateur Amazon.

Pour plus d'informations sur l'association d'une SVM à un Active Directory, consultez [Gestion FSx des machines virtuelles de stockage ONTAP](#).

3. Connectez-vous à votre instance Amazon EC2 Windows. Pour plus d'informations, consultez la section [Connexion à votre instance Windows](#) dans le guide de EC2 l'utilisateur Amazon.
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.
 - Remplacez SHARE_NAME 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, consultez [Gestion 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 de deuxième génération, 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 de volumes 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 de plus amples informations, veuillez consulter [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 EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Créez ou sélectionnez une instance Amazon EC2 Mac 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 EC2 l'utilisateur Amazon.

3. Connectez-vous à votre instance Amazon EC2 Mac. Pour plus d'informations, consultez [Connect to your Linux instance](#) dans le guide de EC2 l'utilisateur Amazon.
4. Ouvrez un terminal sur votre EC2 instance à l'aide du protocole Secure Shell (SSH) et connectez-vous avec les informations d'identification appropriées.
5. Créez un répertoire sur l' EC2 instance 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 de deuxième génération, 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, consultez [Gestion des actions des PME](#).

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

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Créez ou sélectionnez une EC2 instance Amazon 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 EC2 Linux, consultez [Étape 1 : Lancer une instance](#) dans le guide de EC2 l'utilisateur Amazon.

3. Connectez-vous à votre instance Amazon EC2 Linux. Pour plus d'informations, consultez [Connect to your Linux instance](#) dans le guide de EC2 l'utilisateur Amazon.
4. Montez votre volume FSx for ONTAP sur l'EC2 instance Linux 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-01234567890abcdef0.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 de deuxième génération, 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-01234567890abcdef0.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 de deuxième génération, 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
```

Provisionnement iSCSI pour Linux

FSx car ONTAP prend en charge le protocole iSCSI. Vous devez configurer le protocole iSCSI à la fois sur le client Linux et sur votre système de fichiers afin d'utiliser le protocole iSCSI pour transporter des données entre les clients et votre système de fichiers. Le protocole iSCSI est disponible sur tous les systèmes de fichiers dotés de 6 paires de [haute disponibilité \(HA\)](#) ou moins.

Le processus de configuration iSCSI sur votre Amazon FSx pour NetApp ONTAP comporte trois étapes principales, qui sont décrites dans les procédures suivantes :

1. Installez et configurez le client iSCSI sur l'hôte Linux.
2. Configurez l'iSCSI sur la SVM du système de fichiers.
 - Créez un groupe d'initiateurs iSCSI.
 - Mappez le groupe d'initiateurs au LUN.
3. Montez un LUN iSCSI sur le client Linux.

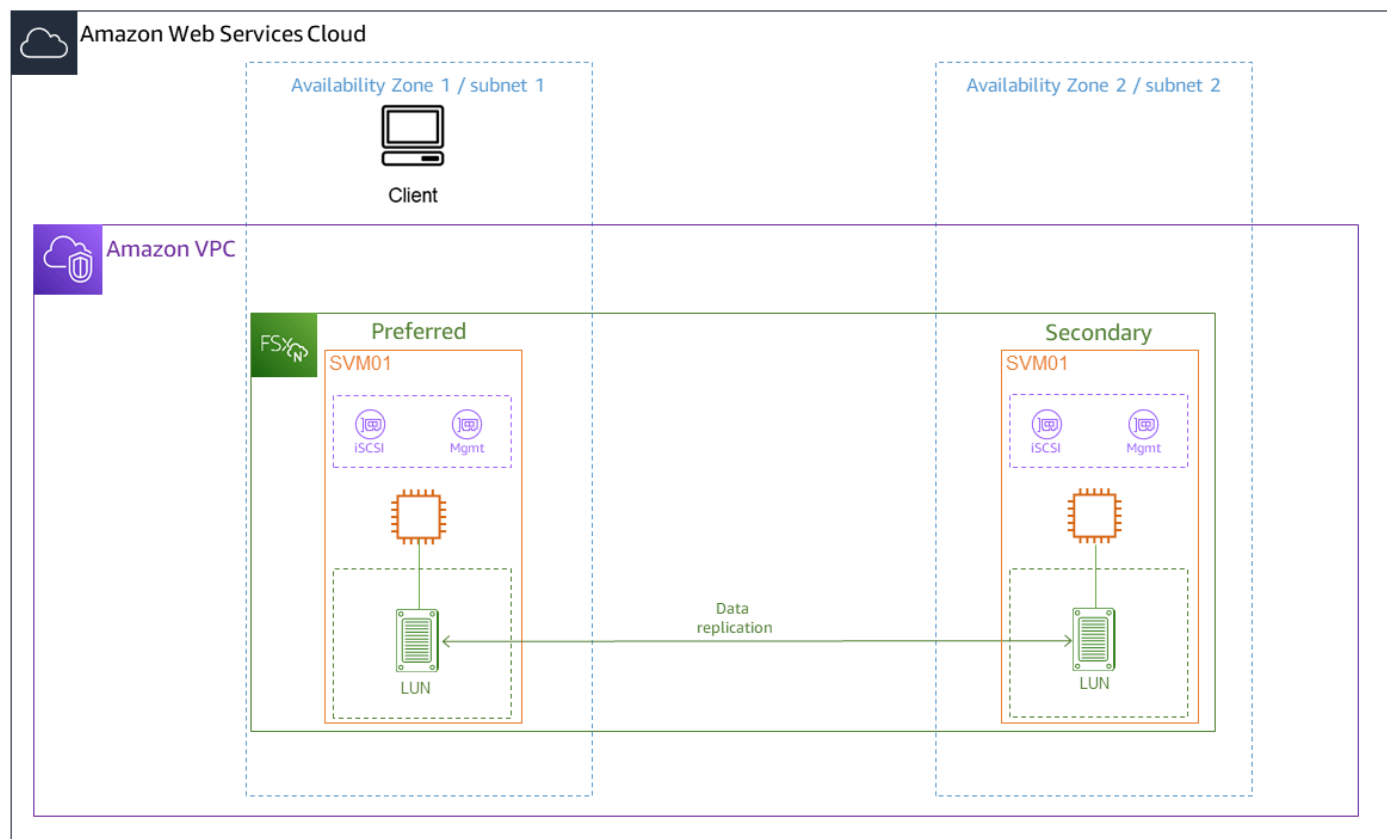
Avant de commencer

Avant de commencer le processus de configuration de votre système de fichiers pour iSCSI, vous devez avoir effectué les étapes suivantes.

- Créez un système de fichiers FSx pour ONTAP. Pour de plus amples informations, veuillez consulter [Création de systèmes de fichiers](#).
- Créez un LUN iSCSI sur le système de fichiers. Pour de plus amples informations, veuillez consulter [Création d'un LUN iSCSI](#).
- Créez une EC2 instance exécutant l'Amazon Machine Image (AMI) Amazon Linux 2 dans le même VPC que le système de fichiers. Il s'agit de l'hôte Linux sur lequel vous allez configurer iSCSI et accéder aux données de vos fichiers.

Au-delà de ces procédures, si l'hôte est situé dans un autre VPC, vous pouvez utiliser le peering VPC ou accorder un autre VPCs accès aux points de AWS Transit Gateway terminaison iSCSI du volume. Pour de plus amples informations, veuillez consulter [Accès aux données depuis l'extérieur du VPC de déploiement](#).

- Configurez les groupes de sécurité VPC de l'hôte Linux pour autoriser le trafic entrant et sortant, comme décrit dans. [Contrôle d'accès au système de fichiers avec Amazon VPC](#)
- Obtenez les informations d'identification pour ONTAP utilisateur doté de `fsxadmin` privilèges que vous utiliserez pour accéder au ONTAP CLI. Pour de plus amples informations, veuillez consulter [ONTAP rôles et utilisateurs](#).
- L'hôte Linux que vous allez configurer pour iSCSI et que vous utiliserez FSx pour accéder au système de fichiers ONTAP se trouve dans le même VPC et. Compte AWS
- Nous recommandons que l' EC2 instance se trouve dans la même zone de disponibilité que le sous-réseau préféré de votre système de fichiers, comme illustré dans le graphique suivant.



Si votre EC2 instance exécute une AMI Linux différente de celle d'Amazon Linux 2, certains des utilitaires utilisés dans ces procédures et exemples sont peut-être déjà installés, et vous pouvez utiliser des commandes différentes pour installer les packages requis. Hormis l'installation des packages, les commandes utilisées dans cette section sont valides pour les autres EC2 systèmes Linux AMIs.

Rubriques

- [Installation et configuration de l'iSCSI sur l'hôte Linux](#)
- [Configuration de l'iSCSI sur le système de fichiers FSx for ONTAP](#)
- [Montez un LUN iSCSI sur votre client Linux](#)

Installation et configuration de l'iSCSI sur l'hôte 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 for ONTAP

1. Connectez-vous à la CLI NetApp ONTAP sur le système FSx de fichiers ONTAP sur lequel vous avez créé le LUN iSCSI à l'aide de la commande suivante. Pour de plus amples informations, veuillez consulter [Utilisation de NetApp ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

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

2. Créez le groupe d'initiateurs (igroup) à l'aide de la NetApp commande ONTAP [lun igroup create](#) CLI. Un groupe d'initiateurs est mappé à LUNs iSCSI et contrôle les initiateurs (clients) auxquels ils ont accès. LUNs `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 le LUNs mappé à cet igroup soit accessible 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 show](#) commande :

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

Le système répond avec le résultat suivant :

Vserver	Igroup	Protocol	OS Type	Initiators
<i>svm_name</i>	<i>igroup_name</i>	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
<i>svm_name</i>	/vol/ <i>vol_name</i> / <i>lun_name</i>	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 :

Vserver	Logical Current Is Interface Port Home	Status Admin/Oper	Network Address/Mask	Current Node
<i>svm_name</i>	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` est 172.31.0.143 et `iscsi_2` est 172.31.21.81.

Montez un LUN iSCSI sur votre client Linux

Le processus de montage du LUN iSCSI sur votre client Linux comporte trois étapes :

1. Découverte des nœuds iSCSI cibles
2. Partitionnement du LUN iSCSI
3. Montage du LUN iSCSI sur le client

Ces questions sont abordées dans les procédures suivantes.

Pour découvrir les nœuds iSCSI cibles

1. Sur votre client Linux, utilisez la commande suivante pour découvrir les nœuds iSCSI cibles à l'aide `iscsi_1` de l'adresse IP. *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) Pour obtenir un débit supérieur au maximum de 5 Gbit/s (~625 MBps) fixé à un client EC2 unique Amazon pour votre LUN iSCSI, suivez les procédures décrites dans la section [Bande passante du EC2 réseau d'instances Amazon dans le guide de l'utilisateur Amazon Elastic Compute Cloud](#) pour les instances Linux afin d'établir des sessions supplémentaires afin d'augmenter le débit.

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 MBps) 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 iSCSI LUNs 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 comme `enabled`.

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

Dans la sortie, le nom du disque est formaté sous la forme `dm-xyz`, où `xyz` est un entier. S'il n'existe aucun autre disque à chemins multiples, cette valeur est `dm-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 au périphérique 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 for 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 pour NetApp ONTAP.
 - `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' $CONF
else
    printf "multipaths {\n\t\tmultipath {\n\t\t\twwid 3600a0980$SN\n\t\t\talias\n\t\t\t\t${ALIAS}\n\t\t\t}\n}" >> $CONF
fi
```

- 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. Vous pouvez créer plusieurs partitions en utilisant une valeur inférieure au dernier secteur (20971519 dans cet exemple).

 Note

La Last sector valeur varie en fonction de la taille de votre LUN iSCSI (10 Go dans cet exemple).

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

L'invite fdisk 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. *partition_name* a le format `<device_name><partition_number>`. 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) Si vous souhaitez attribuer à un utilisateur spécifique la propriété du répertoire de montage, remplacez-le *username* par le nom d'utilisateur du propriétaire.

```
~$ 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.

Provisionnement iSCSI pour Windows

FSx car ONTAP prend en charge le protocole iSCSI. Vous devez configurer le protocole iSCSI à la fois sur le client Windows, sur la SVM et sur le volume afin d'utiliser le protocole iSCSI pour transporter des données entre les clients et votre système de fichiers. Le protocole iSCSI est disponible sur tous les systèmes de fichiers dotés de 6 paires de [haute disponibilité \(HA\)](#) ou moins.

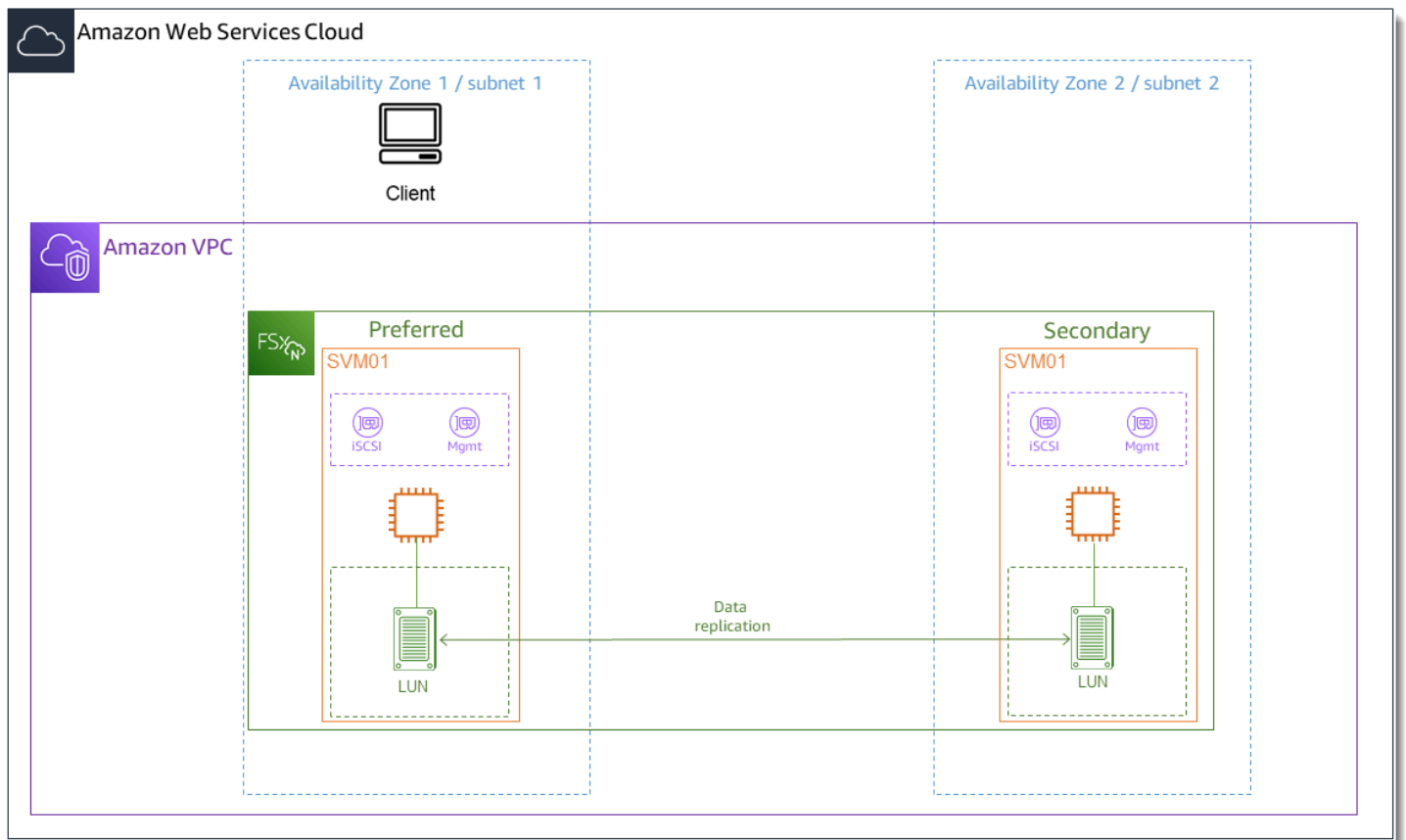
Les exemples présentés dans ces procédures montrent comment configurer le protocole iSCSI sur le client et FSx pour le système de fichiers ONTAP, et comment utiliser la configuration suivante :

- Le LUN iSCSI qui est monté sur un hôte Windows est déjà créé. Pour de plus amples informations, veuillez consulter [Création d'un LUN iSCSI](#).
- L'hôte Microsoft Windows qui monte le LUN iSCSI est une EC2 instance Amazon 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 d'autres accès VPCs aux points de AWS Transit Gateway terminaison iSCSI. Pour de plus amples informations, veuillez consulter [Accès aux données depuis l'extérieur du VPC de déploiement](#).

Nous recommandons que l' EC2 instance 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 for 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 guide de l'utilisateur Amazon Elastic Compute Cloud.
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 NetApp ONTAP.

```
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-I/O (MPIO) sur votre instance Windows. Utilisez la commande suivante :

```
PS C:\> Install-WindowsFeature Multipath-I/O
```

5. Redémarrez votre instance Windows une fois l'Multipath-I/O 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 for ONTAP

1. Pour accéder au ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

2. Utilisation de ONTAP CLI [lun igroup create](#), créez le groupe d'initiateurs, ou *igroup*. Un groupe d'initiateurs est mappé à LUNs iSCSI et contrôle à quels initiateurs (clients) ont accès. LUNs *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
```

Pour rendre ce LUNs mappé igroup accessible à plusieurs hôtes, vous pouvez spécifier plusieurs noms d'initiateurs séparés par des virgules en utilisant [lun igroup create](#) ONTAP Commande CLI.

3. Vérifiez que le igroup a été créé avec succès à l'aide du [lun igroup show](#) ONTAP Commande CLI :

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

Le système répond avec le résultat suivant :

Vserver	Igroup	Protocol	OS Type	Initiators
<i>svm_name</i>	<i>igroup_name</i>	iscsi	windows	iqn.1994-05.com.windows:abcdef12345

Une fois igroup créés, vous êtes prêt à les créer LUNs et à les associer 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
<i>svm_name</i>	/vol/ <i>vol_name</i> / <i>lun_name</i>	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
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
<i>svm_name</i>	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 MBps) de débit global vers le LUN iSCSI. Le fait de disposer de 8 sessions garantit qu'un seul client peut gérer la totalité de la capacité de MBps débit de 4 000, soit le plus haut niveau de capacité de débit FSx ONTAP. Vous pouvez éventuellement augmenter ou diminuer le nombre de sessions (chaque session fournit jusqu'à 625 MBps de débit) en modifiant la `RecommendedConnectionCount` variable. Pour plus d'informations, consultez la section [Bande passante du réseau des EC2 instances](#) Amazon 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 `.ps1` 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.

```
Write-Host "Starting iSCSI connection setup..."
$TargetPortalAddresses = @("iscsi_1","iscsi_2"); $LocaliSCSIAddress = "ec2_ip"
$RecommendedConnectionCount = 8

Foreach ($TargetPortalAddress in $TargetPortalAddresses) {
    New-IscsiTargetPortal -TargetPortalAddress $TargetPortalAddress -
TargetPortalPortNumber 3260 -InitiatorPortalAddress $LocaliSCSIAddress
}

New-MSDSMSupportedHW -VendorId MSFT2005 -ProductId iSCSIBusType_0x9

$currentMPIOSettings = Get-MPIOSetting
if ($currentMPIOSettings.PathVerificationState -ne 'Enabled') {
    Write-Host "Setting MPIO path verification state to Enabled"; Set-
MPIOSetting -NewPathVerificationState Enabled
} else { Write-Host "MPIO path verification state already Enabled" }

$portalConnectionCounts = @{}
foreach ($TargetPortalAddress in $TargetPortalAddresses)
{ $portalConnectionCounts[$TargetPortalAddress] = 0 }

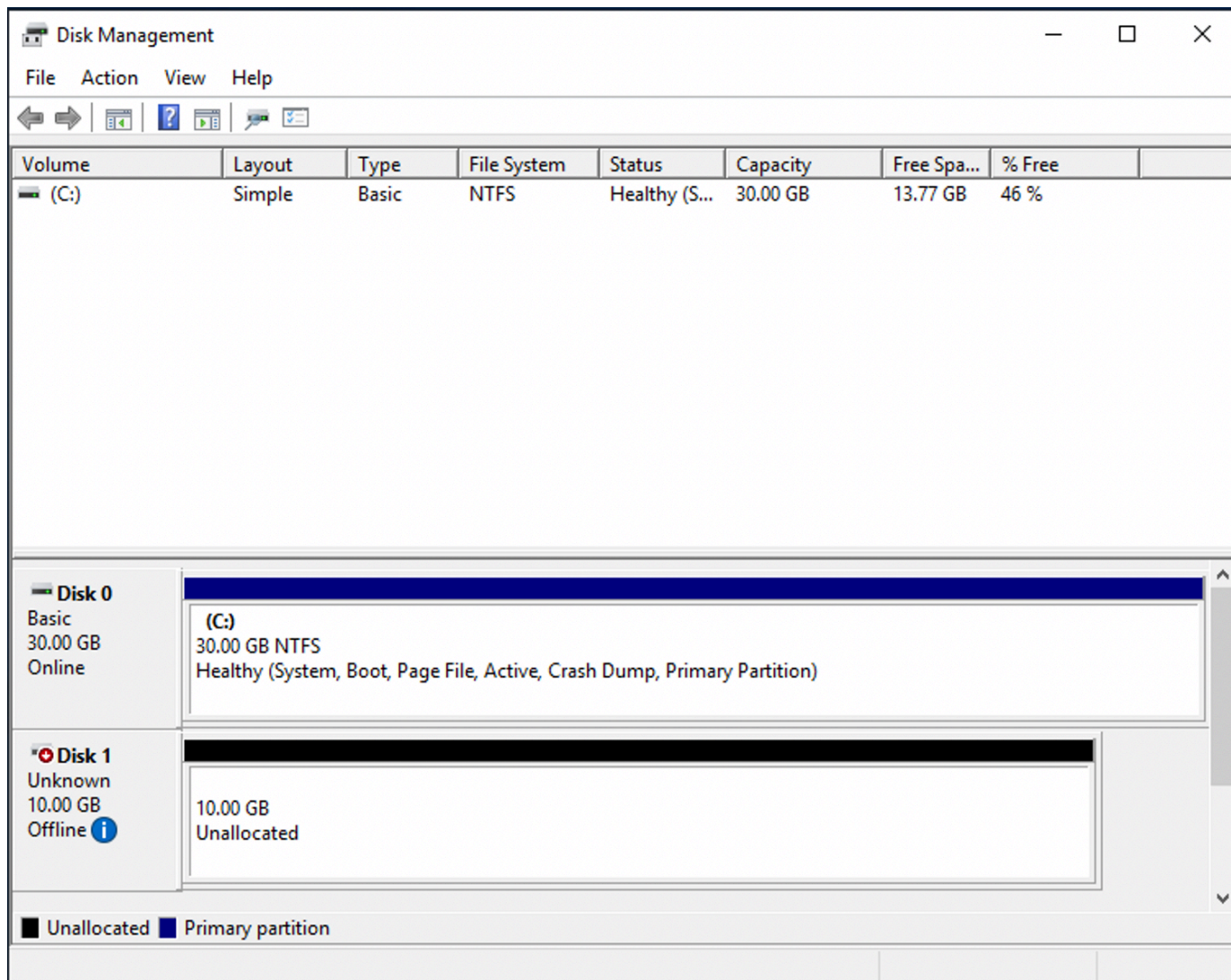
$sessions = Get-IscsiSession
if ($sessions) {
    foreach ($session in $sessions) {
        if ($session.IsConnected) {
            $targetPortal = (Get-IscsiTargetPortal -iSCSISession
$session).TargetPortalAddress
            if ($portalConnectionCounts.ContainsKey($targetPortal))
{ $portalConnectionCounts[$targetPortal]++ }
        }
    }
}

foreach ($TargetPortalAddress in $TargetPortalAddresses) {
    $existingCount = $portalConnectionCounts[$TargetPortalAddress];
$remainingConnections = $RecommendedConnectionCount - $existingCount
```

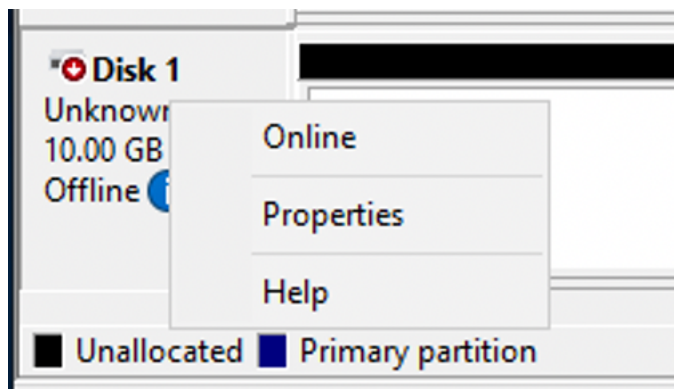
```
Write-Host "Portal $TargetPortalAddress has $existingCount
existing connections, $remainingConnections remaining (max recommended:
$RecommendedConnectionCount)"
    if ($remainingConnections -gt 0) {
        Write-Host "Creating $remainingConnections connections for portal
$TargetPortalAddress"
        1..$remainingConnections | ForEach-Object {
            Get-IscsiTarget | Connect-IscsiTarget -IsMultipathEnabled $true -
TargetPortalAddress $TargetPortalAddress -InitiatorPortalAddress $LocaliSCSIAddress
-IsPersistent $true
        }
        } else { Write-Host "Maximum connections (8) reached for portal
$TargetPortalAddress" }
    }

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. Développez 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.

MPIO Load Balance Policy is set to Round Robin (RR).
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

Provisionnement de NVMe /TCP pour Linux

FSx car ONTAP prend en charge le Non-Volatile Memory Express via TCP (NVMe/TCP) block storage protocol. With NVMe/TCP, vous utilisez le ONTAP CLI pour provisionner des espaces de noms et des sous-systèmes, puis mapper les espaces de noms aux sous-systèmes, de la même manière que LUNs sont provisionnés et mappés aux groupes d'initiateurs (igroups) pour iSCSI. Le protocole NVMe /TCP est disponible sur les systèmes de fichiers de deuxième génération dotés de 6 paires de [haute disponibilité \(HA\)](#) ou moins.

Note

FSx pour les systèmes de fichiers ONTAP, utilisez les points de terminaison iSCSI d'une SVM pour les protocoles de stockage par blocs NVMe iSCSI et /TCP.

Le processus de configuration de NVMe /TCP sur votre Amazon FSx pour NetApp ONTAP comporte trois étapes principales, qui sont décrites dans les procédures suivantes :

1. Installez et configurez le NVMe client sur l'hôte Linux.
2. Configurez NVMe sur la SVM du système de fichiers.
 - Créez un NVMe espace de noms.
 - Créez un NVMe sous-système.

- Mappez l'espace de noms au sous-système.
 - Ajoutez le NQN du client au sous-système.
3. Montez un NVMe appareil sur le client Linux.

Avant de commencer

Avant de commencer le processus de configuration de votre système de fichiers pour NVMe /TCP, vous devez avoir effectué les étapes suivantes.

- Créez un système de fichiers FSx pour ONTAP. Pour de plus amples informations, veuillez consulter [Création de systèmes de fichiers](#).
- Créez une EC2 instance exécutant Red Hat Enterprise Linux (RHEL) 9.3 dans le même VPC que le système de fichiers. Il s'agit de l'hôte Linux sur lequel vous allez configurer NVMe et accéder aux données de vos fichiers à l'aide de NVMe /TCP pour Linux.

Au-delà de ces procédures, si l'hôte est situé dans un autre VPC, vous pouvez utiliser le peering VPC ou accorder un autre VPCs accès aux points de AWS Transit Gateway terminaison iSCSI du volume. Pour de plus amples informations, veuillez consulter [Accès aux données depuis l'extérieur du VPC de déploiement](#).

- Configurez les groupes de sécurité VPC de l'hôte Linux pour autoriser le trafic entrant et sortant, comme décrit dans. [Contrôle d'accès au système de fichiers avec Amazon VPC](#)
- Obtenez les informations d'identification pour ONTAP utilisateur doté de `fsxadmin` privilèges que vous utiliserez pour accéder au ONTAP CLI. Pour de plus amples informations, veuillez consulter [ONTAP rôles et utilisateurs](#).
- L'hôte Linux que vous allez configurer NVMe et utiliser pour accéder au système de fichiers FSx for ONTAP se trouve dans le même Compte AWS VPC et.
- Nous recommandons que l' EC2 instance se trouve dans la même zone de disponibilité que le sous-réseau préféré de votre système de fichiers.

Si votre EC2 instance exécute une AMI Linux différente de RHEL 9.3, certains des utilitaires utilisés dans ces procédures et exemples sont peut-être déjà installés, et vous pouvez utiliser des commandes différentes pour installer les packages requis. Hormis l'installation des packages, les commandes utilisées dans cette section sont valides pour les autres EC2 systèmes Linux AMIs.

Rubriques

- [Installation et configuration NVMe sur l'hôte Linux](#)
- [Configuration NVMe sur le système de fichiers FSx for ONTAP](#)
- [Monter un NVMe appareil sur votre client Linux](#)

Installation et configuration NVMe sur l'hôte Linux

Pour installer le NVMe client

1. Connectez-vous à votre instance Linux à l'aide d'un client SSH. Pour plus d'informations, voir [Se connecter à votre instance Linux depuis Linux ou macOS à l'aide de SSH](#).
2. Installez `nvme-cli` à l'aide de la commande suivante:

```
~$ sudo yum install -y nvme-cli
```

3. Chargez le `nvme-tcp` module sur l'hôte :

```
$ sudo modprobe nvme-tcp
```

4. Obtenez le nom NVMe qualifié (NQN) de l'hôte Linux à l'aide de la commande suivante :

```
$ cat /etc/nvme/hostnqn  
nqn.2014-08.org.nvmexpress:uuid:9ed5b327-b9fc-4cf5-97b3-1b5d986345d1
```

Enregistrez la réponse pour une utilisation ultérieure.

Configuration NVMe sur le système de fichiers FSx for ONTAP

Pour configurer NVMe sur le système de fichiers

Connectez-vous à la CLI NetApp ONTAP sur le système FSx de fichiers ONTAP sur lequel vous souhaitez créer le ou les NVMe appareils.

1. Pour accéder au ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

2. Créez un nouveau volume sur la SVM que vous utilisez pour accéder à l' NVMe interface.

```
::> vol create -vserver fsx -volume nvme_vol1 -aggregate aggr1 -size 1t
[Job 597] Job succeeded: Successful
```

3. Créez l'espace de NVMe noms à l'ns_1 aide de la [vserver nvme namespace create](#) NetApp commande ONTAP CLI. Un espace de noms correspond aux initiateurs (clients) et contrôle quels initiateurs (clients) ont accès aux appareils. NVMe

```
::> vserver nvme namespace create -vserver fsx -path /vol/nvme_vol1/ns_1 -size 100g
-ostype linux
Created a namespace of size 100GB (107374182400).
```

4. Créez le NVMe sous-système à l'aide de la [vserver nvme subsystem create](#) NetApp commande ONTAP CLI.

```
~$ vserver nvme subsystem create -vserver fsx -subsystem sub_1 -ostype linux
```

5. Mappez l'espace de noms au sous-système que vous venez de créer.

```
::> vserver nvme subsystem map add -vserver fsx -subsystem sub_1 -path /vol/
nvme_vol1/ns_1
```

6. Ajoutez le client au sous-système à l'aide du NQN que vous avez récupéré précédemment.

```
::> vserver nvme subsystem host add -subsystem sub_1 -host-nqn
nqn.2014-08.org.nvmexpress:uuid:ec21b083-1860-d690-1f29-44528e4f4e0e -vserver fsx
```

Si vous souhaitez que les périphériques mappés à ce sous-système soient accessibles à plusieurs hôtes, vous pouvez spécifier plusieurs noms d'initiateurs dans une liste séparée par des virgules. Pour plus d'informations, voir [vserver nvme subsystem host add](#) dans la NetApp documentation ONTAP.

7. Vérifiez que l'espace de noms existe à l'aide de la [vserver nvme namespace show](#) commande :


```

::> vservers nvme namespace show -vservers fsx -instance
Vserver Name: fsx
    Namespace Path: /vol/nvme_vol1/ns_1
        Size: 100GB
        Size Used: 90.59GB
        OS Type: linux
        Comment:
        Block Size: 4KB
        State: online
    Space Reservation: false
Space Reservations Honored: false
    Is Read Only: false
    Creation Time: 5/20/2024 17:03:08
    Namespace UUID: c51793c0-8840-4a77-903a-c869186e74e3
    Vdisk ID: 80d42c6f00000000187cca9
    Restore Inaccessible: false
    Inconsistent Filesystem: false
    Inconsistent Blocks: false
    NVFail: false
Node Hosting the Namespace: FsxId062e9bb6e05143fcb-01
    Volume Name: nvme_vol1
    Qtree Name:
    Mapped Subsystem: sub_1
        Subsystem UUID: db526ec7-16ca-11ef-a612-d320bd5b74a9
        Namespace ID: 00000001h
        ANA Group ID: 00000001h
        Vserver UUID: 656d410a-1460-11ef-a612-d320bd5b74a9
        Vserver ID: 3
        Volume MSID: 2161388655
        Volume DSID: 1029
        Aggregate: aggr1
        Aggregate UUID: cfa8e6ee-145f-11ef-a612-d320bd5b74a9
    Namespace Container State: online
        Autodelete Enabled: false
        Application UUID: -
        Application: -
    Has Metadata Provisioned: true

1 entries were displayed.

```

8. Utilisez la [network interface show -vservers](#) commande pour récupérer les adresses des interfaces de stockage par blocs de la SVM dans laquelle vous avez créé vos NVMe appareils.

```

::> network interface show -vserver svm_name -data-protocol nvme-tcp
      Logical      Status      Network      Current
      Current Is
Vserver  Interface  Admin/Oper  Address/Mask  Node
      Port      Home
-----
      -----
svm_name
      iscsi_1      up/up      172.31.16.19/20
FSxId0123456789abcdef8-01  e0e      true
      iscsi_2      up/up      172.31.26.134/20
FSxId0123456789abcdef8-02  e0e      true
2 entries were displayed.

```

Note

Le `iscsi_1` LIF est utilisé à la fois pour iSCSI et /TCP. NVMe

Dans cet exemple, l'adresse IP de `iscsi_1` est 172.31.16.19 et `iscsi_2` est 172.31.26.134.

Monter un NVMe appareil sur votre client Linux

Le processus de montage de l' NVMe appareil sur votre client Linux comporte trois étapes :

1. Découvrir les NVMe nœuds
2. Partitionnement de l'appareil NVMe
3. Montage de NVMe l'appareil sur le client

Ces questions sont abordées dans les procédures suivantes.

Pour découvrir les NVMe nœuds cibles

1. Sur votre client Linux, utilisez la commande suivante pour découvrir les NVMe nœuds cibles.
Remplacez *iscsi_1_IP* par `iscsi_1` l'adresse IP et *client_IP* l'adresse IP du client.

Note

`iscsi_1` et `iscsi_2` LIFs sont utilisés à la fois pour l'iSCSI et NVMe le stockage.

```
~$ sudo nvme discover -t tcp -w client_IP -a iscsi_1_IP
```

```
Discovery Log Number of Records 4, Generation counter 11
=====Discovery Log Entry 0=====
trtype: tcp
adrfam: ipv4
subtype: current discovery subsystem
treq: not specified
portid: 0
trsvcid: 8009
subnqn: nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:discovery
traddr: 172.31.26.134
eflags: explicit discovery connections, duplicate discovery information
sectype: none
=====Discovery Log Entry 1=====
trtype: tcp
adrfam: ipv4
subtype: current discovery subsystem
treq: not specified
portid: 1
trsvcid: 8009
subnqn: nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:discovery
traddr: 172.31.16.19
eflags: explicit discovery connections, duplicate discovery information
sectype: none
```

- (Facultatif) Pour obtenir un débit supérieur à la limite maximale de 5 Gbit/s (~625 MBps) fixée par Amazon à un EC2 seul client, suivez les procédures décrites dans la section [Bande passante du réseau d' EC2 instances Amazon](#) dans le guide de l'utilisateur Amazon Elastic Compute Cloud pour les instances Linux afin d'établir des sessions supplémentaires. NVMe
- Connectez-vous aux initiateurs cibles avec un délai de perte du contrôleur d'au moins 1800 secondes, en utilisant à nouveau `iscsi_1` l'adresse IP pour *iscsi_1_IP* et l'adresse IP du client pour *client_IP* Vos NVMe appareils sont présentés sous forme de disques disponibles.

```
~$ sudo nvme connect-all -t tcp -w client_IP -a iscsi_1 -l 1800
```

- Utilisez la commande suivante pour vérifier que la NVMe pile a identifié et fusionné les multiples sessions et configuré le multiacheminement. La commande est renvoyée Y si la configuration a réussi.

```
~$ cat /sys/module/nvme_core/parameters/multipath
Y
```

- Utilisez les commandes suivantes pour vérifier que le paramètre NVMe -oF model est défini sur NetApp ONTAP Controller et que l'équilibrage de round-robin charge iopolicy est défini sur ONTAP espaces de noms pour distribuer les E/S sur tous les chemins disponibles

```
~$ cat /sys/class/nvme-subsystem/nvme-subsys*/model
Amazon Elastic Block Store
NetApp ONTAP Controller
~$ cat /sys/class/nvme-subsystem/nvme-subsys*/iopolicy
numa
round-robin
```

- Utilisez la commande suivante pour vérifier que les espaces de noms sont créés et correctement découverts sur l'hôte :

```
~$ sudo nvme list
```

Node	Generic Namespace	Usage	SN	Model Format	FW
Rev					
/dev/nvme0n1	/dev/ng0n1	25.77 GB / 25.77 GB	vol05955547c003f0580	Amazon Elastic Block Store	512 B + 0 B
/dev/nvme2n1	/dev/ng2n1	107.37 GB / 107.37 GB	1WB12JWY/XLKAAAAAAC	NetApp ONTAP Controller	4 KiB + 0 B

Le nouveau périphérique dans la sortie est /dev/nvme2n1. Ce schéma de dénomination peut varier en fonction de votre installation Linux.

- Vérifiez que l'état du contrôleur de chaque chemin est actif et que le statut multivoie ANA (Asymmetric Namespace Access) est correct :

```
~$ nvme list-subsys /dev/nvme2n1
nvme-subsys2 -
  NQN=nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:subsystem.rhel
      hostnqn=nqn.2014-08.org.nvmexpress:uuid:ec2a70bf-3ab2-6cb0-
f997-8730057ceb24
      iopolicy=round-robin
\
+- nvme2 tcp
traddr=172.31.26.134,trsvcid=4420,host_traddr=172.31.25.143,src_addr=172.31.25.143
live non-optimized
+- nvme3 tcp
traddr=172.31.16.19,trsvcid=4420,host_traddr=172.31.25.143,src_addr=172.31.25.143
live optimized
```

Dans cet exemple, la NVMe pile a automatiquement découvert le LIF alternatif de votre système de fichiers `iscsi_2`, `172.31.26.134`.

- Vérifiez que le NetApp le plug-in affiche les valeurs correctes pour chaque ONTAP périphérique d'espace de noms :

```
~$ sudo nvme netapp ontapdevices -o column
Device          Vserver          Namespace Path
      NSID  UUID                               Size
-----
-----
-----
/dev/nvme2n1    fsx              /vol/nvme_vol1/ns_1
      1      0441c609-3db1-4b0b-aa83-790d0d448ece  107.37GB
```

Pour partitionner l'appareil

- Utilisez la commande suivante pour vérifier que le chemin d'accès à votre nom_appareil `nvme2n1` est présent.

```
~$ ls /dev/mapper/nvme2n1
/dev/nvme2n1
```

2. Partitionnez le disque en utilisant `fdisk`. Vous allez entrer une invite interactive. Entrez les options dans l'ordre indiqué. Vous pouvez créer plusieurs partitions en utilisant une valeur inférieure au dernier secteur (20971519 dans cet exemple).

 Note

La Last sector valeur varie en fonction de la taille de votre NVMe appareil (100 GiB dans cet exemple).

```
~$ sudo fdisk /dev/mapper/nvme2n1
```

L'invite `fdisk` interactive démarre.

```
Welcome to fdisk (util-linux 2.37.4).
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 (256-26214399, default 256):
Last sector, +sectors or +size{K,M,G,T,P} (256-26214399, default
26214399): 20971519

Created a new partition 1 of type 'Linux' and of size 100 GiB.
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

Une fois que vous êtes entrée, votre nouvelle `/dev/nvme2n1` partition est disponible. `partition_name` a le format `<device_name><partition_number>`. 1a été utilisé comme numéro de partition dans la `fdisk` commande de l'étape précédente.

3. Créez votre système de fichiers en utilisant `/dev/nvme2n1` comme chemin.

```
~$ sudo mkfs.ext4 /dev/nvme2n1
```

Le système répond avec le résultat suivant :

```
mke2fs 1.46.5 (30-Dec-2021)
Found a dos partition table in /dev/nvme2n1
Proceed anyway? (y,N) y
Creating filesystem with 26214400 4k blocks and 6553600 inodes
Filesystem UUID: 372fb2fd-ae0e-4e74-ac06-3eb3eabd55fb
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424, 20480000, 23887872

Allocating group tables: done
Writing inode tables: done
Creating journal (131072 blocks): done
Writing superblocks and filesystem accounting information: done
```

Pour monter le NVMe périphérique sur le client Linux

1. Créez un répertoire *directory_path* comme point de montage pour votre système de fichiers sur l'instance Linux.

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

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

```
~$ sudo mount -t ext4 /dev/nvme2n1 /directory_path/mount_point
```

3. (Facultatif) Si vous souhaitez attribuer à un utilisateur spécifique la propriété du répertoire de montage, remplacez-le *username* par le nom d'utilisateur du propriétaire.

```
~$ 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 NVMe appareil sur votre client Linux.

Provisionnement NVMe/TCP pour Windows

FSx car ONTAP prend en charge le Non-Volatile Memory Express via TCP (NVMe/TCP) block storage protocol for Windows. With NVMe/TCP, vous utilisez la ONTAP CLI pour provisionner des espaces de noms et des sous-systèmes, puis vous mappez les espaces de noms aux sous-systèmes, de la même manière que vous les provisionnez et les mappez aux groupes d' LUNs initiateurs (igroups) pour iSCSI. Le NVMe/TCP protocole est disponible sur les systèmes de fichiers de deuxième génération dotés de 6 paires de [haute disponibilité \(HA\)](#) ou moins. .

Pour effectuer NVMe/TCP le provisionnement sur un hôte Windows, vous devez télécharger un initiateur auprès du fournisseur de votre choix et suivre ses instructions pour l'installer et le provisionner.

Accès aux données via d'autres AWS services

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

Rubriques

- [Utiliser Amazon WorkSpaces avec FSx for ONTAP](#)
- [Utilisation d'Amazon Elastic Container Service avec FSx for ONTAP](#)
- [Utilisation d'Amazon Elastic VMware Service avec FSx for ONTAP](#)
- [Utilisation du VMware cloud avec FSx for ONTAP](#)

Utiliser Amazon WorkSpaces avec FSx for 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 WorkSpaces aux utilisateurs de Windows et Linux. 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 FSx fichiers Amazon, ce qui permet de partager des documents et des paramètres entre différentes WorkSpaces instances, et sauvegardés automatiquement à l'aide des sauvegardes automatiques FSx quotidiennes d'Amazon.

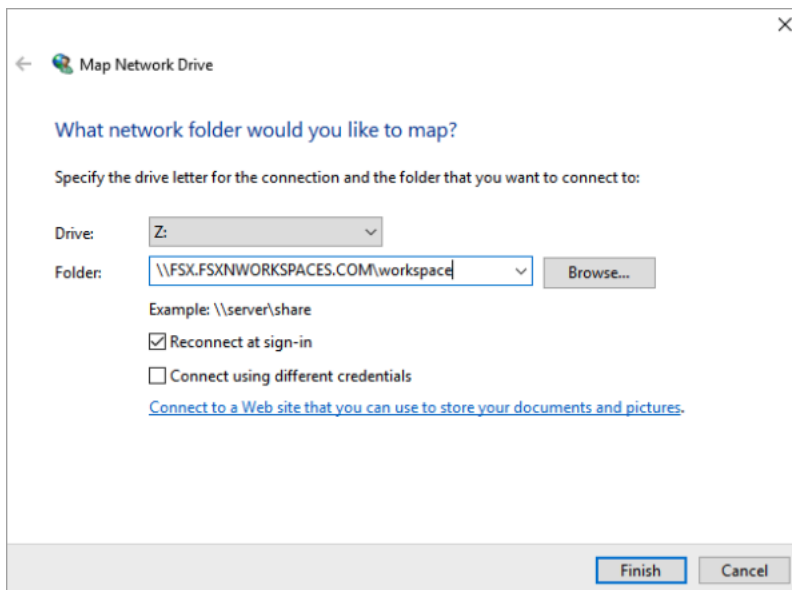
Étape 1 : créer un emplacement de dossier de profil pour les utilisateurs du domaine utilisant Amazon FSx

1. Créez un système de fichiers FSx pour ONTAP à l'aide de la FSx console Amazon. Pour de plus amples informations, veuillez consulter [Pour créer un système de fichiers \(console\)](#).

Important

Chaque système FSx de fichiers 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 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 depuis WorkSpaces, vous devez sélectionner une plage d'adresses IP de point de terminaison qui ne chevauche pas la plage 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 sur NTFS. Pour de plus amples informations, veuillez consulter [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 de plus amples informations, veuillez consulter [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 nommé `fsx-vol`, dans lequel vous créez un dossier nommé `profiles`. Pour de plus amples informations, veuillez consulter [Gestion des actions des PME](#).
5. Accédez à votre Amazon FSx SVM depuis une EC2 instance Amazon exécutant Windows Server ou depuis un WorkSpace. Pour de plus amples informations, veuillez consulter [Accès à vos données FSx for ONTAP](#).
6. Vous mappez votre partage `Z:\` sur votre WorkSpaces instance Windows :



Étape 2 : lier le partage de fichiers FSx pour 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

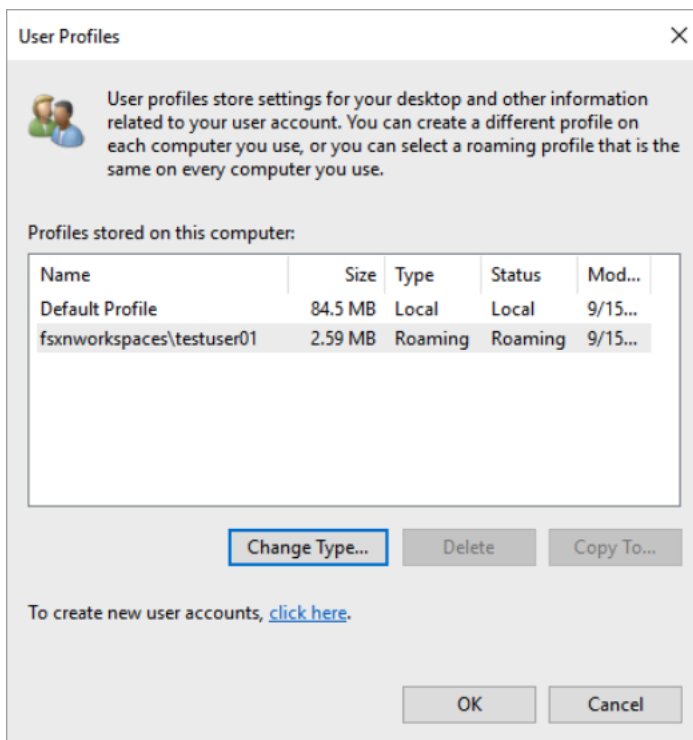
3. Déconnectez l'utilisateur de test du Workspace.
4. Configurez l'utilisateur de test pour qu'il dispose d'un profil d'itinérance situé sur votre système de FSx fichiers Amazon. Dans votre administrateur WorkSpaces, ouvrez une PowerShell console et utilisez une commande similaire à l'exemple suivant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

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

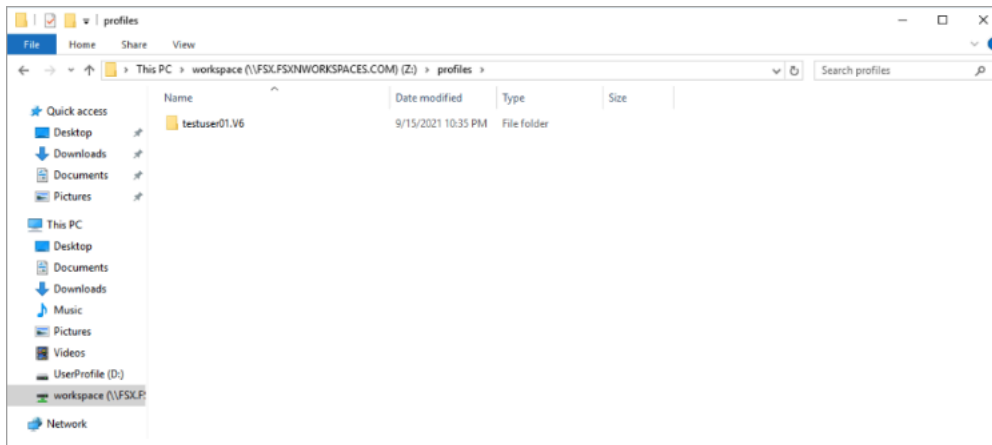
Par exemple :

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

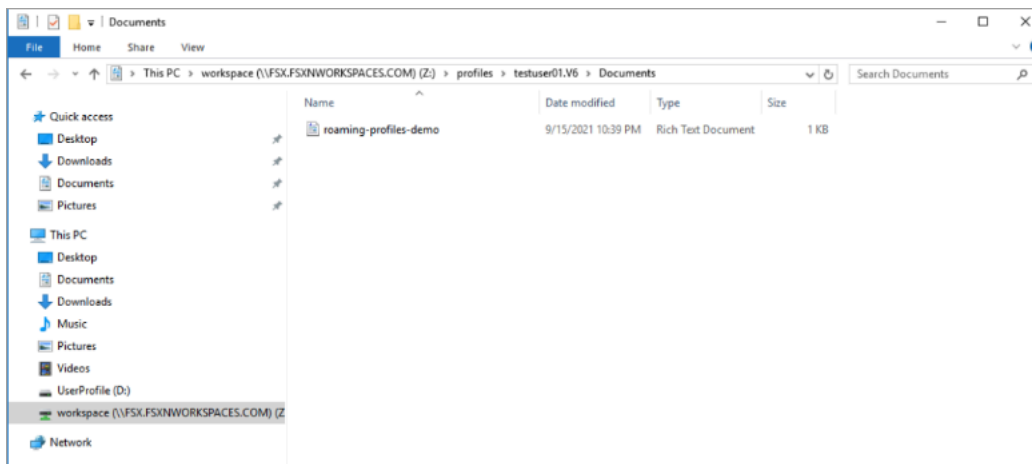
5. Connectez-vous à l'utilisateur de test Workspace.
6. Dans Propriétés du système, sélectionnez l'onglet Avancé et appuyez sur le bouton Paramètres dans la section Profils utilisateur. L'utilisateur connecté aura un type de profil de. Roaming



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 FSx partagé Amazon disponible sans lettre de lecteur, ce qui vous donne une plus grande flexibilité dans l'attribution des 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 Linux WorkSpace, vous n'avez pas besoin de saisir vos informations d'utilisateur si votre Linux WorkSpace appartient au même domaine que le FSx partage Amazon.
 - f. Choisissez Se connecter.

Connect to Server

Server Details

Server: fsx.fsxworkspaces.co Port: 0 - +

Type: Windows share

Share: workspace

Folder: team-shared

User Details

Domain Name:

User Name:

Password:

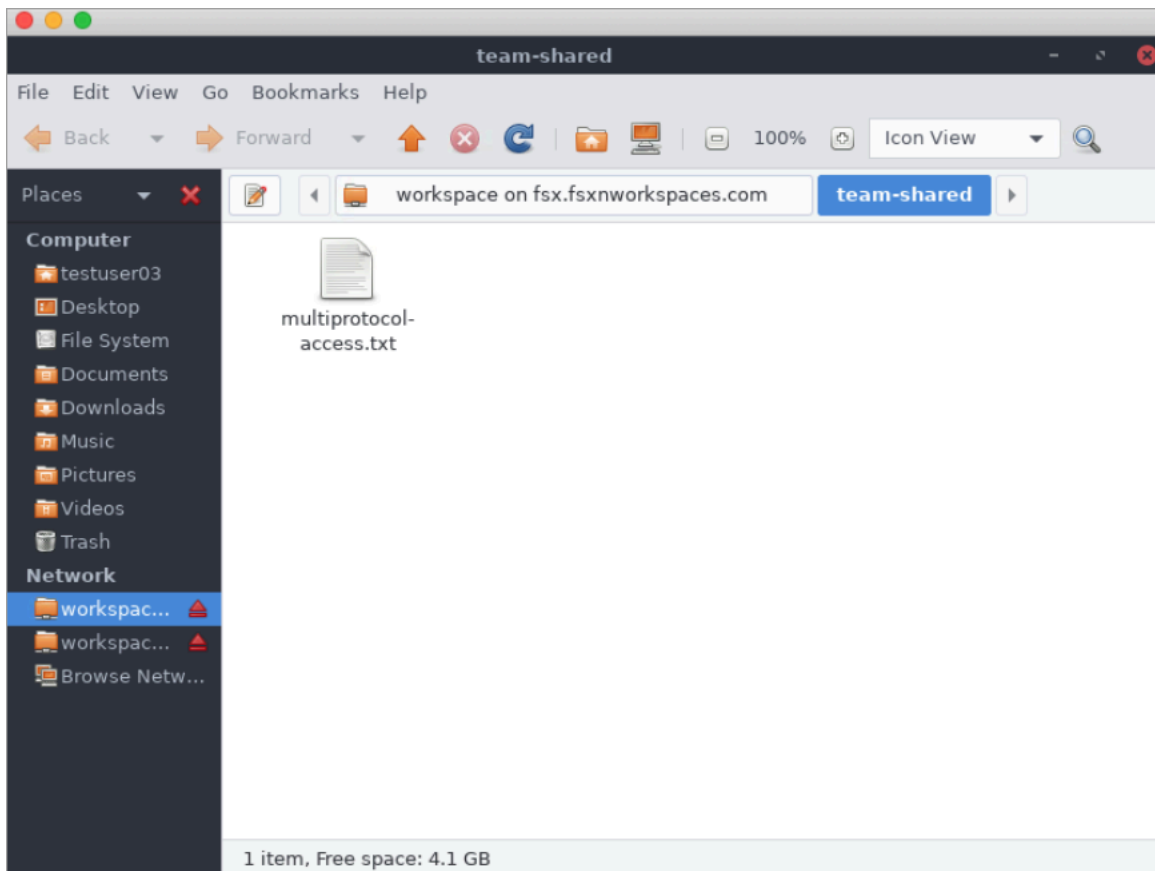
☐ Remember this password

☐ Add bookmark

Bookmark Name:

Help Cancel Connect

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 for 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 EC2 Amazon 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' EC2 instance pour le montage du volume de la SVM comme suit :

```
sudo mkdir /fsxontap
```

3. Montez votre volume FSx for ONTAP sur l' EC2 instance Linux 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-01234567890abcdef0.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 EC2 instance Windows jointe à un domaine au cluster Windows ECS et mappez un partage SMB.

Lancez une EC2 instance Windows optimisée 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' EC2 instance afin de pouvoir mapper votre partage SMB à un lecteur. Remplacez les valeurs situées sous le nom netbios ou DNS pour votre système de FSx fichiers et le nom de partage. Le volume NFS vol1 qui a été monté sur l' EC2 instance Linux 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: FSXONTAPDEMO  
                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' EC2 instance 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 d'Amazon Elastic VMware Service avec FSx for ONTAP

Vous pouvez utiliser ONTAP comme banque de données externe FSx pour les centres de données définis par logiciel Amazon Elastic VMware Service (Amazon EVS) (). SDDCs Pour plus d'informations, consultez [Exécuter des charges de travail à hautes performances avec Amazon FSx pour NetApp ONTAP](#). Pour obtenir des instructions détaillées, consultez [Configurer Amazon FSx pour NetApp ONTAP en tant que banque de données NFS et Configurer Amazon FSx pour NetApp ONTAP en tant que banque](#) de données iSCSI.

Utilisation du VMware cloud avec FSx for ONTAP

Vous pouvez utiliser FSx for ONTAP comme banque de données externe pour le VMware cloud sur des centres de données AWS définis par logiciel (). SDDCs Pour plus d'informations, consultez [Configurer Amazon FSx pour NetApp ONTAP en tant que stockage externe](#) et Guide de [déploiement d'Amazon pour ONTAP sur le VMware cloud AWS avec Amazon FSx pour NetApp ONTAP](#).

Disponibilité, durabilité et options de déploiement

Amazon FSx for NetApp ONTAP utilise les types de déploiement mono-AZ et multi-AZ. Vous pouvez choisir entre quatre options : mono-AZ 1, mono-AZ 2, Multi-AZ 1 et Multi-AZ 2. 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 [Amazon FSx Service Level Agreement](#).

Rubriques

- [Choix d'un type de déploiement de système de fichiers](#)
- [Choix d'une génération de système de fichiers](#)
- [Processus de basculement FSx pour ONTAP](#)
- [Ressources du réseau](#)

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.

Types de déploiement mono-AZ

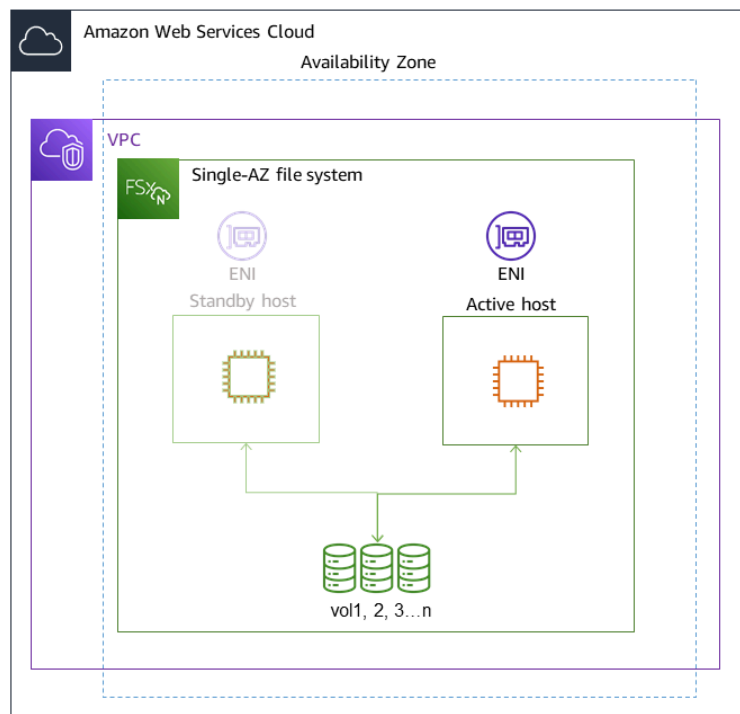
Vous pouvez choisir entre Single-AZ 1 et Single-AZ 2 pour votre système de fichiers mono-AZ. Le Single-AZ 1 est un système de fichiers de première génération avec une paire haute disponibilité (HA), tandis que le Single-AZ 2 est un système de fichiers de deuxième génération avec 1 à 12 paires HA. Pour de plus amples informations, veuillez consulter [Choix d'une génération de système de fichiers](#).

Lorsque vous créez un système de fichiers mono-AZ, Amazon FSx provisionne 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 dans la 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 bascule FSx 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 surveille FSx en permanence les défaillances matérielles et remplace automatiquement les composants de l'infrastructure en cas de panne. Pour garantir une durabilité élevée, Amazon réplique FSx 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 Région 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 de première génération FSx pour ONTAP.

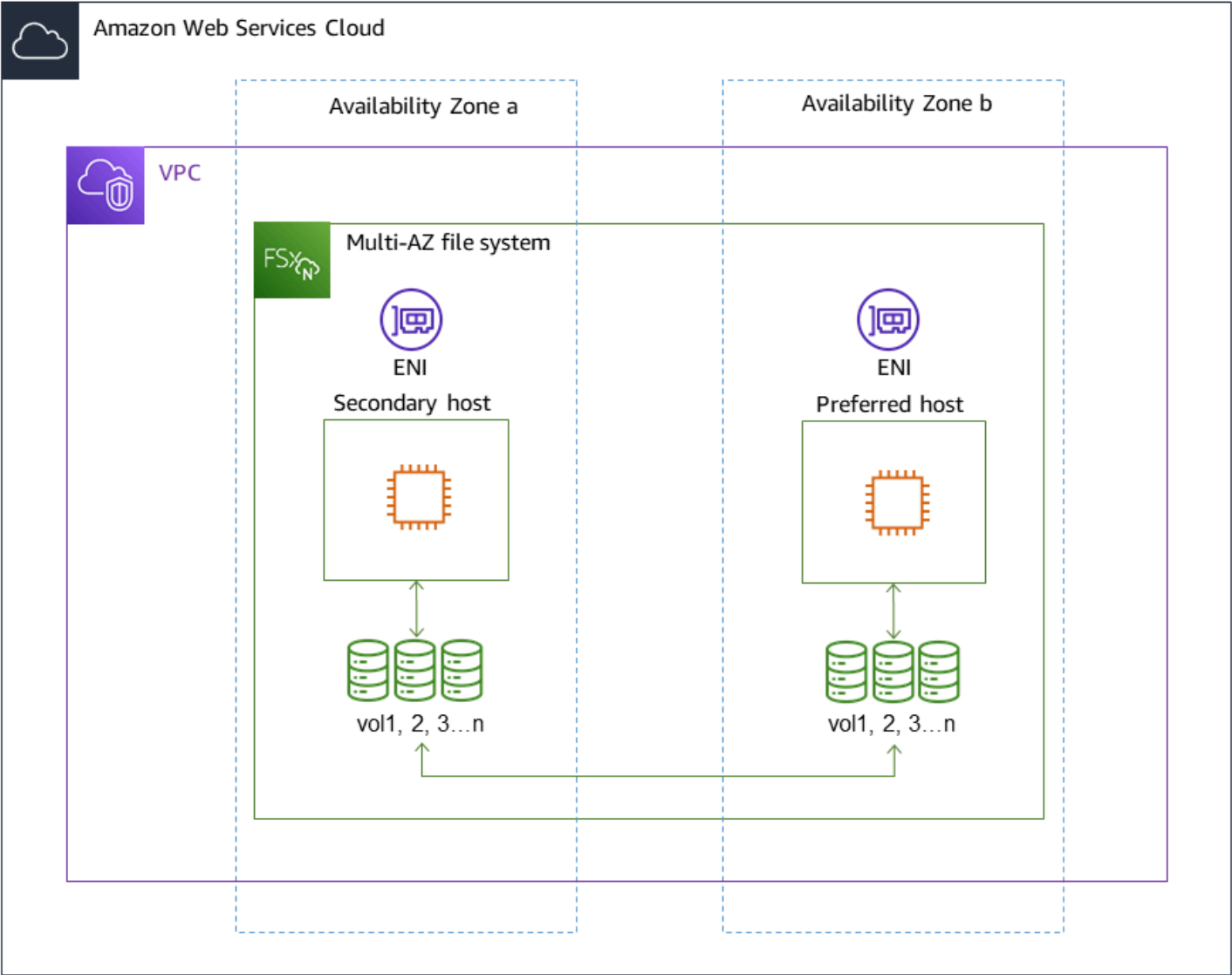


Types de déploiements multi-AZ

Vous pouvez choisir entre Multi-AZ 1 et Multi-AZ 2 pour votre système de fichiers Multi-AZ. Multi-AZ 1 est un système de fichiers de première génération et Multi-AZ 2 est un système de fichiers de deuxième génération. Les deux options ont une paire HA. Pour de plus amples informations, veuillez consulter [Choix d'une génération de système de fichiers](#).

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 FSx système de fichiers ONTAP Multi-AZ de première génération.



Choix d'une génération de système de fichiers

Le tableau suivant illustre les différences entre les systèmes de fichiers MONO-AZ et multi-AZ de première et de deuxième génération FSx pour les systèmes de fichiers ONTAP.

FSx pour les générations de systèmes de fichiers ONTAP

Dimension	Première génération	Deuxième génératio n (paire HA unique)	Deuxième génératio n (paire multiple)
Type de déploiement	SINGLE_AZ_1	SINGLE_AZ_2	SINGLE_AZ_2

Dimension	Première génération	Deuxième génération (paire HA unique)	Deuxième génération (paire multiple)
	MULTI_AZ_1	MULTI_AZ_2	
Paires HA	1 paire HA		1 à 12 paires HA
Stockage SSD	Minimum : 1 TiB Maximum : 192 TiB	Minimum : 1 TiB Maximum : 512 TiB	Minimum : 1 TiB (par paire HA) Maximum : 1 piB (total)
SSD IOPS	Minimum : 3 IOPS/ GIB de SSD Maximum : 160 000	Minimum : 3 IOPS/ GIB de SSD Maximum : 200 000	Minimum : 3 IOPS/ GIB de SSD Maximum : 2 400 000 (200 000 par paire HA)
Capacité de débit	128 MBps ; 256 ; 512 MBps ; 1 024 MBps ; 2 048 MBps ; 4 096 MBps MBps	384 MBps ; 768 ; 1 536 MBps ; 3 MBps MBps 072 ; 6 144 MBps	1 536 MBps (par paire HA) ; 3 072 MBps (par paire HA) ; 6 144 MBps (par paire HA)

Note

Vous ne pouvez pas modifier le type de déploiement de votre système de fichiers après sa création. Si vous souhaitez modifier le type de déploiement (par exemple, passer du mode mono-AZ 1 au mode mono-AZ 2), vous pouvez sauvegarder vos données et les restaurer sur un nouveau système de fichiers. Vous pouvez également migrer vos données avec NetApp SnapMirror AWS DataSync, avec ou avec un outil de copie de données tiers. Pour plus d'informations, consultez [Migration vers FSx for ONTAP à l'aide de NetApp SnapMirror](#) et [Migration vers FSx for ONTAP à l'aide de AWS DataSync](#).

Processus de basculement FSx pour 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 de deuxième génération comportant plusieurs paires HA, 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 y revient FSx 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 FSx pour les clients connectés à vos systèmes de fichiers ONTAP mono-AZ et multi-AZ, voir. [Accès aux données depuis le AWS Cloud](#)

Test du basculement sur un système de fichiers

Vous pouvez tester le basculement sur votre système de fichiers 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 FSx console Amazon, 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, consultez [Gestion 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 en fournit FSx également deux ENIs, un dans chacun des sous-réseaux que vous associez à votre système de fichiers. Les clients communiquent avec votre système de FSx fichiers Amazon 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 de FSx systèmes de fichiers ONTAP :

	Single-AZ de première génération	Single-AZ de deuxième génération	Multi-AZ
Nombre de sous-réseaux	1	1	2
Nombre d'interfa ces réseau élastiques	2	2 par paire HA	2

	Single-AZ de première génération	Single-AZ de deuxième génération	Multi-AZ
Nombre d'adresses IP par ENI	1 + le nombre de SVMs dans le système de fichiers	Nombre de paires HA + nombre de paires HA multiplié par le nombre de paires SVMs dans le système de fichiers	1 + le nombre de SVMs dans le système de fichiers
Nombre de routes de table de routage VPC	N/A	N/A	1 + le nombre de SVMs dans 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 détache FSx automatiquement toute adresse IP élastique qui est une adresse IP publique accessible depuis Internet et qui est attachée à l'interface Elastic Network d'un système de fichiers.

Amazon FSx pour les performances d' NetApp 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 FSx pour les systèmes de fichiers ONTAP](#)
- [Détails des performances](#)
- [Impact du type de déploiement sur les performances](#)
- [Impact de la capacité de stockage sur les performances](#)
- [Impact de la capacité de débit sur les performances](#)
- [Exemple : capacité de stockage et capacité de débit](#)

Comment les performances sont mesurées FSx pour les systèmes de fichiers ONTAP

Les performances du système de fichiers sont mesurées par sa latence, son débit et ses I/O opérations 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. De plus, Amazon FSx dispose de deux couches de mise en cache de lecture sur chaque serveur de fichiers : les lecteurs NVMe (mémoire non volatile express) et la mémoire interne, afin de réduire encore les latences lorsque vous accédez à vos données les plus fréquemment lues.

Débit et IOPS

Chaque système de FSx fichiers Amazon fournit des dizaines de débits et GBps 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

vos 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. NFSv3 et support de la NFSv4 version 1.+ nconnect [La bande passante réseau des EC2 instances Amazon](#) 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 de nconnect, consultez la section [ONTAP prise en charge de NFSv4 1.1](#).

Cadres Jumbo

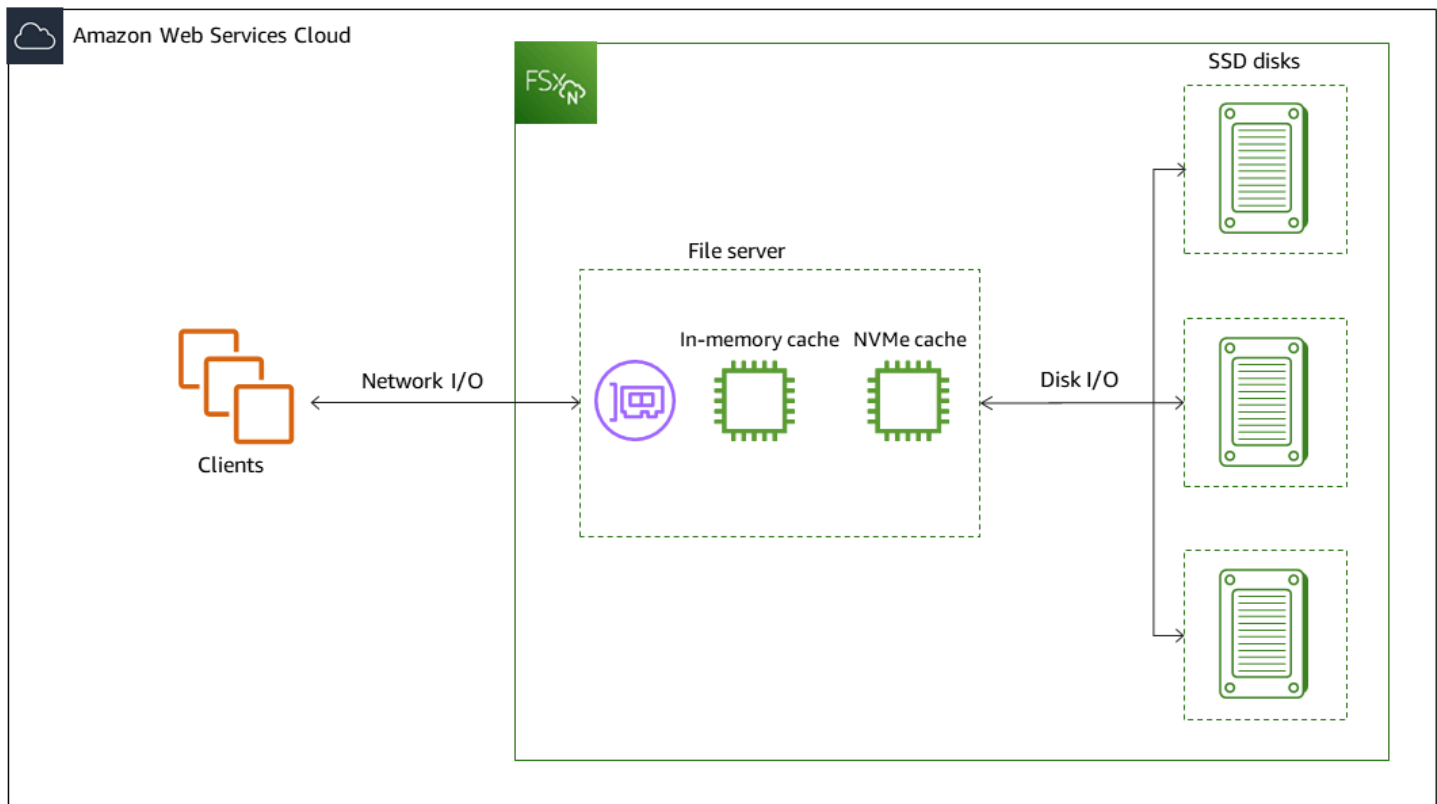
Pour atteindre un débit de lecture ou d'écriture maximal, nous vous recommandons d'activer les trames jumbo sur toutes les interfaces réseau du chemin de données vers votre système de FSx fichiers Amazon, y compris vos instances clientes EC2. Le paramètre d'unité de transmission maximale (MTU) par défaut pour les interfaces réseau de votre système de fichiers FSx for ONTAP est de 9 001 octets.

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 FSx fichiers Amazon. 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 NVMe cache 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 NVMe débit global et les performances d'IOPS correspondent à ces composants architecturaux (interface réseau, cache en mémoire, cache et volumes de stockage).

- I/O Performances throughput/IOPS du réseau : nombre de demandes entre les clients et le serveur de fichiers (agrégées)
- Taille en mémoire et en NVMe cache sur le serveur de fichiers : taille de l'ensemble de travail actif pouvant être adapté à la mise en cache
- I/O Performances throughput/IOPS du disque : des requêtes 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 (I/O performances du réseau et taille de la mémoire et du NVMe cache) 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 de forte intensité, I/O avec de longues périodes d'inactivité entre les rafales. Pour faire face à des 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 offre la possibilité d'atteindre des vitesses plus élevées pendant des périodes de temps, à la fois pour les opérations sur le réseau I/O et sur le disque I/O . Amazon FSx utilise un mécanisme de I/O crédit 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 des IOPS sont inférieurs à leurs limites de base, et peuvent utiliser ces crédits lorsqu'ils effectuent des opérations. I/O

Note

Pour les protocoles iSCSI et NVMe/TCP SAN, les opérations du client de lecture séquentielle peuvent atteindre le débit maximal du réseau I/O ou le débit de base du système de fichiers.

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, de sorte qu'une seule opération d'écriture double le débit du réseau.

Impact du type de déploiement sur les performances

Vous pouvez créer des systèmes de fichiers mono-AZ et multi-AZ avec FSx for ONTAP. Les systèmes de fichiers de première génération (mono-AZ et multi-AZ) et les systèmes de fichiers multi-AZ de deuxième génération sont alimentés par une paire de haute disponibilité (HA). Les systèmes de fichiers mono-AZ de deuxième génération sont alimentés par un maximum de 12 paires HA. Pour de plus amples informations, veuillez consulter [Gestion des paires de haute disponibilité \(HA\)](#).

FSx pour ONTAP, les systèmes de fichiers multi-AZ et mono-AZ 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 NVMe lecture afin de réduire les latences de lecture et d'augmenter le nombre d'IOPS pour les données fréquemment lues :

- Systèmes de fichiers Multi-AZ 1 et Multi-AZ 2
- Systèmes de fichiers mono-AZ 1 créés après le 28 novembre 2022 avec au moins 2 % GBps de capacité de débit
- Systèmes de fichiers mono-AZ 2 avec une capacité GBps de débit d'au moins 6 % par paire

Note

Pour les systèmes de fichiers de deuxième génération (mono-AZ 2 et multi-AZ 2), l'utilisation d'un NVMe cache peut réduire le débit total de votre charge de travail pour les charges de travail à haut débit ou les charges de travail d'E/S importantes. Si votre charge de travail est limitée au débit, nous vous recommandons de désactiver le cache. NVMe Pour de plus amples informations, veuillez consulter [Gestion du NVMe cache](#).

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.

First-generation file systems

Ces spécifications de performance s'appliquent aux systèmes de fichiers mono-AZ et multi-AZ de première génération.

Débit maximal du stockage SSD par paire HA pour les systèmes de fichiers de première génération

Région USA Est (Ohio), Région USA Est (Virginie du Nord), Région USA Ouest (Oregon) et Europe (Irlande)		Tous les autres « Régions AWS where FSx for ONTAP » sont disponibles	
Débit de lecture () MBps	Débit d'écriture () MBps	Débit de lecture () MBps	Débit d'écriture () MBps

	Région USA Est (Ohio), Région USA Est (Virginie du Nord), Région USA Ouest (Oregon) et Europe (Irlande)		Tous les autres « Régions AWS where FSx for ONTAP » sont disponibles	
Mono-AZ	4 096 1	1 000	2 048	750
Multi-AZ	4 096 1	1 800	2 048	1 300

 Note

¹ Pour fournir 4 % GBps de capacité de débit, votre système de fichiers doit être configuré avec un minimum de 5 120 GiB de capacité de stockage SSD et 160 000 IOPS SSD.

Second-generation file systems

Ces spécifications de performance s'appliquent aux systèmes de fichiers mono-AZ et multi-AZ de deuxième génération. En général, les systèmes de fichiers de deuxième génération peuvent fournir la totalité de la capacité de débit allouée pour les lectures et jusqu'à un tiers de la capacité de débit allouée pour les écritures. L'exception est l' MB/s option 6 144, répertoriée dans ce tableau.

Débit maximal du stockage SSD par paire HA pour les systèmes de fichiers de deuxième génération

	Débit de lecture () MBps	Débit d'écriture () MBps
Mono-AZ	6 144 1	1 024 1
Multi-AZ	6 144	2 048

 Note

¹ par paire HA (jusqu'à 12). Pour de plus amples informations, veuillez consulter [Gestion des paires de 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 bas des deux suivants :

- 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 (MBps 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 FSx fichiers Amazon 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 I/O performance 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 d'un stockage non volatile express (NVMe) pour la mise en cache des données sur chaque serveur de fichiers, ainsi que de niveaux de I/O performances 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

First-generation Single-AZ file system

Ces spécifications de performances s'appliquent aux systèmes de fichiers mono-AZ de première génération 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)

FSx capacité de débit (Go) MBps	Capacité de débit du réseau (Go) MBps		IOPS du réseau	Mise en cache en mémoire (Go)	NVMe mise en cache de lecture (Go)	Débit du disque (Go) MBps		IOPS du disque SSD *	
	Base de référence	Éclater				Base de référence	Éclater	Base de référence	Éclater
128	188	1 500	Base de référence de dizaines de milliers	16	–	128	1 250	6 000	40 000
256	375	1 500		32	–	256	1 250	12 000	40 000
512	750	1 500		64	–	512	1 250	20 000	40 000
1,024	1 500	–	de référence de centaines de milliers	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 ou le cache en mémoire de votre serveur de fichiers. NVMe

Ces spécifications de performance s'appliquent aux systèmes de fichiers mono-AZ de première génération dans tous les autres systèmes Régions AWS où FSx ONTAP est disponible.

Spécifications de performance pour les systèmes de fichiers dans [tous les autres Régions AWS pays où FSx ONTAP est disponible](#)

FSx capacité de débit () MBps	Capacité de débit du réseau () MBps		IOPS du réseau	Mise en cache en mémoire (Go)	Débit du disque () MBps		IOPS du disque SSD *	
	Base de référence	Éclater			Base de référence	Éclater	Base de référence	Éclater
128	150	1 250	Base de référence de dizaines de milliers	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 de milliers	64	512	600	18 750	–
1,024	1 500	–		128	1,024	–	40 000	–
2 048	3 125	–		256	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 ou le cache en mémoire de votre serveur de fichiers. NVMe

Second-generation Single-AZ file system

Ces spécifications de performance s'appliquent aux systèmes de fichiers mono-AZ de deuxième génération.

Spécifications de performance pour les systèmes de fichiers mono-AZ de deuxième génération

FSx	Capacité de débit du réseau () MBps		IOPS du réseau	Mise en cache en mémoire (Go)	NVMe mise en cache (Go)	Débit du disque () MBps		IOPS du disque SSD *	
	Base de référence	Éclater				Base de référence	Éclater	Base de référence	Éclater
384**	781	6 250	Base de référence de centaines de milliers	16	–	384	3 125	12 500	65 000
768**	1 563	6 250		32	–	768	3 125	25 000	65 000
1 536	3 125	6 250		64	–	1 536	3 125	50 000	65 000
3 072	6 250	–		128	–	3 072	–	100 000	–
6 144	12 500	–		256	1 900	6 144	–	200 000	–

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 ou le cache en mémoire de votre serveur de fichiers. NVMe

** Les systèmes de fichiers mono-AZ de deuxième génération prennent en charge des capacités de débit 384 et 768, mais uniquement avec une paire HA. Pour ajouter des paires HA, votre système de fichiers doit être configuré avec une capacité de débit MBps d'au moins 1 536.

First-generation Multi-AZ file system

Ces spécifications de performances s'appliquent aux systèmes de fichiers multi-AZ de première génération 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)

FSx	Capacité de débit du réseau () MBps		IOPS du réseau	Mise en cache en mémoire (Go)	NVMe mise en cache (Go)	Débit du disque () MBps		IOPS du disque SSD *	
	Base de référence	Éclater				Base de référence	Éclater	Base de référence	Éclater
128	188	1 500	Base de référence	16	238	128	1 250	6 000	40 000
256	375	1 500	de dizaines de milliers	32	475	256	1 250	12 000	40 000

FSx capacité de débit () MBps	Capacité de débit du réseau () MBps		IOPS du réseau	Mise en cache en mémoire (Go)	NVMe mise en cache (Go)	Débit du disque () MBps		IOPS du disque SSD *	
512	750	1 500	Base	64	950	512	1 250	20 000	40 000
1,024	1 500	–	de référence	128	1 900	1,024	1 250	40 000	–
2 048	3 125	–	de centaines	256	3,800	2 048	–	80 000	–
4 096	6 250	–	de milliers	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 ou le cache en mémoire de votre serveur de fichiers. NVMe

Ces spécifications de performance s'appliquent aux systèmes de fichiers multi-AZ de première génération dans tous les autres systèmes Régions AWS où FSx ONTAP est disponible.

Spécifications de performance pour les systèmes de fichiers dans [tous les autres Régions AWS pays où FSx ONTAP est disponible](#)

FSx capacité de débit () MBps	Capacité de débit du réseau () MBps		IOPS du réseau	Mise en cache en mémoire (Go)	NVMe mise en cache (Go)	Débit du disque () MBps		IOPS du disque SSD *	
	Base de	Éclater				Base de	Éclater	Base de	Éclater

FSx	Capacité de		IOPS	Mise	NVMe	Débit du disque		IOPS du disque	
de	débit du réseau		du	en	mise	() MBps		SSD *	
capacité	() MBps		réseau	cache	en				
de				en	cache				
débit				mémoire	(Go)				
()				(Go)					
MBps									
	référence					référence		référence	
128	150	1 250	Base	16	150	128	600	6 000	18 750
256	300	1 250	de	32	300	256	600	12 000	18 750
			référence						
			de						
			dizaines						
			de						
			milliers						
512	625	1 250	Base	64	600	512	600	18 750	–
1,024	1 500	–	de	128	1 200	1,024	–	40 000	–
			référence						
			de						
2 048	3 125	–	centaines	256	2 400	2 048	–	80 000	–
			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 ou le cache en mémoire de votre serveur de fichiers. NVMe

Second-generation Multi-AZ file systems

Ces spécifications de performance s'appliquent aux systèmes de fichiers multi-AZ de deuxième génération.

Spécifications de performance pour les systèmes de fichiers multi-AZ de deuxième génération

FSx capacité de débit () MBps	Capacité de débit du réseau () MBps		IOPS du réseau	Mise en cache en mémoire (Go)	NVMe mise en cache (Go)	Débit du disque () MBps		IOPS du disque SSD *	
	Base de référence	Éclater				Base de référence	Éclater	Base de référence	Éclater
384	781	6 250	Base de référence de centaines de milliers	16	237	384	3 125	12 500	65 000
768	1 563	6 250		32	474	768	3 125	25 000	65 000
1 536	3 125	6 250		64	950	1 536	3 125	50 000	65 000
3 072	6 250	–		128	1 900	3 072	–	100 000	–
6 144	12 500	–		256	3,800	6 144	–	200 000	–

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 ou le cache en mémoire de votre serveur de fichiers. NVMe

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 de première génération configuré avec 2 TiB de capacité de stockage SSD et MBps 512 de capacité de débit possède les niveaux de débit suivants :

- Débit réseau : 625 points de MBps référence et 1 250 points en MBps rafale (voir le tableau des capacités de débit)
- Débit du disque : 512 en MBps ligne de base et 600 en MBps rafale.

Votre charge de travail accédant au système de fichiers sera donc en mesure d'atteindre un débit de MBps base de 625 et un débit de 1 250 MBps rafales pour les opérations de fichiers effectuées sur les données activement consultées mises en cache dans le cache et le cache en mémoire du serveur de fichiers. NVMe

Administration FSx des ressources ONTAP

À l' AWS Management Console aide de la CLI et de l'API ONTAP, vous pouvez effectuer les actions administratives suivantes FSx pour les ressources ONTAP : AWS CLI

- Création, liste, mise à jour et suppression de systèmes de fichiers, de machines virtuelles de stockage (SVMs), 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 la capacité de stockage](#)
- [Gestion des FSx systèmes de fichiers ONTAP](#)
- [Gestion FSx des machines virtuelles de stockage ONTAP](#)
- [Gestion FSx des volumes ONTAP](#)
- [Création d'un LUN iSCSI](#)
- [Optimisation des performances avec les fenêtres FSx de maintenance Amazon](#)
- [Gestion de la capacité de débit](#)
- [Gestion des actions des PME](#)
- [Gestion des FSx ressources ONTAP à l'aide de NetApp applications](#)
- [Marquer les ressources Amazon FSx](#)

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

- [FSx pour les niveaux de stockage ONTAP](#)
- [Choisir la bonne quantité de stockage SSD pour le système de fichiers](#)
- [Capacité de stockage et IOPS du système de fichiers](#)
- [Capacité de stockage en volume](#)

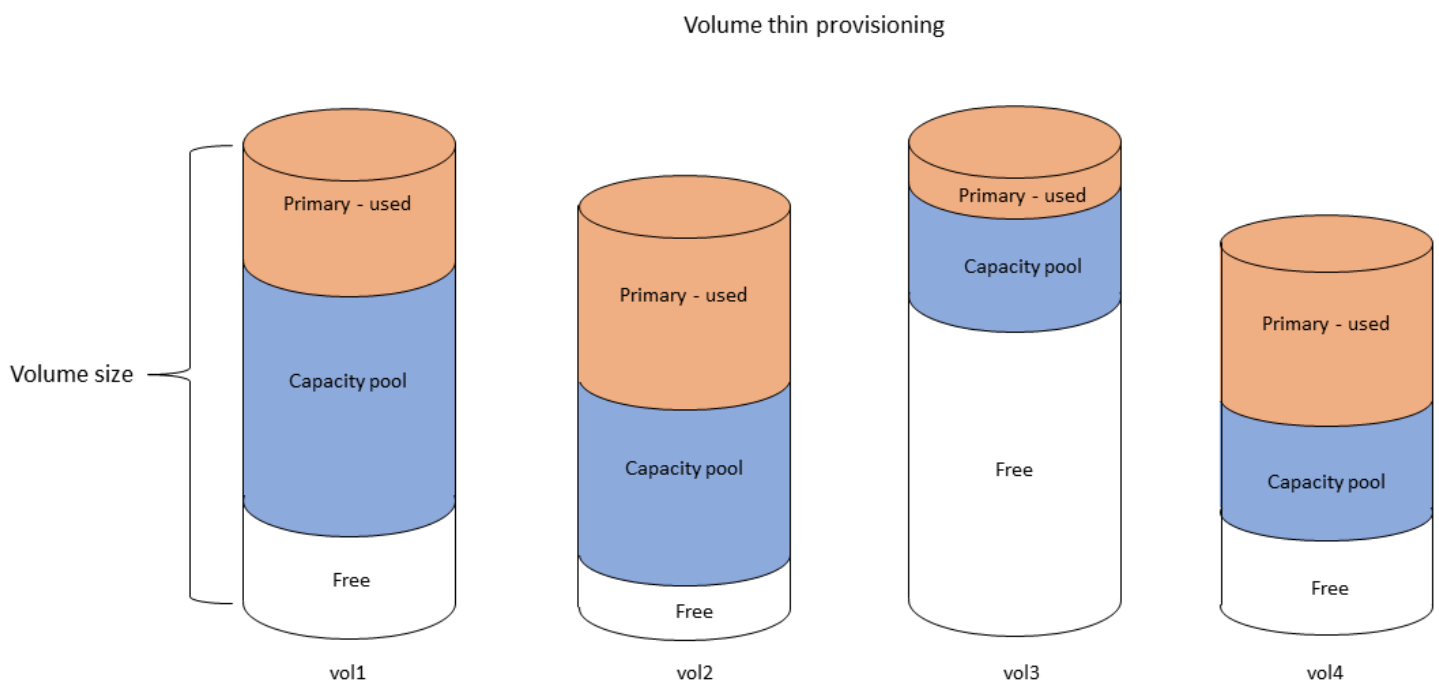
FSx pour les niveaux de stockage ONTAP

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 :

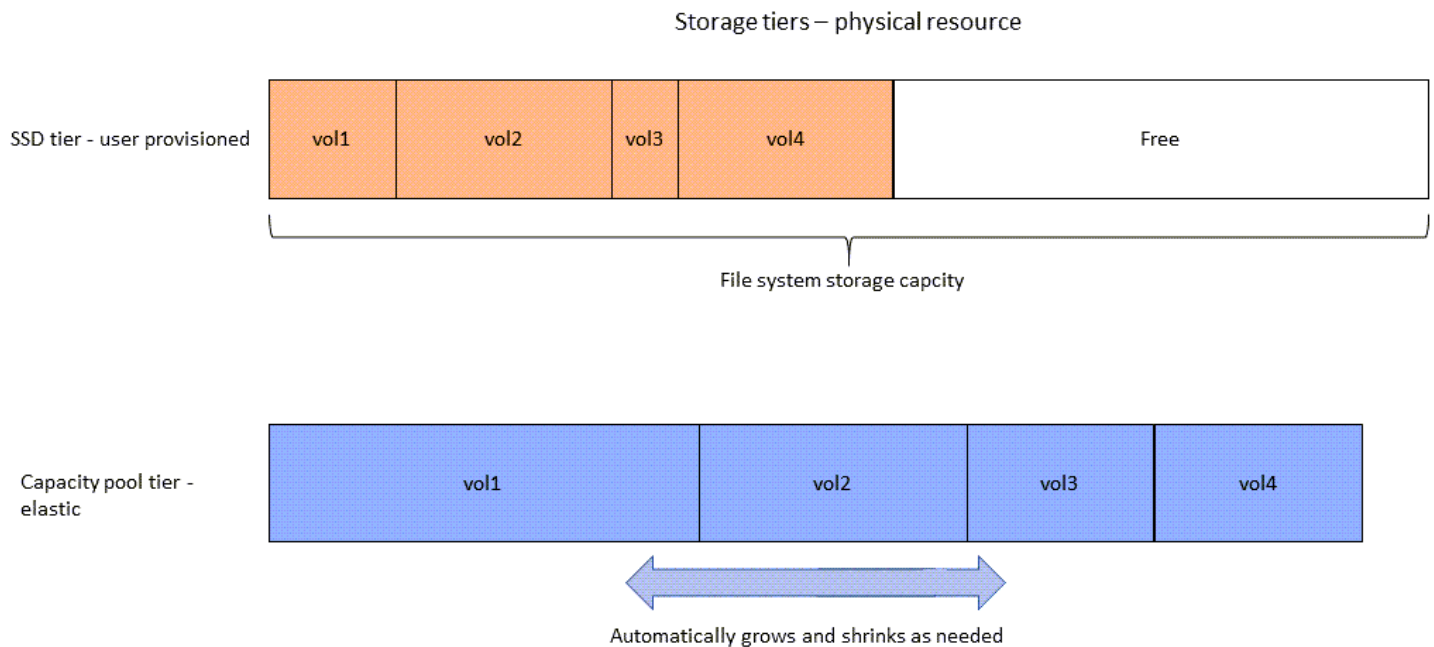
- Niveau SSD : stockage sur disque SSD (SSD) hautes performances, fourni par l'utilisateur, spécialement conçu pour la partie active de votre ensemble de données.
- Niveau du pool de capacité : stockage entièrement élastique qui s'adapte automatiquement à une taille de plusieurs pétaoctets et est optimisé 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. FSx pour ONTAP, les volumes 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 FSx volumes 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 de plus amples informations, veuillez consulter [Hiérarchisation des données de volume](#).

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

Lorsque vous choisissez la quantité de capacité de stockage SSD FSx pour votre système de fichiers ONTAP, vous devez garder à l'esprit les éléments suivants qui ont une incidence 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 tébi-octets (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 fait que les données sont écrites directement sur le stockage du pool de capacité lorsqu'elles sont utilisées SnapMirror sur 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 de plus amples informations, veuillez consulter [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 de deuxième génération, 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 de plus amples informations, veuillez consulter [Seuils de hiérarchisation](#).

Efficacité du stockage

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

par volume. Ces fonctionnalités réduisent la quantité de capacité de stockage consommée par vos données, ce qui vous permet de consommer moins d'espace de stockage sur les SSD, le pool de capacité et le stockage des sauvegardes. Vous pouvez activer la compression et la déduplication sur chaque volume pour les données stockées sur SSD. Les économies de stockage résultant de la compression et de la déduplication sur le stockage SSD sont préservées lorsque les données sont hiérarchisées en fonction de la capacité de stockage du pool. L'efficacité du stockage est toujours activée pour les données de sauvegarde, quelle que soit la configuration d'efficacité du stockage de votre système de fichiers.

Le tableau suivant présente des exemples d'économies de stockage typiques.

	Compression uniquement	Déduplication uniquement	Compression et déduplication
Partage de fichiers à usage général	50%	30 %	65 %
Serveurs et bureaux virtuels	55 %	70 %	70 %
Bases de données	65 à 70 %	0 %	65 à 70 %
Données d'ingénierie	55 %	30 %	75%
Données géosismiques	40 %	3 %	40 %

Pour la plupart des charges de travail, l'activation de la compression et de la déduplication n'aura pas d'impact négatif sur les performances du système de fichiers. Pour la plupart des charges de travail, la compression améliore les performances globales. Pour permettre des lectures et des écritures rapides à partir du cache RAM, FSx les serveurs de fichiers ONTAP sont équipés de niveaux de bande passante réseau supérieurs sur les cartes d'interface réseau frontales (NICs) à ceux disponibles entre les serveurs de fichiers et les disques de stockage. Étant donné que la compression des données réduit la quantité de données envoyées entre les serveurs de fichiers et les disques de stockage, pour la plupart des charges de travail, vous constaterez une augmentation de la capacité de débit globale du système de fichiers lors de l'utilisation de la compression de données. Les augmentations de capacité de débit liées à la compression des données seront plafonnées une fois que vous aurez saturé la carte réseau frontale de votre système de fichiers.

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

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, voir [Surveillance des économies d'efficacité du stockage](#).

Calcul des économies d'efficacité du stockage

Vous pouvez utiliser les métriques LogicalDataStored et StorageUsed FSx pour le système de CloudWatch fichiers 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 de plus amples informations, veuillez consulter [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 même période. Divisez ensuite la différence par le Average 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 TiB) de vos données sont automatiquement hiérarchisées selon le niveau du pool de capacité et les 20 % restants (20 TiB) 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 pour ONTAP, vous spécifiez la capacité de stockage du niveau SSD. Pour les systèmes de fichiers mono-AZ de deuxième génération, 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 provisionne FSx 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 mono-AZ de deuxième génération, 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](#)
- [Création d'une alarme d'utilisation de la capacité de stockage pour votre système de fichiers](#)
- [Mise à jour de la capacité de stockage et des IOPS provisionnées](#)
- [Mise à jour dynamique de la capacité de stockage](#)
- [Surveillance de l'utilisation du stockage SSD](#)
- [Surveillance des économies d'efficacité du stockage](#)
- [Surveillance de la capacité de stockage et des mises à jour des IOPS](#)

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 FSx console Amazon, FSx l'API Amazon ou AWS Command Line Interface (AWS CLI) pour augmenter la capacité de stockage SSD. Pour de plus amples informations, veuillez consulter [Mise à jour de la capacité de stockage et des IOPS provisionnées](#).

Lorsque vous augmentez la capacité de stockage SSD de votre système de FSx fichiers Amazon, 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 les tarifs, 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 FSx console, de la CLI et de l'API Amazon. Pour de plus amples informations, veuillez consulter [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.
- (Systèmes de fichiers mono-AZ de deuxième génération 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 adapte FSx automatiquement le nombre d'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 les tarifs, 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 de plus amples informations, veuillez consulter [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 de deuxième génération, 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, consultez [Choisir la bonne quantité de stockage SSD pour le système de fichiers](#).

Création d'une alarme d'utilisation de la capacité de stockage pour votre 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 d'utilisation de la capacité de stockage du 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> Métriques 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.

Mise à jour de la capacité de stockage 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 à l'aide de la FSx console Amazon, du et de 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 FSx console Amazon 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 ONTAP FSx 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 le nombre d'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 de deuxième génération, la per-HA-pair valeur 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-system](#) ou 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 IOPS valeur doit être supérieure ou égale à trois fois la capacité de stockage SSD actuelle.
 - Si vous souhaitez qu'Amazon FSx augmente automatiquement le nombre d'IOPS de votre SSD, utilisez `Mode=AUTOMATIC` et n'utilisez pas le `Iops` paramètre. 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 [AdministrativeAction](#) le manuel Amazon FSx for NetApp ONTAP API Reference.

Mise à jour dynamique de la capacité de stockage

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 :

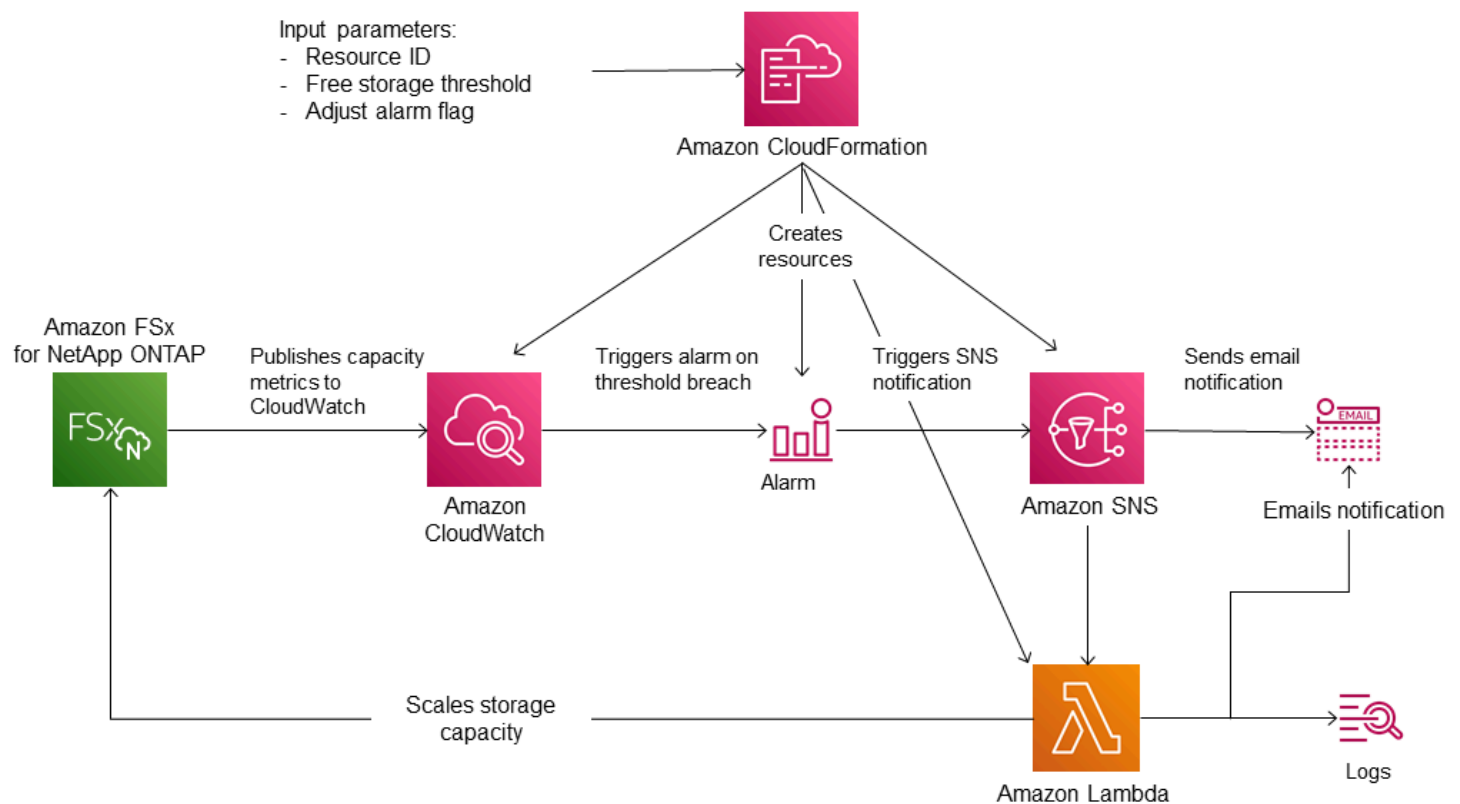
- Votre identifiant FSx de système de fichiers pour ONTAP.
- Le seuil de capacité de stockage SSD utilisé (valeur numérique). Il s'agit du pourcentage auquel l' CloudWatch alarme sera déclenchée.
- Pourcentage d'augmentation de la capacité de stockage (%).
- Adresse e-mail utilisée pour recevoir les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

Rubriques

- [Présentation de l'architecture](#)
- [AWS CloudFormation modèle](#)
- [Déploiement automatisé avec AWS CloudFormation](#)

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 d'API FSx Amazon.
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 de manière continue 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 [FSxOntapDynamicStorageScaling](#) AWS CloudFormation modèle.

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.

FSxSizeinGiB maximum

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 FSx fichiers Amazon qui s'exécute dans Amazon Virtual Private Cloud (Amazon VPC) dans votre. Compte AWS Pour plus d'informations sur la création de FSx ressources Amazon, consultez [Commencer à utiliser Amazon FSx pour NetApp ONTAP](#).

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

1. Téléchargez le modèle [FSxOntapDynamicStorageScaling](#) AWS CloudFormation .

Note

Amazon n' FSx 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 [FSx Points de terminaison et quotas Amazon](#) 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.

Stack name

Stack name

FsxN-Storage-Scaling

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

Dynamic Storage Scaling Parameters

File system ID
Amazon FSx file system ID

fs-0123456789abcd

Threshold
Used storage capacity threshold (%)

70

Percentage Capacity Increase
The percentage increase in storage capacity when used storage exceeds LowFreeDataStorageCapacityThreshold. Minimum increase is 10 %

20

Email address
The email address for alarm notification.

storagescaler@example.com

Maximum supported file system storage capacity (DO NOT MODIFY)
Maximum size supported for the primary SSD storage tier.

196608

Cancel Previous Next

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.

Mettre à jour 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.

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 d'une variété AWS de 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 de plus amples informations, veuillez consulter [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 FSx console Amazon. Le graphique de la capacité de stockage principale 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 FSx console Amazon à l'adresse <https://console.aws.amazon.com/fsx/>.
2. Choisissez Systèmes de fichiers dans la colonne de navigation de gauche, puis sélectionnez ONTAP système de 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.

Surveillance des économies d'efficacité du stockage

Lorsque cette option est activée, vous pouvez voir la capacité de stockage que vous économisez dans la FSx console Amazon, 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 FSx console Amazon FSx pour un système de fichiers ONTAP incluent les économies réalisées grâce à FlexClones et Snapshots.

1. Ouvrez la FSx console Amazon à l'adresse <https://console.aws.amazon.com/fsx/>.
2. Dans la liste FSx des systèmes de fichiers ONTAP, sélectionnez le système de fichiers ONTAP pour lequel vous souhaitez vérifier l'efficacité du stockage et économiser.
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 visualiser les économies réalisées en termes d'efficacité du stockage (ONTAP CLI)

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 et FlexClones — en exécutant la `storage aggregate show-efficiency` commande à l'aide du ONTAP CLI. Pour plus d'informations, reportez-vous à la section Démonstration de l'[efficacité des agrégats de stockage](#) dans le NetApp ONTAP Centre de documentation.

1. Pour accéder au ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

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

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 d'un SSD et des IOPS à l'aide de la FSx console, de la CLI et de l'API Amazon.

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 pour ONTAP, vous pouvez consulter les 10 mises à jour les plus récentes pour chaque type de mise à jour.

Updates (2) ↻				
Filter updates < 1 > ⚙️				
Update type ▾	Target value ▾	Status ▾	Progress % ▾	Request time ▾
Throughput capacity	256	✅ Completed	-	2022-03-12T12:16:46-05:00
Storage capacity	1127	🕒 Updated; Optimizing	-	2022-03-12T12:17:02-05:00

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 encore commencé à la traiter.
- En cours — Amazon traite FSx 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 [DescribeFileSystems](#) API. 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 exécute 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"
      }
    }
  ]
}
```

Capacité de stockage en volume

FSx les volumes 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 for ONTAP à l'aide de l' AWS Management Console API AWS CLI et de la CLI ONTAP.

Rubriques

- [Hiérarchisation des données de volume](#)
- [Instantanés et capacité de stockage en volume](#)
- [Capacité du fichier de volume](#)
- [Gestion de l'efficacité du stockage](#)
- [Activation du dimensionnement automatique](#)
- [Activation du mode d'écriture dans le cloud](#)
- [Mettre à jour la capacité de stockage](#)
- [Mettre à jour une politique de hiérarchisation](#)
- [Mise à jour des jours de refroidissement minimaux](#)
- [Mettre à jour la politique de récupération d'un volume dans le cloud](#)

- [Mettre à jour le nombre maximum de fichiers sur un volume](#)
- [Surveillance de la capacité de stockage des volumes](#)
- [Surveillance de la capacité de fichiers 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.

Note

FSx for ONTAP prend en charge la hiérarchisation des données en fonction du pool de capacités sur tous les SnapLock volumes, quel qu'en soit le SnapLock type. Pour de plus amples informations, veuillez consulter [Comment ? SnapLock fonctionnement](#).

Politiques de hiérarchisation des volumes

Vous déterminez comment utiliser FSx les niveaux de stockage de votre système de fichiers 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 FSx console Amazon AWS CLI, de l'API ou à l'aide d'[outils NetApp 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 de plus amples informations, veuillez consulter [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 FSx console Amazon.
- **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' FSx API Amazon 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. Si la politique Tout est appliquée à un volume qui contient déjà des données, les données existantes sont hiérarchisées entre le SSD et le pool de capacités. 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 sur un volume après qu'il ait utilisé une autre politique, les données existantes (y compris les instantanés) du volume qui se trouvaient dans le pool de capacité de stockage sont déplacées

vers le stockage SSD par un processus en arrière-plan. Cette migration de données ne se produit que lorsque l'utilisation de votre SSD est inférieure à 90 % et que la politique de récupération dans le cloud est définie sur `promote or on-read`. Ce processus en arrière-plan peut être accéléré en lisant intentionnellement les données. Pour de plus amples informations, veuillez consulter [Politiques de récupération dans le cloud](#).

Pour plus d'informations sur la définition ou la modification de la politique de hiérarchisation d'un volume, consultez [Mettre à jour une politique de hiérarchisation](#).

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. ONTAP exécute régulièrement la déduplication post-traitement sur les données stockées dans le niveau de stockage SSD, en ajustant automatiquement la fréquence en fonction du taux de variation des données dans le volume. Des taux plus élevés déclenchent des tâches de déduplication post-traitement plus fréquentes.

Par défaut, la compression post-traitement est désactivée en ONTAP raison de l'impact qu'elle peut avoir sur les performances des charges de travail continues du système de fichiers. Vous devez évaluer l'impact sur les performances de votre charge de travail avant d'activer la compression après le traitement. Pour activer la compression après le traitement, utilisez le niveau de privilège de diagnostic dans la ONTAP CLI et exécutez la commande suivante :

```
::> volume efficiency inactive-data-compression modify -vserver svm-name -volume vol-name -is-enabled true
```

ONTAP exécute une compression post-traitement pour les données conservées sur le stockage SSD pendant au moins 14 jours. Pour les charges de travail où il est peu probable que les données soient accessibles après une période plus courte, vous pouvez modifier les paramètres de compression post-traitement pour exécuter la compression post-traitement plus rapidement. Par exemple, pour appliquer les économies de compression après le traitement aux données non consultées depuis 5 jours, exécutez la commande ONTAP CLI suivante :

```
::> volume efficiency inactive-data-compression modify -vserver svm-name -volume vol-name -threshold-days 5 -threshold-days-min 2 -threshold-days-max 14
```

Pour plus d'informations sur la commande, voir [inactive-data-compression](#) [Modification de l'efficacité du volume](#)

En conservant les données sur SSD, vous optimisez les vitesses de transfert des sauvegardes de volume que vous créez, car les taux de transfert de données sont plus élevés pour le stockage SSD.

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, consultez [Mise à jour des jours de refroidissement minimaux](#).

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, consultez [Mettre à jour 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, consultez [Surveillance 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 de deuxième génération, 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 de plus amples informations, veuillez consulter [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 de plus amples informations, veuillez consulter [Protection de vos données grâce à 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 écrire de données supplémentaires sur ce volume.

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, consultez [Surveillance de la capacité de fichiers 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 :

$$\text{Volume\_Size\_in\_bytes} \times (1 \text{ fichier} \div \text{inode\_size\_in\_bytes}) = \text{nombre\_maximum\_de\_fichiers}$$
$$1\,073\,741\,824 \text{ octets} \times (1 \text{ fichier} \div 32\,768 \text{ octets}) = 32\,768 \text{ fichiers}$$

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 :

$$1\,073\,741\,824 \text{ octets} \times (1 \text{ fichier} \div 4\,096 \text{ octets}) = 262\,144 \text{ fichiers}$$

Et FSx pour ONTAP, le volume 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, consultez [Mettre à jour le nombre maximum de fichiers sur un volume](#).

Gestion de l'efficacité du stockage

En optimisant l'efficacité du stockage sur vos volumes FSx for ONTAP, vous pouvez optimiser l'utilisation du stockage, réduire les coûts de stockage et améliorer les performances globales de votre système de fichiers.

ONTAP organise les fichiers en blocs de données de 4 kibioctets (KiB). L'efficacité du stockage se fait au niveau des blocs de données plutôt qu'au niveau des fichiers individuels. Lorsque l'efficacité du stockage est atteinte, ONTAP utilise une combinaison de techniques de réduction des données pour éliminer les doublons, compresser la taille des données et réorganiser la disposition des données pour une utilisation optimale du disque.

L'efficacité du stockage s'applique de deux manières. Ils sont appliqués aux données en ligne (avant que les données ne soient écrites sur le disque, en mémoire) afin de réaliser des économies de stockage immédiates. Ils sont également appliqués aux données en arrière-plan (une fois les données écrites sur le disque) dans le niveau de stockage SSD par le biais de tâches d'efficacité périodiques visant à optimiser l'utilisation du stockage au fil du temps. L'efficacité du stockage en arrière-plan ne repose pas sur les données une fois celles-ci hiérarchisées en fonction du pool de capacités. Toutefois, si les données ont fait l'objet d'économies de stockage lorsqu'elles se trouvaient sur un SSD, ces économies sont préservées lorsque les données sont hiérarchisées en fonction du pool de capacité.

Note

ONTAP ne prend pas en charge l'amélioration de l'efficacité du stockage sur les volumes de protection des données (DP). Toutefois, les économies de stockage réalisées dans le volume source en lecture-écriture (RW) sont préservées lorsque les données sont répliquées sur le volume DP de destination.

Compression de blocs de données

Les groupes de compression sont des regroupements logiques de données qui sont gérés et compressés ensemble sous la forme d'un seul bloc. ONTAP regroupe automatiquement les blocs de données dans des groupes de compression, ce qui réduit l'espace consommé sur le disque. Pour

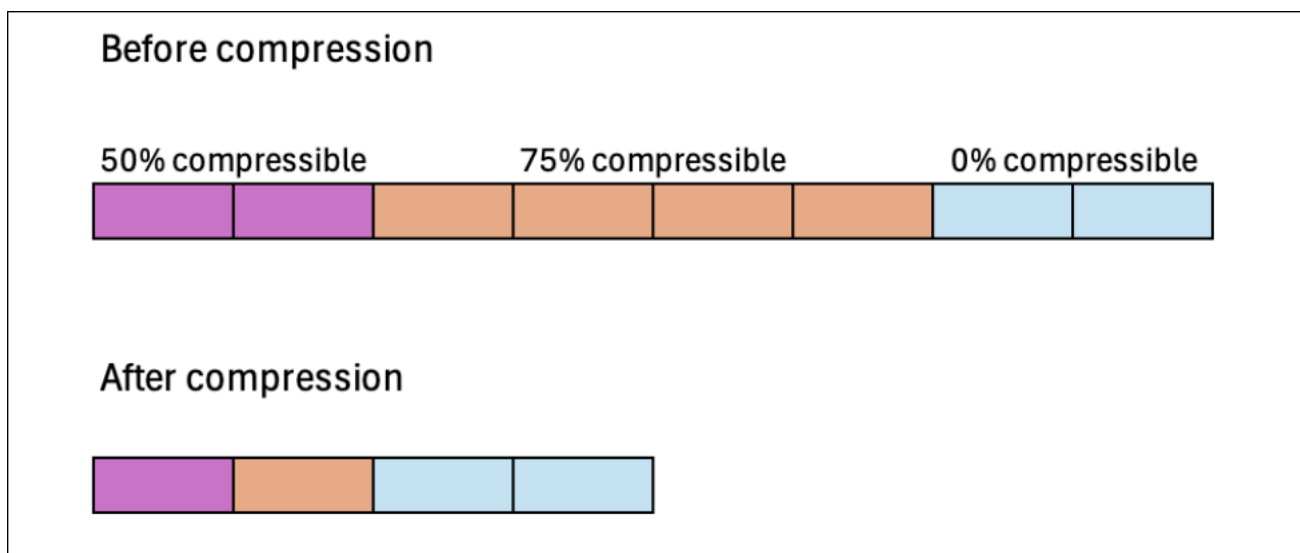
optimiser les performances et l'utilisation du stockage, ONTAP propose une approche équilibrée de la gestion des données en ajustant le degré de compression appliqué aux données en fonction de leurs modèles d'accès.

Par défaut, les données sont compressées en ligne à l'aide de groupes de compression de 8 Ko afin de garantir des performances optimales lors de l'écriture de données sur un volume. Vous pouvez éventuellement appliquer une compression plus importante aux données en activant la compression des données inactive sur un volume afin de compresser davantage les données sur le SSD. La compression des données inactives utilise des groupes de compression de 32 Ko sur les données froides afin de réaliser des économies de stockage supplémentaires. Pour plus d'informations, consultez la [volume efficiency inactive-data-compression modify](#) commande dans le NetApp ONTAP Documentation Center.

Note

La compression de données inactive consomme des IOPS supplémentaires sur le processeur et le disque et peut être une tâche gourmande en ressources. Nous vous recommandons d'évaluer l'impact sur les performances de l'exécution d'une compression de données inactive sur votre charge de travail avant d'activer cette fonctionnalité.

L'image suivante illustre les économies de stockage qui peuvent être réalisées en compressant des blocs de données.



Déduplication de blocs de données

ONTAP détecte et élimine les blocs de données dupliqués afin de réduire les redondances de données. Les blocs dupliqués sont remplacés par des références à des blocs uniques partagés.

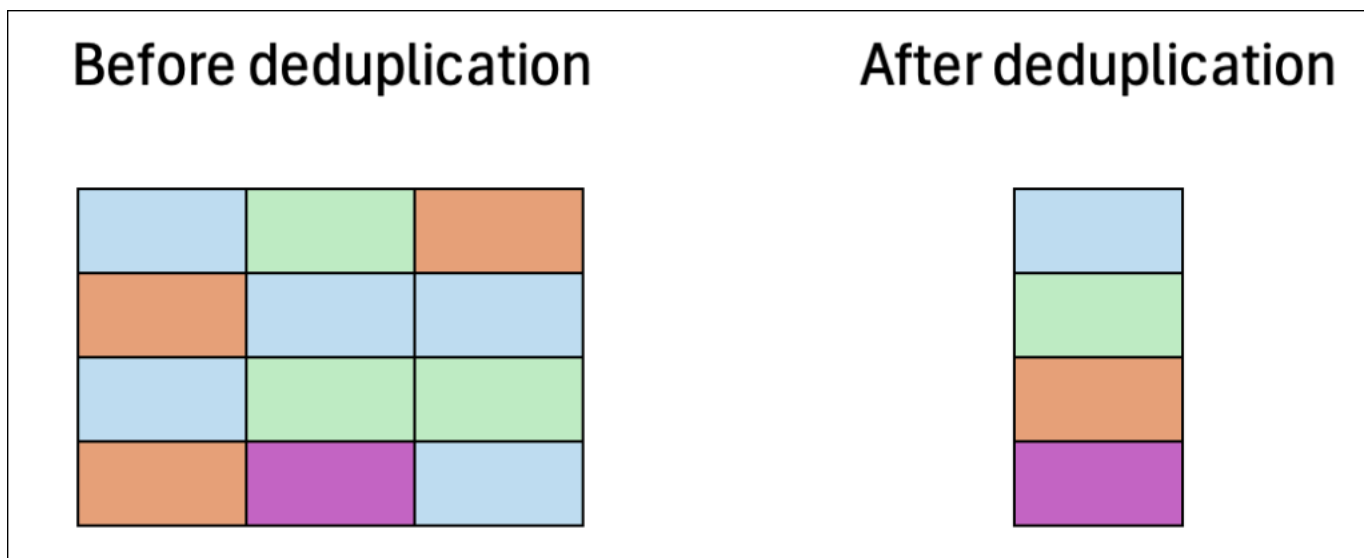
Par défaut, les données sont déduplicuées en ligne afin de réduire l'encombrement du stockage avant que les données ne soient écrites sur le disque. ONTAP exécute également un scanner de déduplication en arrière-plan à des intervalles spécifiés pour identifier et éliminer les doublons une fois qu'ils ont été écrits sur le disque. Au cours de ces analyses planifiées, ONTAP traite un journal des modifications pour identifier les blocs de données nouveaux ou modifiés depuis le dernier scan qui n'ont pas encore été déduplicués. Lorsque des doublons sont détectés, ONTAP met à jour les métadonnées pour qu'elles pointent vers une seule copie des blocs dupliqués et marque les blocs redondants comme de l'espace libre prêt à être récupéré.

Note

ONTAP applique la déduplication à 4 Ko d'écritures entrantes à la fois. Vous pouvez donc réaliser des économies de déduplication moindres lorsque vous exécutez des charges de travail avec des écritures d'une taille inférieure à 4 Ko.

FSx for ONTAP ne prend pas en charge la déduplication entre volumes.

L'image suivante illustre les économies de stockage qui peuvent être réalisées grâce à la déduplication.



Compaction de blocs de données

ONTAP consolide les blocs de données partiellement remplis de moins de 4 Ko chacun en un bloc de 4 Ko utilisé plus efficacement.

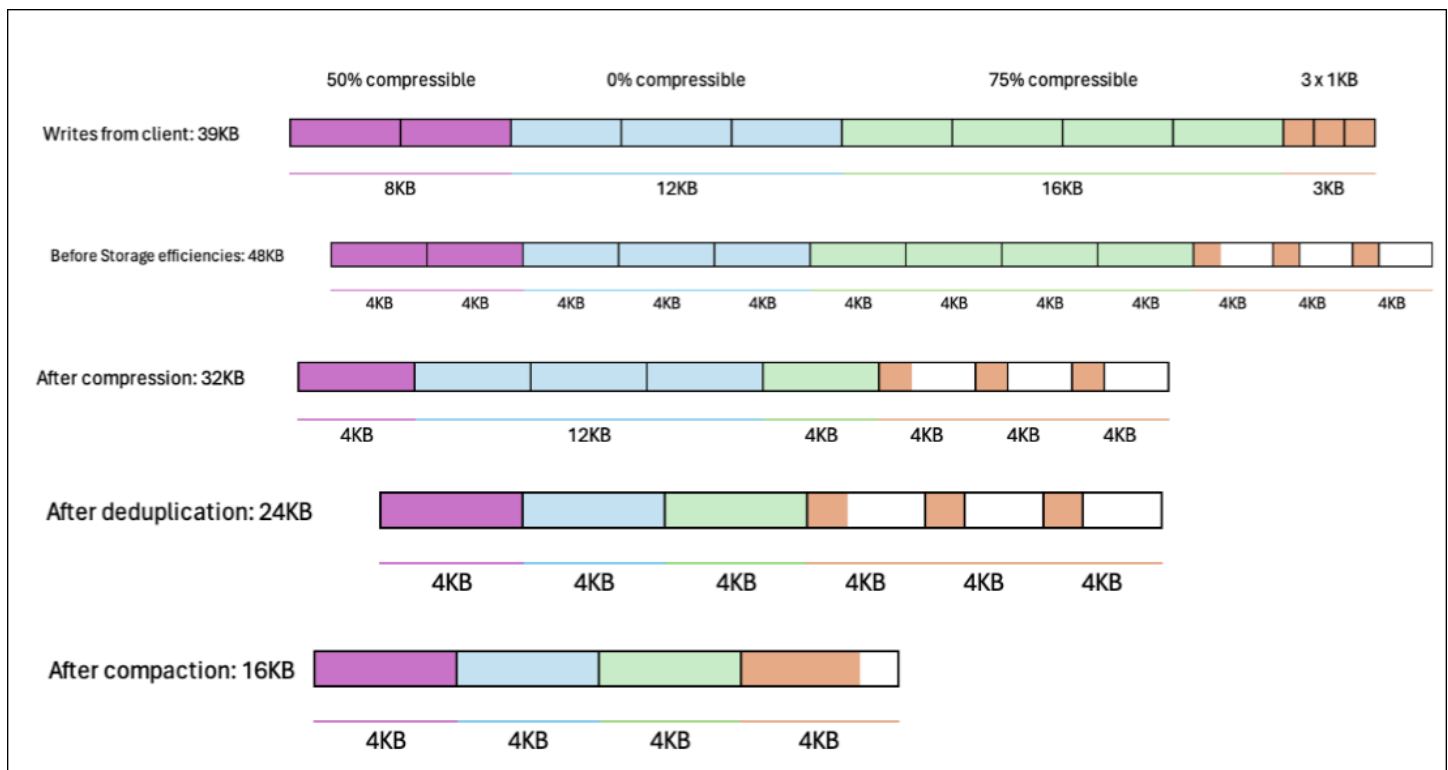
Par défaut, les données sont compactées en ligne afin d'optimiser la disposition des données lorsqu'elles sont écrites sur le disque afin de minimiser les frais de stockage, de réduire la fragmentation et d'améliorer les performances de lecture.

L'image suivante illustre les économies de stockage qui peuvent être réalisées grâce au compactage.



Exemple : efficacité du stockage

L'image suivante montre comment l'efficacité du stockage est appliquée aux données.



Activation du dimensionnement automatique

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 volume (le type de volume par défaut FSx pour ONTAP) à l'aide de la [volume autosize](#) commande ONTAP CLI.

Pour activer le dimensionnement automatique des volumes (CLI ONTAP)

1. Pour accéder à la ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

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).
 - Remplacez *max_size* 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.
 - *min_size* Remplacez-le 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 le 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
```

3. Pour afficher le paramètre de dimensionnement automatique actuel, exécutez la commande suivante. Remplacez *svm_name* et *vol_name* par vos informations.

```
::> volume autosize -vserver svm_name -volume vol_name
```

Activation du mode d'écriture dans le cloud

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 être soumis à la politique de hiérarchisation complète. Pour plus d'informations sur la modification de la politique de hiérarchisation d'un volume, consultez [Mettre à jour une politique de hiérarchisation](#).

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 ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

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.
```

Mettre à jour la capacité de stockage

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 FSx console Amazon et de l'API. AWS CLI Pour de plus amples informations, veuillez consulter [Mise à jour des volumes](#).

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 ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

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
```

Mettre à jour une politique de hiérarchisation

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 FSx console Amazon 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 de plus amples informations, veuillez consulter [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 FSx Amazon). 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 ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

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 de plus amples informations, veuillez consulter [Politiques de hiérarchisation des volumes](#).

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

Mise à jour des jours de refroidissement minimaux

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](#) ([UpdateVolume](#) action équivalente de l' FSx API Amazon). 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 ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

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.
```

Mettre à jour 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 ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

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.
```

Mettre à jour le nombre maximum de fichiers sur un volume

FSx pour les volumes ONTAP, la capacité de fichier peut être épuisée lorsque le nombre d'inodes ou de pointeurs de fichiers disponibles est épuisé.

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

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 ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

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
```

Surveillance de la capacité de stockage des volumes

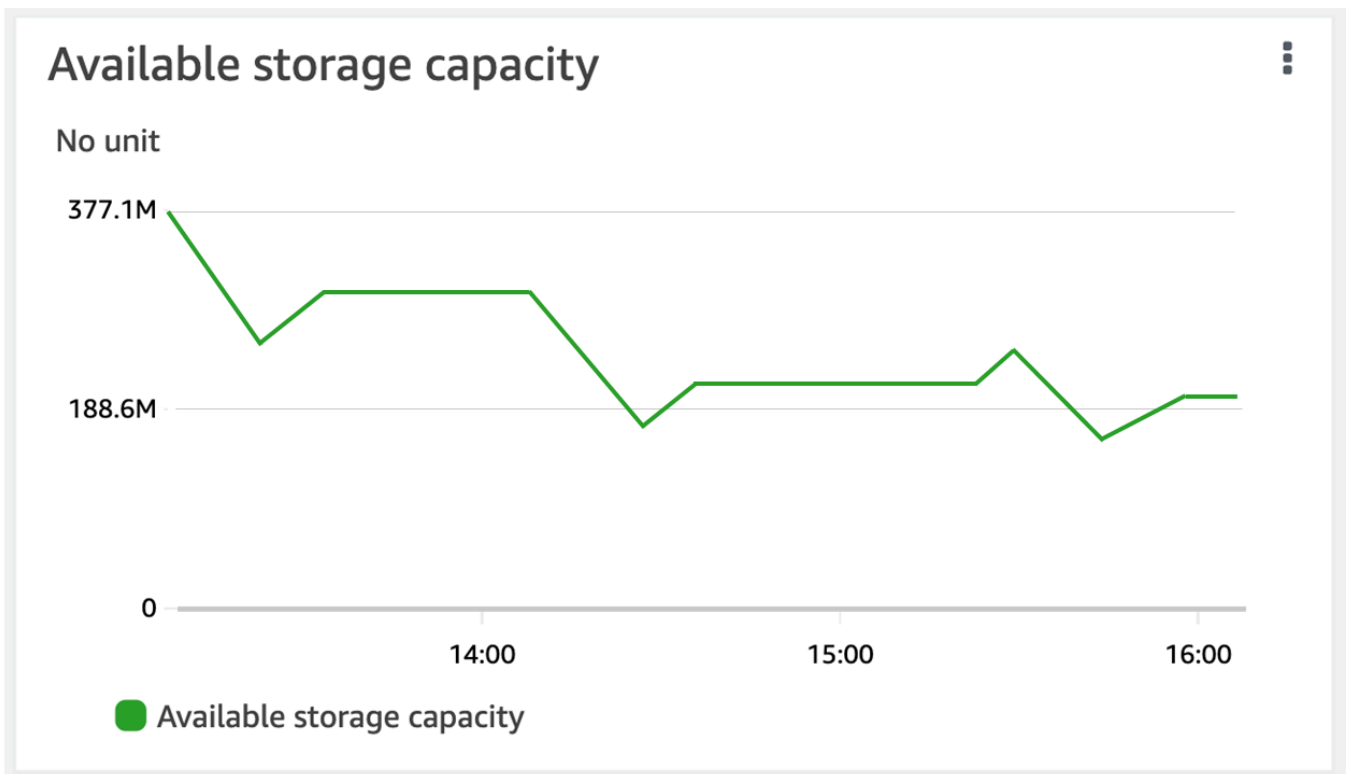
Vous pouvez consulter le stockage disponible d'un volume et sa distribution dans et dans AWS Management Console la CLI NetApp ONTAP. AWS CLI

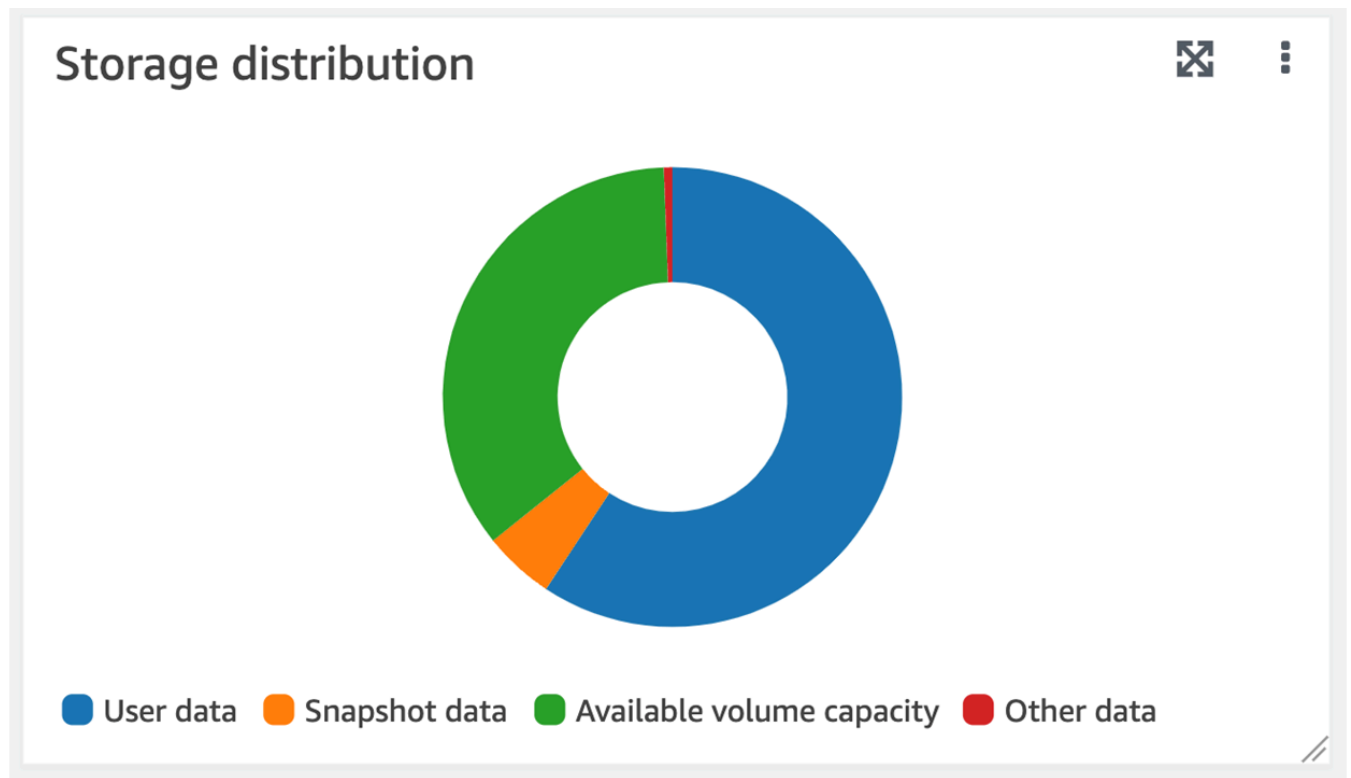
Pour surveiller la capacité de stockage d'un volume (console)

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

1. Ouvrez la FSx console Amazon 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.





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 ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

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 consomment 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.

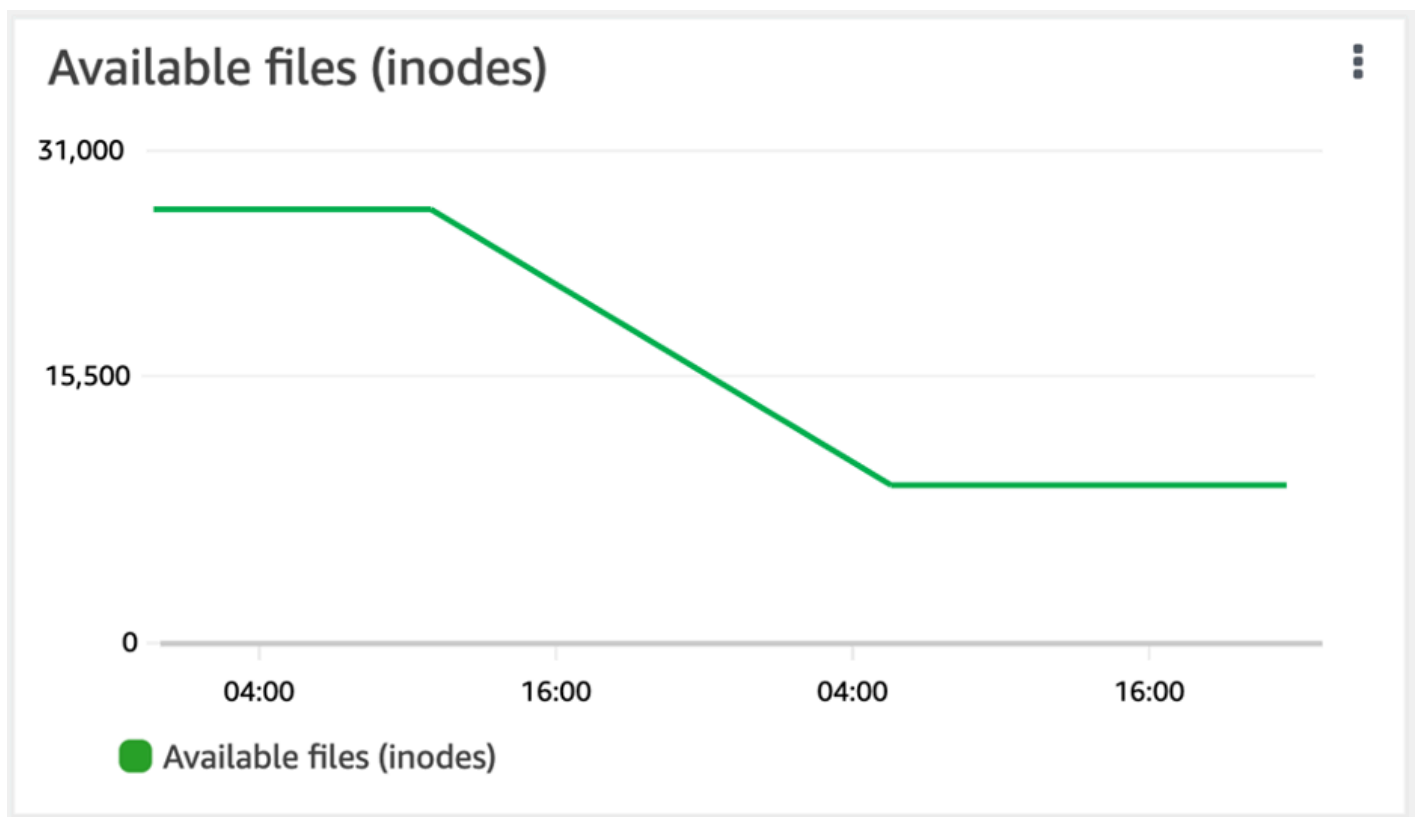
Pour les FlexVol types de volumes (type de volume par défaut FSx pour les volumes ONTAP), vous pouvez également activer le dimensionnement [automatique des volumes](#). Lorsque vous activez le dimensionnement automatique, la taille du volume augmente automatiquement lorsqu'elle

atteint certains seuils. Vous pouvez également désactiver les instantanés automatiques. Ces deux fonctionnalités sont expliquées dans les sections suivantes.

Surveillance de la capacité de fichiers 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 etFilesUsed.
- Dans la FSx console Amazon, 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.



Gestion des FSx systèmes de fichiers ONTAP

Un système de fichiers est la principale FSx ressource Amazon, à l'instar d'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

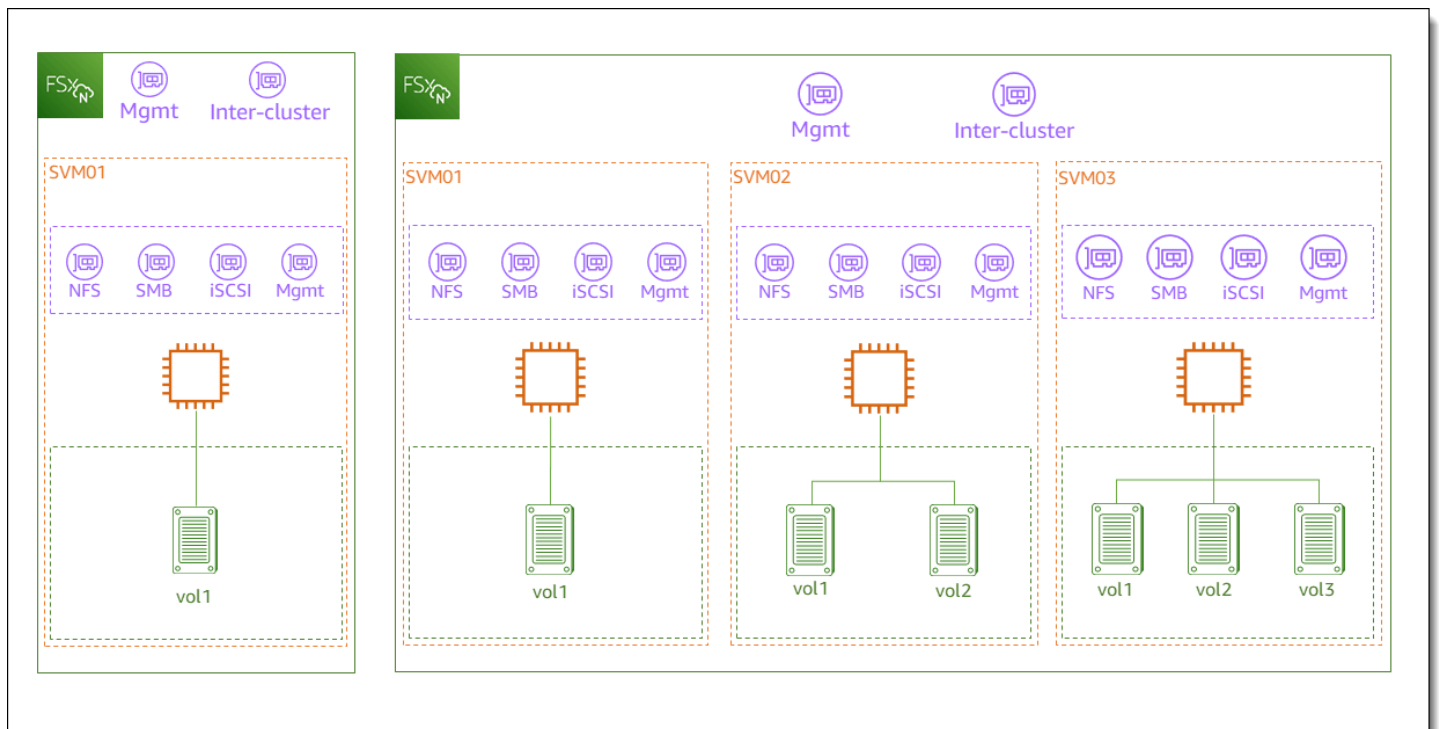
de fichiers. Chaque système de fichiers possède un point de terminaison de gestion que vous pouvez utiliser pour gérer les ressources et les données à l'aide de la CLI ONTAP ou de l'API REST.

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 (SVMs). Les systèmes de fichiers de première génération et les systèmes de fichiers multi-AZ de deuxième génération possèdent une paire HA, tandis que les systèmes de fichiers mono-AZ de deuxième génération ont jusqu'à 12 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.
- Un ou plusieurs SVMs 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 ONTAP FSx de première génération 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 volumes SVMs, certains SVMs comportant plusieurs volumes. Les systèmes de fichiers possèdent SVMs chacun plusieurs points de terminaison de gestion, SVMs ainsi que des points de terminaison d'accès aux données.



Lorsque vous créez un système de fichiers FSx pour 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. Les systèmes de fichiers mono-AZ de première génération prennent en charge une paire HA. Les systèmes de fichiers mono-AZ de deuxième génération prennent en charge jusqu'à 12 paires HA. 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 Les systèmes de fichiers multi-AZ de première et de deuxième génération prennent tous deux en charge une paire HA.

Note

Vous ne pouvez pas modifier le type de déploiement de votre système de fichiers après sa création. Si vous souhaitez modifier le type de déploiement (par exemple, passer du mode mono-AZ 1 au mode mono-AZ 2), vous pouvez sauvegarder vos données et les restaurer sur un nouveau système de fichiers. Vous pouvez également migrer vos données avec NetApp SnapMirror AWS DataSync, avec ou avec un outil de copie de données tiers.

Pour plus d'informations, consultez [Migration vers FSx for ONTAP à l'aide de NetApp SnapMirror](#) et [Migration vers FSx for ONTAP à l'aide de AWS DataSync](#).

- Capacité de stockage — Il s'agit de la quantité de stockage SSD, jusqu'à 192 tébioctets (TiB) pour les systèmes de fichiers de première génération, 512 TiB pour les systèmes de fichiers multi-AZ de deuxième génération et 1 pébioctet (PiB) pour les systèmes de fichiers mono-AZ de deuxième génération.
- 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 les systèmes FSx 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 FSx fichiers Amazon et un autre déploiement ONTAP (y compris un autre système de FSx fichiers Amazon). Chaque système de fichiers FSx pour ONTAP possède les points de terminaison suivants qui permettent d'accéder aux NetApp applications :

- 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 FSx ressources ONTAP à l'aide de NetApp applications](#) et [Réplication de vos données à l'aide de NetApp SnapMirror](#).

Création de systèmes de fichiers

Cette section explique comment créer un système de fichiers FSx pour ONTAP à l'aide de la FSx console Amazon ou de l' FSx API Amazon. AWS CLI 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 depuis la FSx console Amazon, Amazon crée FSx 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 volumes SVMs 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 pour 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, voir [Création d'un système de fichiers Amazon FSx for NetApp ONTAP](#).

1. Ouvrez la FSx console Amazon 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 pour 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 2, Single-AZ 2, Multi-AZ 1 ou Single-AZ 1.

- 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 Multi-AZ 1 est un système de fichiers de première génération FSx pour ONTAP. Multi-AZ 2 est un système de fichiers de deuxième génération. Ils prennent tous deux en charge une paire de haute disponibilité (HA).
- Les systèmes de fichiers mono-AZ répliquent vos données et offrent un basculement automatique au sein d'une seule zone de disponibilité. Le système de fichiers Single-AZ 1 est un système de fichiers ONTAP de première génération FSx qui prend en charge une paire HA. Le système de fichiers Single-AZ 2 est un système de fichiers de deuxième génération qui prend en charge jusqu'à 12 paires HA. Pour de plus amples informations, veuillez consulter [Gestion des paires de haute disponibilité \(HA\)](#).

Pour plus d'informations sur les types de déploiement, consultez [Disponibilité, durabilité et options de déploiement](#).

 Note

Vous ne pouvez pas modifier le type de déploiement de votre système de fichiers après sa création. Si vous souhaitez modifier le type de déploiement (par exemple, passer du mode mono-AZ 1 au mode mono-AZ 2), vous pouvez sauvegarder vos données et les restaurer sur un nouveau système de fichiers. Vous pouvez également migrer vos données avec NetApp SnapMirror AWS DataSync, avec ou avec un outil de copie de données tiers. Pour plus d'informations, consultez [Migration vers FSx for ONTAP à l'aide de NetApp SnapMirror](#) et [Migration vers FSx for ONTAP à l'aide de AWS DataSync](#).

- Pour la capacité de stockage SSD, entrez la capacité de stockage de votre système de fichiers, en gïbi-octets (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 de plus amples informations, veuillez consulter [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 la capacité de débit, deux options s'offrent à vous pour déterminer votre capacité de débit en mégaoctets par seconde () : MBps
 - Choisissez Capacité de débit recommandée si vous souhaitez qu'Amazon FSx choisisse automatiquement la capacité de débit en fonction de la 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 de plus amples informations, veuillez consulter [Gestion des paires de 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 de plus amples informations, veuillez consulter [Amazon FSx pour les performances d' NetApp 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 de plus amples informations, veuillez consulter [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`. Lorsque vous créez FSx des systèmes de fichiers ONTAP Multi-AZ à l'aide de AWS CloudFormation nous, nous vous recommandons d'ajouter la `Key: AmazonFSx; Value: ManagedByAmazonFSx` balise manuellement.

- (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 : FSx Amazon 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 : FSx Amazon 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 flottantes 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 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 Chiffrement, pour Clé de chiffrement, choisissez la clé de chiffrement AWS Key Management Service (AWS KMS) qui protège les données de votre système de fichiers au repos.
8. Pour le mot de passe administratif du système de fichiers, entrez un mot de passe sécurisé pour l'fsxadminutilisateur. Confirmez le mot de passe.

Vous pouvez utiliser l'fsxadminutilisateur pour administrer votre système de fichiers à l'aide de la CLI ONTAP et de l'API REST. Pour plus d'informations sur l'fsxadminutilisateur, consultez [Gestion des systèmes de fichiers à l'aide du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

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'vsadminutilisateur pour administrer la SVM à l'aide de la CLI ONTAP ou de l'API REST. Pour plus d'informations sur l'vsadminutilisateur, consultez [Gérer SVMs avec le ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

Si vous choisissez Ne pas spécifier de mot de passe (valeur par défaut), vous pouvez toujours utiliser l'fsxadminutilisateur 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.

- Pour le style de sécurité du volume, choisissez entre Unix (Linux) et NTFS pour le volume. Pour de plus amples informations, veuillez consulter [Style de sécurité des volumes](#).
- Dans la section Active Directory, vous pouvez associer un Active Directory à la SVM. Pour de plus amples informations, veuillez consulter [Utilisation de Microsoft Active Directory dans FSx 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 : IPv4 adresses 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 FSx les administrateurs 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 avec une seule paire HA) Pour le style de volume, choisissez l'un des deux FlexVol ou FlexGroup. FlexVol les volumes sont des volumes à usage général dont la taille peut atteindre 300 tébioctets (TiB). FlexGroup les 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 20 et 314 572 800 mégaoctets (MiB) pour FlexVol volumes ou 800 Gibioctets (GiB) —2 400 TiB par paire HA pour FlexGroup volumes. Par exemple, un système de fichiers comportant 12 paires HA aurait une taille de volume minimale de 9 600 GiB et une taille maximale de 20 480 TiB.
- 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'un NetApp SnapMirror or SnapVault relation. Pour de plus amples informations, veuillez consulter [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 de plus amples informations, veuillez consulter [Efficacité du stockage](#).
- 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, consultez [Règles 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 le NetApp Documentation du produit 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, consultez [Politiques 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, les politiques valides 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 la section SnapLock Configuration du volume par défaut, pour SnapLock Configuration, choisissez entre Activé et Désactivé. Pour plus d'informations sur la configuration d'un SnapLock Volume de conformité ou SnapLock Volume d'entreprise, voir [Compréhension SnapLock Conformité d'](#) et [Compréhension SnapLock Enterprise](#). Pour plus d'informations sur SnapLock, voir [Protégez vos données avec SnapLock](#).
13. 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.
14. 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.

15. 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.

16. Choisissez Create file system (Créer un système de fichiers).

Pour créer un système de fichiers (CLI)

- Pour créer un système de fichiers FSx pour ONTAP, utilisez la commande [create-file-system](#) CLI (ou l'opération [CreateFileSystem](#) API équivalente), comme indiqué dans l'exemple suivant.

Note

Vous ne pouvez pas modifier le type de déploiement de votre système de fichiers après sa création. Si vous souhaitez modifier le type de déploiement (par exemple, passer du mode mono-AZ 1 au mode mono-AZ 2), vous pouvez sauvegarder vos données et les restaurer sur un nouveau système de fichiers. Vous pouvez également migrer vos données avec NetApp SnapMirror AWS DataSync, avec ou avec un outil de copie de données tiers. Pour plus d'informations, consultez [Migration vers FSx for ONTAP à l'aide de NetApp SnapMirror](#) et [Migration vers FSx for ONTAP à l'aide de AWS DataSync](#).

```
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
```

Après avoir créé le système de fichiers 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 `CreateFileSystemAPI`

ne créent pas de SVM ou de volume par défaut. Pour créer une SVM, voir [Création de machines virtuelles de stockage \(SVM\)](#) ; pour créer un volume, voir [Création de volumes](#).

Création de systèmes de fichiers FSx pour ONTAP dans des sous-réseaux partagés

Le partage VPC permet Comptes AWS à plusieurs utilisateurs de créer des ressources dans des clouds privés virtuels partagés et gérés de manière centralisée (). VPCs 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 être créés FSx pour les systèmes de fichiers ONTAP mono-AZ et 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 FSx autoriser Amazon à modifier les tables de routage dans les sous-réseaux partagés au nom du compte participant. Pour de plus amples informations, veuillez consulter [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 FSx des systèmes de fichiers 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 pour 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 FSx service Amazon les autorisations nécessaires pour modifier les tables de routage dans les sous-réseaux partagés au nom du compte du participant. Pour de plus amples 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 seront créés FSx pour les systèmes de fichiers ONTAP dans les sous-réseaux partagés, vous devez effectuer les opérations suivantes :

- Le propriétaire du VPC doit l'utiliser pour AWS Resource Access Manager partager en toute sécurité des sous-réseaux avec VPCs 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 en partager un ou plusieurs VPCs 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 des comptes participants puissent être créés FSx pour les systèmes de fichiers ONTAP Multi-AZ, le propriétaire du VPC doit également accorder au FSx service Amazon 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 FSx les systèmes de fichiers ONTAP Multi-AZ 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 incident 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 multi-AZ FSx pour ONTAP dans des sous-réseaux VPC que le propriétaire a partagés avec les participants à l'aide de l'API, et AWS Management Console AWS CLI, comme décrit dans les sections suivantes.

Pour gérer le partage VPC pour les systèmes de fichiers multi-AZ (console)

Ouvrez la FSx console Amazon 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 ceux VPCs 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 [describe-shared-vpc-configuration](#)CLI, ou la commande API [DescribeSharedVpcConfiguration](#)équivalente, illustrée ci-dessous :

```
$ 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 [update-shared-vpc-configuration](#)CLI ou la commande API [UpdateSharedVpcConfiguration](#)équivalente. 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"
}
```

Mise à jour des systèmes de fichiers

Cette rubrique explique les propriétés d'un système de fichiers existant que vous pouvez mettre à jour et fournit des procédures pour ce faire à l'aide de la FSx console et de la CLI Amazon. Vous pouvez mettre à jour les éléments suivants FSx pour les propriétés du système de fichiers ONTAP à l'aide de la FSx console Amazon et de l'API : AWS CLI

- Sauvegardes quotidiennes automatiques. Active ou désactive les sauvegardes quotidiennes automatiques, modifie la fenêtre de sauvegarde et la période de conservation des sauvegardes. Pour de plus amples informations, veuillez consulter [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 de plus amples informations, veuillez consulter [Optimisation des performances avec les fenêtres FSx de maintenance Amazon](#).
- Mot de passe administratif du système de fichiers. Modifie le mot de passe de l'fsxadminutilisateur du système de fichiers. Vous pouvez utiliser l'fsxadminutilisateur pour administrer votre système de fichiers à l'aide de la CLI ONTAP et de l'API REST. Pour plus d'informations sur l'fsxadminutilisateur, consultez [Gestion des systèmes de fichiers à l'aide du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).
- 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`. Lors de la création ou de FSx la mise à jour de systèmes de fichiers ONTAP Multi-AZ, AWS CloudFormation nous vous recommandons d'ajouter la `Key: AmazonFSx; Value: ManagedByAmazonFSx` balise manuellement.

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 pour ONTAP existant à l'aide du AWS Management Console.

Pour mettre à jour les sauvegardes quotidiennes automatiques

1. Ouvrez la FSx console Amazon 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 FSx de fichiers 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 FSx console Amazon 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 FSx de fichiers 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 FSx console Amazon 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 FSx de fichiers 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, vous pouvez utiliser [security login role config show](#) ONTAP Commande CLI pour afficher les paramètres d'exigence de mot de passe sur le système de fichiers. Pour plus d'informations, notamment pour savoir comment modifier le paramètre du mot de passe, consultez [La 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 FSx console Amazon 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 FSx de fichiers 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 pour 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 [update-file-system](#) CLI (ou l'opération [UpdateFileSystem](#) API équivalente), 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
```

Gestion des paires de haute disponibilité (HA)

Chaque système de fichiers FSx pour ONTAP est alimenté par une ou plusieurs paires de serveurs de fichiers à haute disponibilité (HA) dans une configuration en mode 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. FSx pour ONTAP, les systèmes de fichiers de première génération sont alimentés par une paire HA, qui fournit jusqu'à 4 % de capacité GBps de débit et 160 000 SSD. IOPS FSx pour ONTAP, les systèmes de fichiers multi-AZ de deuxième génération sont également alimentés par une paire HA et fournissent jusqu'à 6 % de capacité GBps de débit et 200 000 IOPS sur SSD. FSx pour ONTAP, les systèmes de fichiers mono-AZ de deuxième génération sont alimentés par un maximum de 12 paires HA, qui peuvent fournir jusqu'à 72 % de capacité GBps de débit et 2 400 000 IOPS SSD (6 % de capacité GBps de débit et 200 000 IOPS SSD par paire HA).

Lorsque vous créez votre système de fichiers depuis la FSx console Amazon, 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 un maximum GBps de 6 % de capacité de débit et 200 000 SSD IOPs, 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 pouvez ajouter des paires HA aux systèmes de fichiers mono-AZ de deuxième génération. Pour de plus amples informations, veuillez consulter [Ajouter des paires à haute disponibilité \(HA\)](#). Sinon, vous pouvez migrer des données entre des systèmes de fichiers (avec différentes paires HA) en utilisant SnapMirror AWS DataSync, ou en restaurant vos données d'une sauvegarde vers un nouveau système de fichiers.

Ajouter des paires à haute disponibilité (HA)

FSx pour ONTAP, les systèmes de fichiers sont composés d'une ou de plusieurs paires HA de serveurs de fichiers. Les systèmes de fichiers de première génération et les systèmes de fichiers multi-AZ de deuxième génération prennent en charge une paire HA, tandis que les systèmes de fichiers mono-AZ de deuxième génération prennent en charge jusqu'à 12 paires HA. Vous pouvez également ajouter d'autres paires HA après avoir créé un système de fichiers mono-AZ de deuxième génération (jusqu'à 12 au maximum). L'ajout de paires HA n'est pas perturbant et ne prend généralement que quelques minutes.

Tenez compte des points suivants lorsque vous ajoutez des paires HA à votre système de fichiers :

- L'ajout de paires HA à votre système de fichiers introduit de nouveaux serveurs de fichiers dotés de leur propre stockage (ou agrégat). Les nouvelles paires HA ont les mêmes capacités de débit et de stockage que les paires HA existantes de votre système de fichiers. Supposons, par exemple, que votre système de fichiers possède deux paires HA avec un total de 12 % GBps de capacité de débit et 2 tébioctets (TiB) de stockage SSD. Si vous ajoutez une nouvelle paire HA, votre système de fichiers disposera d'une capacité GBps de débit de 18 % et de 3 TiB de stockage SSD.
- Pour bénéficier des performances supplémentaires des nouvelles paires HA, vous devez déplacer certains de vos volumes existants vers les nouvelles paires HA et remonter les clients pour s'y

connecter. Pour de plus amples informations, veuillez consulter [Équilibrer les charges de travail entre les paires HA](#).

- Vous ne pouvez pas modifier la capacité de débit de votre système de fichiers, la capacité de stockage SSD ou les IOPS SSD provisionnées lorsque vous ajoutez des paires HA ou lorsqu'une mise à jour pour ajouter des paires HA est en cours.
- Vous ne pouvez pas supprimer les paires HA après les avoir ajoutées. Nous vous recommandons d'augmenter la capacité de débit de votre système de fichiers si vous avez temporairement besoin de performances accrues (en supposant que votre système de fichiers n'atteint pas la capacité de débit maximale). Cela augmente la capacité de débit des paires HA existantes de votre système de fichiers.
- Pour augmenter le nombre de paires HA d'un système de fichiers de deuxième génération de un à deux ou plus, votre système de fichiers peut comporter cinq SVM au maximum.
- Le protocole iSCSI est disponible sur les systèmes de fichiers dotés de six paires haute disponibilité (paires HA) ou moins. Le protocole NVMe /TCP est disponible sur les systèmes de fichiers de deuxième génération comportant six paires HA ou moins. Pour de plus amples informations, veuillez consulter [Accès à vos données FSx for ONTAP](#).
- Lorsque vous ajoutez de nouvelles paires HA à votre système de fichiers, le NVMe cache est activé par défaut pour les nouveaux nœuds du système de fichiers. Nous vous recommandons de le désactiver pour les charges de travail gourmandes en débit. Pour de plus amples informations, veuillez consulter [Gestion du NVMe cache](#).

Pour ajouter des paires HA

1. Ouvrez la FSx console Amazon 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 FSx de fichiers ONTAP que vous souhaitez mettre à jour.
3. Dans le panneau Résumé, pour Nombre de paires HA, choisissez Mettre à jour.
4. Dans la liste déroulante des paires HA, sélectionnez le nombre de paires HA que vous souhaitez ajouter à votre système de fichiers.
5. Cliquez sur le bouton Mettre à jour.

Après avoir ajouté des paires HA, il est important de rééquilibrer vos données existantes afin de garantir que vos E/S restent réparties uniformément entre les paires HA de votre système de fichiers.

Pour de plus amples informations, veuillez consulter [Équilibrer les charges de travail entre les paires HA](#).

Équilibrer les charges de travail entre les paires HA

Si votre système de fichiers comporte plusieurs paires de haute disponibilité (HA), son débit et son stockage sont répartis sur chacune de vos paires de haute disponibilité. FSx for ONTAP équilibre automatiquement vos fichiers au fur et à mesure qu'ils sont écrits dans votre système de fichiers, mais vos données de charge de travail et vos E/S ne sont plus équilibrées une fois que vous ajoutez des paires HA. En outre, dans de rares cas, les données ou les E/S de votre charge de travail peuvent être déséquilibrées entre les paires HA existantes de votre système de fichiers, ce qui peut avoir un impact sur les performances globales de votre charge de travail. Si votre charge de travail est déséquilibrée, vous pouvez la rééquilibrer sur chacune des paires HA de votre système de fichiers (ainsi que sur les serveurs de fichiers et les agrégats correspondants, à savoir 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](#)
- [Rééquilibrage des volumes](#)

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. Pour de plus amples informations, veuillez consulter [Déplacement de volumes entre agrégats](#).

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'informations sur cette procédure, consultez Rééquilibrage des volumes .
Le débit du réseau est déséquilibré, mais le débit du disque de votre serveur de fichiers, le nombre d'IOPS du disque du	Vos données sont réparties uniformément entre les paires HA, mais pas vos clients. Pour les serveurs de fichiers dont l'utilisation du débit réseau 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

Si votre système de fichiers est...	Alors...
serveur de fichiers ou le nombre d'IOPS du disque ne sont pas déséquilibrés	terminaison différent sur une paire HA différente. Pour plus d'informations sur cette procédure, consultez Rééquilibrage des clients .

Mappage des CloudWatch dimensions aux ressources de la CLI ONTAP et de l'API REST

Votre système de fichiers de deuxième génération contient CloudWatch des métriques Amazon avec la Aggregate dimension `FileServer` or. 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, `FsxD01234567890abcdef-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 `FsxD01234567890abcdef-01` (le serveur de fichiers actif) et `FsxD01234567890abcdef-02` (le serveur de fichiers secondaire) dans une paire HA, l'agrégat `aggr2` est partagé par `FsxD01234567890abcdef-03` les serveurs de fichiers `FsxD01234567890abcdef-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 NetApp ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#) section du guide de l'utilisateur d'Amazon FSx pour NetApp ONTAP.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

- 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

Après avoir ajouté des paires HA ou si vous rencontrez un déséquilibre des E/S sur les serveurs de fichiers (en particulier en ce qui concerne l'utilisation du débit réseau), vous pouvez rééquilibrer vos clients. Si vous rééquilibrez les clients après avoir ajouté des paires HA, vous pouvez passer à [Remontage de clients](#). Sinon, vous devez d'abord identifier les clients à fort trafic que vous souhaitez déplacer afin de rééquilibrer les E/S de votre charge de travail.

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.

Identifiez les clients à fort trafic

- Pour accéder en SSH à la NetApp CLI ONTAP de votre système de fichiers, suivez les étapes décrites dans la [Utilisation de NetApp ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#) section du guide de l'utilisateur d'Amazon FSx pour NetApp ONTAP.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

- 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.

Client	Vserver	Node	*Total Ops	Total (Bps)
172.17.236.53:938	svm01	FsxId01234567890abcdef-01	2143	140443648
172.17.236.160:898	svm02	FsxId01234567890abcdef-01	812	53215232

Remontage de clients

- Vous pouvez rééquilibrer les clients vers d'autres paires HA. 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 le montage d'un client sur un point de terminaison différent, vous pouvez spécifier une adresse IP de point de terminaison différente de celle correspondant au serveur de fichiers qui reçoit 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 `FsxD01234567890abcdef-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 `FsxD01234567890abcdef-03`).

Rééquilibrage des volumes

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 NetApp ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#) section du guide de l'utilisateur d'Amazon FSx pour 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.

Volume	Vserver	Aggregate	*Total Ops	Read Ops	Write Ops	Other Ops	Read (Bps)	Write (Bps)	Latency (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.

- Si vous avez ajouté de nouvelles paires HA, vous devez déplacer les volumes existants vers de nouveaux agrégats. Pour de plus amples informations, veuillez consulter [Déplacement de volumes entre agrégats](#).

Gestion du NVMe cache

Le NVMe cache est activé par défaut sur votre système de fichiers de deuxième génération. Si la charge de travail de votre système de fichiers de deuxième génération est importante, vous pouvez désactiver le NVMe cache pour améliorer les performances. La procédure suivante explique comment activer, désactiver et valider le NVMe cache de votre système de fichiers.

Pour gérer le NVMe cache

1. Connectez-vous en SSH à votre ONTAP système de fichiers. Pour de plus amples informations, veuillez consulter [the section called “Utilisation de NetApp ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)”](#).

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Utilisation de la [system node external-cache modify](#) ONTAP commande CLI. Choisissez **true** d'activer le NVMe cache ou **false** de le désactiver.

```
::> system node external-cache modify -node * -is-enabled [true|false]
```

3. Utilisation de la [system node external-cache show](#) ONTAP Commande CLI pour vérifier si le NVMe cache est activé ou désactivé.

```
::> system node external-cache show -node * -fields is-enabled
```

Le NVMe cache est activé ou désactivé par nœud. Lorsque vous ajoutez de nouvelles paires de haute disponibilité (HA) à votre système de fichiers, chaque nouveau nœud présente le même comportement par défaut que les nœuds d'un nouveau système de fichiers. Par conséquent, le NVMe cache serait activé pour tous les nouveaux nœuds d'un système de fichiers, même si les nœuds existants l'ont désactivé. Pour de plus amples informations, veuillez consulter [Ajouter des paires à haute disponibilité \(HA\)](#).

Surveillance 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 FSx console Amazon, de l' AWS CLI API et de l'assistance. AWS SDKs

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 de plus amples informations, veuillez consulter [Surveillance avec Amazon CloudWatch](#).

- Administration : affiche les informations d'administration du système de fichiers suivantes :
 - Le DNS noms et IP adresses des points de terminaison entre clusters et de gestion du système de fichiers.
 - Le ONTAP nom d'utilisateur de l'administrateur.
 - La possibilité de mettre à jour le ONTAP mot de passe administrateur.
- Liste des systèmes de fichiers SVMs
- 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 [describe-file-systems](#)CLI ou l'opération [DescribeFileSystems](#)API.

FSx pour connaître l'état du système de fichiers ONTAP

Vous pouvez consulter l'état d'un système de FSx fichiers Amazon à l'aide de la FSx console Amazon, de la AWS CLI commande [describe-file-systems](#) ou de l'opération API [DescribeFileSystems](#).

État du système de fichiers	Description
DISPONIBLE	Le système de fichiers a été créé avec succès et est prêt à être utilisé.

État du système de fichiers	Description
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 ne FSx parvient pas à le récupérer. 2. Lors de la création d'un nouveau système de fichiers, Amazon n' FSx a pas été en mesure de créer un nouveau système de fichiers.

Suppression de systèmes de fichiers

Vous pouvez supprimer un système de fichiers FSx pour ONTAP à l'aide de la FSx console Amazon, du AWS CLI, et de l' FSx API Amazon et SDKs.

Pour supprimer un système de fichiers :

- Utilisation de la console : suivez la procédure décrite dans [Nettoyage des ressources](#).
- À l'aide de la CLI ou de l'API : supprimez d'abord tous les volumes et tous les SVMs éléments de votre système de fichiers. Utilisez ensuite la commande [delete-file-system](#)CLI ou l'opération [DeleteFileSystem](#)API.

Gestion FSx des machines virtuelles de stockage ONTAP

Dans FSx ONTAP, les volumes sont hébergés sur des serveurs de fichiers virtuels appelés machines virtuelles de stockage (SVMs). 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 d'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. FSx

Amazon crée FSx 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 en créer d'autres SVMs sur votre système de fichiers à tout moment à l'aide de la console ou de FSx l'API Amazon et SDKs. AWS CLI Vous ne pouvez pas créer SVMs à l'aide de la CLI ONTAP ou de l'API REST.

Vous pouvez vous connecter SVMs à un Microsoft Active Directory pour l'authentification et l'autorisation d'accès aux fichiers. Pour de plus amples informations, veuillez consulter [Utilisation de Microsoft Active Directory dans FSx ONTAP](#).

Nombre maximum de systèmes de fichiers SVMs par système de fichiers

Le tableau suivant indique le nombre maximum de fichiers SVMs que vous pouvez créer pour un système de fichiers. Le nombre maximum de SVMs dépend de la capacité de débit allouée en mégaoctets par seconde (). MBps

Paires à haute disponibilité (HA)	Quantité de capacité de débit () MBps	Nombre maximum de systèmes de fichiers SVMs par système de fichiers
1 paire HA	128	6
	256	6
	384	6
	512	14
	768	14
	1,024	14
	1 536	14
	2 048	24
	3 072	14
	4 096	24
	6 144	24

Paires à haute disponibilité (HA)	Quantité de capacité de débit () MBps	Nombre maximum de systèmes de fichiers SVMs par système de fichiers
2 à 12 paires HA	N'importe quel compte	5

Rubriques

- [Création de machines virtuelles de stockage \(SVM\)](#)
- [Mise à jour des machines virtuelles de stockage \(SVM\)](#)
- [Audit de l'accès aux fichiers](#)
- [Configuration d'un serveur SMB dans un groupe de travail](#)
- [Surveillance des détails de configuration des machines virtuelles de stockage \(SVM\)](#)
- [Suppression de machines virtuelles de stockage \(SVM\)](#)

Création de machines virtuelles de stockage (SVM)

Vous pouvez créer une SVM FSx pour ONTAP à l'aide de l' AWS Management Console API AWS CLI, et.

Le nombre maximum SVMs que vous pouvez créer pour un système de fichiers dépend du type de déploiement de votre système de fichiers et de la capacité de débit allouée. Pour de plus amples informations, veuillez consulter [Nombre maximum de systèmes de fichiers SVMs 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 de plus amples informations, veuillez consulter [Utilisation de Microsoft Active Directory dans FSx ONTAP](#).
- Style de sécurité du volume racine — Définissez le style de sécurité du volume racine (Unix ou NTFS) en fonction du type de clients que vous utilisez pour accéder à vos données dans la SVM. Pour de plus amples informations, veuillez consulter [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 de plus amples informations, veuillez consulter [Gérer SVMs avec le ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

Pour créer une machine virtuelle de stockage (console)

1. Ouvrez la FSx console Amazon 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'utilisateur `vsadmin` pour administrer la SVM à l'aide de la CLI ONTAP ou de l'API REST. Pour plus d'informations sur l'utilisateur `vsadmin`, consultez [Gérer SVMs avec le ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

Si vous choisissez Ne pas spécifier de mot de passe (valeur par défaut), vous pouvez toujours utiliser l'utilisateur `fsxadmin` 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 de plus amples informations, veuillez consulter [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 : IPv4 adresses 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 FSx les administrateurs 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 de plus amples informations, veuillez consulter [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)

- FSx Pour créer une machine virtuelle de stockage (SVM) pour ONTAP, utilisez la commande [create-storage-virtual-machine](#) CLI (ou l'opération [CreateStorageVirtualMachine](#) API 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",
        "IpAddresses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com",
        "IpAddresses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddresses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddresses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com",
        "IpAddresses": ["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 des machines virtuelles de stockage (SVM)

Vous pouvez mettre à jour les propriétés de configuration de la machine virtuelle de stockage (SVM) suivantes à l'aide de la FSx console Amazon et de FSx l'API Amazon : AWS CLI

- 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 de plus amples informations, veuillez consulter [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 FSx console Amazon 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 une liste de toutes les machines SVMs disponibles Compte AWS dans votre espace actuel Région AWS, développez ONTAP et choisissez 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 apparaît.
5. Entrez le nouveau mot de passe de l'vsadminutilisateur et 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 SVM FSx pour ONTAP, utilisez la commande [update-storage-virtual-machine](#)CLI (ou l'opération [UpdateStorageVirtualMachine](#)API 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",
        "IpAddresses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com",
        "IpAddresses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddresses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddresses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com",
```

```

    "IpAddresses": ["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"
    }
  }
}

```

Audit de l'accès aux fichiers

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 d'accès aux fichiers](#)
- [Vue d'ensemble des tâches de configuration de l'audit d'accès aux fichiers](#)

Présentation de l'audit d'accès aux fichiers

L'audit d'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 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, lorsqu'un utilisateur disposant des autorisations suffisantes accède à un fichier avec succès), des tentatives infructueuses, ou les 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.

ID d'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 dans l'intention de le supprimer	ACCÈS À L'OBJET : Un descripteur d'un objet (fichier ou répertoire) a été demandé dans le but de le supprimer	Accès aux fichiers
564/4660	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

ID d'événement (EVT/ EVTX)	Événement	Description	Catégorie
567/4663	Lire les attributs de Object/Write Object/ Get Object Attributes/ Set l'objet	ACCÈS À UN OBJET : tentative d'accès à un objet (lecture, écriture, obtention d'un attribut, définition d'un attribut) .  Note Pour cet événement, ONTAP n'audite que 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 nombreuses	Accès aux fichiers

ID d'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 AUX OBJETS : Une tentative a été faite pour créer un lien physique	Accès aux fichiers
N/A/N/A Numéro d'événement ONTAP 9999	Renommer 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 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 d'accès aux fichiers

La configuration d'ONTAP FSx pour l'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 for ONTAP les aura émis.

Les détails des tâches sont fournis dans les procédures suivantes.

Répétez les tâches pour toutes les autres SVM de votre système de fichiers pour lesquelles vous souhaitez activer l'audit d'accès aux fichiers.

Exigences en matière d'audit

Avant de configurer et d'activer l'audit sur une SVM, vous devez connaître les exigences et considérations suivantes.

- L'audit NFS prend en charge les entrées de contrôle d'accès d'audit (ACEs) désignées par type, qui génèrent une entrée dans le journal d'audit lorsque l'accès est tenté sur l'objet. Pour l'audit NFS, il n'existe aucun mappage entre les bits de mode et l'audit ACEs. Lors de la conversion ACLs en mode bits, ACEs les audits sont ignorés. Lors de la conversion des bits de mode en ACLs, aucun audit ACEs n'est généré.
- 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 où les enregistrements d'audit sont stockés avant la conversion au format de fichier EVT 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 qu'il y a suffisamment d'espace disponible pour les journaux d'audit dans le volume.

Création de configurations d'audit sur SVMs

Avant de commencer à auditer les événements relatifs aux fichiers et aux répertoires, vous devez créer une configuration d'audit sur la machine virtuelle de stockage (SVM). Après avoir créé la configuration d'audit, vous devez l'activer sur la SVM.

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 nommée `svm1` qui analyse 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 de journal est EVTX (par défaut), les journaux sont stockés dans le `/audit_log` répertoire et vous n'aurez qu'un seul fichier journal à la fois (d'une taille maximale de 200 Mo).

```
vserver audit create -vserver svm1 -destination /audit_log -rotate-size 200MB
```

- Pour faire pivoter les journaux d'audit selon 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 `svm2` avec une rotation basée sur le temps. Le format des journaux est EVTX (par défaut) et les journaux d'audit font l'objet d'une rotation mensuelle, 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 dans le EVTX format converti (par défaut) ou dans le format de XML fichier. Le EVTX format vous permet d'afficher 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 consigner grâce au `-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 [Création d'une configuration d'audit](#).

Activation de l'audit sur une SVM

Après avoir configuré la configuration d'audit, vous devez activer l'audit sur la SVM. Pour ce faire, utilisez la commande suivante :

```
vserver audit enable -vserver svm_name
```

Par exemple, utilisez la commande suivante pour activer l'audit sur la SVM nommée `vm1`.

```
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 `vm4`.

```
vserver audit disable -vserver svm4
```

Lorsque vous désactivez l'audit, la configuration d'audit n'est pas supprimée de 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 dossiers que vous souhaitez auditer pour les tentatives d'accès des utilisateurs. Vous pouvez configurer des politiques d'audit pour surveiller 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 capacités d'audit différentes en fonction du style de sécurité du volume.

Politiques d'audit sur les fichiers et répertoires de type sécurité NTFS

Vous pouvez configurer les politiques d'audit NTFS à l'aide de l'onglet Sécurité de Windows ou de la CLI ONTAP.

Pour configurer les politiques d'audit NTFS (onglet Sécurité Windows)

Vous configurez les politiques d'audit NTFS en ajoutant des entrées au système NTFS SACLs 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 Windows. Le descripteur de sécurité peut contenir des listes de contrôle d'accès discrétionnaires (DACLS) pour appliquer des autorisations d'accès aux fichiers et aux dossiers, SACLs pour l'audit des fichiers et des dossiers, ou les deux SACLs et. DACLS

1. Dans le menu Outils de l'Explorateur Windows, sélectionnez Cartographeur 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 avec la fenêtre de l'Explorateur Windows affichant les fichiers et les dossiers contenus dans le partage.

3. Sélectionnez le fichier ou le répertoire pour lequel vous souhaitez activer l'accès aux audits.
4. Cliquez avec le bouton droit sur le fichier ou le répertoire, puis sélectionnez Propriétés.
5. Choisissez l'onglet Security (Sécurité).
6. Cliquez sur Avancé.
7. Choisissez l'onglet Audit.
8. Effectuez les actions souhaitées :

Si vous souhaitez...	Procédez comme suit
Configurer l'audit pour un nouvel	1. Choisissez Ajouter. 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.

Si vous souhaitez...	Procédez comme suit
utilisateur ou un nouveau groupe	3. Choisissez 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. Sélectionnez Remove (Supprimer). 3. Choisissez 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 Modifier. 3. Choisissez 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 **object** zone Entrée d'audit pour s'ouvre.

9. Dans le champ 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 la valeur par défaut est Cet objet uniquement.

10. Dans le champ Accès, sélectionnez ce que vous souhaitez auditer et si vous souhaitez auditer les événements réussis, les événements d'échec ou les deux.
 - Pour auditer les événements réussis, cochez la case Réussite.
 - Pour auditer les événements de défaillance, cochez la case Défaillance.

Choisissez les actions que vous devez surveiller pour répondre à vos exigences de sécurité. Pour plus d'informations sur ces événements vérifiables, consultez votre documentation Windows. Vous pouvez auditer les événements suivants :

- Contrôle total
- Traverse le dossier/exécuter le fichier

- Répertorier les dossiers/lire les données
 - Lire les attributs
 - Lire les attributs étendus
 - Création de fichiers/écriture de données
 - Création de dossiers/ajout de données
 - Écrire des attributs
 - Écrire des attributs étendus
 - Supprimer des sous-dossiers et des fichiers
 - Suppression
 - Autorisations de lecture
 - Modifier les autorisations
 - Prenez possession
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 Appliquer.
13. Une fois que vous avez terminé d'ajouter, de supprimer ou de modifier des entrées d'audit, cliquez sur OK.

L'entrée d'audit pour la **object** boîte 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 la case Inclure les entrées d'audit hérissables dans la zone parent de cet objet.
- Choisissez la case Remplacer toutes les entrées d'audit hérissables existantes sur tous les descendants par des entrées d'audit hérissables dans cet objet.
- Choisissez les deux cases.
- Ne choisissez aucune des deux cases.

Si vous définissez SACLs un seul fichier, la zone Remplacer toutes les entrées d'audit héritables existantes sur tous les descendants par des entrées d'audit héritables de cet objet n'est pas présente dans la zone Audit.

15. Choisissez OK.

Pour configurer les politiques d'audit NTFS (ONTAP CLI)

À l'aide de la CLI ONTAP, vous pouvez configurer les politiques d'audit NTFS sans avoir à vous connecter aux données à l'aide d'un partage SMB sur un client Windows.

- Vous pouvez configurer les politiques d'audit NTFS à l'aide de la famille de [commandes vservers security file-directory ntfs](#) `sACL add`.

Par exemple, la commande suivante crée une politique de sécurité nommée `p1` d'après la SVM nommée `vs0`.

```
vservers security file-directory policy create -policy-name p1 -vservers vs0
```

La commande suivante applique ensuite la politique `p1` de sécurité à la `vs0` SVM.

```
vservers security file-directory apply -vservers vs0 -policy-name p1
```

Politiques d'audit sur les fichiers et répertoires de type sécurité UNIX

Vous configurez l'audit pour les fichiers et répertoires de type sécurité UNIX en ajoutant l'audit ACEs (expressions de contrôle d'accès) à NFS v4.x ACLs (listes de contrôle d'accès). Cela vous permet de surveiller certains événements d'accès aux fichiers et aux répertoires NFS pour des raisons de sécurité.

Note

Pour NFS v4.x, le système et le système ACEs sont stockés dans la même ACL. Par conséquent, vous devez être prudent lorsque vous ajoutez un audit ACEs à une ACL existante afin d'éviter de la remplacer et de perdre une ACL existante. L'ordre dans lequel vous ajoutez l'audit ACEs 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 commande `nfs4_getfacl` ou équivalente.
2. Ajoutez l'audit ACEs souhaité.
3. Appliquez l'ACL mise à jour au fichier ou au répertoire à l'aide de la commande `nfs4_setfacl` ou équivalente.

Cet exemple utilise l'-a option permettant d'accorder à un utilisateur (nommé `testuser`) des autorisations de lecture sur le fichier nommé `file1`.

```
nfs4_setfacl -a "A::testuser@example.com:R" file1
```

Afficher les journaux des événements d'audit

Vous pouvez consulter les journaux des événements d'audit enregistrés au format EVT X ou au format de XML fichier.

- EVT X format de fichier — Vous pouvez ouvrir les journaux EVT X d'événements d'audit convertis sous forme de 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 un 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.
- XML format de fichier — Vous pouvez afficher et traiter les journaux d'événements d'audit XML sur des applications tierces qui prennent en charge le format de fichier XML. Les outils de visualisation XML peuvent être utilisés pour consulter les journaux d'audit à condition que vous disposiez du schéma XML et des informations sur les définitions des champs XML.

Configuration d'un serveur SMB dans un groupe de travail

Vous pouvez configurer un serveur SMB (Server Message Block) dans un groupe de travail plutôt que de joindre une [SVM à un Microsoft Active Directory](#) lorsque l'infrastructure de domaine Microsoft Active Directory n'est pas disponible. Un groupe de travail est un peer-to-peer réseau qui utilise le protocole SMB et ne possède que des comptes et des groupes locaux.

Le processus de configuration d'un serveur SMB en tant que membre d'un groupe de travail comprend les étapes suivantes :

- Création du serveur SMB sur une machine virtuelle de stockage (SVM).
- Création d'utilisateurs et de groupes locaux.
- Ajouter des utilisateurs ou des groupes locaux en tant que membres du groupe de travail.

N'oubliez pas que les serveurs SMB en mode groupe de travail ne prennent pas en charge les fonctionnalités SMB suivantes :

- SMB3 Protocole relatif aux témoins
- SMB3 Actions CA
- SQL sur SMB
- Redirection de dossiers
- Profils d'itinérance
- Objet de stratégie de groupe (GPO)
- Service de capture instantanée des volumes (VSS)

En outre, un serveur SMB en mode groupe de travail prend uniquement en charge l'authentification NTLM et ne prend pas en charge l'authentification Kerberos.

Les procédures suivantes vous guident dans le processus de configuration d'un serveur SMB sur une SVM dans un groupe de travail, de création de comptes locaux et d'ajout de ces comptes aux membres du groupe de travail. Vous utiliserez la NetApp ONTAP CLI depuis le système de fichiers ou l'interface de gestion de la SVM pour implémenter ces procédures. Pour de plus amples informations, veuillez consulter [Utilisation de NetApp ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

Rubriques

- [Création d'un serveur SMB dans un groupe de travail](#)
- [Création d'un compte utilisateur local sur le serveur SMB](#)
- [Création de groupes locaux sur le serveur SMB](#)
- [Ajouter des utilisateurs locaux au groupe local](#)

Création d'un serveur SMB dans un groupe de travail

Vous pouvez utiliser cette [vserver cifs create](#) ONTAP CLI commande pour créer un serveur SMB sur la SVM et spécifier le groupe de travail auquel il appartient.

Avant de commencer

La SVM et les volumes (et interfaces) que vous utilisez pour diffuser les données doivent avoir été configurés pour autoriser le protocole SMB.

Ils LIFs doivent être en mesure de se connecter aux serveurs DNS configurés sur la SVM. Une licence CIFS peut être requise sur le système de fichiers, mais aucune licence CIFS n'est requise si le serveur SMB ne doit être utilisé qu'à des fins d'authentification.

Pour créer un serveur SMB dans un groupe de travail

1. Pour accéder à la ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

2. Créez le serveur SMB dans un groupe de travail :

```
FSxIdabcde123456::> vserver cifs create -vserver vserver_name -cifs-  
server cifs_server_name -workgroup workgroup_name [-comment workgroup_description]
```

La commande suivante crée le serveur SMB smb_server01 dans le groupe de travail workgroup01 :

```
FSxIdabcde123456::> vserver cifs create -vserver svm1 -cifs-server SMB_SERVER01 -  
workgroup workgroup01
```

Si vous êtes connecté au port de gestion de la SVM, il n'est pas nécessaire de spécifier un `vserver`.

3. Vérifiez la configuration du serveur SMB à l'aide de la `vserver cifs show` commande.

Dans l'exemple suivant, le résultat de la commande indique qu'un serveur SMB nommé `smb_server01` a été créé sur la SVM `svm1` au sein du groupe de travail : `workgroup01`

```
FSxIdabcde123456::> vserver cifs show -vserver svm1  
  
Vserver: svm1  
CIFS Server NetBIOS Name: SMB_SERVER01  
NetBIOS Domain/Workgroup Name: workgroup01  
Fully Qualified Domain Name: -  
Organizational Unit: -  
Default Site Used by LIFs Without Site Membership: -  
Workgroup Name: workgroup01  
Authentication Style: workgroup  
CIFS Server Administrative Status: up  
CIFS Server Description:  
List of NetBIOS Aliases: -
```

Création d'un compte utilisateur local sur le serveur SMB

Vous pouvez créer un compte utilisateur local qui permet d'autoriser l'accès aux données contenues dans la SVM via une connexion SMB. Vous pouvez également utiliser des comptes d'utilisateurs locaux pour l'authentification lors de la création d'une session SMB. La fonctionnalité utilisateur local est activée par défaut lors de la création de la SVM. Lorsque vous créez un compte utilisateur local, vous devez indiquer un nom d'utilisateur ainsi que la SVM à laquelle associer le compte.

Pour créer des comptes utilisateurs locaux sur le serveur SMB

1. Créez l'utilisateur local à l'aide de la commande [vserver cifs users-and-groups local-user create](#) ONTAPCLI :

```
vserver cifs users-and-groups local-user create -vserver svm_name -user-  
name user_name optional_parameters
```

Les paramètres facultatifs suivants peuvent être utiles :

- `-full-name`— Le nom complet de l'utilisateur.
- `-description`— Description de l'utilisateur local.
- `-is-account-disabled {true|false}`— Spécifie si le compte utilisateur est activé ou désactivé. Si ce paramètre n'est pas spécifié, le compte utilisateur est activé par défaut.

La commande demande le mot de passe de l'utilisateur local.

2. Entrez un mot de passe pour l'utilisateur local, puis confirmez-le.
3. Vérifiez que l'utilisateur a bien été créé :

```
vserver cifs users-and-groups local-user show -vserver svm_name
```

L'exemple suivant crée un utilisateur local `SMB_SERVER01\sue`, avec un nom complet `Sue Chang`, associé à la SVM `svm1` :

```
FSxIdabcde123456::> vserver cifs users-and-groups local-user create -vserver svm1  
-user-name SMB_SERVER01\sue -full-name "Sue Chang"
```

Enter the password:

Confirm the password:

```
FSxIdabcde123456::> vserver cifs users-and-groups local-user show
```

Vserver	User Name	Full Name	Description
svm1	SMB_SERVER01\Administrator		Built-in administrator account
svm1	SMB_SERVER01\sue	Sue Chang	

Création de groupes locaux sur le serveur SMB

Vous pouvez créer des groupes locaux qui peuvent être utilisés pour autoriser l'accès aux données associées à la SVM via une connexion SMB. Vous pouvez également attribuer des privilèges qui définissent les droits ou les capacités d'un membre du groupe en tant qu'utilisateur.

La fonctionnalité de groupe local est activée par défaut lors de la création de la SVM. Lorsque vous créez un groupe local, vous devez donner un nom au groupe et indiquer la SVM à laquelle associer le groupe. Vous pouvez spécifier un nom de groupe avec ou sans le nom de domaine local, et vous pouvez éventuellement spécifier une description pour le groupe local. Vous ne pouvez pas ajouter un groupe local à un autre groupe local.

Pour créer un groupe local sur le serveur SMB

1. créez le groupe local à l'aide de la commande [vserver cifs users-and-groups local-group create](#) ONTAPCLI.

```
vserver cifs users-and-groups local-group create -vserver svm_name -group-name group_name [-description local_group_description]
```

Il est utile d'inclure une description du groupe local.

2. Vérifiez que le groupe a bien été créé :

```
vserver cifs users-and-groups local-group show -vserver svm_name
```

L'exemple suivant crée un groupe local SMB_SERVER01\engineering associé à la SVM svm1 :

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group create -vserver svm1 -group-name SMB_SERVER01\engineering
```

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group show -vserver svm1
```

Vserver	Group Name	Description
svm1	BUILTIN\Administrators	Built-in Administrators group
svm1	BUILTIN\Backup Operators	Backup Operators group
svm1	BUILTIN\Guests	Built-in Guests group
svm1	BUILTIN\Power Users	Restricted administrative privileges
svm1	BUILTIN\Users	All users
svm1	SMB_SERVER01\engineering	

Ajouter des utilisateurs locaux au groupe local

Vous pouvez gérer l'appartenance aux groupes locaux en ajoutant et en supprimant des utilisateurs locaux ou de domaine, ou en ajoutant et en supprimant des groupes de domaines. Cela est utile si

vous souhaitez contrôler l'accès aux données en fonction des contrôles d'accès placés sur le groupe, ou si vous souhaitez que les utilisateurs disposent de privilèges associés à ce groupe. Si vous ne souhaitez plus qu'un utilisateur local, un utilisateur de domaine ou un groupe de domaines dispose de droits d'accès ou de privilèges basés sur l'appartenance à un groupe, vous pouvez supprimer le membre du groupe.

Lorsque vous ajoutez des membres à un groupe local, gardez les points suivants à l'esprit :

- Vous ne pouvez pas ajouter d'utilisateurs au groupe spécial Tout le monde.
- Vous ne pouvez pas ajouter un groupe local à un autre groupe local.
- Pour ajouter un utilisateur ou un groupe de domaine à un groupe local, vous ONTAP devez être en mesure de convertir le nom en SID.

Lorsque vous supprimez des membres d'un groupe local, gardez les points suivants à l'esprit :

- Vous ne pouvez pas supprimer des membres du groupe spécial Tout le monde.
- Pour supprimer un membre d'un groupe local, vous ONTAP devez être en mesure de convertir son nom en SID.

Vous devez avoir le `fsxadmin` rôle nécessaire pour exécuter les commandes utilisées dans cette procédure. Pour de plus amples informations, veuillez consulter [ONTAP rôles et utilisateurs](#).

Pour gérer l'adhésion au groupe local

- Ajoutez un membre à un groupe ou supprimez-en un à l'aide des commandes CLI [vserver cifs users-and-groups local-group add-members](#) et [vserver cifs users-and-groups local-group ONTAP remove-members](#).

- Pour ajouter des membres à un groupe de travail :

```
vserver cifs users-and-groups local-group add-members -vserver svm_name -group-name group_name -member-names name[,...]
```

Vous pouvez spécifier une liste séparée par des virgules d'utilisateurs locaux, d'utilisateurs de domaine ou de groupes de domaines à ajouter au groupe local spécifié.

- Pour afficher les membres d'un groupe de travail :

```
vserver cifs users-and-groups local-group show-members -vserver svm_name -group-  
name group_name
```

- Pour supprimer des membres d'un groupe de travail :

```
vserver cifs users-and-groups local-group remove-members -vserver svm_name -  
group-name group_name -member-names name[,...]
```

Vous pouvez spécifier une liste séparée par des virgules d'utilisateurs locaux, d'utilisateurs de domaine ou de groupes de domaines à supprimer du groupe local spécifié.

L'exemple suivant ajoute un utilisateur local SMB_SERVER01\sue au groupe local SMB_SERVER01\engineering sur SVM svm1 :

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group add-members -vserver svm1  
-group-name SMB_SERVER01\engineering -member-names SMB_SERVER01\sue
```

L'exemple suivant supprime l'utilisateur local SMB_SERVER01\sue et le supprime SMB_SERVER01\james du groupe local SMB_SERVER01\engineering sur la SVM svm1 :

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group remove-  
members -vserver svm1 -group-name SMB_SERVER01\engineering -member-names  
SMB_SERVER01\sue,SMB_SERVER01\james
```

L'exemple suivant répertorie les membres du groupe local SMB_SERVER01\engineering :

```
FsxIdabcdef01234::> vserver cifs users-and-groups local-group show-members -  
vserver svm_name -group-name group_name
```

```
Vserver: svm1  
Domain Name: SMB_SERVER01  
Group Name: SMB_SERVER01\engineering  
Member Name: SMB_SERVER01\anita  
              SMB_SERVER01\james  
              SMB_SERVER01\liang
```


Surveillance des détails de configuration des machines virtuelles de stockage (SVM)

Vous pouvez consulter les machines virtuelles FSx de stockage ONTAP qui se trouvent actuellement sur votre système de fichiers à l'aide de la FSx console Amazon, du AWS CLI, et de l' FSx API Amazon.

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-machines](#)CLI ou l'opération [DescribeStorageVirtualMachines](#)API.

La réponse du système est une liste de descriptions complètes de tout ce qui se trouve SVMs dans votre compte Région AWS.

Suppression de machines virtuelles de stockage (SVM)

Vous ne pouvez supprimer une SVM FSx pour ONTAP qu'à l'aide de la FSx console Amazon, de l'API AWS CLI et. Avant de pouvoir supprimer une SVM, vous devez d'abord supprimer tous les volumes non root attachés à la SVM.

Important

Vous ne pouvez pas 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 FSx console Amazon 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 machines SVMs 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 [Supprimer des volumes](#).
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 FSx destinée au stockage ONTAP, utilisez la commande [delete-storage-virtual-machine](#)CLI (ou l'opération [DeleteStorageVirtualMachine](#)API équivalente), comme indiqué dans l'exemple suivant.

```
aws fsx delete-storage-virtual-machine --storage-virtual-machine-id svm-
abcdef0123456789d
```

Gestion FSx des 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 de stockage logiques iSCSI (i)LUNs. 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 AWS CLI de l'FSx API Amazon, 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 en utilisant NetApp CLI ONTAP ou API REST.

 Note

Vous pouvez créer 500 volumes par paire HA, jusqu'à 1 000 volumes pour toutes les paires HA. FlexGroup les volumes de constituants sont pris en compte dans cette limite. Par défaut, il existe huit volumes constitutifs par agrégat, par FlexGroup.

Lorsque vous créez un volume, vous définissez les propriétés suivantes :

- Style de volume — Le [style de volume](#) peut être soit FlexVol or FlexGroup.
- 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 un NetApp SnapMirror or SnapVault relation.
- 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 ou NTFS) : 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 qui sont 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.
- [Copiez les balises dans les sauvegardes](#) : Amazon FSx copiera 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' FSx API Amazon AWS CLI ou de l'API Amazon.

Rubriques

- [Styles de volume](#)
- [Types de volume](#)
- [Style de sécurité des volumes](#)
- [Création de volumes](#)
- [Mise à jour des volumes](#)
- [Déplacement de volumes entre agrégats](#)
- [Volumes de surveillance](#)
- [Supprimer des volumes](#)

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 FSx console Amazon AWS CLI, du, et de l' FSx API Amazon.

- FlexVol les volumes offrent l'expérience la plus simple pour les systèmes de fichiers dotés d'une paire haute disponibilité (HA). Ils constituent donc le style de volume par défaut pour les systèmes de fichiers de première génération et les systèmes de fichiers de deuxième génération dotés d'une paire HA. La taille minimale d'un FlexVol le volume est de 20 mégaoctets (Mio), et la taille maximale est de 314 572 800 MiB.

- FlexGroup les volumes sont composés de plusieurs composants FlexVol volumes, ce qui leur permet de fournir des performances et une évolutivité de stockage supérieures à celles FlexVol volumes pour les systèmes de fichiers comportant plusieurs paires HA. FlexGroup les volumes sont le style de volume par défaut pour les systèmes de fichiers de deuxième génération comportant plusieurs paires HA. La taille minimale d'un FlexGroup le volume est de 100 gibioctets (GiB) par constituant, et la taille maximale est de 20 pebioctets (PiB).

Vous pouvez convertir un volume à l'aide du FlexVol style pour le FlexGroup style avec le ONTAP CLI, qui crée un FlexGroup avec un seul constituant. Toutefois, nous vous recommandons de l'utiliser AWS DataSync pour déplacer des données entre FlexVol volume et un nouveau FlexGroup volume pour garantir que les données sont réparties de manière uniforme sur FlexGroup's constituants. Pour de plus amples informations, veuillez consulter [FlexGroup constituants](#).

Note

Si vous souhaitez utiliser ONTAP CLI pour convertir un FlexVol volume vers un FlexGroup volume, assurez-vous de supprimer toutes les sauvegardes du FlexVol volume avant de le convertir. ONTAP ne rééquilibre pas automatiquement les données dans le cadre de la conversion, de sorte que les données peuvent être déséquilibrées entre les FlexGroup constituants.

FlexGroup constituants

A FlexGroup le volume est composé de constituants, qui sont FlexVol volumes. Par défaut, FSx pour ONTAP, assigne huit composants à un FlexGroup volume par paire HA.

Lorsque vous créez votre FlexGroup volume, sa taille est répartie uniformément entre ses constituants. Par exemple, si vous créez un fichier de 800 gigaoctets (Go) FlexGroup volume avec huit constituants, chaque constituant a une taille de 100 Go. A FlexGroup le volume peut être compris 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 Un 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 du ONTAP CLI ou 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 système équilibré FlexGroup volume. Lorsque de nouvelles données sont écrites dans FlexGroup volume, l'ONTAP donne la priorité à sa distribution entre les nouveaux constituants jusqu'à ce que les constituants 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 votre FlexGroup volume à un état antérieur. Les instantanés précédents ne peuvent pas offrir 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 FSx console Amazon, le AWS CLI, et l' FSx API Amazon.

- 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'un NetApp SnapMirror or SnapVault relation. Vous devez utiliser des volumes DP lorsque vous souhaitez [migrer](#) ou [protéger les](#) données d'un seul volume.

FlexVol and FlexGroup les volumes peuvent être RW ou DP.

 Note

Vous ne pouvez pas mettre à jour le type d'un volume une fois celui-ci créé.

Style de sécurité des volumes

Lorsque vous créez un volume FSx pour ONTAP, vous pouvez choisir entre deux styles de sécurité : Unix et NTFS. 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 qu'ONTAP utilise FSx 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 FSx console, la CLI et l'API Amazon, 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 [Mise à jour des volumes](#).

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 NFS v4.x. ACLs

- 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 NTFS ACLs.

Création de volumes

Vous pouvez créer un FSx pour ONTAP FlexVol or FlexGroup volume à l'aide de la FSx console Amazon AWS CLI, du, et de FSx l'API Amazon, en plus du NetApp Interface de ligne de commande (CLI) ONTAP et 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 FSx console Amazon 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 pour 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'un NetApp SnapMirror or SnapVault relation. Pour de plus amples informations, veuillez consulter [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) sur ce volume. Pour de plus amples informations, veuillez consulter [Efficacité du stockage](#).
- Pour le style de sécurité du volume, choisissez entre Unix (Linux) et NTFS pour le volume. Pour de plus amples informations, veuillez consulter [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, consultez [Règles 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 NetApp Documentation du produit 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 de plus amples informations, veuillez consulter [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 SnapLock Configuration, choisissez entre Activé et Désactivé. Pour plus d'informations sur la configuration d'un SnapLock Volume de conformité ou SnapLock

Volume d'entreprise, voir [Compréhension SnapLock Conformité d'Enterprise](#) et [Compréhension SnapLock Enterprise](#). Pour plus d'informations sur SnapLock, voir [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 que créer FlexGroup volumes pour les systèmes de fichiers comportant plusieurs paires HA à l'aide de la FSx console Amazon. Pour créer FlexVol volumes pour les systèmes de fichiers comportant plusieurs paires HA, utilisez l' AWS CLI FSx API Amazon ou les outils NetApp de gestion.

1. Ouvrez la FSx console Amazon 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 pour 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 Gibioctets (GiB) et 2 400 tebioctets (TiB) par paire HA. Par exemple, un système de fichiers comportant 12 paires de haute disponibilité (HA) aurait une taille de volume minimale de 9 600 GiB et une taille maximale de 20 480 TiB.

- 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'un NetApp SnapMirror or SnapVault relation. Pour de plus amples informations, veuillez consulter [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 de plus amples informations, veuillez consulter [Efficacité du stockage](#).
- Pour le style de sécurité du volume, choisissez entre Unix (Linux) et NTFS pour le volume. Pour de plus amples informations, veuillez consulter [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, consultez [Règles 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 NetApp Documentation du produit 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 de plus amples informations, veuillez consulter [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 SnapLock Configuration, choisissez entre Activé et Désactivé. Pour plus d'informations sur la configuration d'un SnapLock Volume de conformité ou SnapLock Volume d'entreprise, voir [Compréhension SnapLock Conformité d'](#) et [Compréhension SnapLock Enterprise](#). Pour plus d'informations sur SnapLock, voir [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 [create-volume](#) CLI (ou l'opération API [CreateVolume](#) 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 de plus amples informations, veuillez consulter [Restauration des sauvegardes sur un nouveau volume](#).

Mise à jour des volumes

Vous pouvez mettre à jour la configuration d'un volume FSx for ONTAP à l'aide de la FSx console Amazon AWS CLI, du, et de l' FSx API Amazon, en plus du NetApp Interface de ligne de commande (CLI) ONTAP et API REST. Vous pouvez modifier les propriétés suivantes d'un volume existant FSx pour ONTAP :

- 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' FSx API AWS CLI et Amazon)

Pour de plus amples informations, veuillez consulter [Gestion FSx des volumes ONTAP](#).

Pour mettre à jour la configuration d'un volume (console)

1. Ouvrez la FSx console Amazon 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 /vo15.
7. Pour la taille du volume, vous pouvez augmenter ou diminuer la taille du volume dans la plage spécifiée dans la FSx console Amazon. Dans FlexVol volumes, la taille maximale est de 300 TiB. Dans FlexGroup volumes, la taille maximale est de 300 TiB multipliés par le nombre total de volumes constitutifs que votre FlexGroup a, 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) sur le volume, 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, consultez [Politiques 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 à NTFS ou à UNIX ACLs 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, consultez [Règles 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 NetApp Documentation du produit 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 on n'a pas accédé 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 API [UpdateVolume](#) 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
```

Expansion FlexGroup volumes

Vous pouvez ajouter des volumes constitutifs supplémentaires à votre FlexGroup volume avec la `volume expand` commande dans le ONTAP CLI. Il s'agit d'une bonne pratique après avoir ajouté des paires de haute disponibilité (HA) à votre système de fichiers, car elle garantit que votre FlexGroup le volume reste équilibré.

Avant d'agrandir votre FlexGroup volume, considérez les points suivants :

- L'ensemble d'un FlexGroup's les volumes constitutifs ont la même capacité de stockage. Lorsque vous étendez votre FlexGroup volume avec des constituants supplémentaires, chaque constituant a la même taille que les constituants existants. Par conséquent, assurez-vous que chaque agrégat dispose d'un espace suffisant avant d'ajouter des composants.

- AWS recommande de maintenir huit volumes de composants par agrégat pour chacun FlexGroup volume. Huit volumes constitutifs par agrégat maximisent le parallélisme de FlexGroup volumes et offre les performances les plus optimales pour votre charge de travail. En général, nous vous recommandons uniquement d'étendre votre FlexGroup volume avec des composants supplémentaires si vous ajoutez des paires HA. C'est le seul scénario dans lequel vous devez ajouter des constituants pour conserver huit constituants par agrégat.
- Si vos recettes FlexGroup le volume est dans un SnapMirror relation, puis à la fois la source et la destination FlexGroup les volumes doivent avoir le même nombre de composants. Dans le cas contraire, SnapMirror les transferts échoueront. SnapMirror fonctionne au niveau du constituant et transfère les données entre chaque constituant individuel. Par conséquent, si vous développez un FlexGroup avec des volumes constitutifs supplémentaires, vous devez également étendre manuellement tout volume se trouvant dans un SnapMirror relation avec elle.
- Lorsque vous développez un FlexGroup volume contenant des composants supplémentaires, toutes ses copies instantanées existantes deviennent des copies « partielles ». Les copies partielles ne peuvent pas être restaurées, mais elles peuvent être consultées et les fichiers individuels peuvent être restaurés. En outre, cela entraîne la perte de toute incrémentalité pour les FSx sauvegardes, AWS les sauvegardes ou SnapMirror relations.
- Vous ne pouvez pas supprimer les volumes constitutifs une fois que vous les avez ajoutés.

Ajouter FlexGroup constituants volumiques

Vous pouvez utiliser le plugin ONTAP CLI pour ajouter des volumes constitutifs à votre FlexGroup volume.

Pour ajouter FlexGroup constituants volumiques

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

2. Utilisez l'[extension du volume](#) ONTAP Commande CLI pour étendre votre FlexGroup volume avec des constituants supplémentaires. Remplacez les valeurs suivantes :
- `svm_name` avec le nom de la machine virtuelle de stockage (SVM) qui héberge votre FlexGroup volume (par exemple, `svm1`).
 - `vol_name` avec le nom du FlexGroup volume que vous souhaitez étendre (par exemple, `vol1`).
 - `aggregates` avec une liste d'agrégats séparés par des virgules que vous souhaitez ajouter FlexGroup volumes constitutifs en. Par exemple, `aggr1` pour un seul agrégat ou `aggr1, aggr2` pour plusieurs agrégats.
 - `constituent_per_aggregate` avec le nombre de composants supplémentaires que vous souhaitez ajouter à chacun des composants spécifiés `aggregates`. Vous ne devez ajouter qu'un nombre suffisant de composants pour garantir que votre FlexGroup le volume possède un nombre équilibré de constituants parmi les agrégats sur lesquels il réside.

```
::> volume expand -vserver svm_name -volume vol_name -aggr-list aggregates -aggr-list-multiplier constituents_per_aggregate
```

Important

Vous ne pouvez pas supprimer FlexGroup constituants une fois que vous les avez ajoutés, vérifiez donc vos entrées avant d'exécuter la commande précédente.

Déplacement de volumes entre agrégats

Lorsque vous ajoutez des paires de haute disponibilité (HA) à votre système de fichiers, vous devez rééquilibrer les données existantes en déplaçant les volumes vers les nouveaux agrégats. Pour déplacer un volume entre des agrégats, vous pouvez utiliser la `volume move` commande dans la CLI ONTAP.

Avant d'utiliser la `volume move` commande, tenez compte des points suivants :

- L'utilisation de `volume move` cette commande peut avoir un impact sur les performances car elle consomme les ressources réseau et disque de votre système de fichiers. Par conséquent, nous recommandons de déplacer les volumes entre les agrégats pendant les périodes de faible activité.

Vous pouvez également réduire l'utilisation du débit réseau et du débit du disque sur votre système de fichiers à 50 % maximum lors du déplacement de volumes.

- Pour réduire l'impact sur les performances de votre système de fichiers, nous vous recommandons de déplacer un seul volume entre deux paires HA et deux agrégats à la fois. Par exemple, si votre système de fichiers comporte quatre paires HA, nous vous recommandons de déplacer deux volumes à la fois (en supposant que les volumes ne sont pas déplacés depuis ou vers les mêmes paires HA). ONTAP permet de déplacer jusqu'à huit volumes sur chaque paire HA à la fois, mais un plus grand nombre de mouvements de volume simultanés réduira les performances des E/S du client et de tout déplacement de volume en cours.
- Toutes les données stockées sur le niveau SSD du volume concerné sont physiquement déplacées vers un autre ensemble de disques sur un autre serveur de fichiers. Cette opération s'effectue en arrière-plan et prend du temps. La durée du transfert dépend de la capacité de débit de votre système de fichiers et du niveau d'activité de votre système de fichiers. Cependant, le déplacement du volume peut être limité. Pour de plus amples informations, veuillez consulter [Régulation des mouvements de volume](#).
- Les données stockées sur le niveau de capacité ne sont pas déplacées physiquement car les paires HA partagent la même capacité de stockage du pool. Par conséquent, le déplacement de volumes avec la plupart de leurs données hiérarchisées sera plus rapide. N'oubliez pas que les métadonnées des fichiers sont toujours stockées sur le niveau SSD. Pour de plus amples informations, veuillez consulter [Hiérarchisation des données de volume](#).

Phases du déplacement d'un volume

Une opération de déplacement de volume comporte deux phases : la phase de réplication et la phase de transition. Pendant la phase de réplication, les données existantes sont répliquées vers le nouvel agrégat du volume. Pendant la phase de transition, ONTAP tente un dernier transfert rapide vers le nouvel agrégat du volume. Cela inclut le transfert de toutes les données écrites pendant la phase de transfert et la redirection du nouveau trafic vers le nouvel agrégat du volume. Par défaut, la fenêtre de transition est de 30 secondes et interrompt toutes les E/S vers votre volume. Si ONTAP ne parvient pas à effectuer toutes ces étapes pendant la fenêtre de transition, il échouera. Par défaut, ONTAP essaiera de couper plus de trois fois de suite. Si les trois tentatives consécutives échouent, ONTAP réessaiera une fois par heure jusqu'à ce qu'il aboutisse. Vous pouvez réduire la charge sur votre système de fichiers pour garantir le succès de la phase de transition en réduisant ou en interrompant le trafic d'E/S vers le volume avant le début de la phase de transition.

Déplacements de volume de départ

Pour démarrer un déplacement de volume

1. Pour accéder à la CLI NetApp ONTAP, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

2. Exécutez la commande [volume move start](#) ONTAP CLI. Remplacez les valeurs suivantes :
 - *vserver_name* avec le nom de la SVM hébergeant le volume que vous déplacez.
 - *volume_name* avec le nom du composant du volume (par exemple, *vol1__0001*).
 - *aggregate_name* avec le nom de l'agrégat de destination pour le volume.
 - *-enforce-network-throttling* pour limiter le débit total du déplacement du volume. Ce nom est facultatif.

```
::> volume move start -vserver svm_name -volume volume_name --destination-  
aggregate 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.
```

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. De plus, votre trafic d'E/S vers le volume sera temporairement suspendu pendant la phase de transition du déplacement du volume.

Surveillance des mouvements de volume

Pour surveiller un déplacement de volume

- 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: aggr1  
Source Node: FsxId01234567890abcdef-01  
Move State: healthy
```

La sortie de la commande indique le temps estimé pour terminer le déplacement. Une fois terminé, le `Move phase` message affichera le `completed` statut.

Maintien de l'équilibre FlexGroup volumes

Afin que votre charge de travail fonctionne de manière optimale, votre FlexGroup les volumes doivent couvrir tous les agrégats et comporter un nombre pair de volumes constitutifs par agrégat. Nous recommandons d'avoir huit constituants par agrégat. Tenez compte des scénarios suivants lors du rééquilibrage FlexGroup volumes :

- Déménagement FlexGroup constituants parmi les agrégats existants : si vous déplacez un FlexGroup's volume constitutif par rapport à un autre agrégat d'un autre équilibre FlexGroup, vous

devez ensuite déplacer un autre constituant moins utilisé vers l'agrégat d'origine. Cela garantit que votre FlexGroup possède un nombre pair de constituants par agrégat.

Déménagement FlexGroup constituants dans de nouveaux agrégats après avoir ajouté des paires HA : si vous déplacez un FlexGroup's volumes constitutifs vers de nouveaux agrégats après avoir ajouté des paires HA, vous devez alors étendre le FlexGroup avec des constituants supplémentaires sur les agrégats qui ont perdu des constituants. Cela garantit que votre FlexGroup possède un nombre pair de constituants par agrégat. Pour de plus amples informations, veuillez consulter [the section called “Expansion FlexGroup volumes”](#).

Régulation des mouvements de volume

Si vous souhaitez limiter la bande passante d'un déplacement de volume sur votre système de fichiers, vous pouvez ajouter `-enforce-network-throttling` cette option au début de l'opération.

Note

L'utilisation de cette option affecte les entrées SnapMirror transferts de données de réplication pour le système de fichiers. Suivez la façon dont vous configurez les options de réplication de votre système de fichiers, car vous ne pouvez pas les afficher une fois définies.

Pour ralentir un mouvement de volume

1. L'accélérateur utilise le régulateur de réplication global. Pour définir la limitation globale de la réplication, utilisez la commande suivante dans ONTAP CLI.

```
::> options -option-name replication.throttle.enable on
```

2. Spécifiez la bande passante totale maximale pouvant être utilisée par la réplication, en remplaçant l'option suivante :

- `kbs_throttle` avec le débit maximal souhaité à utiliser pour toute réplication (y compris SnapMirror et mouvements de volume), en kilo-octets par seconde.

```
::> options -option-name replication.throttle.incoming.max_kbs kbs_throttle  
::> options -option-name replication.throttle.outgoing.max_kbs kbs_throttle
```

Volumes de surveillance

Vous pouvez voir les volumes qui se trouvent actuellement sur votre système de fichiers à l'aide de la FSx console Amazon, du AWS CLI, et de l' FSx API Amazon et SDKs.

Pour surveiller 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 [DescribeVolumes](#) API.

```
$ aws fsx describe-volumes
{
  "Volumes": [
    {
      "CreationTime": "2024-03-04T20:17:44+00:00",
      "FileSystemId": "fs-abcdef0123a0bb087",
      "Lifecycle": "CREATED",
      "Name": "SVM8_ext_root",
      "OntapConfiguration": {
        "FlexCacheEndpointType": "NONE",
        "JunctionPath": "/",
        "SecurityStyle": "NTFS",
        "SizeInMegabytes": 1024,
        "StorageEfficiencyEnabled": false,
        "StorageVirtualMachineId": "svm-01234567890abcdef",
        "StorageVirtualMachineRoot": true,
        "TieringPolicy": {
          "Name": "NONE"
        },
        "UUID": "42ce3de0-da64-11ee-a22d-7f7cdfb8d381",
        "OntapVolumeType": "RW",
        "SnapshotPolicy": "default",
        "CopyTagsToBackups": false,
        "VolumeStyle": "FLEXVOL",
        "AggregateConfiguration": {
          "Aggregates": [
            "aggr1"
          ]
        }
      },
      "UUID": "42ce3de0-da64-11ee-a22d-7f7cdfb8d381",
      "OntapVolumeType": "RW",
      "SnapshotPolicy": "default",
      "CopyTagsToBackups": false,
      "VolumeStyle": "FLEXVOL",
      "AggregateConfiguration": {
        "Aggregates": [
          "aggr1"
        ]
      }
    }
  ]
}
```

```

        "SizeInBytes": 1073741824
      },
      "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcdef0123a0bb087/fsvol-abcdef0123456789a",
      "VolumeId": "fsvol-abcdef0123456789a",
      "VolumeType": "ONTAP"
    }
  ]
}

```

Affichage de volumes hors ligne

Vous ne pouvez pas créer ou supprimer des sauvegardes de volumes lorsque le volume source est hors ligne. Vous pouvez utiliser le [volume show](#) ONTAP Commande CLI pour déterminer l'état actuel d'un volume.

```
volume show -vserver svm-name
```

Pour plus d'informations sur l'accès au ONTAP CLI sur votre système de fichiers, voir [Utilisation de NetApp ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

```
FsxIdabc12345::> volume show -vserver vs1
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used%
vs1	vol1	aggr1	online	RW	2GB	1.9GB	5%
vs1	vol1_dr	aggr0_dp	online	DP	200GB	160.0GB	20%
vs1	vol2	aggr0	online	RW	150GB	110.3GB	26%
vs1	vol2_dr	aggr0_dp	online	DP	150GB	110.3GB	26%
vs1	vol3	aggr1	online	RW	150GB	120.0GB	20%
vs1	vol3_dr	aggr1_dp	online	DP	150GB	120.0GB	20%
vs1	vol4	aggr1	online	RW	200GB	159.8GB	20%

```
7 entries were displayed.
```

Pour remettre en ligne un volume hors ligne, utilisez [volume online](#) ONTAP Commande CLI, comme indiqué dans l'exemple suivant. S'il n'existe qu'une seule SVM (Vserver), il n'est pas nécessaire de spécifier le `-vserver` paramètre.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

Supprimer des volumes

Vous pouvez supprimer un volume FSx pour ONTAP à l'aide de la FSx console Amazon, du AWS CLI, et de l' FSx API Amazon, en plus du NetApp Interface de ligne de commande (CLI) ONTAP et API REST.

Avant de supprimer un volume, assurez-vous qu'aucune application n'accède aux données du volume que vous souhaitez supprimer.

Important

Vous ne pouvez supprimer des volumes à l'aide de la FSx console, de l'API ou de la CLI Amazon que si les FSx sauvegardes Amazon sont activées sur le volume.

Réalisation d'une sauvegarde finale du volume

Lorsque vous supprimez un volume à l'aide de la FSx console Amazon, vous avez la possibilité d'effectuer une sauvegarde finale du volume. En tant que bonne pratique, nous vous recommandons de choisir d'effectuer une sauvegarde finale. 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.

Pour plus d'informations sur les sauvegardes de volumes, consultez [Protection de vos données grâce à des sauvegardes en volume](#).

Pour supprimer un volume (console)

1. Ouvrez la FSx console Amazon 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. (SnapLock Enterprise volumes uniquement) Pour Bypass SnapLock Enterprise Retention, sélectionnez Yes.

7. 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.
8. Confirmez la suppression du volume en saisissant supprimer dans le champ Confirmer la suppression.
9. Choisissez Supprimer le ou les volumes.

Pour supprimer un volume (CLI)

- Pour supprimer un volume FSx for ONTAP, utilisez la commande de la CLI [delete-volume](#) (ou l'opération API [DeleteVolume](#) équivalente), comme indiqué dans l'exemple suivant.

```
aws fsx delete-volume --volume-id fsvol-1234567890abcde
```

Suppression SnapLock volumes

Cette section explique comment supprimer un SnapLock volume.

Vous pouvez supprimer un SnapLock Volume de conformité si les périodes de conservation de tous les fichiers WORM (écriture unique, lecture multiple) qu'ils contiennent sont expirées.

Note

Lorsque vous fermez un Compte AWS annonce contenant SnapLock Enterprise or Compliance volumes, AWS et FSx pour ONTAP, suspendez votre compte pendant 90 jours en laissant vos données intactes. Si vous ne rouvrez pas votre compte pendant ces 90 jours, AWS supprime vos données, y compris les données contenues dans SnapLock volumes quels que soient vos paramètres de rétention.

Vous pouvez supprimer un SnapLock Volume d'entreprise à tout moment si vous disposez des autorisations requises. Pour supprimer un SnapLock Volume d'entreprise utilisant le ONTAP CLI,

vous devez avoir le `fsxadmin` rôle. Pour de plus amples informations, veuillez consulter [Rôles et utilisateurs de l'administrateur du système de fichiers](#).

Pour supprimer un SnapLock Volume d'entreprise contenant des données WORM avec une politique de rétention active utilisant la FSx console Amazon, la CLI ou FSx l'API Amazon, vous devez disposer de l'autorisation `fsx:BypassSnapLockEnterpriseRetention` IAM.

Warning

La durée de conservation minimale pour un SnapLock le volume du journal d'audit est de six mois. Tant que cette période de conservation n'est pas expirée, vous ne pouvez pas supprimer le SnapLock le volume du journal d'audit, la machine virtuelle de stockage (SVM) ou le système de fichiers associé à la SVM, même si le volume a été créé dans SnapLock Mode entreprise. Pour de plus amples informations, veuillez consulter [SnapLock volumes des journaux d'audit](#).

Création d'un LUN iSCSI

Ce processus décrit comment créer un LUN iSCSI sur un système de fichiers Amazon FSx for NetApp ONTAP à l'aide du NetApp ONTAP `lun create` Commande CLI. Pour plus d'informations, consultez [lun create](#) le NetApp ONTAP Centre de documentation.

Note

Le protocole iSCSI n'est pas pris en charge pour les systèmes de fichiers comportant plus de six paires HA.

Ce processus suppose qu'un volume a déjà été créé sur votre système de fichiers. Pour de plus amples informations, veuillez consulter [Création de volumes](#).

1. Pour accéder au ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

2. Créez un LUN à l'aide du `lun create` NetApp CLI commande, 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
<i>svm_name</i>	<i>/vol/vol_name/lun_name</i>	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 [Provisionnement iSCSI pour Linux](#) ou [Provisionnement iSCSI pour Windows](#).

Optimisation des performances avec les fenêtres FSx de maintenance Amazon

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 vous FSx permet d'utiliser la fenêtre de maintenance pour contrôler le moment où de telles activités de maintenance potentielles ont lieu.

L'application de correctifs est peu fréquente, généralement une fois toutes les quelques semaines. Lors de l'application de correctifs, chacun des serveurs de fichiers de votre système de fichiers est corrigé un par un, et chaque serveur de fichiers prend généralement jusqu'à une heure pour être corrigé. Avant qu'un correctif ne soit appliqué à un serveur de fichiers au sein d'une paire HA, votre système de fichiers bascule automatiquement vers le partenaire HA des serveurs de fichiers, ce qui peut entraîner une brève pause d'E/S (moins de 60 secondes) pour toute E/S dirigée vers cette paire HA. Votre système de fichiers tombera alors en panne, ce qui peut entraîner une nouvelle brève pause d'E/S (moins de 60 secondes). Vous choisissez l'heure de début de la fenêtre de maintenance lors de la création du système de fichiers. Si vous ne choisissez pas de fenêtre, une fenêtre est automatiquement attribuée.

 Important

Pour garantir que les correctifs peuvent être correctement appliqués à votre système de fichiers, car FSx ONTAP mettra en ligne tous les volumes hors ligne pendant la durée du processus d'application des correctifs. Les volumes remis en ligne par Amazon FSx ne seront pas accessibles aux clients.

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, car FSx 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 l'Amazon FSx Management Console AWS CLI, AWS l'API ou l'une des API AWS SDKs pour modifier la fenêtre de maintenance de vos systèmes de fichiers.

Pour modifier le créneau de maintenance hebdomadaire (console)

1. Ouvrez la FSx console Amazon 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-system](#) CLI, consultez [Pour mettre à jour un système de fichiers \(CLI\)](#).

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 à tout moment. N'oubliez pas que votre système de fichiers nécessite une configuration spécifique pour atteindre une capacité de débit maximale. Par exemple, pour fournir 4 % de capacité GBps de débit à un système de fichiers de première génération, 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 de plus amples informations, veuillez consulter [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 sur disque par seconde (IOPS) et de capacité de mise en cache des données sur le serveur de fichiers. Pour de plus amples informations, veuillez consulter [Performances](#).

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 de plus amples informations, veuillez consulter [the section called “Mise à jour des fenêtres de maintenance”](#).

Rubriques

- [Quand modifier la capacité de débit](#)
- [Comment les demandes simultanées sont traitées](#)
- [Mise à jour de la capacité de débit](#)
- [Surveillance des variations de capacité de débit](#)

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 de plus amples informations, veuillez consulter [the section called “Surveillance dans la FSx console Amazon”](#).

Comment les demandes simultanées sont traitées

Pour les systèmes de fichiers de première génération, vous pouvez demander une mise à jour de la capacité de débit juste avant le début du flux de travail de mise à jour de la capacité de stockage SSD et des IOPS provisionnées ou pendant qu'il est en cours. La séquence dans laquelle Amazon FSx traite les deux demandes est la suivante :

- Si vous soumettez une SSD/IOPS update and throughput capacity update at the same time, both requests are accepted. The SSD/IOPS mise à jour, elle 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 SSD/IOPS update is in progress, the throughput capacity update request is accepted and queued to occur after the SSD/

IOPS update. The throughput capacity update starts after SSD/IOPS est mise à jour (de nouvelles valeurs sont disponibles) et pendant l'étape d'optimisation. Cela prend généralement moins de 10 minutes.

- Si vous soumettez une demande SSD/IOPS update while a throughput capacity update is in progress, the SSD/IOPS de mise à jour du stockage, celle-ci 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.

Tenez compte des points suivants lorsque vous demandez une mise à jour de la capacité de débit pour les systèmes de fichiers de deuxième génération :

- Vous devez attendre au moins six heures entre la mise à jour de la capacité de débit des systèmes de fichiers de deuxième génération.
- La période de refroidissement de la capacité de débit est partagée avec le dimensionnement des SSD/IOPS.
- La mise à l'échelle de la capacité de débit et la mise à l'échelle des SSD/IOPS ne peuvent pas être effectuées simultanément ou en file d'attente pendant que l'une ou l'autre est en cours.
- Vous ne pouvez pas ajouter de paires de haute disponibilité (HA) conjointement ou pendant le dimensionnement de la capacité de débit et le dimensionnement de la capacité de débit. SSD/IOPS scaling are in progress. However, adding HA pairs doesn't share a cooldown with SSD/IOPS. Pour de plus amples informations, veuillez consulter [Ajouter des paires à haute disponibilité \(HA\)](#).

Pour plus d'informations sur le stockage SSD et les mises à jour des IOPS provisionnées, consultez. [Gestion de la capacité de stockage](#)

Mise à jour de la capacité de débit

Vous pouvez modifier la capacité de débit d'un système de fichiers à l'aide de la FSx console Amazon, du AWS Command Line Interface (AWS CLI) ou de l' FSx API Amazon.

Note

Vous devez attendre au moins six heures entre la mise à jour de la capacité de débit des systèmes de fichiers de deuxième génération.

Pour modifier la capacité de débit d'un système de fichiers (console)

1. Ouvrez la FSx console Amazon 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, choisissez 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.
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 FSx console Amazon, du AWS CLI, et de l'API. Pour de plus amples informations, veuillez consulter [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 FSx console Amazon, du AWS CLI, et de l'API. Pour de plus amples informations, veuillez consulter [Surveillance des variations de capacité de débit](#).

Surveillance des variations de capacité de débit

Vous pouvez suivre la progression d'une modification de capacité de débit à l'aide de la FSx console Amazon, 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 traite FSx 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-systems](#) CLI et de l'action [DescribeFileSystems](#) API. 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 MBps et une capacité de débit cible de 256. MBps

.

```

.
.
  "ThroughputCapacity": 128,
"AdministrativeActions": [
  {
    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
    "RequestTime": 1581694764.757,
    "Status": "PENDING",
    "TargetFileSystemValues": {
      "OntapConfiguration": {
        "ThroughputCapacity": 256
      }
    }
  }
]

```

Lorsque 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.

Gestion des actions des PME

Pour gérer les partages de fichiers SMB sur votre système de FSx fichiers Amazon, vous pouvez utiliser l'interface utilisateur Microsoft Windows Shared Folders. 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 de plus amples informations, veuillez consulter [Utilisation NetApp Gestionnaire de système avec BlueXP](#).

Pour connecter des dossiers partagés à votre système de FSx fichiers Amazon

1. Lancez votre EC2 instance Amazon et connectez-la au Microsoft Active Directory auquel votre système de FSx fichiers Amazon est joint. Pour ce faire, choisissez l'une des procédures suivantes dans le guide AWS Directory Service d'administration :
 - [Rejoindre facilement une EC2 instance Windows](#)
 - [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 EC2 l'utilisateur Amazon.
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 FSx console Amazon, 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 FSx fichiers Amazon apparaît alors dans la liste de l'outil Dossiers partagés.

Maintenant que Shared Folders est connecté à votre système de FSx fichiers Amazon, 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 FSx fichiers Amazon. 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.

Gestion des FSx ressources ONTAP à l'aide de NetApp applications

En plus des AWS API AWS Management Console AWS CLI, et SDKs, vous pouvez également les utiliser NetApp outils de gestion et applications pour gérer vos ressources FSx for ONTAP :

Rubriques

- [S'inscrire à un NetApp compte](#)
- [Utilisation NetApp BlueXP](#)
- [Utilisation de NetApp ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#)
- [Utilisation de ONTAP API REST](#)

Important

Amazon FSx se synchronise régulièrement avec ONTAP pour garantir la cohérence. Si vous créez ou modifiez des volumes à l'aide de NetApp applications, plusieurs minutes peuvent être nécessaires pour que ces modifications soient reflétées dans l'API AWS Management Console AWS CLI,, et SDKs.

S'inscrire à un NetApp compte

Pour télécharger certains NetApp des logiciels, tels que BlueXP, SnapCenter, et le ONTAP Connecteur antivirus, vous devez disposer d'un NetApp . Pour vous inscrire à un NetApp compte, effectuez les étapes suivantes :

1. Accédez au [NetApp](#)Page d'enregistrement de l'utilisateur et inscription pour une nouvelle NetApp compte utilisateur.
2. Complétez le (s) formulaire (s) avec vos informations. Assurez-vous de sélectionner le NetApp Niveau d'accès client/utilisateur final. Dans le champ NUMÉRO DE SÉRIE, copiez et collez l'ID du système de fichiers FSx pour votre système de fichiers ONTAP. Consultez l'exemple suivant:

USER ACCESS LEVEL

- ☐ Guest User ☒ NetApp Customer / End User
☐ NetApp Reseller / Service Provider / System Integrator / Partner

Product Information (Optional)

Please enter a Serial Number or System ID to help us validate your access level.

Please note: Not providing a Serial Number or System ID may delay processing of your request.

SERIAL NUMBER

fs-0de9123abcf12368a

(Either a NetApp hardware Serial Number, often located on back of unit; or a NetApp software Serial Number.)

OR

SYSTEM ID

(Run a "sysconfig -a" command on your NetApp product. The output should list the System ID.)

NETAPP TOKEN

À quoi s'attendre après votre inscription

Clients ayant déjà NetApp les produits verront leur compte NSS passer à un accès de niveau client dans un délai d'un jour ouvrable. 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.

Utilisation 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 BlueXP pour FSx Amazon NetApp for ONTAP](#).

 Note

NetApp BlueXP n'est pas pris en charge pour les systèmes de fichiers de deuxième génération comportant plusieurs paires de haute disponibilité (HA).

Utilisation NetApp Gestionnaire de système avec BlueXP

Vous pouvez gérer vos systèmes de fichiers Amazon FSx for NetApp ONTAP à l'aide de System Manager directement depuis BlueXP. BlueXP vous 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 le NetApp Documentation ONTAP.

 Note

NetApp System Manager n'est pas pris en charge pour les systèmes de fichiers de deuxième génération comportant plusieurs paires HA.

Utilisation de NetApp ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

Vous pouvez gérer vos ressources Amazon FSx for NetApp ONTAP à l'aide du NetApp ONTAP CLI. Vous pouvez gérer les ressources dans le système de fichiers (de la même manière que NetApp ONTAP (cluster) et au niveau de la SVM.

Gestion des systèmes de fichiers à l'aide du ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

Tu peux courir ONTAP Commandes CLI sur votre système de fichiers FSx for ONTAP, similaires à leur exécution sur un NetApp ONTAP grappe. Vous accédez au ONTAP CLI sur votre système de fichiers en établissant une connexion shell sécurisée (SSH) au point de terminaison de gestion

du système de fichiers et en vous connectant à l'aide du `fsxadmin` nom d'utilisateur et du mot de passe. Vous avez la possibilité de définir le `fsxadmin` 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 mot de `fsxadmin` passe n'a pas été défini. Vous devrez donc en définir un pour vous connecter au ONTAP CLI. Pour plus d'informations sur la définition du mot de passe du `fsxadmin` système de fichiers, consultez [Mise à jour des systèmes de fichiers](#). Vous trouverez le nom DNS et l'adresse IP du point de terminaison de gestion de votre système de fichiers dans la FSx console Amazon, dans l'onglet Administration de la FSx page de détails du système de fichiers ONTAP.

Pour vous connecter au point de terminaison de gestion du système de fichiers via SSH, connectez-vous d'abord à une EC2 instance du même VPC que FSx le système de fichiers for ONTAP. Une fois connecté à l' EC2 instance, utilisez l'`fsxadmin` utilisateur et le mot de passe pour accéder par SSH à l'adresse IP ou au nom DNS du point de terminaison de gestion du système de fichiers, comme dans les exemples suivants.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

La commande SSH avec des exemples de valeurs :

```
ec2user $ ssh fsxadmin@198.51.100.0
```

La commande SSH utilisant le nom DNS du point de terminaison de gestion :

```
ec2user $ ssh fsxadmin@file-system-management-endpoint-dns-name
```

La commande SSH utilisant un exemple de nom DNS :

```
ec2user $ ssh fsxadmin@management.fs-0abcdef123456789.fsx.us-east-2.aws.com
Password: fsxadmin_password
```

```
This is your first recorded login.
FsxId0abcdef123456789::>
```

Champ d'application de ONTAP Commandes CLI disponibles pour **fsxadmin**

La `fsxadmin` vue administrative se situe au niveau du système de fichiers, qui inclut tous SVMs les volumes du système de fichiers. Le `fsxadmin` rôle joue le rôle de ONTAP administrateur du cluster.

Les systèmes de fichiers Amazon FSx for NetApp ONTAP étant entièrement gérés, le `fsxadmin` rôle peut exécuter un sous-ensemble des systèmes disponibles ONTAP Commandes CLI.

Pour voir la liste des commandes `fsxadmin` pouvant être exécutées, utilisez ce qui suit [security login role show](#) ONTAP Commande CLI :

```
FsxId0abc123def456::> security login role show -role fsxadmin -access !none
```

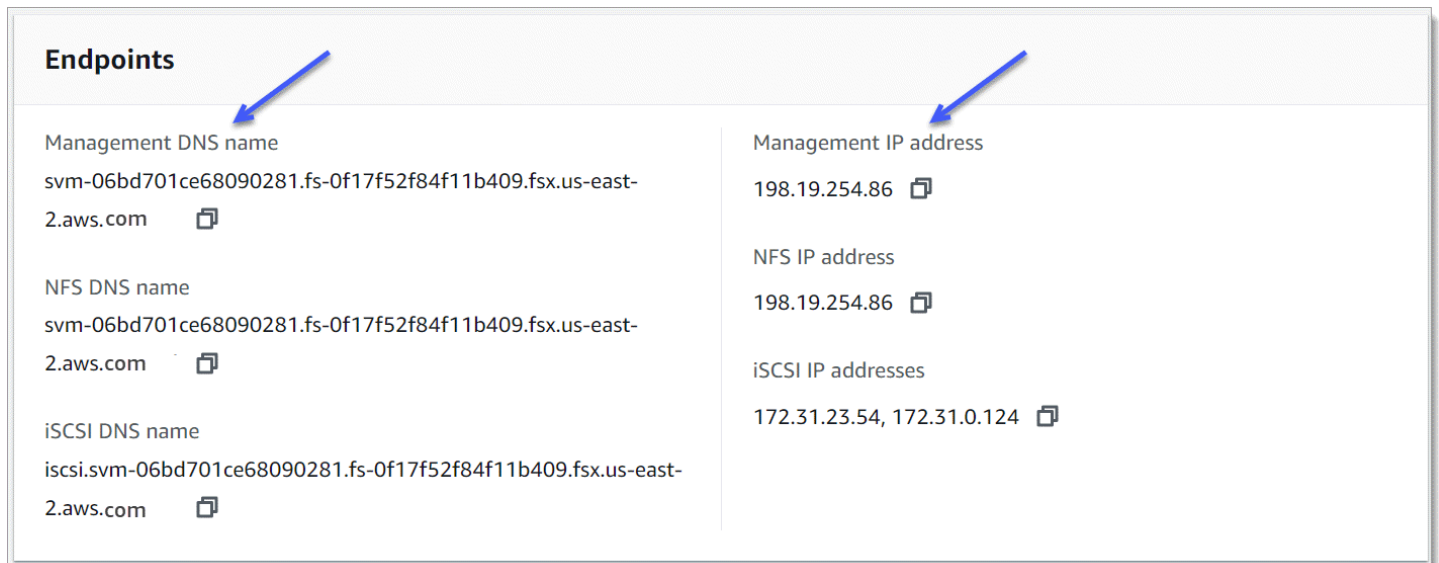
Vserver	Role Name	Command/ Directory	Access Query Level

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
.			
.			
.			
378 entries were displayed.			

Gérer SVMs avec le ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

Vous pouvez accéder au ONTAP CLI sur 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 et

du mot de passe. Vous trouverez le nom DNS et l'adresse IP du point de gestion de la SVM dans la FSx console Amazon, 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 `vsadmin` nom d'utilisateur et le 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 de plus amples informations, veuillez consulter [Mise à jour des machines virtuelles de stockage \(SVM\)](#). 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 pour NetApp ONTAP prend en charge le NetApp ONTAP Commandes CLI.

Pour une référence complète de NetApp ONTAP Commandes CLI, reportez-vous à la section [Commandes ONTAP : référence de page de manuel](#).

Utilisation de ONTAP API REST

Lorsque vous accédez à votre système de fichiers FSx for ONTAP à l'aide du ONTAP API 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 (CAs) — Le bundle de certificats pour chaque région se trouve à l'adresse suivante URLs : CAs
 - [https://fsx-aws-certificates.s3.amazonaws.com/bundle-aws-region](https://fsx-aws-certificates.s3.amazonaws.com/bundle-aws-region.pem) .pem pour public Régions AWS
 - [https://fsx-aws-us-gov-certificates.s3.us-gov-west-1.amazonaws.com/bundle-aws-region](https://fsx-aws-us-gov-certificates.s3.us-gov-west-1.amazonaws.com/bundle-aws-region.pem) .pem pour les régions AWS GovCloud
 - [https://fsx-aws-cn-certificates.s3.cn-north-1.amazonaws.com.cn/bundle-aws-region](https://fsx-aws-cn-certificates.s3.cn-north-1.amazonaws.com.cn/bundle-aws-region.pem) .pem pour les régions de Chine AWS

Pour une référence complète de NetApp ONTAP Commandes de l'API REST, consultez le [NetApp ONTAP Référence en ligne de l'API REST](#).

Marquer les ressources Amazon FSx

Pour vous aider à gérer vos systèmes de fichiers et les autres FSx ressources Amazon, vous pouvez attribuer vos propres métadonnées à chaque ressource sous forme de balises. Les balises vous permettent de classer vos AWS ressources de différentes manières, par exemple par objectif, propriétaire ou environnement. Cette classification 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](#)
- [Balisage de vos ressources](#)
- [Copier des balises dans les sauvegardes](#)
- [Restrictions liées aux étiquettes](#)
- [Autorisations et balisage](#)

Principes de base des étiquettes

Une étiquette est une étiquette que vous attribuez à une AWS ressource. Chaque balise est composée 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, propriétaire ou environnement. Par exemple, vous pouvez définir un ensemble de balises pour les systèmes de FSx fichiers Amazon de votre compte afin de suivre le propriétaire et le niveau de pile 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 de balisage des ressources efficace, consultez la section [Marquage AWS des ressources](#) dans le. Références générales AWS

Voici quelques comportements de balisage à prendre en compte :

- Les tags n'ont aucune signification sémantique pour Amazon FSx et sont interprétés strictement comme des chaînes de caractères.
- Les balises ne sont pas automatiquement affectées à vos ressources.
- Vous pouvez modifier les clés et valeurs de balise, et vous pouvez retirer des balises 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, ses balises sont également supprimées.
- Si vous utilisez l' FSx API Amazon, le AWS Command Line Interface (AWS CLI) ou un AWS SDK, vous pouvez effectuer les opérations suivantes :
 - Vous pouvez utiliser l'action 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 sa création. En attribuant des balises aux ressources au moment de la création, vous pouvez supprimer la nécessité d'exécuter des scripts de balisage personnalisés après la création de ressources.

Si les balises ne peuvent pas être appliquées lors de la création des ressources, Amazon FSx annule le processus de création des 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 n'est laissée non étiquetée à aucun moment.

Note

Certaines autorisations AWS Identity and Access Management (IAM) sont requises pour que les utilisateurs puissent étiqueter les ressources lors de leur création. Pour de plus amples informations, veuillez consulter [Accorder l'autorisation de baliser les ressources lors de la création](#).

Balisage de vos ressources

Vous pouvez étiqueter FSx les ressources Amazon présentes dans votre compte. Si vous utilisez la FSx console Amazon, vous pouvez appliquer des balises aux ressources en utilisant l'onglet Tags

sur l'écran des ressources concerné. Lorsque vous créez des ressources, vous pouvez appliquer la clé Nom avec une valeur, 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 les ressources en fonction de la clé Name, cette clé n'a aucune signification sémantique pour le FSx service Amazon.

Pour mettre en œuvre un contrôle granulaire sur les utilisateurs et les groupes autorisés à étiqueter les ressources lors de la création, vous pouvez appliquer des autorisations au niveau des ressources basées sur des balises dans vos politiques IAM aux actions d' FSxAPI Amazon qui prennent en charge le balisage lors de la création. En utilisant ces autorisations dans vos politiques, vous bénéficiez des avantages suivants :

- Vos ressources sont correctement sécurisées dès leur création.
- Les balises étant appliquées immédiatement à vos ressources, toutes les autorisations au niveau des ressources basées sur des balises contrôlant l'utilisation des ressources sont immédiatement effectives.
- 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 les valeurs de balise définies sur vos ressources existantes, vous pouvez appliquer des autorisations au niveau des ressources aux actions et aux actions de l' FSx API TagResource UntagResource Amazon dans vos politiques IAM.

Pour plus d'informations sur les autorisations requises pour baliser les FSx ressources Amazon lors de leur création, consultez [Accorder l'autorisation de baliser les ressources lors de la création](#).

Pour plus d'informations sur l'utilisation de balises pour restreindre l'accès aux FSx ressources Amazon dans les politiques IAM, consultez [Utilisation de balises pour contrôler l'accès à vos FSx ressources Amazon](#).

Pour plus d'informations sur le balisage de vos ressources pour la facturation, consultez la section [Utilisation des balises de répartition des coûts](#) dans le Guide de AWS Billing l'utilisateur.

Copier des balises dans les sauvegardes

Lorsque vous créez ou mettez à jour un volume dans l' FSx API Amazon AWS CLI, vous pouvez CopyTagsToBackups activer la copie automatique des balises de vos volumes vers les sauvegardes.

Note

Si vous spécifiez des balises lors de la création d'une sauvegarde initiée par l'utilisateur (y compris le badge lorsque vous créez une sauvegarde à l'aide de la FSx console Amazon), les balises ne sont pas copiées depuis le volume, même si vous les avez activées `CopyTagsToBackups`.

Pour plus d'informations sur les sauvegardes, consultez [Protection de vos données grâce à des sauvegardes en volume](#). Pour plus d'informations sur l'activation `CopyTagsToBackups`, consultez [Pour créer un volume \(CLI\)](#) le guide [Pour mettre à jour la configuration d'un volume \(CLI\)](#) de l'utilisateur Amazon FSx pour NetApp ONTAP ou le manuel de [CreateVolume](#) référence [UpdateVolume](#) de 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 la clé est de 128 caractères Unicode en UTF-8.
- La longueur maximale de la valeur est de 256 caractères Unicode en UTF-8.
- Les caractères autorisés sont les lettres, les chiffres et les espaces représentables en UTF-8, ainsi que les caractères suivants : + - (tiret) (trait de soulignement) = . _ . : / @
- 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 `aws :` préfixe est réservé à l' AWS usage. Si une balise possède une clé de balise avec ce préfixe, vous ne pouvez ni modifier ni supprimer la clé ou la valeur de la 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'identifiant de la ressource. Par exemple, pour supprimer un système de fichiers que vous avez balisé avec une clé de balise appelée `DeleteMe`, vous devez utiliser l'`DeleteFileSystem` action avec l'identifiant de ressource du système de fichiers, tel que `fs-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 AWS a accès à ces balises. Pour le contrôle d'accès basé sur des balises aux ressources partagées, chacun Compte AWS 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 les FSx ressources Amazon lors de leur création, consultez [Accorder l'autorisation de baliser les ressources lors de la création](#).

Pour plus d'informations sur l'utilisation de balises pour restreindre l'accès aux FSx ressources Amazon dans les politiques IAM, consultez [Utilisation de balises pour contrôler l'accès à vos FSx ressources Amazon](#).

Protection de vos données

Outre la réplication automatique des données de votre système de fichiers pour garantir [une durabilité élevée](#), Amazon FSx vous propose également les options suivantes pour mieux protéger vos données :

- Des sauvegardes de FSx volumes Amazon natives qui répondent à vos besoins en matière de conservation des sauvegardes et de conformité au sein d'Amazon FSx.
- Utilisation AWS Backup pour mettre en œuvre une stratégie de sauvegarde et de conservation automatisée et gérée de manière centralisée sur plusieurs sites Services AWS.
- Des instantanés qui permettent à vos utilisateurs d'annuler facilement les modifications de fichiers indésirables, en rétablissant les versions précédentes des fichiers.
- Utiliser SnapLock pour créer des volumes de stockage WORM (Write Once, Read Many) afin d'empêcher la modification ou la suppression de fichiers une fois validés, pendant une période de conservation spécifiée.
- FlexCache les volumes offrent une réplication des données efficace, rentable et performante pour les charges de travail exigeantes en lecture avec des données pratiquement inchangées.
- Utiliser SnapMirror pour créer une réplication automatique planifiée du système de fichiers vers un second système de fichiers à des fins de protection des données et de reprise après sinistre.

Rubriques

- [Protection de vos données grâce à des sauvegardes en volume](#)
- [Protection de vos données grâce à des instantanés](#)
- [Protégez vos données grâce à une protection autonome contre les ransomwares](#)
- [Protégez vos données avec SnapLock](#)
- [Répliquer vos données avec FlexCache](#)
- [Réplication de vos données à l'aide de NetApp SnapMirror](#)

Protection de vos données grâce à des sauvegardes en volume

Avec FSx for ONTAP, vous pouvez protéger vos données en effectuant des sauvegardes quotidiennes automatiques et des sauvegardes initiées par l'utilisateur des volumes de votre 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. Vous pouvez restaurer des sauvegardes de volumes sur n'importe quel système FSx de fichiers ONTAP existant auquel vous avez accès et qui se trouve dans le même système que celui Région AWS où la sauvegarde est stockée. L'utilisation FSx des sauvegardes Amazon facilite la création, l'affichage, la restauration et la suppression de sauvegardes de vos volumes.

Amazon FSx prend en charge la sauvegarde de ONTAP volumes à l'aide d'un `OntapVolumeType` système de lecture-écriture (RW).

Note

Amazon FSx ne prend pas en charge la sauvegarde des volumes de protection des données (DP), des volumes miroir de partage de charge (LSM) ou des volumes de destination pour FlexCache et SnapMirror.

Rubriques

- [Comment fonctionnent les sauvegardes](#)
- [Besoins de stockage](#)
- [Sauvegardes quotidiennes automatiques](#)
- [Sauvegardes initiées par l'utilisateur](#)
- [Copier des balises dans les sauvegardes](#)
- [Utilisation AWS Backup avec Amazon FSx](#)
- [Restauration des sauvegardes sur un nouveau volume](#)
- [Performances de sauvegarde et de restauration](#)
- [Sauvegarde de SnapLock volumes](#)
- [Création de sauvegardes initiées par l'utilisateur](#)
- [Restauration d'une sauvegarde sur un nouveau volume](#)
- [Restauration d'un sous-ensemble de données](#)
- [Surveillance de la progression lors de la restauration d'une sauvegarde](#)
- [Suppression de sauvegardes](#)

Comment fonctionnent les sauvegardes

Toutes les FSx sauvegardes Amazon (sauvegardes quotidiennes automatiques et sauvegardes initiées par l'utilisateur) sont incrémentielles, ce qui signifie qu'elles ne stockent que les modifications apportées aux données depuis la fin de la sauvegarde précédente. Cela permet de réduire à la fois le temps nécessaire à la création d'une sauvegarde et la quantité de stockage utilisée par chaque sauvegarde. Les sauvegardes incrémentielles optimisent les coûts de stockage en évitant de stocker des données dupliquées. FSx pour ONTAP, les sauvegardes sont effectuées par volume, chaque sauvegarde ne contenant que les données d'un volume spécifique. Les FSx sauvegardes Amazon sont stockées de manière redondante dans plusieurs zones de disponibilité pour garantir une durabilité élevée.

FSx Les sauvegardes Amazon utilisent des instantanés (point-in-time images en lecture seule de vos volumes) pour maintenir l'incrémentalité entre les sauvegardes. Chaque fois qu'une sauvegarde est effectuée, Amazon prend d'abord un instantané de votre volume. L'instantané de sauvegarde est stocké dans votre volume et consomme de l'espace de stockage sur le volume. Amazon 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.

Lorsque vous [supprimez](#) une sauvegarde, seules les données propres à cette sauvegarde sont supprimées. Chaque FSx sauvegarde Amazon 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.

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

Besoins de stockage

Votre volume et votre système de fichiers doivent chacun 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.

Sauvegardes quotidiennes automatiques

Lorsque vous créez un système de fichiers, les sauvegardes quotidiennes automatiques sont activées par défaut pour les volumes de votre système de fichiers. Vous pouvez activer ou désactiver les sauvegardes quotidiennes automatiques pour les systèmes de fichiers existants à tout moment. Les sauvegardes quotidiennes automatiques de tous les volumes ont lieu pendant la fenêtre de sauvegarde quotidienne du système de fichiers, qui est automatiquement définie lorsque vous créez un système de fichiers. Vous pouvez modifier la fenêtre de sauvegarde quotidienne à tout moment. Pour des [performances de sauvegarde](#) optimales, nous vous recommandons de choisir une fenêtre de sauvegarde quotidienne en dehors des heures normales de fonctionnement lorsque les clients et les applications accèdent aux données de vos volumes.

À l'aide de la console, vous pouvez définir la période de conservation des sauvegardes quotidiennes automatiques sur une valeur comprise entre 1 et 90 jours 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. Amazon FSx supprime une sauvegarde quotidienne automatique à l'expiration de sa période de conservation. À l'aide de l'API AWS CLI and, vous pouvez définir la période de rétention sur une valeur comprise entre 0 et 90 jours ; la définir sur 0 désactive les sauvegardes quotidiennes automatiques.

Les sauvegardes quotidiennes automatiques, la fenêtre de sauvegarde quotidienne et la période de conservation des sauvegardes sont des paramètres du système de fichiers qui s'appliquent à tous les volumes de votre système de fichiers. Vous pouvez utiliser la FSx console Amazon AWS CLI, l'API ou l'API pour modifier ces paramètres. Pour de plus amples informations, veuillez consulter [Mise à jour des systèmes de fichiers](#).

Vous ne pouvez pas créer de sauvegarde de volume (sauvegardes quotidiennes automatiques ou sauvegardes initiées par l'utilisateur) si le volume est hors ligne. Pour de plus amples informations, veuillez consulter [Affichage de 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 pour toujours, sauf si vous les supprimez ou si vous AWS Backup les supprimez.

Vous pouvez [supprimer](#) manuellement une sauvegarde quotidienne automatique à l'aide de la FSx console, de la CLI et de l'API Amazon. Lorsque vous supprimez un volume, vous supprimez également les sauvegardes quotidiennes automatiques de ce volume. Amazon FSx propose la possibilité de créer une sauvegarde finale d'un volume avant de le supprimer. La sauvegarde finale est conservée pour toujours, sauf si vous la supprimez.

Sauvegardes initiées par l'utilisateur

Avec Amazon FSx, vous pouvez sauvegarder manuellement les 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 FSx console, de l'API ou de la CLI Amazon. Ils ne sont jamais automatiquement supprimés par Amazon FSx.

Pour obtenir des instructions sur la création d'une sauvegarde initiée par l'utilisateur, consultez [Création de sauvegardes initiées par l'utilisateur](#).

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, Amazon FSx ne copie pas les balises depuis le volume, même si celui-ci CopyTagsToBackups est activé.

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. Son utilisation AWS Backup facilite le développement d'une stratégie de sauvegarde centralisée aux fins de conformité légale, réglementaire et professionnelle. Il 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 politiques 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 de votre volume FSx initiées par un utilisateur Amazon et offrent les mêmes options de restauration que les sauvegardes effectuées à l'aide de la console Amazon FSx . L'utilisation AWS Backup pour gérer ces sauvegardes fournit des fonctionnalités supplémentaires, notamment 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 coffre-fort de [sauvegarde](#).

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 de plus amples informations, veuillez consulter [Les quotas que vous pouvez augmenter](#). Vous pouvez afficher et restaurer les sauvegardes créées à AWS Backup l'aide de la FSx console, de la CLI et de l'API Amazon. Toutefois, vous ne pouvez pas supprimer les sauvegardes créées par AWS Backup la FSx console, la CLI ou l'API Amazon. Pour plus d'informations, consultez la section [Getting started with AWS Backup](#) dans le guide du AWS Backup développeur.

AWS Backup Impossible de sauvegarder des volumes hors ligne.

Vous pouvez utiliser des balises pour sélectionner celles de vos ressources FSx for ONTAP qui sont protégées dans un plan de sauvegarde. Ces balises doivent être appliquées au niveau du volume plutôt qu'au niveau du système de fichiers dans son ensemble. Pour plus d'informations, consultez la section [Affectation de ressources à un plan de sauvegarde](#) dans le Guide du AWS Backup développeur.

Restauration des sauvegardes sur un nouveau volume

Vous pouvez restaurer une sauvegarde de volume sur un nouveau volume d'un système de fichiers qui se trouve dans le même Région AWS que celui dans lequel la sauvegarde est stockée. Vous ne pouvez pas restaurer une sauvegarde sur un système de fichiers situé dans un autre endroit Région AWS que celui de la sauvegarde.

Lors de la restauration d'une sauvegarde sur FSx des systèmes de fichiers ONTAP de deuxième génération, les clients peuvent monter et lire les données d'un volume pendant sa restauration. Les clients peuvent monter le volume que vous restaurez et lire les données du fichier une fois qu'Amazon FSx aura chargé toutes les métadonnées sur le nouveau volume et que le volume aura indiqué un état de cycle de vie de `CREATED`. Vous trouverez l'état du cycle de vie d'un volume sur la page [détaillée des volumes](#) de la FSx console Amazon et dans la réponse à la commande [describe-volumes CLI](#).

Lorsque vous lisez des données d'un volume alors que celui-ci est en cours de restauration à partir d'une sauvegarde, si les données n'ont pas encore été téléchargées sur le volume, des latences de lecture allant jusqu'à plusieurs dizaines de millisecondes seront encourues lors du premier accès. Ces lectures sont mises en cache au niveau SSD, et vous pouvez vous attendre à des latences de lecture inférieures à la milliseconde pour les lectures suivantes.

Le temps nécessaire FSx à Amazon pour rendre un volume disponible en lecture seule est proportionnel à la quantité de métadonnées du fichier stockées dans la sauvegarde. Les métadonnées des fichiers consomment généralement 1 à 7 % de l'ensemble des données de sauvegarde en fonction de la taille moyenne des fichiers de votre ensemble de données (les petits ensembles de données consomment plus de métadonnées que les grands ensembles de données).

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 ajoute des volumes constitutifs supplémentaires pour garantir une distribution uniforme des composants.

 Note

Amazon FSx ne prend pas en charge l'accès en lecture aux données pendant la restauration d'un volume à partir d'une sauvegarde, que ce soit pour un SnapLock volume ou pour un volume sur des systèmes de fichiers de première génération. Lors de la restauration de ces sauvegardes, le volume devient disponible pour le montage et l'accès aux données une fois le processus de restauration terminé, et toutes les métadonnées et données sont chargées sur le nouveau volume.

Lors de la restauration d'une sauvegarde, toutes les données sont initialement écrites sur le niveau de stockage SSD. Pendant la restauration, les données sont hiérarchisées en fonction de la capacité de stockage du pool conformément à la [politique de hiérarchisation](#) du volume à restaurer. Comme les données sont d'abord écrites sur le niveau SSD, Amazon FSx interrompt le processus de restauration si le système de fichiers n'a plus d'espace de stockage SSD. La restauration reprend automatiquement dès que suffisamment d'espace SSD est disponible pour poursuivre le processus. Si la politique de hiérarchisation du volume restauré est la même `All`, un processus d'arrière-plan périodique hiérarchise les données en fonction du pool de capacités. Si la politique de hiérarchisation du volume restauré est `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.

Si votre charge de travail nécessite des latences de lecture constantes inférieures à la milliseconde lors de la restauration d'une sauvegarde sur un nouveau volume sur des systèmes de fichiers de deuxième génération, nous vous recommandons de définir la politique de hiérarchisation du volume sur `None` lors du lancement de la restauration, puis d'attendre que toutes les données soient entièrement téléchargées sur le volume avant d'y accéder. Toutes les données seront chargées sur le stockage SSD avant que vous ne tentiez d'y accéder, vous offrant ainsi un accès constant à faible latence à vos données.

Pour step-by-step obtenir des instructions sur la restauration d'une sauvegarde sur un nouveau volume, reportez-vous à [Restauration d'une sauvegarde sur un nouveau volume](#).

Sur les systèmes de fichiers de deuxième génération, vous pouvez également restaurer uniquement un sous-ensemble de données à partir d'une sauvegarde sans avoir à attendre la fin de l'opération de restauration complète. La restauration d'un sous-ensemble des données d'une sauvegarde vous permet de reprendre les opérations plus rapidement en cas de suppression, de modification

ou de corruption accidentelle des données. Pour de plus amples informations, veuillez consulter [Restauration d'un sous-ensemble de données](#).

Vous pouvez suivre la progression de la restauration d'une sauvegarde sur un système de fichiers de deuxième génération dans l'API AWS Management Console AWS CLI, et. Pour de plus amples informations, veuillez consulter [Surveillance de la progression lors de la restauration d'une sauvegarde](#).

 Note

- Vous ne pouvez pas créer un instantané de volume ou effectuer des opérations basées sur des instantanés, telles que le clonage, la SnapMirror réplication ou la création de sauvegardes d'un volume pendant sa restauration à partir d'une sauvegarde.
- 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.

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 et de métadonnées NFS, CIFS et iSCSI. Tous les processus en arrière-plan n'utilisent que la partie inutilisée de la capacité de débit de votre système de fichiers, et leur exécution peut 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.

Parmi les autres facteurs qui influent sur les performances de sauvegarde et de restauration, citons 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 MBps sur plusieurs sauvegardes simultanées contenant principalement des fichiers volumineux.
- 100 MBps sur plusieurs sauvegardes simultanées contenant principalement de petits fichiers.

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

- 250 MBps sur plusieurs restaurations simultanées contenant principalement des fichiers volumineux.
- 100 MBps sur plusieurs restaurations simultanées contenant principalement de petits fichiers.

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. Cependant, vous ne pouvez pas restaurer la sauvegarde d'un SnapLock non-volume en tant que SnapLock volume.

Pour de plus amples informations, veuillez consulter [Comment ? SnapLock fonctionnement](#).

Création de sauvegardes initiées par l'utilisateur

La procédure suivante décrit comment 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 de plus amples informations, veuillez consulter [Affichage de volumes hors ligne](#).

Pour créer une sauvegarde initiée par l'utilisateur (console)

1. Ouvrez la FSx console Amazon 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 voir toutes vos sauvegardes dans la FSx console Amazon en choisissant Backups 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 pour ONTAP sur un nouveau volume à l'aide du AWS Management Console et AWS CLI. Lorsque vous restaurez un volume sur un système de fichiers de deuxième génération, vous pouvez [suivre](#) la progression à l'aide de l'API AWS Management Console AWS CLI, et.

Pour restaurer une sauvegarde de volume sur un nouveau volume (console)

1. Ouvrez la FSx console Amazon à l'adresse <https://console.aws.amazon.com/fsx/>.
2. Dans le volet de navigation, choisissez Backups, puis choisissez la FSx sauvegarde du volume 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 FSx de fichiers ONTAP et la machine virtuelle de stockage sur lesquels vous souhaitez restaurer la sauvegarde dans les menus déroulants.
5. Dans le menu Actions en haut à droite, choisissez Restaurer la sauvegarde. La page Créer un volume à partir d'une sauvegarde apparaît.
6. Choisissez le système FSx de fichiers ONTAP et la machine virtuelle de stockage sur lesquels vous souhaitez restaurer la sauvegarde dans les menus déroulants.
7. 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 (_).
8. Pour Taille du volume, entrez un nombre entier compris entre 20 et 314572800 pour spécifier la taille en mégaoctets (MiB).
9. 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 de plus amples informations, veuillez consulter [Types de volume](#).
10. 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.
11. Pour l'efficacité du stockage, choisissez Activé pour activer les fonctionnalités d'ONTAP efficacité du stockage (déduplication, compression et compactage). Pour de plus amples informations, veuillez consulter [Efficacité du stockage](#).
12. 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 à NTFS ou à UNIX ACLs pour l'accès multiprotocole. Le mode MIXED n'est pas requis pour l'accès multiprotocole et n'est recommandé qu'aux utilisateurs expérimentés.
13. 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, consultez [Règles 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.

14. 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.

15. 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 volume SnapLock Compliance ou SnapLock d'un volume Enterprise, consultez [Compréhension SnapLock Conformité d'](#) et [Compréhension SnapLock Enterprise](#). Pour plus d'informations sur SnapLock, consultez [Protégez vos données avec SnapLock](#).
16. Choisissez Confirmer pour créer le volume.
17. Si vous restaurez la sauvegarde sur un système de fichiers de deuxième génération, vous pouvez suivre la progression de la restauration de la sauvegarde dans l'onglet Mises à jour de la page Volume. Pour de plus amples informations, veuillez consulter [Surveillance de la progression lors de la restauration d'une sauvegarde](#).

Pour restaurer une sauvegarde sur un nouveau volume (CLI)

Utilisez la commande [create-volume-from-backup](#) CLI ou la commande [CreateVolumeFromBackup](#) API 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 à une demande de restauration réussie visant à restaurer une sauvegarde sur un système de fichiers de deuxième génération est la suivante. La réponse inclut l'"AdministrativeActions" objet qui fournit des informations sur l'état et la progression de la demande.

```
{
 "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",
 ---> "AdministrativeActions": [
 {
 "AdministrativeActionType": "DOWNLOAD_DATA_FROM_BACKUP",
 "RequestTime": 1685729972.069,
 "Status": "PENDING"
 }
]
 <----
}

```

La réponse du système à une demande réussie de restauration d'une sauvegarde sur un système de fichiers de première génération est la suivante.

```

{
 "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",
}
}
```

Lorsque vous restaurez un volume sur un système de fichiers de deuxième génération, vous pouvez [suivre la progression](#) à l'aide de l'API AWS Management Console AWS CLI, et.

## Restauration d'un sous-ensemble de données

Vous pouvez restaurer un sous-ensemble de données à partir d'une sauvegarde alors qu'il est en cours de restauration sur un nouveau volume sur des systèmes de fichiers de deuxième génération sans avoir à attendre que l'ensemble de données de sauvegarde soit entièrement restauré.

La procédure suivante répertorie les étapes à suivre lorsque vous devez récupérer un sous-ensemble de données lors de la restauration d'une sauvegarde et que vous ne pouvez pas attendre que la restauration soit terminée dans son intégralité :

Pour restaurer un sous-ensemble de données lors de la restauration d'une sauvegarde

1. Ouvrez la FSx console Amazon à l'adresse <https://console.aws.amazon.com/fsx/>.
2. Sur la page Sauvegardes, recherchez la sauvegarde contenant la version des données 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 FSx de fichiers ONTAP et la machine virtuelle de stockage sur lesquels vous souhaitez restaurer la sauvegarde dans les menus déroulants.
5. Sous Détails du volume, configurez le volume en fonction de vos besoins.
6. Choisissez Confirmer pour créer le volume.
7. [Surveillez la progression](#) de la restauration de la sauvegarde.
8. [Montez le volume](#) à restaurer lorsqu'il indique un état de cycle de vie deCREATED.



9. Localisez le sous-ensemble de données sur le volume que vous devez copier.
10. Copiez les données sur le volume existant utilisé par votre application.
11. Une fois que les données requises de la sauvegarde ont été copiées vers l'emplacement cible, vous pouvez supprimer le volume en cours de restauration avant qu'il ne soit terminé afin d'optimiser l'utilisation des ressources du système de fichiers.

## Surveillance de la progression lors de la restauration d'une sauvegarde

Vous pouvez suivre la progression lors de la restauration d'une sauvegarde de volume sur un système de fichiers de deuxième génération dans l'API AWS Management Console AWS CLI, et. Comme pour toutes les actions FSx administratives d'Amazon, l'état de restauration des sauvegardes est disponible dans la console, la CLI et l'API pendant 30 jours après la fin de l'opération.

Pour suivre la progression lors de la restauration d'une sauvegarde (console)

Ouvrez la FSx console Amazon à l'adresse <https://console.aws.amazon.com/fsx/>.

1. Dans le menu de navigation de gauche, sélectionnez Volumes.
2. Choisissez le volume sur lequel la sauvegarde doit être restaurée.
3. Choisissez l'onglet Mises à jour.
4. Le type Backup Restore Update fournit les informations suivantes :
  - PENDING indique que les métadonnées du fichier sont en cours de téléchargement sur le volume. L'état du cycle de vie du volume est CREATING.
  - IN\_PROGRESS indique que le volume est disponible et que les clients peuvent le monter avec un accès en lecture seule aux données. Le % de progression indique le pourcentage de données téléchargées sur le volume.
  - COMPLETED indique que toutes les données ont été téléchargées sur le volume et que la restauration de la sauvegarde est terminée. Les clients disposent désormais d'un accès en lecture-écriture. Pour les RW volumes, le type du volume passe de DP à à RW à à ce stade.

Pour suivre la progression lors de la restauration d'une sauvegarde (CLI)

- Lorsque vous restaurez une sauvegarde sur un nouveau volume sur un système de fichiers de deuxième génération FSx pour ONTAP, vous pouvez suivre la progression de la restauration à l'aide de la commande [describe-volumes](#)CLI.

Lors de la restauration d'une sauvegarde sur un système de fichiers de deuxième génération, la réponse inclut l'AdministrativeActionsobjet, qui fournit des informations d'état sur le processus de téléchargement des données. Le

```
$ aws fsx describe-volumes
{
 "Volumes": [
 {
 "CreationTime": 1691686114.674,
 "FileSystemId": fs-029ff92192bd4d375,
 "LifeCycle": "CREATING",
 "Name": vol1,
 "OntapConfiguration": {
 "FlexCacheEndpointType": "NONE",
 "JunctionPath": "/vol1",
 "SizeInMegabytes": 100000,
 "StorageEfficiencyEnabled": true,
 "StorageVirtualMachineId": "svm-0ed1d714019426ca9",
 "StorageVirtualMachineRoot": false,
 "TieringPolicy": {
 "Name": "ALL"
 },
 "OntapVolumeType": "DP",
 "SnapshotPolicy": "default",
 "CopyTagsToBackups": false,
 },
 "ResourceARN": "arn:aws:fsx:us-east-1:630831496844:volume/
fs-08ac75f715c6aec76/fsvol-094c015af930790fa",
 "VolumeId": "fsvol-094c015af930790fa",
 "VolumeType": "ONTAP",
 "AdministrativeActions": [
 {
 "AdministrativeActionType": "DOWNLOAD_DATA_FROM_BACKUP",
 "RequestTime": 1685729972.069,
 "Status": "PENDING"
 }
]
 }
]
}
```

Une fois FSx qu'Amazon a chargé toutes les métadonnées du fichier sur le volume restauré, ces champs ont les valeurs suivantes :

- "LifeCycle": "CREATED"— indique que le volume est prêt à être monté.
- "OntapVolumeType": "DP"— indique que le volume est en lecture seule pendant le téléchargement des données du fichier.
- "ProgressPercent": indique le pourcentage de données de fichier chargées sur le volume.
- "Status": "IN\_PROGRESS"— le téléchargement des données du fichier sur le volume est en cours.

À ce stade du processus de restauration, vous pouvez monter le volume avec un accès en lecture seule à toutes les données de la sauvegarde que vous restaurez.

Une fois FSx qu'Amazon a terminé de télécharger toutes les données du fichier sur le nouveau volume, les clients disposent d'un accès complet en lecture-écriture s'il s'agit RW d'un volume. Les indicateurs ont les valeurs suivantes :

- "LifeCycle": "CREATED"— inchangé
- "OntapVolumeType": "RW"— indique que les clients disposent d'un accès complet en lecture-écriture.
- "Status": "COMPLETED"— indique que la restauration est terminée.

Si le processus de restauration échoue, le `AdministrativeAction > Status` aura une valeur de `FAILED`. Un message d'erreur est fourni dans `FailureDetails` objet. Pour plus d'informations, consultez [AdministrativeActionFailureDetails](#) le Amazon FSx API Reference

## Suppression de sauvegardes

Vous pouvez supprimer à la fois les sauvegardes quotidiennes automatiques et les sauvegardes initiées par l'utilisateur de vos volumes à l'aide de la FSx console Amazon, de FSx l'API Amazon ou AWS Command Line Interface (AWS CLI). La suppression d'une sauvegarde est une action permanente irréversible. 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. Vous ne pouvez pas supprimer une sauvegarde si le volume source est [hors ligne](#).

Vous pouvez supprimer un volume pendant sa restauration à partir d'une sauvegarde sur tous les systèmes FSx de fichiers ONTAP. La suppression d'un volume pendant la restauration annule effectivement l'opération de restauration en cours.

 Note

Amazon FSx ne prend pas en charge la suppression de la AVAILABLE sauvegarde la plus récente d'un ONTAP volume, sauf si toutes les autres sauvegardes du volume ont été supprimées.

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 FSx console Amazon 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 delete-backup CLI ou l'action DeleteBackup API équivalente pour supprimer une sauvegarde de volume FSx pour ONTAP, comme indiqué 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 avec une valeur de `DELETED`, indiquant que la demande a été acceptée.

```
{
 "BackupId": "backup-a0123456789abcdef",
 "Lifecycle": "DELETED"
}
```

## Protection de vos données grâce à 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](#)
- [Restaurer des fichiers à partir de snapshots](#)
- [Affichage de l'instantané commun](#)
- [Mettre à jour la réserve d'instantanés de votre volume](#)
- [Désactivation des instantanés automatiques](#)
- [Suppression d'instantanés](#)
- [Suppression d'instantanés](#)
- [Réserve d'instantanés](#)

## 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 intégrées relatives aux instantanés FSx pour 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). Vous pouvez définir un fuseau horaire FSx pour le système de fichiers ONTAP à l'aide de la commande `timezone - timezone time_zone` ONTAP CLI. Pour plus d'informations sur l'accès à la ONTAP CLI, consultez [Utilisation de NetApp ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

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 FSx console Amazon, dans l' AWS CLI API Amazon ou dans l' FSx API Amazon. Pour plus d'informations, consultez [Création de volumes](#) et [Mise à jour des volumes](#).

## Restaurer des fichiers à partir de snapshots

À l'aide des instantanés de votre système de FSx fichiers Amazon, vous pouvez rapidement restaurer les versions précédentes de fichiers ou de dossiers individuels.

Si vous utilisez des clients Linux et macOS, vous pouvez afficher les instantanés dans le `.snapshot` répertoire situé à la racine d'un volume. Si vous utilisez des clients Windows, vous pouvez afficher les instantanés dans l'`Previous Versions` onglet de l'Explorateur Windows (lorsque vous cliquez avec le bouton droit sur un fichier ou un dossier).

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.

## Affichage de l'instantané commun

Le snapshot commun est utilisé pour maintenir l'incrémentalité entre vos sauvegardes. Cette procédure explique comment identifier le cliché commun sur votre volume.

Pour afficher l'instantané commun d'un volume

- Pour déterminer quel instantané est le cliché commun d'un volume, utilisez la commande [volume snapshot show](#) ONTAPCLI.

```
volume snapshot show -volume volume-name
```

Dans la sortie, le nom de l'instantané commun a le format suivant : il *id* s'agit d'une chaîne alphanumérique de 17 chiffres, comme indiqué dans l'exemple suivant : backup-*id*

```
FsxIdabc12345::> volume snapshot show -volume test_vol
 ---Blocks---
Vserver Volume Snapshot Size Total% Used%

dest-svm test_vol
 snap1 144KB 0% 3%
 snap2 832KB 0% 16%
 ---> backup-abcdef0123456789a 4.87MB 0% 53% <---
 weekly.2024-05-26_0015 5.02MB 0% 54%
 weekly.2024-06-02_0015 2.22MB 0% 34%
 daily.2024-06-04_0010 284KB 0% 6%
 daily.2024-06-05_0010 4.29MB 0% 50%
 hourly.2024-06-05_0705 168KB 0% 4%

8 entries were displayed.
```

### 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 d'un volume fera de la sauvegarde suivante une sauvegarde complète du volume au lieu d'une sauvegarde incrémentielle.



## Mettre à jour la réserve d'instantanés de votre 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 ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

2. Utilisez la commande `volume modify` ONTAPCLI pour modifier le pourcentage d'espace disque utilisé pour la réserve de copies Snapshot. 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.
  - *percent*: le pourcentage d'espace disque que vous souhaitez réserver pour les copies Snapshot.

```
::> volume modify -vserver svm_name -volume vol_name -percent-snapshot-space percent
```

L'exemple suivant modifie la réserve d'instantanés pour le volume 1 à 25 % de la capacité de stockage du volume.

```
::> volume modify -vserver vs0 -volume vol1 -percent-snapshot-space 25
```

## Désactivation des instantanés automatiques

Les instantanés automatiques sont activés par la politique d'instantanés 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 ne pas 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 FSx console Amazon 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 [UpdateVolume](#) API équivalente) pour définir le SnapshotPolicy sur none, 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

 - - - -

```

- 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.

```

## 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](#) ONTAP CLI 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. Les instantanés étant incrémentiels, vous ne récupérez pas une quantité de stockage égale à la taille de l'instantané lorsque vous le supprimez. Vous pouvez voir la quantité d'espace de stockage que vous pouvez récupérer lors de la suppression d'un instantané à l'aide de la commande [volume snapshot compute-reclaimable -vserver](#) ONTAP CLI, en utilisant vos données pour remplacer, et. *svm\_name vol\_name snapshot\_name*

```
fsid8970abc52::> volume snapshot compute-reclaimable -vserver svm_name -volume vol_name
 -snapshot snapshot_name
A total of 667648 bytes can be reclaimed.
```

Vous pouvez supprimer des instantanés soit en créant une [politique de suppression automatique des instantanés](#), soit en [supprimant manuellement](#) les instantanés. La suppression d'un instantané entraîne la suppression des données modifiées enregistrées sur le cliché.

## Suppression d'instantanés

Utilisez la commande [volume snapshot delete](#) ONTAP CLI 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 FSx sauvegardes Amazon sont activées, Amazon FSx conserve un instantané de la FSx sauvegarde Amazon la plus récente 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. Pour de plus amples informations, veuillez consulter [Affichage de l'instantané commun](#).

```
FsxIdabcdef01234567892::> volume snapshot delete -vserver svm_name -volume vol_name -
snapshot snapshot_name
```

## 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.

## 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, celui-ci 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 instantanés dans la réserve d'instantanés, la suppression de fichiers du niveau SSD principal libère de l'espace disque pour de nouveaux fichiers, tandis que les copies d'instantanés qui font référence à ces fichiers ne consomment que l'espace de la réserve de copies d'instantanés.

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 snapshot 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 de plus amples informations, veuillez consulter [Mettre à jour la réserve d'instantanés de votre volume](#).

# Protégez vos données grâce à une protection autonome contre les ransomwares

La protection autonome contre les ransomwares (ARP) est une NetApp ONTAP Fonctionnalité pilotée par l'IA qui surveille et protège vos données contre les attaques de ransomwares et de logiciels malveillants si vos clients Windows ou Linux sont compromis. Grâce à l'apprentissage automatique, ARP se familiarise avec vos systèmes de fichiers FSx pour ONTAP afin de détecter de manière proactive les activités anormales. L'ARP est disponible pour tous les systèmes de fichiers ONTAP, nouveaux ou existants FSx , partout où Régions AWS Amazon FSx for NetApp ONTAP est disponible.

## Comment fonctionne l'ARP

Vous pouvez activer l'ARP par volume ou par défaut sur tous les nouveaux volumes d'une SVM à l'aide du ONTAP CLI ou API REST. Pour plus d'informations sur l'activation de l'ARP, consultez [Activer la protection autonome contre les ransomwares](#).

L'ARP fonctionne selon deux modes : apprentissage et mode actif. Lorsque vous activez ARP pour la première fois pour votre volume FSx for ONTAP, celui-ci s'exécute en mode apprentissage. En mode apprentissage, l'ARP analyse les modèles d'accès à votre charge de travail. ONTAP détermine automatiquement la période d'apprentissage optimale en fonction de la charge de travail de votre volume, qui peut prendre jusqu'à 30 jours. Lorsque c'est fait, ARP passe en mode actif. En mode actif, l'ARP surveille les données entrantes et l'activité sur le volume afin d'identifier les attaques potentielles de ransomwares et de malwares. Pour de plus amples informations, veuillez consulter [Ce que recherche ARP](#). Si l'ARP détecte une activité anormale, un ONTAP Un instantané est automatiquement créé pour vous aider à récupérer vos données le plus près possible du moment de l'attaque potentielle. L'instantané aura un préfixe de `Anti_ransomware_backup`, ce qui le rend facile à identifier. S'il est déterminé que la probabilité d'attaque est modérée, ONTAP générera un message du système de gestion des événements (EMS) que vous pourrez consulter. Pour plus d'informations, consultez [Comment répondre à une attaque présumée avec l'ARP](#) et [Comprendre les alertes EMS pour une protection autonome contre les ransomwares](#).

La surcharge de performance de l'ARP est minimale pour la plupart des charges de travail. Si vos volumes sont soumis à des charges de travail intensives en lecture, NetApp recommande de ne pas protéger plus de 150 volumes de ce type par système de fichiers. Si vous dépassez ce nombre, les IOPS pour cette charge de travail peuvent chuter jusqu'à 4 %. Si vos volumes ont des charges de travail intensives en écriture, NetApp recommande de ne pas protéger plus de 60 volumes de ce

type par système de fichiers. Dans le cas contraire, les IOPS pour cette charge de travail risquent de chuter jusqu'à 10 %. Pour plus d'informations sur les performances, consultez [Amazon FSx pour les performances d' NetApp ONTAP](#).

L'activation de l'ARP sur votre système de fichiers FSx for ONTAP n'entraîne aucun coût supplémentaire.

## Ce que recherche ARP

L'ARP recherche les signes indiquant que vos clients Windows ou Linux sont compromis. Une fois qu'ARP a pris connaissance de votre volume FSx for ONTAP et est passé en mode actif, il recherche les types d'activité suivants sur le volume :

- Changements d'entropie, c'est-à-dire des différences dans le caractère aléatoire des données d'un fichier.
- Modifications des types d'extension de fichier, ce qui signifie que la nouvelle extension n'est pas cohérente avec le type d'extension normalement utilisé. La valeur par défaut est de 20 fichiers dont l'extension n'avait pas été observée auparavant dans le volume.
- Modifications des IOPS des fichiers, ce qui entraîne une augmentation de l'activité anormale du volume avec des données chiffrées.

Vous pouvez modifier les paramètres de détection des ransomwares pour votre volume si nécessaire. Par exemple, si votre volume héberge de nombreux types d'extensions de fichiers. Pour plus d'informations, consultez la section [Gérer les paramètres de détection des attaques de la protection autonome contre les ransomwares ONTAP](#) dans le centre de NetApp documentation.

### Note

L'ARP n'empêche pas les administrateurs malhonnêtes munis d'informations d'identification d'accéder à votre système de fichiers FSx for ONTAP. AWS recommande une approche de sécurité à plusieurs niveaux AWS Backup, y compris, ONTAP des instantanés, et SnapLock.

## Comment répondre à une attaque présumée avec l'ARP

Si l'ARP détecte une attaque, il génère un instantané qui peut être utilisé comme point de reprise. L'instantané est verrouillé et ne peut pas être supprimé par des moyens normaux. En fonction de la



gravité de l'attaque, il générera également une alerte EMS indiquant le volume affecté, la probabilité d'attaque et la chronologie de l'attaque. Si vous souhaitez recevoir des alertes lors de la création d'un nouvel instantané ou de l'observation d'une nouvelle extension de fichier sur votre volume, vous pouvez configurer ARP pour envoyer ces alertes. Pour plus d'informations, consultez [Configurer les alertes ARP](#) dans le Centre de NetApp documentation.

Vous pouvez générer un rapport pour afficher des informations détaillées sur une attaque présumée. Après avoir examiné le rapport, vous pouvez savoir ONTAP si l'alerte a été générée par un faux positif ou une attaque présumée. Si vous qualifiez l'alerte d'attaque présumée, vous devez déterminer l'étendue de l'attaque, puis récupérer les données à partir du snapshot créé par l'ARP. Si vous qualifiez l'attaque de faux positif, l'instantané créé par l'ARP est automatiquement supprimé. Pour de plus amples informations, veuillez consulter [Répondre aux alertes de protection autonome contre les ransomwares](#).

Nous vous recommandons de surveiller les messages EMS de votre système de fichiers et l'état de vos volumes dans ONTAP CLI et API REST. Pour plus d'informations sur les messages EMS pour ARP, consultez [Comprendre les alertes EMS pour une protection autonome contre les ransomwares](#).

## Rubriques

- [Activer la protection autonome contre les ransomwares](#)
- [Répondre aux alertes de protection autonome contre les ransomwares](#)
- [Comprendre les alertes EMS pour une protection autonome contre les ransomwares](#)

## Activer la protection autonome contre les ransomwares

Les procédures suivantes expliquent comment utiliser le ONTAP CLI pour activer la protection autonome contre les ransomwares (ARP) en mode apprentissage et en mode actif, ainsi que pour vérifier que l'ARP est activé. Pour plus d'informations sur l'ARP, consultez [Comment fonctionne l'ARP](#).

### Activation de l'ARP en mode apprentissage

Pour activer l'ARP en mode apprentissage sur un volume existant à l'aide du ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

- Exécutez la commande suivante. Remplacez *vol\_name* et *svm\_name* par vos propres informations.

```
security anti-ransomware volume dry-run -volume vol_name -vserver svm_name
```

Pour plus d'informations sur cette commande, consultez [security anti-ransomware volume dry-run](#)le NetApp centre de documentation.

 Note

Le mode d'apprentissage s'applique uniquement aux données nouvellement écrites. Les données existantes ne sont ni scannées ni analysées. Les comportements normaux du trafic de données sont déterminés en fonction des nouvelles données écrites après l'activation de l'ARP sur le volume.

Pour activer l'ARP en mode apprentissage sur un nouveau volume à l'aide du ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

- Exécutez la commande suivante. Remplacez *vol\_name*, *svm\_name*, *size*, et */path\_name* par vos informations.

```
volume create -volume vol_name -vserver svm_name -aggregate aggr_name -size size -
anti-ransomware-state dry-run -junction-path /path_name
```

Pour plus d'informations sur cette commande, consultez [volume create](#)le NetApp centre de documentation.

Activation de l'ARP en mode actif

Pour activer l'ARP en mode actif sur un volume existant à l'aide du ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

- Exécutez la commande suivante. Remplacez *vol\_name* et *svm\_name* par vos propres informations.

```
security anti-ransomware volume enable -volume vol_name -vserver svm_name
```

Pour plus d'informations sur cette commande, consultez [security anti-ransomware volume enable](#)le NetApp centre de documentation.

 Note

Nous recommandons de conserver un volume en mode apprentissage pendant au moins 30 jours avant de le convertir en mode actif. L'ARP détermine automatiquement la période d'apprentissage optimale et passe du mode d'apprentissage lorsqu'il est prêt. Ce processus peut avoir lieu dans moins de 30 jours.

## Activation de l'ARP par défaut au niveau de la SVM

Pour activer l'ARP par défaut sur une SVM existante à l'aide du ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

- Exécutez la commande suivante. Remplacez *svm\_name* par vos propres informations.

```
vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run
```

Pour plus d'informations sur cette commande, consultez [vserver modify](#) le NetApp centre de documentation.

## Vérifier le statut de l'ARP

Pour vérifier l'état de l'ARP à l'aide du ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

- Exécutez la commande suivante.

```
security anti-ransomware volume show
```

Pour plus d'informations sur cette commande, consultez [security anti-ransomware volume show](#) le NetApp centre de documentation.

Vous pouvez suspendre temporairement (puis reprendre) l'ARP si vous prévoyez des événements impliquant une charge de travail importante. Pour plus d'informations, consultez [Suspendre la protection autonome contre les ransomwares ONTAP pour exclure les événements liés à la charge de travail de l'analyse](#) dans le centre de NetApp documentation.

## Répondre aux alertes de protection autonome contre les ransomwares

Les procédures suivantes expliquent comment utiliser le ONTAP CLI pour afficher les alertes de protection autonome contre les ransomwares (ARP), générer des rapports d'attaques et prendre des mesures en fonction des rapports. Pour plus d'informations sur la façon dont l'ARP détecte les attaques et y répond, consultez [Ce que recherche ARP](#) et [Comment répondre à une attaque présumée avec l'ARP](#).

### Afficher les alertes ARP

Pour afficher une alerte ARP sur un volume à l'aide du ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

- Exécutez la commande suivante. Remplacez *svm\_name* et *vol\_name* par vos propres informations.

```
security anti-ransomware volume show -vserver svm_name -volume vol_name
```

Après avoir exécuté la commande, vous verrez un résultat similaire à l'exemple suivant :

```
Vserver Name: fsx
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 9/14/2021 01:03:23
Number of Attacks: 1
```

Pour plus d'informations sur cette commande, consultez [security anti-ransomware volume show](#) le NetApp centre de documentation.

### Génération de rapports ARP

Pour générer des rapports ARP à l'aide du ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

- Exécutez la commande suivante. Remplacez *vol\_name* et */file\_location/* par vos propres informations. Après avoir généré le rapport, vous pouvez le consulter sur un système client.

```
security anti-ransomware volume attack generate-report -volume vol_name -dest-path /file_location/
```

Pour plus d'informations sur cette commande, consultez [security anti-ransomware volume attack generate-report](#)le NetApp centre de documentation.

## Prendre des mesures concernant les rapports ARP

Pour agir en cas d'attaque faussement positive provenant d'un rapport ARP à l'aide du ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

- Exécutez la commande suivante. Remplacez *svm\_name**vol\_name*, et *[extension identifiers]* par vos propres informations.

```
security anti-ransomware volume attack clear-suspect -vserver svm_name -
volume vol_name [extension identifiers] -false-positive true
```

Pour plus d'informations sur cette commande, consultez [security anti-ransomware volume attack clear-suspect](#)le NetApp centre de documentation.

### Note

Lorsque vous marquez une alerte comme un faux positif, le profil du ransomware est mis à jour. Une fois cela fait, vous ne recevrez plus d'alerte concernant ce scénario en particulier.

Pour agir face à une attaque potentielle à partir d'un rapport ARP à l'aide du ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

- Exécutez la commande suivante. Remplacez *svm\_name**vol\_name*, et *[extension identifiers]* par vos propres informations.

```
security anti-ransomware volume attack clear-suspect -vserver svm_name -
volume vol_name [extension identifiers] -false-positive false
```

Pour plus d'informations sur cette commande, consultez [security anti-ransomware volume attack clear-suspect](#)le NetApp centre de documentation.

## Comprendre les alertes EMS pour une protection autonome contre les ransomwares

Vous pouvez utiliser ... NetApp ONTAP's Système de gestion des événements (EMS) pour surveiller les événements liés à l'ARP, y compris les attaques potentielles. Pour plus d'informations sur l'ARP et sur la façon dont il détecte les attaques, consultez [Comment fonctionne l'ARP](#) et [Ce que recherche ARP](#).

Le tableau suivant contient toutes les alertes liées à l'ARP. Pour plus d'informations sur l'EMS, consultez [Surveillance FSx des événements ONTAP EMS](#).

| Nom du message EMS                      | Description du message EMS                                                                                                                                                                    |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>arw.analytics.ext.report</code>   | Ce message apparaît lorsque les analyses anti-ransomware génèrent ou mettent à jour le rapport sur les extensions de fichiers suspects pour un volume.                                        |
| <code>arw.analytics.high.entropy</code> | Ce message apparaît lorsque le nombre de messages du journal de données à entropie élevée (relatifs à la détection et à l'analyse des ransomwares) dépasse le seuil prédéfini pour un volume. |
| <code>arw.analytics.probability</code>  | Ce message apparaît lorsque la probabilité d'une attaque anti-ransomware est passée de low à high sur un volume.                                                                              |
| <code>arw.analytics.report</code>       | Ce message apparaît lorsqu'un rapport d'analyse anti-ransomware est généré ou mis à jour pour un volume.                                                                                      |
| <code>arw.analytics.suspects</code>     | Ce message apparaît lorsqu'une liste de suspects générée par les analyses anti-ransomware s'allonge au point de nécessiter une enquête plus approfondie.                                      |

| Nom du message EMS                   | Description du message EMS                                                                                                                                                                                                                                                                                  |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>arw.auto.switch.enabled</code> | Ce message apparaît lorsque l'anti-ransomware passe automatiquement du mode apprentissage au mode activé une fois que diverses conditions ont été remplies, telles que la période d'apprentissage, la création de fichiers, l'écriture de fichiers et les activités de découverte d'extensions de fichiers. |
| <code>arw.new.file.extn.seen</code>  | Ce message apparaît lorsqu'une nouvelle extension de fichier est détectée dans un volume activé contre les ransomwares. Son objectif est d'informer rapidement l'utilisateur de l'extension observée, ce qui permet une enquête rapide.                                                                     |
| <code>arw.snapshot.created</code>    | Ce message apparaît lorsqu'un nouvel instantané ARP est créé dans un volume activé contre les ransomwares. En outre, il fournit des informations sur la raison pour laquelle l'instantané a été créé.                                                                                                       |
| <code>arw.volume.state</code>        | Ce message apparaît lorsque l'état anti-ransomware d'un volume est modifié.                                                                                                                                                                                                                                 |
| <code>arw.vserver.state</code>       | Ce message apparaît lorsque l'état anti-ransomware d'une SVM est modifié.                                                                                                                                                                                                                                   |

## Protégez vos données avec SnapLock

SnapLock est 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 utiliser ... SnapLock pour respecter la conformité réglementaire, 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, reportez-vous [Compréhension SnapLock Conformité d'](#) aux sections et [Compréhension SnapLock Enterprise](#).

Vous pouvez créer SnapLock volumes activés FSx pour les systèmes de fichiers ONTAP créés le 13 juillet 2023 ou après cette date. Les systèmes de fichiers existants obtiendront SnapLock support lors d'une prochaine fenêtre de maintenance hebdomadaire.

## Rubriques

- [Comment ? SnapLock fonctionnement](#)
- [Compréhension SnapLock Conformité d'](#)
- [Compréhension SnapLock Enterprise](#)
- [Comprendre le SnapLock période de conservation](#)
- [Validation de fichiers à l'état WORM](#)

## Comment ? SnapLock fonctionnement

SnapLock peut 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 un stockage 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 spécifier si un volume utilisera SnapLock paramètres au moment de la création. Un non...SnapLock le volume ne peut pas être converti en SnapLock volume après création.

## Modes de conservation

SnapLock propose 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.



| SnapLock fonctionnalité                                              | <a href="#">Compréhension SnapLock Conformité d'</a>                                                                                                                                                                                                                                               | <a href="#">Compréhension SnapLock Enterprise</a>                                                                                                                                                                              |
|----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 conservation à l'aide de la suppression privilégiée.                    |
| Cas d'utilisation                                                    | <ul style="list-style-type: none"> <li>• Pour répondre à des mandats spécifiques au gouvernement ou à l'industrie tels que la règle 17a-4 (f) de la SEC, la règle 4511 de la FINRA et le règlement 1.31 de la CFTC.</li> <li>• Pour vous protéger contre les attaques de rançongiciels.</li> </ul> | <ul style="list-style-type: none"> <li>• Pour améliorer l'intégrité des données et la conformité interne d'une entreprise.</li> <li>• Pour tester les paramètres de rétention avant d'utiliser SnapLock Conformité.</li> </ul> |
| <a href="#">Commission automatique</a>                               | Oui                                                                                                                                                                                                                                                                                                | Oui                                                                                                                                                                                                                            |
| <a href="#">Rétention basée sur les événements (EBR)<sup>1</sup></a> | Oui                                                                                                                                                                                                                                                                                                | Oui                                                                                                                                                                                                                            |
| <a href="#">Maintien légal<sup>1</sup></a>                           | Oui                                                                                                                                                                                                                                                                                                | Non                                                                                                                                                                                                                            |
| <a href="#">Utilisation de la suppression privilégiée</a>            | Non                                                                                                                                                                                                                                                                                                | Oui                                                                                                                                                                                                                            |
| <a href="#">Mode d'ajout de volumes</a>                              | Oui                                                                                                                                                                                                                                                                                                | Oui                                                                                                                                                                                                                            |
| <a href="#">SnapLock volumes des journaux d'audit</a>                | Oui                                                                                                                                                                                                                                                                                                | Oui                                                                                                                                                                                                                            |

 Note

<sup>1</sup> Les opérations EBR et Legal Hold sont prises en charge dans le ONTAP CLI et API REST.

 Note

FSx car ONTAP prend en charge la hiérarchisation des données en fonction du pool de capacités sur tous SnapLock volumes, quels que soient les SnapLock Type Pour de plus amples informations, veuillez consulter [Hiérarchisation des données de volume](#).

## SnapLock administrateur

Vous devez avoir ... SnapLock privilèges d'administrateur pour effectuer certaines actions sur SnapLock volumes. SnapLock les privilèges d'administrateur sont définis dans le `vsadmin-snaplock` rôle du ONTAP CLI. Vous devez être administrateur de cluster pour créer un compte d'administrateur de machine virtuelle de stockage (SVM) avec le SnapLock rôle d'administrateur.

Vous pouvez effectuer les actions suivantes avec le `vsadmin-snaplock` rôle dans 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
- Exécuter SnapLock actions, y compris 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 le 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 le ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

- 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
```

Pour de plus amples informations, veuillez consulter [ONTAP rôles et utilisateurs](#).

## SnapLock volumes des journaux d'audit

A SnapLock le volume du journal d'audit contient SnapLock journaux d'audit, qui contiennent les horodatages d'événements tels que lorsqu'un SnapLock un administrateur a été créé, lorsque des opérations de suppression privilégiées ont été exécutées ou lorsqu'un blocage légal a été placé sur des fichiers. Le SnapLock le volume du journal d'audit est un enregistrement non effaçable des événements.

Vous devez créer un SnapLock volume du journal d'audit dans la même SVM que SnapLock volume pour les actions suivantes :

- Pour activer ou désactiver la suppression privilégiée sur un SnapLock Volume d'entreprise.
- Pour appliquer la suspension légale à un fichier dans un SnapLock Volume de conformité.

### Warning

- La durée de conservation minimale pour un SnapLock le volume du journal d'audit est de six mois. Jusqu'à l'expiration de cette période de conservation, SnapLock le volume du journal 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 dans SnapLock Mode entreprise.
- 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 période 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 en avoir qu'un seul actif SnapLock volume du journal d'audit d'une SVM, mais il peut être partagé par plusieurs SnapLock volumes dans la SVM. Pour monter un SnapLock volume du journal d'audit réussi, 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.

Vous pouvez trouver SnapLock journaux d'audit 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 SnapLock volume du journal d'audit avec la FSx console Amazon AWS CLI, l' FSx API Amazon et le ONTAP CLI et API REST.

#### Note

Un volume de protection des données (DP) ne peut pas être utilisé comme SnapLock volume du journal d'audit.

Pour activer le SnapLock volume du journal d'audit avec l' FSx API Amazon, `AuditLogVolume` à utiliser dans le [CreateSnaplockConfiguration](#). Dans la FSx console Amazon, pour Audit log Volume, sélectionnez Enabled. Assurez-vous que le chemin de jonction est défini sur `/snaplock_audit_log`.

## 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. Il n'y a aucun impact sur les performances lié à l'écriture de données dans un SnapLock volume ou de la lecture de données protégées par WORM.

Vous pouvez copier des fichiers sur SnapLock volumes avec NFS et SMB, mais ils ne conserveront pas leurs propriétés WORM sur la destination SnapLock volume. Vous devez réattribuer les

fichiers copiés à WORM pour éviter qu'ils ne soient modifiés ou supprimés. Pour de plus amples informations, veuillez consulter [Validation de fichiers à l'état WORM](#).

Vous pouvez également répliquer SnapLock données avec SnapMirror, mais les volumes source et de destination doivent être SnapLock volumes dotés du même mode de rétention (par exemple, les deux doivent être Compliance ou Enterprise).

## Compréhension SnapLock Conformité d'

Cette section décrit les cas d'utilisation et les considérations relatives au SnapLock Mode de conservation de la conformité.

Vous pouvez choisir le mode de conservation de la conformité pour les cas d'utilisation suivants.

- Vous pouvez utiliser ... SnapLock Conformité pour répondre aux mandats spécifiques du gouvernement ou du secteur 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 d'Amazon FSx pour 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 d'Amazon FSx pour NetApp ONTAP](#).
- Vous pouvez utiliser ... SnapLock Conformité pour compléter ou améliorer une stratégie complète de protection des données afin de lutter contre les attaques par ransomware.

Voici quelques points importants à prendre en compte au sujet de SnapLock Mode de conservation de la conformité.

- Une fois qu'un fichier est passé à l'état Write Once, Read Many (WORM) sur un SnapLock Volume de conformité, il ne peut être supprimé avant l'expiration de sa période de conservation par aucun utilisateur.
- A SnapLock Le volume de 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 SnapLock Volume de conformité après 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).

- A SnapLock Le volume de conformité ne peut pas être converti en SnapLock Volume d'entreprise, et vice versa.

## Compréhension SnapLock Enterprise

Cette section décrit les cas d'utilisation et les considérations relatives au SnapLock Mode de rétention d'entreprise.

Vous pouvez choisir le SnapLock Mode de rétention d'entreprise pour les cas d'utilisation suivants.

- Vous pouvez utiliser ... SnapLock Enterprise autorisera 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 L'entreprise doit tester les paramètres de rétention avant de les utiliser SnapLock Conformité.

Voici quelques points importants à prendre en compte au sujet de SnapLock Mode de rétention d'entreprise.

- Vous pouvez 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).
- A SnapLock le volume ne peut pas être converti de Enterprise en Compliance, ou de Compliance en Enterprise.
- SnapLock Enterprise ne prend pas en charge Legal Hold.

## Utilisation de la suppression privilégiée

L'une des principales différences entre SnapLock Enterprise et SnapLock La conformité est qu'un SnapLock l'administrateur peut activer la suppression privilégiée sur un SnapLock Volume Enterprise pour permettre la suppression d'un fichier avant l'expiration de sa période de conservation. Le SnapLock l'administrateur est le seul utilisateur autorisé à supprimer des fichiers d'un SnapLock Volume d'entreprise auquel des politiques de rétention actives sont appliquées. Pour de plus amples informations, veuillez consulter [SnapLock administrateur](#).

Vous pouvez activer ou désactiver la suppression privilégiée à l'aide de la FSx console Amazon AWS CLI, de l' FSx API Amazon et du ONTAP CLI et API REST. Pour activer la suppression privilégiée, vous devez d'abord créer un SnapLock volume du journal d'audit dans la même SVM que SnapLock volume. Pour de plus amples informations, veuillez consulter [SnapLock volumes des journaux d'audit](#).

Pour activer la suppression privilégiée avec l' FSx API Amazon, utilisez `PrivilegedDelete` dans le [CreateSnaplockConfiguration](#). Dans la FSx console Amazon, pour Privileged Delete, choisissez Enabled.

#### 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, vous n'avez pas besoin de SnapLock volume du journal d'audit associé au SnapLock Volume d'entreprise.

Pour désactiver définitivement la suppression privilégiée avec l' FSx API Amazon, utilisez `PrivilegedDelete` dans le [CreateSnaplockConfiguration](#). Dans la FSx console Amazon, pour Privileged Delete, choisissez Permanently disabled.

## Contournement SnapLock Mode entreprise

Si vous utilisez la FSx console Amazon ou l' FSx API Amazon, vous devez disposer de `lfsx:BypassSnapLockEnterpriseRetention` autorisation IAM pour supprimer un SnapLock Volume d'entreprise contenant des fichiers WORM dotés de politiques de rétention actives.

Pour de plus amples informations, veuillez consulter [Suppression SnapLock volumes](#).

## Comprendre le SnapLock période de conservation

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, consultez [Validation 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 :

- Conservation 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 pouvant 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 différentes unités de temps. 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      |           |



| Type                      | Valeur  | Remarques                                                                                                                                            |
|---------------------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Années                    | 0 À 100 |                                                                                                                                                      |
| Infini                    | -       | <p>Conserve les fichiers pour toujours.</p> <p>Disponible pour la rétention par défaut, la rétention maximale et la rétention minimale.</p>          |
| Non spécifié <sup>1</sup> | -       | <p>Conserve les fichiers jusqu'à ce que vous définissiez une période de conservation.</p> <p>Disponible uniquement pour la rétention par défaut.</p> |

#### Note

<sup>1</sup> Lorsque vous transférez des fichiers vers WORM avec une période de conservation non spécifiée, la période de conservation minimale configurée pour le SnapLock volume. 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 durée de conservation d'un SnapLock volume avec la FSx console Amazon AWS CLI, l' FSx API Amazon et le ONTAP CLI et API REST.

Pour définir la période de rétention avec l' FSx API Amazon, utilisez la [SnaplockRetentionPeriod](#) configuration. Dans la FSx console Amazon, pour Période de rétention, entrez les valeurs pour la rétention par défaut, la rétention minimale et la rétention maximale. Choisissez ensuite une unité correspondante pour chacune d'entre elles.

## 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 FSx console Amazon AWS CLI, de l' FSx API Amazon et du ONTAP CLI et 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 |
| Jours   | 1 - 3 650  |
| cal.    | 1 à 120    |
| Années  | 1 à 10     |

Pour activer la validation automatique avec l' FSx API Amazon, utilisez `AutocommitPeriod` dans le [CreateSnaplockConfiguration](#). Dans la FSx console Amazon, pour Autocommit, choisissez

Enabled. Ensuite, 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.

## Mode d'ajout de volumes

Vous ne pouvez pas modifier les données existantes dans un fichier protégé par Worm. Cependant, SnapLock vous permet 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 FSx console Amazon, de AWS CLI l' FSx API Amazon et du ONTAP CLI et API REST.

### Exigences relatives à la mise à jour du mode d'ajout de volumes

- Le SnapLock le volume doit être démonté.
- Le SnapLock le volume doit être vide de copies instantanées et de données utilisateur.

Pour activer le mode d'ajout de volumes avec l' FSx API Amazon, utilisez `VolumeAppendModeEnabled` dans le [CreateSnaplockConfiguration](#) Dans la FSx console Amazon, pour le mode d'ajout de volumes, choisissez Enabled.

## 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 du chemin spécifié.

L'EBR est soutenu par le ONTAP CLI et API REST.

### Note

ONTAP ne prend pas en charge l'EBR avec des FlexGroup volumes.

Les procédures suivantes expliquent comment créer, appliquer, modifier et supprimer une politique EBR. Tu dois être un SnapLock administrateur (ayant le `vsadmin-snaplock` rôle) pour effectuer ces tâches dans le ONTAP CLI. Pour de plus amples informations, veuillez consulter [SnapLock administrateur](#).

### Création d'une politique EBR dans le ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

#### Pour créer une politique EBR dans ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

- Exécutez la commande suivante. Remplacez *p1* et *"10 years"* par vos propres informations.

```
vs1::> snaplock event-retention policy create -name p1 -retention-period "10 years"
```

### Appliquer une politique EBR dans le ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

#### Pour appliquer une politique EBR dans le ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

- 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. Sinon, cette commande applique la politique EBR à tous les fichiers du volume.

```
vs1::> snaplock event-retention apply -policy-name p1 -volume slc -path /
```

### Modification d'une politique EBR dans ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

#### Pour modifier une politique EBR dans ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

- Exécutez la commande suivante. Remplacez *p1* et *"5 years"* par vos propres informations.

```
vs1::> snaplock event-retention policy modify -name p1 -retention-period "5 years"
```

### Suppression d'une politique EBR dans le ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

#### Pour supprimer une politique EBR dans ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

- Exécutez la commande suivante. Remplacez *p1* par vos propres informations.

```
vs1::> snaplock event-retention policy delete -name p1
```

Commandes associées dans NetApp Centre de 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 soutenu par le ONTAP CLI et API REST.

### Note

ONTAP ne prend pas en charge la conservation légale des FlexGroup volumes.

Les procédures suivantes expliquent comment démarrer et mettre fin à une suspension légale. Tu dois être un SnapLock administrateur (ayant le vsadmin-snaplock rôle) pour effectuer ces tâches dans le ONTAP CLI. Pour de plus amples informations, veuillez consulter [SnapLock administrateur](#).

Commencer la mise en attente légale d'un fichier dans un SnapLock Volume de conformité avec le ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

Pour démarrer un blocage légal sur un fichier dans un SnapLock Volume de conformité avec le ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

- Exécutez la commande suivante. Remplacez *litigation1slc\_vol1*, et *file1* par vos propres informations.

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

Commencer un blocage légal sur tous les fichiers d'un SnapLock Volume de conformité avec le ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

Pour démarrer un blocage légal sur tous les fichiers d'un SnapLock Volume de conformité avec le ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

- Exécutez la commande suivante. Remplacez *litigation1* et *slc\_voll* par vos propres informations.

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_voll -
path /
```

Mettre fin à la suspension légale d'un fichier dans un SnapLock Volume de conformité avec le ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

Pour mettre fin à la suspension légale d'un fichier dans un SnapLock Volume de conformité avec le ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

- Exécutez la commande suivante. Remplacez *litigation1slc\_voll*, et *file1* par vos propres informations.

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_voll -
path /file1
```

#### Note

Nous vous recommandons de surveiller la commande à l'-operation-statusaide de la `snaplock legal-hold show` commande lorsque vous émettez une suspension légale pour vous assurer qu'elle n'échoue pas.

Mettre fin à un blocage légal sur tous les fichiers d'un SnapLock Volume de conformité avec le ONTAP INTERFACE DE LIGNE DE COMMANDE (CLI)

Pour mettre fin à une suspension légale sur tous les fichiers d'un SnapLock Volume de conformité avec le ONTAP INTERFACE DE LIGNE DE COMMANDE (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-statusaide de la `snaplock legal-hold show` commande lorsque vous émettez une suspension légale pour vous assurer qu'elle n'échoue pas.

Commandes associées dans NetApp Centre de documentation :

- [Snaplock Legal-Hold Abort](#)
- [fichiers de vidage légaux SnapLock](#)
- [litiges relatifs à la détention légale de Snaplock](#)
- [émission Snaplock Legal Hold](#)

## Répliquer vos données avec FlexCache

FlexCacheest une fonctionnalité de mise en cache à NetApp ONTAP's distance qui rapproche les ensembles de données des clients, améliore les performances d'accès et réduit les coûts. Il simplifie la distribution des fichiers et réduit les coûts du WAN. Lorsque vous créez un FlexCache volume, il copie initialement uniquement les métadonnées du système de fichiers d'origine. Cette approche est plus rapide et moins encombrante qu'une copie complète des données, car elle ne consomme qu'une fraction de la capacité de stockage.

## Fonctionnement d'FlexCache

Un FlexCache volume est un cache peu peuplé qui permet d'accéder aux données stockées dans un volume d'origine. Le cache peut être situé dans un système de fichiers différent, éventuellement distant. Au lieu de copier toutes les données du volume d'origine, FlexCache copie les données uniquement selon les besoins. FlexCache volumes sont particulièrement adaptés aux flux de travail à lecture intensive avec des modifications de données peu fréquentes, car toute modification des données d'origine nécessite l'actualisation du cache.

Vous pouvez utiliser FlexCache with FSx for ONTAP dans les configurations suivantes :

| Volume d'origine      | FlexCache volume      |
|-----------------------|-----------------------|
| Sur site NetApp ONTAP | FSx pour ONTAP        |
| FSx pour ONTAP        | Sur site NetApp ONTAP |
| FSx pour ONTAP        | FSx pour ONTAP        |

## FlexCachemodes d'écriture

FlexCache volumes prennent en charge deux modes de fonctionnement pour les opérations d'écriture : le mode écriture différée et le mode écriture différée.

En mode écriture différée, qui est le mode par défaut, les écritures sont transférées du cache vers le volume d'origine. L'opération d'écriture n'est confirmée au client qu'une fois que les données ont été enregistrées dans le volume d'origine et que l'origine a accusé réception de la réécriture dans le cache. Comme chaque écriture doit traverser le réseau entre le cache et l'origine, ce mode présente une latence plus élevée que le mode écriture différée.

En mode écriture différée, introduit dans la version ONTAP 9.15.1, les écritures sont enregistrées à l'emplacement du cache et sont immédiatement confirmées au client. Les données sont ensuite écrites de manière asynchrone sur le volume d'origine. Ce mode permet aux écritures de s'exécuter à des vitesses proches de la vitesse locale, ce qui peut améliorer considérablement les performances des charges de travail distribuées.

Utilisez le mode écriture différée pour les charges de travail intensives en écriture qui nécessitent des écritures de cache à faible latence. Utilisez le mode écriture différée pour les charges de travail



gourmandes en lecture qui ne sont pas sensibles à la latence, ou lorsque votre système de fichiers d'origine comporte plus de 10 volumes d'origine. FlexCache

## FlexCache aperçu de la création de volumes

La création d'un FlexCache volume comprend les étapes suivantes :

- Rassemblez les interfaces logiques source et destination (LIFs)
- Établissez un peering de cluster entre les systèmes de fichiers d'origine et de cache
- Création d'une relation d'appairage entre machines virtuelles de stockage (SVM)
- Créez le FlexCache volume et sélectionnez un mode d'écriture
- Augmentez le FlexCache volume sur vos clients

Pour obtenir des instructions complètes, veuillez consulter [Création d'un FlexCache](#).

## Création d'un FlexCache

À l'aide des procédures suivantes, vous allez créer un FlexCache volume sur un système de fichiers Amazon FSx for NetApp ONTAP, qui est soutenu par un volume d'origine situé dans un cluster sur site NetApp ONTAP.

### Utilisation de l'ONTAP CLI

Vous utiliserez la ONTAP CLI pour créer et gérer une FlexCache configuration sur votre système de fichiers FSx for ONTAP.

Les commandes de ces procédures utilisent les alias suivants pour le cluster, la SVM et le volume :

- `Cache_ID`— l'ID du cluster de cache (au format FSx IDABCDEF1234567890A)
- `Origin_ID`— l'ID du cluster d'origine
- `CacheSVM`— le nom de la SVM du cache
- `OriginSVM`— le nom de la SVM d'origine
- `OriginVol`— le nom du volume d'origine
- `CacheVol`— le nom FlexCache du volume

Les procédures décrites dans cette section utilisent les commandes NetApp ONTAP CLI suivantes.

- [network interfaces show](#)
- Commandes de l'[cluster peer](#)
- [volume flexcache create](#)

## Prérequis

Avant de commencer à utiliser les procédures décrites dans les sections suivantes, assurez-vous de remplir les conditions préalables suivantes :

- Les systèmes de fichiers source et de destination sont connectés dans le même VPC ou se trouvent dans des réseaux homologues à l'aide d'Amazon VPC,, ou. AWS Transit Gateway AWS Direct Connect AWS VPN Pour plus d'informations, consultez [Accès aux données depuis le AWS Cloud](#) 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 l'ICMP ainsi que le TCP sur les ports 11104 et 11105 pour vos points de terminaison inter-clusters (). LIFs
- Vous avez créé une destination FSx pour le système de fichiers ONTAP à l'aide d'une SVM, mais vous n'avez pas créé le volume qui sera utilisé en tant que. FlexCache Pour de plus amples informations, veuillez consulter [Création de systèmes de fichiers](#).

## Enregistrez l'inter-cluster source et de destination LIFs

1. Pour le système de fichiers FSx for ONTAP qui est le cluster de destination :
  - a. Ouvrez la FSx console Amazon à l'adresse <https://console.aws.amazon.com/fsx/>.
  - b. Choisissez Systèmes de fichiers, puis choisissez le système FSx de fichiers ONTAP qui est le cluster de destination pour ouvrir la page de détails du système de fichiers.
  - c. Dans Administration, recherchez le point de terminaison inter-clusters - adresses IP et enregistrez la valeur.

### Note

Pour les systèmes de fichiers évolutifs, il existe deux adresses IP de point de terminaison inter-clusters pour chaque paire de haute disponibilité (HA).

2. Pour le cluster source sur site, récupérez les adresses IP LIF inter-clusters à l'aide de la commande CLI ONTAP suivante :

```
Origin::> network interface show -role intercluster
Logical
Vserver Interface Status Network

OriginSVM
 inter_1 up/up 10.0.0.36/24
 inter_2 up/up 10.0.1.69/24
```

3. Enregistrez les inter\_2 IP adresses inter\_1 et ils sont référencés dans l'OriginSVMalias en tant que origin\_inter\_1 origin\_inter\_2 et dans l'CacheSVMalias en tant que cache\_inter\_1 et cache\_inter\_2.

## Établissez un peering de cluster entre l'origine et le cache

Établissez une relation entre pairs du cluster sur le Source cluster Cache et à l'aide de la commande [cluster peer create](#) ONTAP CLI. Vous allez fournir les adresses IP inter-clusters que vous avez enregistrées précédemment dans la [Enregistrez l'inter-cluster source et de destination LIFs](#) procédure. Lorsque vous y êtes invité, il vous sera demandé de créer un *cluster-peer-passphrase* fichier que vous devrez saisir lorsque vous établirez le peering de cluster sur le Origin cluster.

1. Configurez le peering de cluster sur le Cache cluster (votre système FSx de fichiers ONTAP).
  - a. Pour accéder à la ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

- b. Utilisez la commande suivante et enregistrez le mot de passe que vous avez créé. Pour les systèmes de fichiers évolutifs, fournissez les adresses inter\_2 IP inter\_1 et pour chaque paire HA.

```
FSx-Cache::> cluster peer create -address-family ipv4 -peer-
addrs origin_inter_1,origin_inter_2
```

Enter the passphrase: **cluster-peer-passphrase**

Confirm the passphrase: **cluster-peer-passphrase**

Notice: Now use the same passphrase in the "cluster peer create" command in the other cluster.

- Utilisez la commande suivante pour configurer le peering de cluster sur le cluster source (sur site). Vous devrez saisir le mot de passe que vous avez créé à l'étape précédente pour vous authentifier. Pour les systèmes de fichiers évolutifs, vous devez fournir l'adresse IP inter-clusters pour chaque paire HA.

```
Origin::> cluster peer create -address-family ipv4 -peer-
addrs cache_inter_1,cache_inter_2
```

Enter the passphrase: **cluster-peer-passphrase**

Confirm the passphrase: **cluster-peer-passphrase**

- Sur le source cluster, vérifiez que le peering du cluster a été correctement configuré à l'aide de la commande suivante. Dans la sortie, Availability doit être défini sur Available.

```
Origin::> cluster peer show
```

| Peer Cluster Name | Availability | Authentication |
|-------------------|--------------|----------------|
| -----             | -----        | -----          |
| Cache_ID          | Available    | ok             |

Si le résultat ne s'affiche pas Available, répétez les étapes précédentes sur les cache clusters source et.

## Configuration de l'appairage des machines virtuelles de stockage (SVM)

Après avoir correctement établi l'appairage du cluster, l'étape suivante consiste à créer une relation d'appairage de la SVM sur le cluster de cache (Cache) à l'aide de la commande. `vserver peer` Les alias supplémentaires utilisés dans la procédure suivante sont les suivants :

- CacheLocalName**— le nom utilisé pour identifier la cache SVM lors de la configuration de l'appairage de la SVM sur la SVM. `origin`

- **OriginLocalName**— le nom utilisé pour identifier la origin SVM lors de la configuration de l'appairage de la SVM sur la SVM. cache

1. Sur la cache SVM, utilisez la commande suivante pour créer une relation d'appairage entre SVM.

```
FSx-Cache::> vservers peer create -vservers CacheSVM -peer-vservers OriginSVM -peer-cluster Origin_ID -local-name OriginLocalName -application flexcache
```

2. Sur le cluster source, utilisez la commande suivante pour accepter la relation d'appairage de la SVM.

```
Origin::> vservers peer accept -vservers OriginSVM -peer-vservers CacheSVM -local-name CacheLocalName
```

3. Sur le cluster source, acceptez la relation d'appairage.

```
Origin::> vservers peer accept -vservers OriginSVM -peer-vservers CacheSVM -local-name CacheLocalName
```

4. Vérifiez que l'appairage de la SVM a réussi à l'aide de la commande suivante ; elle Peer State doit être définie sur peered dans la réponse.

```
Origin::> vservers peer show
```

| Vserver   | Peer Vserver | Peer State | Peering Cluster | Remote Applications |
|-----------|--------------|------------|-----------------|---------------------|
| -----     | -----        | -----      | -----           |                     |
| OriginSVM | CacheSVM     | peered     | FSx-Cache       | flexcache           |

## Créez le FlexCache volume

Après avoir créé avec succès la relation d'appairage de la SVM, l'étape suivante consiste à créer le FlexCache volume sur la SVM en cache. Le FlexCache volume doit être un FlexGroup. Vous allez également choisir un mode de fonctionnement pour votre FlexCache volume. Pour de plus amples informations, veuillez consulter [FlexCachemodes d'écriture](#).

1. Sur le cluster de cache, utilisez la commande ONTAP CLI suivante pour créer votre FlexCache volume. L'exemple crée un FlexCache volume de 2 To nommé *CacheVol*.

- Pour créer un FlexCache volume d'écriture arrondie, utilisez la commande suivante.

```
FSx-Cache::> volume flexcache create -vserver CacheSVM -size 2t -volume CacheVol
 -origin-volume OriginVol -origin-vserver OriginSVM -junction-path /flexcache -
 aggr-list aggr1
```

- Pour créer un FlexCache volume à écriture différée, utilisez la commande suivante.

```
FSx-Cache::> volume flexcache create -vserver CacheSVM -size 2t -volume CacheVol
 -origin-volume OriginVol -origin-vserver OriginSVM -junction-path /flexcache -
 aggr-list aggr1 -is-writeback-enabled true
```

#### Note

Vous pouvez utiliser la [volume flexcache config modify -is-writeback-enabled {true|false}](#) commande pour modifier le mode d'écriture. Avant d'utiliser cette commande, assurez-vous de passer en mode avancé ONTAP CLI à l'aide de la [set -privilege advanced](#) commande.

2. Vérifiez la FlexCache relation entre le FlexCache volume et le volume d'origine.

- Pour un volume FlexCache à réécriture, votre sortie ressemblera à l'exemple suivant.

```
FSx-Cache::> volume flexcache show
```

| Vserver  | Volume   | Size  | Origin-Vserver | Origin-Volume | Origin-Cluster |
|----------|----------|-------|----------------|---------------|----------------|
| -----    | -----    | ----- | -----          | -----         | -----          |
| CacheSVM | CacheVol | 2TB   | OriginSVM      | OriginVol     | Origin         |

- Pour un volume FlexCache à écriture différée, votre sortie ressemblera à l'exemple suivant.

```
FSx-Cache::> volume flexcache show
```

| Vserver  | Volume   | Size  | Origin-Vserver | Origin-Volume | Origin-Cluster |
|----------|----------|-------|----------------|---------------|----------------|
| -----    | -----    | ----- | -----          | -----         | -----          |
| CacheSVM | CacheVol | 2TB   | OriginSVM      | OriginVol     | Origin         |

|          |          |     |           |           |        |
|----------|----------|-----|-----------|-----------|--------|
| CacheSVM | CacheVol | 2TB | OriginSVM | OriginVol | Origin |
| true     |          |     |           |           |        |

## Monter le FlexCache volume

Une fois que le FlexCache volume devient DISPONIBLE NFSv3,, NFSv4, les clients SMB peuvent le monter. Une fois installé, les FlexCache clients ont accès à l'ensemble de données sur le volume d'origine sur site.

- Pour créer un point de montage et le monter FlexCache, exécutez les commandes suivantes sur le client :

```
$ sudo mkdir -p /fsx/CacheVol
$ sudo mount -t nfs management.fs-01d2f606463087f6d.fsx.us-east-1.amazonaws.com:/
CacheVol /fsx/CacheVol
```

## Réplication de vos données à l'aide de NetApp SnapMirror

Vous pouvez 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 d'obtenir une haute disponibilité des données et une réplication rapide des données sur ONTAP systèmes, que vous effectuiez une réplication entre deux systèmes de FSx fichiers Amazon dans AWS ou depuis un système sur site vers. AWS La réplication peut être planifiée toutes les 5 minutes, mais les intervalles doivent être choisis avec soin en fonction RPOs (objectifs de point de restauration), RTOs (objectifs de temps de restauration) et de considérations relatives aux performances.

Lorsque vous répliquez des données vers NetApp systèmes de stockage et mise à jour continue des données secondaires, vos données sont maintenues 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 le NetApp BlueXP documentation.

Vous pouvez créer un volume de destination de protection des données (DP) pour NetApp SnapMirror à l'aide de la FSx console Amazon AWS CLI, du, et de FSx l'API Amazon, en plus du

NetApp ONTAP CLI et API REST. Pour plus d'informations sur la création d'un volume de destination à l'aide de FSx la console Amazon et AWS CLI consultez [Création de volumes](#).

Vous pouvez utiliser ... NetApp BlueXP ou le ONTAP CLI 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). Uniquement au niveau du volume SnapMirror la réplication est prise en charge par FSx for ONTAP. Synchronous SnapMirror, y compris StrictSync, n'est pas pris en charge.

## Utilisation NetApp BlueXP pour planifier la réplication

Vous pouvez utiliser NetApp BlueXP pour configurer la réplication avec votre système de SnapMirror fichiers FSx for ONTAP. Pour plus d'informations, consultez la section [Réplication de données entre systèmes](#) dans la documentation NetApp BlueXP.

## Utilisation de ONTAP CLI pour planifier la réplication

Vous pouvez utiliser le plugin ONTAP CLI pour configurer la réplication planifiée des volumes. Pour plus d'informations, consultez [la section Gestion de la réplication de SnapMirror volumes](#) dans NetApp ONTAP Centre de documentation.



# AWS rapports de facturation et d'utilisation FSx pour ONTAP

AWS fournit deux rapports d'utilisation FSx pour ONTAP :

- Le rapport AWS de facturation est une vue globale de toutes les activités Services AWS que vous utilisez, y compris FSx pour ONTAP.
- Le rapport AWS d'utilisation est un résumé de l'activité d'un service spécifique, agrégé par heure, jour ou mois. Il inclut également des tableaux d'utilisation qui fournissent une représentation graphique de votre utilisation FSx pour ONTAP.

## Note

Comme les autres Services AWS, FSx car ONTAP ne vous facture que ce que vous utilisez. Pour plus d'informations, consultez [Amazon FSx for NetApp ONTAP Pricing](#).

## Afficher le rapport AWS de facturation FSx pour ONTAP

Vous pouvez consulter un résumé de votre AWS consommation et de vos frais, listé par service, sur la page Factures de la AWS Billing and Cost Management console.

Pour consulter le rapport AWS de facturation

1. Connectez-vous à la AWS Billing and Cost Management console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/costmanagement/>.
2. Dans le volet de navigation, choisissez Factures.
3. Choisissez une période de facturation (par exemple, août 2024).
4. Pour voir les FSx frais Amazon, FSx dans l'onglet Frais par service, entrez le champ de texte Filtrer par service, puis développez FSx pour afficher les frais par Région AWS.

Les frais relatifs FSx aux systèmes de fichiers ONTAP figurent dans les FSx CreateFileSystem entrées Amazon:ONTAP du rapport.

5. Pour télécharger le rapport de facturation détaillé au format CSV, choisissez Tout télécharger au format CSV en haut de la page des factures.

Pour plus d'informations sur votre AWS facture, consultez la section [Consulter votre facture](#) dans le Guide de AWS Billing l'utilisateur.

Le rapport de facturation inclut les types d'utilisation suivants qui s'appliquent FSx aux systèmes de fichiers ONTAP :

#### First generation FSx for ONTAP file systems

| Type de frais                          | Unités         | Description                                                                                                        |  |
|----------------------------------------|----------------|--------------------------------------------------------------------------------------------------------------------|--|
| Stockage SSD ONTAP mono-AZ             | Go-mois        | La quantité de stockage SSD provisionnée sur un système de fichiers ONTAP mono-AZ de première génération           |  |
| Stockage SSD ONTAP Multi-AZ            | Go-mois        | La quantité de stockage SSD provisionnée sur un système de fichiers Multi-AZ FSx pour ONTAP de première génération |  |
| Capacité de débit ONTAP mono-AZ        | MBps-Mois      | Quantité de capacité de débit allouée sur un système de fichiers Single-AZ FSx for ONTAP de première génération    |  |
| Capacité de débit ONTAP Multi-AZ       | MBps-Mois      | Quantité de capacité de débit allouée sur un système de fichiers Multi-AZ FSx pour ONTAP de première génération    |  |
| IOPS de SSD ONTAP mono-AZ provisionnés | Mois de l'IOPS | Quantité d'IOPS SSD provisionnées sur un système de fichiers Single-AZ FSx for ONTAP de première génération        |  |

| Type de frais                           | Unités         | Description                                                                                                 |  |
|-----------------------------------------|----------------|-------------------------------------------------------------------------------------------------------------|--|
| IOPS de SSD ONTAP Multi-AZ provisionnés | Mois de l'IOPS | Le nombre d'IOPS SSD provisionnés sur un système de fichiers Multi-AZ FSx pour ONTAP de première génération |  |

## Second generation FSx for ONTAP file systems

| Type de frais                       | Unités    | Description                                                                                                        |  |
|-------------------------------------|-----------|--------------------------------------------------------------------------------------------------------------------|--|
| Stockage SSD ONTAP Single-AZ-2      | Go-mois   | La quantité de stockage SSD provisionnée sur un système de fichiers Single-AZ FSx for ONTAP de deuxième génération |  |
| Stockage SSD ONTAP Multi-AZ-2       | Go-mois   | La quantité de stockage SSD provisionnée sur un système de fichiers Multi-AZ FSx pour ONTAP de deuxième génération |  |
| Capacité de débit ONTAP Single-AZ-2 | MBps-Mois | Quantité de capacité de débit allouée sur un système de fichiers Single-AZ FSx for ONTAP de deuxième génération    |  |
| Capacité de débit ONTAP Multi-AZ-2  | MBps-Mois | Quantité de capacité de débit allouée sur un système de fichiers Multi-AZ FSx pour ONTAP de deuxième génération    |  |

| Type de frais                              | Unités         | Description                                                                                                  |  |
|--------------------------------------------|----------------|--------------------------------------------------------------------------------------------------------------|--|
| IOPS d'un SSD ONTAP mono-AZ-2 provisionné  | Mois de l'IOPS | Quantité d'IOPS SSD provisionnées sur un système de fichiers Single-AZ FSx pour ONTAP de deuxième génération |  |
| IOPS de SSD ONTAP Multi-AZ-2 provisionnées | Mois de l'IOPS | Quantité d'IOPS SSD provisionnées sur un système de fichiers Multi-AZ FSx pour ONTAP de deuxième génération  |  |

#### All FSx for ONTAP filesystems

| Type de frais                                                              | Unités     | Description                                                                                                                   |  |
|----------------------------------------------------------------------------|------------|-------------------------------------------------------------------------------------------------------------------------------|--|
| Stockage en pool de capacité standard ONTAP                                | Go-mois    | La quantité de stockage du pool de capacité utilisée par le système de fichiers FSx for ONTAP.                                |  |
| Stockage de sauvegarde ONTAP                                               | Go-mois    | La quantité de capacité de stockage utilisée pour les sauvegardes                                                             |  |
| SnapLock utilisation                                                       | Go-mois    | La quantité de capacité de stockage utilisée par SnapLock volumes                                                             |  |
| Lire les demandes adressées au pool de stockage de capacité standard ONTAP | Opérations | Le nombre de demandes de lecture adressées au stockage de pool de capacité standard sur un système de fichiers FSx pour ONTAP |  |

| Type de frais                                                       | Unités     | Description                                                                                                                   |  |
|---------------------------------------------------------------------|------------|-------------------------------------------------------------------------------------------------------------------------------|--|
| Rédiger des demandes au stockage en pool de capacité standard ONTAP | Opérations | Le nombre de demandes d'écriture adressées au stockage de pool de capacité standard sur un système de fichiers FSx pour ONTAP |  |

## Afficher le rapport AWS d'utilisation de FSx for ONTAP

AWS fournit un rapport FSx d'utilisation plus détaillé que le rapport de facturation. Le rapport d'utilisation fournit des données d'utilisation agrégées par heure, jour ou mois, et répertorie les opérations par région et par type d'utilisation.

Pour consulter le rapport AWS d'utilisation

1. Connectez-vous à la AWS Billing and Cost Management console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/costmanagement/>.
2. Dans le panneau de navigation, choisissez Cost Explorer.
3. Dans la section Paramètres du rapport, choisissez la plage de dates et la granularité de votre rapport.
4. Laissez la dimension Grouper par > définie sur Service.
5. Sous Filtres > Service, sélectionnez FSx
6. Choisissez le type d'utilisation. Consultez le tableau suivant cette procédure pour obtenir une liste des types FSx d'utilisation d'ONTAP.
7. Sélectionnez des filtres supplémentaires pour votre rapport.
8. Pour télécharger les détails du rapport dans un fichier, choisissez Télécharger au format CSV.

Le tableau suivant répertorie les types d'utilisation ONTAP que vous pouvez utiliser FSx pour filtrer le rapport afin d'afficher les données d'utilisation des systèmes de fichiers ONTAP. Pour plus d'informations sur l'utilisation du Cost Explorer, consultez la section [Analyse de vos coûts et de votre utilisation AWS Cost Explorer](#) dans le guide de AWS Cost Management l'utilisateur.

## First generation FSx for ONTAP file systems

| Type d'utilisation                         | Unités    | Description                                                                                                                                                |
|--------------------------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>region</i> -Storage.SAZ_2N : SSD        | Go-mois   | Quantité de stockage SSD provisionnée sur un système de fichiers Single-AZ FSx for ONTAP de première génération.                                           |
| <i>region</i> - Stockage .maz : SSD        | Go-mois   | Quantité de stockage SSD provisionnée sur un système de fichiers Multi-AZ FSx pour ONTAP de première génération.                                           |
| <i>region</i> - ThroughputCapacity .SAZ_2N | MiBps-Non | Quantité de capacité de débit allouée sur un système de fichiers Single-AZ FSx for ONTAP de première génération.                                           |
| <i>region</i> - ThroughputCapacity .MAZ    | MiBps-Non | Quantité de capacité de débit allouée sur un système de fichiers Multi-AZ FSx pour ONTAP de première génération.                                           |
| <i>region</i> - SSDIOPS.SAZ_2N             | IOPS-Mo   | La quantité d'IOPS SSD provisionnée au-dessus de 3 IOPS par GiB de stockage SSD sur un système de fichiers Single-AZ for ONTAP de première génération. FSx |
| <i>region</i> - SSDIOPS.maz approvisionné  | IOPS-Mo   | La quantité d'IOPS SSD provisionnée au-dessus de 3 IOPS par GiB de stockage SSD sur un système de fichiers Multi-AZ for ONTAP de première génération. FSx  |

## Second generation FSx for ONTAP file systems

| Type d'utilisation                          | Unités    | Description                                                                                                                                                |
|---------------------------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>region</i> -Stockage.SAZ_2N2 : SSD       | Go-mois   | Quantité de stockage SSD provisionnée sur un système de fichiers Single-AZ FSx for ONTAP de deuxième génération.                                           |
| <i>region</i> -Rangement. MAZ2:SSD          | Go-mois   | Quantité de stockage SSD provisionnée sur un système de fichiers Multi-AZ FSx pour ONTAP de deuxième génération.                                           |
| <i>region</i> - ThroughputCapacity .SAZ_2N2 | MiBps-Non | Quantité de capacité de débit allouée sur un système de fichiers Single-AZ FSx for ONTAP de deuxième génération.                                           |
| <i>region</i> -ThroughputCapacity.MAZ2      | MiBps-Non | Quantité de capacité de débit allouée sur un système de fichiers Multi-AZ FSx pour ONTAP de deuxième génération.                                           |
| <i>region</i> - SSD fournis. SAZ_2N2        | IOPS-Mo   | La quantité d'IOPS SSD provisionnée au-dessus de 3 IOPS par GiB de stockage SSD sur un système de fichiers Single-AZ for ONTAP de deuxième génération. FSx |
| <i>region</i> - Disp SSD fournis. MAZ2      | IOPS-Mo   | La quantité d'IOPS SSD provisionnée au-dessus de 3 IOPS par GiB de stockage SSD sur un système de fichiers Multi-AZ for ONTAP de deuxième génération. FSx  |

## All FSx for ONTAP file systems

| Type d'utilisation                                  | Unités     | Description                                                                                                                                          |
|-----------------------------------------------------|------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>region</i> -Storage.SAZ_2N :<br>standard CPool   | Go Mo      | Quantité de stockage en pool de capacité standard utilisée sur un système de fichiers Single-AZ FSx for ONTAP de première ou deuxième génération.    |
| <i>region</i> -Storage.maz : Std CPool              | Go Mo      | Quantité de stockage en pool de capacité standard utilisée sur un système de fichiers Multi-AZ FSx pour ONTAP de première ou de deuxième génération. |
| <i>region</i> -BackupUsage                          | Go-mois    | Quantité de capacité de stockage utilisée pour les sauvegardes.                                                                                      |
| <i>region</i> -SnaplockUsage                        | Go-mois    | La quantité de capacité de stockage utilisée par SnapLock volumes.                                                                                   |
| <i>region</i> - Demande à S.SAZ_2N :<br>CPool StdRd | Opérations | Nombre de demandes de lecture adressées au stockage de pool de capacité standard sur un système de fichiers mono-AZ FSx pour ONTAP.                  |
| <i>region</i> - Demande à S.SAZ_2N :<br>CPool StdWr | Opérations | Nombre de demandes d'écriture adressées au stockage de pool de capacité standard sur un système de fichiers mono-AZ FSx pour ONTAP.                  |
| <i>region</i> - Demande à .maz : CPool<br>StdRd     | Opérations | Nombre de demandes de lecture adressées au stockage de pool de capacité standard sur un système                                                      |



| Type d'utilisation                           | Unités     | Description                                                                                                                            |
|----------------------------------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------|
|                                              |            | de fichiers Multi-AZ FSx pour ONTAP.                                                                                                   |
| <i>region</i> - Demande à .maz : CPool StdWr | Opérations | Nombre de demandes d'écriture adressées à un pool de stockage de capacité standard sur un système de fichiers Multi-AZ FSx pour ONTAP. |

# Surveillance d'Amazon FSx pour NetApp ONTAP

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 en 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 FSx système de fichiers 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 Informations sur l'infrastructure de données** — 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 Data Infrastructure 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 NetApp et Grafana. NetApp Harvest surveille les systèmes de fichiers ONTAP en collectant des indicateurs de performance, de capacité et de matériel à partir des systèmes FSx de fichiers ONTAP. Grafana fournit un tableau de bord où les métriques 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 sur Amazon FSx.

## Rubriques

- [Surveillance avec Amazon CloudWatch](#)
- [Surveillance FSx des événements ONTAP EMS](#)
- [Surveillance à l'aide d'informations sur l'infrastructure de données](#)
- [Surveillance des systèmes FSx de fichiers ONTAP à l'aide de Harvest et Grafana](#)

- [Surveillance des FSx appels d'API ONTAP avec AWS 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 pour NetApp ONTAP en indicateurs 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. FSx pour ONTAP, les données métriques sont automatiquement envoyées par défaut CloudWatch à des 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, car FSx ONTAP envoie des données métriques à des CloudWatch intervalles d'une minute, à l'exception des métriques suivantes qui sont envoyées à intervalles de 5 minutes :

- `FileServerDiskThroughputBalance`
- `FileServerDiskIopsBalance`

CloudWatch les métriques FSx pour 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 File-system-level de performance et de capacité de stockage.
- Métriques du serveur de fichiers : File-server-level métriques.
- Mesures agrégées détaillées du système de fichiers : mesures détaillées du système de fichiers par agrégat.
- Mesures détaillées du système de fichiers : mesures File-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 FSx pour ONTAP sont publiées dans l'espace de AWS/FSx noms dans CloudWatch

## Rubriques

- [Accès aux CloudWatch métriques](#)
- [Surveillance dans la FSx console Amazon](#)
- [Métriques du système de fichiers](#)
- [Métriques du système de fichiers de deuxième génération](#)
- [Métriques de volume](#)

## Accès aux CloudWatch métriques

Vous pouvez consulter les CloudWatch statistiques Amazon relatives FSx à Amazon de la manière suivante :

- La FSx console Amazon
- 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 FSx console Amazon.

Pour consulter CloudWatch les statistiques de votre système de fichiers à l'aide de la FSx console Amazon

1. Ouvrez la FSx console Amazon 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 FSx console Amazon

Pour consulter CloudWatch les statistiques de votre volume à l'aide de la FSx console Amazon

1. Ouvrez la FSx console Amazon 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 des métriques du système FSx de fichiers ONTAP à un tableau de bord dans la CloudWatch console Amazon.

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 FSx console Amazon.
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 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 de l'API [GetMetricStatistics](#). Pour plus d'informations, consultez le [Amazon CloudWatch API Reference](#).

## Surveillance dans la FSx console Amazon

Les CloudWatch statistiques communiquées par Amazon FSx fournissent des informations précieuses sur vos systèmes de fichiers et volumes FSx pour ONTAP.

Rubriques

- [Surveillance des métriques du système de fichiers dans la FSx console Amazon](#)
- [Surveillance des statistiques de volume dans la FSx console Amazon](#)
- [Avertissements et recommandations en matière de performances](#)
- [Création d' CloudWatch alarmes Amazon pour surveiller Amazon FSx](#)

## Surveillance des métriques du système de fichiers dans la FSx console Amazon

Vous pouvez utiliser le panneau Surveillance et performance du tableau de bord de votre système de fichiers dans la FSx console Amazon pour consulter les statistiques décrites dans le tableau suivant. Pour de plus amples informations, veuillez consulter [Accès aux CloudWatch métriques](#).

| Surveillance et performance | Comment puis-je...                                                                                                          | Diagramme                                                | Métriques pertinentes                                                                          |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|------------------------------------------------------------------------------------------------|
|                             | ... déterminer la capacité de stockage disponible sur mon système de fichiers ?                                             | Capacité de stockage principal disponible (octets)       | StorageCapacity {SSD} - StorageUsed {SSD}                                                      |
|                             | ... déterminer le débit client total de mon système de fichiers ?                                                           | Débit client total (octets/s)                            | SOMME (DataReadBytes + DataWriteBytes) / PÉRIODE (en secondes)                                 |
| Récapitulatif               | ... 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 : $\text{DataReadOperationTime} * 1000 / \text{DataReadOperations}$ |

| Surveillance et performance | Comment puis-je...                                                                                                   | Diagramme                                          | Métriques pertinentes                                                                                                                                                                                                                                                                                                   |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                             |                                                                                                                      |                                                    | <p>Latence d'écriture moyenne : <math>\text{DataWriteOperationTime} * 1000 / \text{DataWriteOperations}</math></p> <p>Latence moyenne des métadonnées : <math>\text{MetadataOperationTime} * 1000 / \text{MetadataOperations}</math></p>                                                                                |
|                             | ... déterminer la répartition de la capacité de stockage utilisée et gratuite sur mon système de fichiers ?          | Distribution du stockage                           | <p>Niveau principal disponible : <math>\text{StorageCapacity} \{ \text{SSD} \} - \text{StorageUsed} \{ \text{SSD} \}</math></p> <p>Niveau principal utilisé : <math>\text{StorageUsed} \{ \text{SSD} \}</math></p> <p>Pool de capacités utilisé : <math>\text{StorageUsed} \{ \text{StandardCapacityPool} \}</math></p> |
|                             | ... déterminer les économies réalisées grâce à l'efficacité du stockage (compression, déduplication et compactage) ? | Économies d'efficacité du stockage                 | $\text{StorageEfficiencySavings}$                                                                                                                                                                                                                                                                                       |
| Stockage                    | ... déterminer la quantité de stockage principal disponible ?                                                        | Capacité de stockage principal disponible (octets) | $\text{StorageCapacity} \{ \text{SSD} \} - \text{StorageUsed} \{ \text{SSD} \}$                                                                                                                                                                                                                                         |



| Surveillance et performance         | Comment puis-je...                                                                                           | Diagramme                                                             | Métriques pertinentes                                                               |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|                                     | ... déterminer le pourcentage de stockage principal utilisé pour mon système de fichiers ?                   | Taux d'utilisation de la capacité de stockage principal (pourcentage) | $\text{StorageUsed } \{\text{SSD}\} * 100 / \text{StorageCapacity } \{\text{SSD}\}$ |
|                                     | ... déterminer si mon système de fichiers approche de sa limite de débit réseau ?                            | Débit du réseau — utilisation (pourcentage)                           | NetworkThroughputUtilization                                                        |
| Performances du serveur de fichiers | ... 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                                                     |

| Surveillance et performance | Comment puis-je...                                                                                                                             | Diagramme                                                                       | Métriques pertinentes             |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|-----------------------------------|
|                             | ... déterminer si mon système de fichiers approche la limite d'IOPS SSD de ses serveurs de fichiers ?                                          | IOPS sur disque :<br>taux d'utilisation (pourcentage)                           | FileServerDiskIops<br>Utilization |
|                             | ... 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 :<br>équilibre des rafales (pourcentage) | FileServerDiskIops<br>Balance     |
|                             | ... 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 NVMe lecture de mon système de fichiers ?                  | Taux de réussite du cache (pourcentage)                                         | FileServerCacheHit<br>Ratio       |

| Surveillance et performance | Comment puis-je...                                                                                    | Diagramme                                        | Métriques pertinentes |
|-----------------------------|-------------------------------------------------------------------------------------------------------|--------------------------------------------------|-----------------------|
| 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 de réserve 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 statistiques de volume dans la FSx console Amazon

Vous pouvez consulter le panneau de surveillance sur le tableau de bord de votre volume dans la FSx console Amazon pour consulter des indicateurs de performance supplémentaires. Pour de plus amples informations, veuillez consulter [Accès aux CloudWatch métriques](#).

| Surveillance | Comment puis-je...                                                | Diagramme            | Métriques pertinentes |
|--------------|-------------------------------------------------------------------|----------------------|-----------------------|
|              | ... déterminer la capacité de stockage disponible de mon volume ? | Capacité de stockage | StorageCapacity       |

| Surveillance | Comment puis-je...                                                                                                     | Diagramme                                                      | Métriques pertinentes                                                                                         |
|--------------|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
|              |                                                                                                                        | disponible                                                     |                                                                                                               |
|              | ... 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 (opérations/s)       | SOMME (DataReadOperations + DataWriteOperations + MetadataOperations) / PÉRIODE (en secondes)                 |
|              | ... déterminer le nombre d'opérations de lecture et d'écriture provenant ou destinées au niveau du pool de capacités ? | Nombre d'E/S par seconde du pool de capacités (opérations/sec) | Opérations de lecture : CapacityPoolReadOperations<br><br>Opérations d'écriture : CapacityPoolWriteOperations |

| Surveillance | Comment puis-je...                                                                                             | Diagramme                      | Métriques pertinentes                                                                                                                                                                                                                                                                                                                                          |
|--------------|----------------------------------------------------------------------------------------------------------------|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | ... déterminer la latence moyenne pour les opérations de lecture, d'écriture et de métadonnées de mon volume ? | Latence moyenne (ms/opération) | <p>Latence de lecture moyenne : <math>\text{DataRead0operationTime} * 1000 / \text{DataRead0operations}</math></p> <p>Latence d'écriture moyenne : <math>\text{DataWriteOperationTime} * 1000 / \text{DataWrite0operations}</math></p> <p>Latence moyenne des métadonnées : <math>\text{Metadata0operationTime} * 1000 / \text{Metadata0operations}</math></p> |
|              | ... déterminer le nombre de fichiers ou d'inodes disponibles sur mon volume ?                                  | Fichiers disponibles (inodes)  | $\text{FilesCapacity} - \text{FilesUsed}$                                                                                                                                                                                                                                                                                                                      |
|              | ... déterminer la répartition de la capacité de stockage utilisée et gratuite sur mon volume ?                 | Distribution du stockage       | $\text{StorageCapacity} - \text{StorageUsed}$                                                                                                                                                                                                                                                                                                                  |

## 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 FSx performance Amazon actifs ou récents et toutes les CloudWatch alarmes configurées pour le système de fichiers qui sont en 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 n'importe laquelle des FSx métriques Amazon. Pour de plus amples informations, veuillez consulter [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 | <p>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 de plus amples informations, veuillez consulter <a href="#">Mise à jour de la capacité de stockage et des IOPS provisionnées</a>.</p> <p>Si votre système de fichiers comporte plusieurs paires HA et que l'utilisation de votre capacité de stockage 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</p> |

| Section du tableau de bord          | S'il existe un avertissement pour cette métrique | Faites ceci                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                     |                                                  | charges de travail, consultez. <a href="#">Équilibrer les charges de travail entre les paires HA</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Performances du serveur de fichiers | Débit réseau                                     | <p>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, consultez <a href="#">Mise à jour de la capacité de débit</a>.</p> <p>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. <a href="#">Équilibrer les charges de travail entre les paires HA</a></p> |
|                                     | Débit du disque                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|                                     | IOPS sur disque                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|                                     | Utilisation de l'UC                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Section du tableau de bord | S'il existe un avertissement pour cette métrique | Faites ceci                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Performances disque        | IOPS sur disque                                  | <p>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. <a href="#">Mise à jour de la capacité de stockage et des IOPS provisionnées</a></p> <p>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. <a href="#">Équilibrer les charges de travail entre les paires HA</a></p> |

Pour plus d'informations sur les performances du système de fichiers, consultez [Amazon FSx pour les performances d' NetApp 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 FSx console Amazon ou de la CloudWatch console Amazon.

Les procédures suivantes décrivent comment créer des alarmes à l'aide de la FSx console Amazon, AWS Command Line Interface (AWS CLI) et de l'API.

Pour définir des alarmes à l'aide de la FSx console Amazon

1. Ouvrez la FSx console Amazon 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 Métriques, 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 FSx console Amazon, en commençant par l'étape 6.

Pour régler une alarme à l'aide du AWS CLI

- Appelez la commande [put-metric-alarm](#)CLI. 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 de l'API [PutMetricAlarm](#). Pour plus d'informations, consultez le [Amazon CloudWatch API Reference](#).

## Métriques du système de fichiers

Les statistiques de votre système de fichiers Amazon FSx for NetApp ONTAP sont classées soit en métriques de système de fichiers, soit 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](#)
- [Métriques du serveur de fichiers](#)
- [Métriques d'E/S sur disque](#)

- [Indicateurs de capacité de stockage](#)
- [Mesures détaillées du système de fichiers](#)

## Métriques d'E/S réseau

Toutes ces mesures ont une dimension, `FileSystemId`.

| Métrique                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>NetworkThroughputUtilization</code> | <p>Pourcentage d'utilisation du débit réseau pour le système de fichiers.</p> <p>La Average statistique représente l'utilisation moyenne du débit réseau du système de fichiers sur une période spécifiée.</p> <p>La Minimum statistique représente le taux d'utilisation du débit réseau le plus faible du système de fichiers sur une période spécifiée.</p> <p>La Maximum statistique représente le taux d'utilisation du débit réseau le plus élevé du système de fichiers sur une période spécifiée.</p> <p>Unités : pourcentage</p> <p>Statistiques valides : AverageMinimum, et Maximum</p> |
| <code>NetworkSentBytes</code>             | <p>Nombre d'octets (E/S réseau) envoyés par le système de fichiers.</p> <p>La Sum statistique est le nombre total d'octets envoyés par le système de fichiers sur une période spécifiée.</p> <p>Pour calculer le débit envoyé (octets par seconde) pour n'importe quelle statistique,</p>                                                                                                                                                                                                                                                                                                          |

| Métrique             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | <p>divisez la statistique par les secondes pendant la période spécifiée.</p> <p>Unités : octets</p> <p>Statistiques valides : Sum</p>                                                                                                                                                                                                                                                                                                                       |
| NetworkReceivedBytes | <p>Nombre d'octets (E/S réseau) reçus par le système de fichiers.</p> <p>La Sum statistique représente le nombre total d'octets reçus par le système de fichiers au cours d'une période spécifiée.</p> <p>Pour calculer le débit reçu (octets par seconde) pour n'importe quelle statistique, divisez la statistique par les secondes pendant la période spécifiée.</p> <p>Unités : octets</p> <p>Statistiques valides : Sum</p>                            |
| DataReadBytes        | <p>Nombre d'octets (E/S réseau) entre les lectures effectuées par les clients et le système de fichiers.</p> <p>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.</p> <p>Unités : octets</p> <p>Statistiques valides : Sum</p> |

| Métrique           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DataWriteBytes     | <p>Nombre d'octets (E/S réseau) provenant des écritures effectuées par les clients sur le système de fichiers.</p> <p>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.</p> <p>Unités : octets</p> <p>Statistiques valides : Sum</p>                  |
| DataReadOperations | <p>Nombre d'opérations de lecture (E/S réseau) entre les lectures effectuées par les clients et le système de fichiers.</p> <p>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.</p> <p>Unités : nombre</p> <p>Statistiques valides : Sum</p> |

| Métrique            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DataWriteOperations | <p>Nombre d'opérations d'écriture (E/S réseau) effectuées par les clients dans le système de fichiers.</p> <p>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.</p> <p>Unités : nombre</p> <p>Statistiques valides : Sum</p>           |
| MetadataOperations  | <p>Nombre d'opérations de métadonnées (E/S réseau) effectuées par les clients sur le système de fichiers.</p> <p>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.</p> <p>Unités : nombre</p> <p>Statistiques valides : Sum</p> |

| Métrique               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DataReadOperationTime  | <p>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.</p> <p>La Sum statistique représente le nombre total de secondes consacrées aux opérations de lecture au cours de 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.</p> <p>Unités : secondes</p> <p>Statistiques valides : Sum</p> |
| DataWriteOperationTime | <p>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.</p> <p>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.</p> <p>Unités : secondes</p> <p>Statistiques valides : Sum</p>            |



| Métrique              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CapacityPoolReadBytes | <p>Nombre d'octets lus (E/S réseau) depuis le niveau du pool de capacités du système de fichiers.</p> <p>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.</p> <p>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.</p> <p>Unités : octets</p> <p>Statistiques valides : Sum</p> |

| Métrique                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CapacityPoolReadOperations | <p>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.</p> <p>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.</p> <p>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 statistique par les secondes sur une période spécifiée.</p> <p>Unités : nombre</p> <p>Statistiques valides : Sum</p> |

| Métrique               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CapacityPoolWriteBytes | <p>Nombre d'octets écrits (E/S réseau) dans le niveau du pool de capacités du système de fichiers.</p> <p>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.</p> <p>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 statistique par les secondes au cours d'une période spécifiée.</p> <p>Unités : octets</p> <p>Statistiques valides : Sum</p> |

| Métrique                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CapacityPoolWriteOperations | <p>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.</p> <p>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.</p> <p>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 statistique par les secondes sur une période spécifiée.</p> <p>Unités : nombre</p> <p>Statistiques valides : Sum</p> |

## Métriques du serveur de fichiers

Toutes ces mesures ont une dimension, `FileSystemId`.

| Métrique       | Description                                                                                                                                                                                                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPUUtilization | <p>Pourcentage d'utilisation des ressources du processeur du système de fichiers.</p> <p>La Average statistique représente l'utilisation moyenne du processeur du système de fichiers sur une période spécifiée.</p> |

| Métrique                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                     | <p>La Minimum statistique représente le taux d'utilisation du processeur le plus faible du système de fichiers sur une période donnée.</p> <p>La Maximum statistique représente le taux d'utilisation du processeur le plus élevé du système de fichiers sur une période donnée.</p> <p>Unités : pourcentage</p> <p>Statistiques valides : AverageMinimum, et Maximum</p>                                                                                                                                                                                                                                                                                                                              |
| FileServerDiskThroughputUtilization | <p>Débit du disque entre votre serveur de fichiers et le niveau principal, en pourcentage de la limite allouée déterminée par la capacité de débit.</p> <p>La Average statistique représente le pourcentage moyen d'utilisation du débit de disque des serveurs de fichiers sur une période donnée.</p> <p>La Minimum statistique représente le pourcentage le plus faible d'utilisation du débit de disque des serveurs de fichiers sur une période donnée.</p> <p>La Maximum statistique représente le taux d'utilisation le plus élevé du débit de disque des serveurs de fichiers sur une période donnée.</p> <p>Unités : pourcentage</p> <p>Statistiques valides : AverageMinimum, et Maximum</p> |

| Métrique                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FileServerDiskThroughputBalance | <p>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 à 512. MBps</p> <p>La Average statistique est le solde de rafale moyen disponible sur une période spécifiée.</p> <p>La Minimum statistique est le solde de rafale minimum disponible sur une période spécifiée.</p> <p>La Maximum statistique représente le solde de rafale maximal disponible sur une période spécifiée.</p> <p>Unités : pourcentage</p> <p>Statistiques valides : AverageMinimum, et Maximum</p> |

| Métrique                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FileServerDiskIopsBalance | <p>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 à 512. MBps</p> <p>La Average statistique est le solde de rafale moyen disponible sur une période spécifiée.</p> <p>La Minimum statistique est le solde de rafale minimum disponible sur une période spécifiée.</p> <p>La Maximum statistique représente le solde de rafale maximal disponible sur une période spécifiée.</p> <p>Unités : pourcentage</p> <p>Statistiques valides : AverageMinimum, et Maximum</p> |

| Métrique                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FileServerDiskIopsUtilization | <p>Pourcentage d'utilisation des IOPS par rapport à la capacité d'IOPS du disque disponible pour votre serveur de fichiers.</p> <p>La Average statistique représente l'utilisation moyenne des IOPS sur le disque par le système de fichiers sur une période donnée.</p> <p>La Minimum statistique représente l'utilisation minimale d'IOPS sur le disque du système de fichiers sur une période spécifiée.</p> <p>La Maximum statistique représente l'utilisation maximale d'IOPS sur le disque par le système de fichiers sur une période spécifiée.</p> <p>Unités : pourcentage</p> <p>Statistiques valides : AverageMinimum, et Maximum</p> |



| Métrique                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>FileServerCacheHitRatio</code> | <p>Pourcentage de toutes les demandes de lecture traitées par des données contenues dans la RAM et les NVMe caches du système de fichiers. Un pourcentage plus élevé signifie que davantage de lectures sont effectuées par les caches de lecture du système de fichiers.</p> <p>Unités : pourcentage</p> <p>La Average statistique représente le pourcentage moyen d'accès au cache pour le système de fichiers sur une période donnée.</p> <p>La Minimum statistique représente le plus faible pourcentage d'accès au cache du système de fichiers sur une période donnée.</p> <p>Maximum Cette statistique représente le pourcentage d'accès au cache le plus élevé pour le système de fichiers sur une période donnée.</p> <p>Statistiques valides : AverageMinimum, et Maximum</p> |

## Métriques d'E/S sur disque

Toutes ces mesures ont une dimension, `FileSystemId`.

| Métrique                   | Description                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------|
| <code>DiskReadBytes</code> | Nombre d'octets (E/S de disque) d'un disque lu vers le niveau principal du système de fichiers. |

| Métrique       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                | <p>La Sum statistique est le nombre total d'octets lus depuis le système de fichiers sur une période spécifiée.</p> <p>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.</p> <p>Unités : octets</p> <p>Statistiques valides : Sum</p>                                                                                                                |
| DiskWriteBytes | <p>Le nombre d'octets (E/S de disque) d'un disque écrit sur le niveau principal du système de fichiers.</p> <p>La Sum statistique est le nombre total d'octets écrits depuis le système de fichiers sur une période spécifiée.</p> <p>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.</p> <p>Unités : octets</p> <p>Statistiques valides : Sum</p> |

| Métrique            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DiskIopsUtilization | <p>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.</p> <p>La Average statistique représente l'utilisation moyenne des IOPS sur le disque par le système de fichiers sur une période donnée.</p> <p>La Minimum statistique représente l'utilisation minimale d'IOPS sur le disque du système de fichiers sur une période spécifiée.</p> <p>La Maximum statistique représente l'utilisation maximale d'IOPS sur le disque par le système de fichiers sur une période spécifiée.</p> <p>Unités : pourcentage</p> <p>Statistiques valides : AverageMinimum, et Maximum</p> |
| DiskReadOperations  | <p>Nombre d'opérations de lecture (E/S sur disque) depuis le niveau principal du système de fichiers.</p> <p>La Sum statistique représente le nombre total d'opérations de lecture depuis le niveau principal sur une période spécifiée.</p> <p>Unités : nombre</p> <p>Statistiques valides : Sum</p>                                                                                                                                                                                                                                                                                                                                                                                                  |

| Métrique            | Description                                                                                                                                                                                                                                                                                           |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DiskWriteOperations | <p>Nombre d'opérations d'écriture (E/S de disque) sur le niveau principal du système de fichiers.</p> <p>La Sum statistique représente le nombre total d'opérations d'écriture sur le niveau principal au cours d'une période spécifiée.</p> <p>Unités : nombre</p> <p>Statistiques valides : Sum</p> |

## Indicateurs de capacité de stockage

Toutes ces mesures ont une dimension, `FileSystemId`.

| Métrique                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| StorageEfficiencySavings | <p>Les octets économisés grâce aux fonctionnalités d'efficacité du stockage (compression, déduplication et compactage).</p> <p>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 <code>StorageEfficiencySavings</code> par la somme de <code>StorageEfficiencySavings</code> et la métrique du système de <code>StorageUsed</code> fichiers, à l'aide de la Sum statistique pour <code>StorageUsed</code>.</p> <p>La Minimum statistique représente les économies minimales en termes d'efficacité du stockage sur une période donnée.</p> |

| Métrique                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          | <p>La <code>Maximum</code> statistique représente les économies maximales en termes d'efficacité du stockage sur une période donnée.</p> <p>Unités : octets</p> <p>Statistiques valides : <code>AverageMinimum</code>, et <code>Maximum</code></p>                                                                                                                                                                                |
| <code>StorageUsed</code> | <p>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.</p> <p>Unités : octets</p> <p>Statistiques valides : <code>AverageMinimum</code>, et <code>Maximum</code></p> |

| Métrique          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LogicalDataStored | <p>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.</p> <p>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.</p> <p>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.</p> <p>Unités : octets</p> <p>Statistiques valides : AverageMinimum, et Maximum</p> |

## 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, etDataType.

- 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>StorageCapacityUtilization</code> | <p>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.</p> <p>La <code>Average</code> 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.</p> <p><code>Minimum</code>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.</p> <p><code>Maximum</code>Cette statistique représente le taux le plus élevé d'utilisation de la capacité de stockage pour le niveau de performance de votre système de fichiers au cours de la période spécifiée.</p> <p>Unités : pourcentage</p> |

| Métrique        | Description                                                                                                         |
|-----------------|---------------------------------------------------------------------------------------------------------------------|
|                 | Statistiques valides : AverageMinimum, et Maximum                                                                   |
| StorageCapacity | Capacité de stockage totale du niveau principal (SSD).<br><br>Unités : octets<br><br>Statistiques valides : Maximum |



| Métrique    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| StorageUsed | <p>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 <code>StorageTier</code> sont <code>SSD</code> et <code>StandardCapacityPool</code>, correspondant au niveau de stockage mesuré par cette métrique. Cette métrique nécessite également la <code>DataType</code> dimension avec la valeur <code>All</code>.</p> <p>Les <code>Maximum</code> statistiques <code>Average</code>, <code>Minimum</code>, et <code>Maximum</code> sont la consommation de stockage par niveau en octets pour la période donnée.</p> <p>Pour calculer l'utilisation de la capacité de stockage de votre niveau de stockage principal (SSD), divisez l'une de ces statistiques par le <code>Maximum StorageCapacity</code> chiffre correspondant à la même période, avec <code>StorageTier</code> une dimension égale à <code>SSD</code>.</p> <p>Pour calculer la capacité de stockage disponible de votre niveau de stockage principal (SSD) en octets, soustrayez l'une de ces statistiques de la <code>Maximum StorageCapacity</code> même période, avec une dimension <code>StorageTier</code> égale à <code>SSD</code>.</p> <p>Unités : octets</p> <p>Statistiques valides : <code>Average</code>, <code>Minimum</code>, et <code>Maximum</code></p> |

## Métriques du système de fichiers de deuxième génération

Les métriques suivantes sont fournies FSx pour les systèmes de fichiers ONTAP de deuxième génération. 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](#)
- [Métriques du serveur de fichiers](#)
- [Métriques d'E/S sur disque](#)
- [Mesures détaillées du système de fichiers](#)

### 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                                                                                                                        |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <code>NetworkThroughputUtilization</code> | Utilisation du débit réseau en pourcentage du débit réseau disponible pour votre système de fichiers. Cette métrique est équivalen |

| Métrique | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <p>te au maximum <code>NetworkSentBytes</code> et <code>NetworkReceivedBytes</code> 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 <code>SnapMirror</code> la hiérarchisation et les sauvegardes). Une métrique est émise chaque minute pour chacun des serveurs de fichiers de votre système de fichiers.</p> <p>La <code>Average</code> statistique représente l'utilisation moyenne du débit réseau pour le serveur de fichiers donné au cours de la période spécifiée.</p> <p>La <code>Minimum</code> statistique représente l'utilisation du débit réseau la plus faible pour le serveur de fichiers donné sur une minute, pendant la période spécifiée.</p> <p>La <code>Maximum</code> 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.</p> <p>Unités : pourcentage</p> <p>Statistiques valides : <code>AverageMinimum</code>, et <code>Maximum</code></p> |

| Métrique         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NetworkSentBytes | <p>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 sauvegardes). Une métrique est émise chaque minute pour chacun des serveurs de fichiers de votre système de fichiers.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Pour calculer le débit envoyé (octets par seconde) pour n'importe quelle statistique, divisez la statistique par les secondes pendant la période spécifiée.</p> <p>Unités : octets</p> |

| Métrique | Description                                            |
|----------|--------------------------------------------------------|
|          | Statistiques valides : SumAverage, Minimum, et Maximum |

| Métrique             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NetworkReceivedBytes | <p>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 SnapMirror la hiérarchisation et les sauvegardes). Une métrique est émise chaque minute pour chacun des serveurs de fichiers de votre système de fichiers.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Pour calculer le débit reçu (octets par seconde) pour n'importe quelle statistique, divisez la statistique par les secondes de la période.</p> <p>Unités : octets</p> <p>Statistiques valides : SumAverage,Minimum, et Maximum</p> |

## Métriques du serveur de fichiers

Toutes ces mesures prennent deux dimensions, `FileSystemId` et `FileServer`.

| Métrique                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>CPUUtilization</code>                      | <p>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.</p> <p>La <code>Average</code> statistique représente l'utilisation moyenne du processeur du système de fichiers sur une période spécifiée.</p> <p>La <code>Minimum</code> statistique représente le taux d'utilisation du processeur le plus faible pour le serveur de fichiers donné au cours de la période spécifiée.</p> <p>La <code>Maximum</code> statistique représente le taux d'utilisation du processeur le plus élevé pour le serveur de fichiers donné au cours de la période spécifiée.</p> <p>Unités : pourcentage</p> <p>Statistiques valides : <code>Average</code>, <code>Minimum</code>, et <code>Maximum</code></p> |
| <code>FileServerDiskThroughputUtilization</code> | <p>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 <code>SnapMirror</code> la hiérarchisation et les sauvegardes). Cette métrique est équivalente à la somme <code>DiskReadBytes</code> et <code>DiskWrite</code></p>                                                                                                                                                                                                                                                                                                                                                                                                       |

| Métrique | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Unités : pourcentage</p> <p>Statistiques valides : AverageMinimum, et Maximum</p> |



| Métrique                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FileServerDiskIopsUtilization | <p>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 <code>DiskIopsUtilization</code> 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.</p> <p>La <code>Average</code> statistique représente l'utilisation moyenne des IOPS sur le disque pour le serveur de fichiers donné au cours de la période spécifiée.</p> <p>La <code>Minimum</code> statistique représente le taux d'utilisation IOPS le plus faible du disque pour le serveur de fichiers donné au cours de la période spécifiée.</p> <p>La <code>Maximum</code> statistique représente le taux d'utilisation IOPS le plus élevé du disque pour le serveur de fichiers donné au cours de la période spécifiée.</p> <p>Unités : pourcentage</p> <p>Statistiques valides : <code>AverageMinimum</code>, et <code>Maximum</code></p> |

| Métrique                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>FileServerCacheHitRatio</code> | <p>Pourcentage de toutes les demandes de lecture traitées par des données se trouvant dans la RAM ou les NVMe caches 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 sauvegardes). Une métrique est émise chaque minute pour chacun des serveurs de fichiers de votre système de fichiers.</p> <p>Unités : pourcentage</p> <p>La <code>Average</code> 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.</p> <p><code>Minimum</code> 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.</p> <p><code>Maximum</code> 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.</p> <p>Statistiques valides : <code>Average</code>, <code>Minimum</code>, et <code>Maximum</code></p> |

## 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 `FsxD01234567890abcdef-01` (le serveur de fichiers actif) et le serveur de fichiers `FsxD01234567890abcdef-02` (le serveur de fichiers secondaire) dans une paire HA.

| Métrique                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>DiskReadBytes</code> | <p>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 SnapMirror la hiérarchisation et les sauvegardes). Une métrique est émise chaque minute pour chacun des agrégats de votre système de fichiers.</p> <p>La Sum statistique est le nombre total d'octets lus chaque minute à partir de l'agrégat donné au cours de la période spécifiée.</p> <p>La Average statistique est le nombre moyen d'octets lus par minute à partir de l'agrégat donné sur la période spécifiée.</p> <p>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.</p> <p>La Maximum statistique représente le plus grand nombre d'octets lus par minute à partir</p> |

| Métrique | Description                                                                                                                                                                                                                                                                                                        |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <p>de l'agrégat donné au cours de la période spécifiée.</p> <p>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.</p> <p>Unités : octets</p> <p>Statistiques valides : SumAverage, Minimum, et Maximum</p> |

| Métrique       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DiskWriteBytes | <p>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 SnapMirror la hiérarchisation et les sauvegardes). Une métrique est émise chaque minute pour chacun des agrégats de votre système de fichiers.</p> <p>La Sum statistique est le nombre total d'octets écrits dans l'agrégat donné au cours de la période spécifiée.</p> <p>La Average statistique est le nombre moyen d'octets écrits sur l'agrégat donné chaque minute au cours de la période spécifiée.</p> <p>La Minimum statistique est le plus petit nombre d'octets écrits dans l'agrégat donné chaque minute au cours de la période spécifiée.</p> <p>La Maximum statistique représente le plus grand nombre d'octets écrits dans l'agrégat donné chaque minute au cours de la période spécifiée.</p> <p>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.</p> <p>Unités : octets</p> <p>Statistiques valides : SumAverage,Minimum, et Maximum</p> |

| Métrique            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DiskIopsUtilization | <p>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 FileServe <code>rDiskIopsUtilization</code> 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.</p> <p>La Average statistique représente l'utilisation moyenne des IOPS du disque pour l'agrégat donné sur la période spécifiée.</p> <p>La Minimum statistique représente le taux d'utilisation IOPS le plus faible du disque pour l'agrégat donné au cours de la période spécifiée.</p> <p>La Maximum statistique est le taux d'utilisation IOPS le plus élevé du disque pour un agrégat donné au cours de la période spécifiée.</p> <p>Unités : pourcentage</p> |

| Métrique | Description                                       |
|----------|---------------------------------------------------|
|          | Statistiques valides : AverageMinimum, et Maximum |

| Métrique           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DiskReadOperations | <p>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 sauvegardes). Une métrique est émise chaque minute pour chacun des agrégats de votre système de fichiers.</p> <p>La Sum statistique est le nombre total d'opérations de lecture effectuées par l'agrégat donné au cours de la période spécifiée.</p> <p>La Average statistique est le nombre moyen d'opérations de lecture effectuées chaque minute par l'agrégat donné au cours de la période spécifiée.</p> <p>La Minimum statistique représente le plus petit nombre d'opérations de lecture effectuées chaque minute par l'agrégat donné sur la période spécifiée.</p> <p>La Maximum statistique représente le plus grand nombre d'opérations de lecture effectuées chaque minute par l'agrégat donné au cours de la période spécifiée.</p> <p>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).</p> <p>Unités : nombre</p> |



| Métrique            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | Statistiques valides : SumAverage,Minimum, et Maximum                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| DiskWriteOperations | <p>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 SnapMirror la hiérarchisation et les sauvegardes). Une métrique est émise chaque minute pour chacun des agrégats de votre système de fichiers.</p> <p>La Sum statistique est le nombre total d'opérations d'écriture effectuées par l'agrégat donné au cours de la période spécifiée.</p> <p>La Average statistique est le nombre moyen d'opérations d'écriture effectuées chaque minute par l'agrégat donné sur la période spécifiée.</p> <p>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).</p> <p>Unités : nombre</p> <p>Statistiques valides : Sum et Average</p> |

## 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 etStandardCapacityPool.
- DataType— Indique le type de données mesuré par la métrique, avec la valeur possibleAll.

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 | <p>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.</p> <p>La Average statistique représente le taux moyen d'utilisation de la capacité de stockage pour un agrégat donné au cours de la période spécifiée.</p> <p>La Minimum statistique représente le niveau minimum d'utilisation de la capacité de</p> |

| Métrique        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | <p>stockage pour un agrégat donné au cours de la période spécifiée.</p> <p>La <code>Maximum</code> statistique représente le niveau maximal d'utilisation de la capacité de stockage pour un agrégat donné au cours de la période spécifiée.</p> <p>Unités : pourcentage</p> <p>Statistiques valides : <code>AverageMinimum</code>, et <code>Maximum</code></p>                                                                                                                                                                                                                                                                                                                                                 |
| StorageCapacity | <p>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.</p> <p>La <code>Average</code> statistique représente la capacité de stockage moyenne pour un agrégat donné sur la période spécifiée.</p> <p>La <code>Minimum</code> statistique représente la quantité minimale de capacité de stockage pour un agrégat donné sur la période spécifiée.</p> <p>La <code>Maximum</code> statistique représente la capacité de stockage maximale pour un agrégat donné sur la période spécifiée.</p> <p>Unités : octets</p> <p>Statistiques valides : <code>AverageMinimum</code>, et <code>Maximum</code></p> |

| Métrique    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| StorageUsed | <p>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 <code>StorageTier</code> sont <code>SSD</code> et <code>StandardCapacityPool</code>, correspondant au niveau de stockage mesuré par cette métrique. Une métrique est émise chaque minute pour chacun des agrégats de votre système de fichiers.</p> <p>La <code>Average</code> 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.</p> <p>La <code>Minimum</code> 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.</p> <p>La <code>Maximum</code> 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.</p> <p>Unités : octets</p> <p>Statistiques valides : <code>AverageMinimum</code>, et <code>Maximum</code></p> |

## 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 CloudWatch 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](#)
- [Indicateurs de capacité de stockage](#)
- [Mesures de volume détaillées](#)

## Métriques d'E/S réseau

Toutes ces mesures prennent deux dimensions, `FileSystemId` et `VolumeId`.

| Métrique                   | Description                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>DataReadBytes</code> | <p>Nombre d'octets (E/S réseau) lus depuis le volume par les clients.</p> <p>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.</p> |

| Métrique           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | Unités : octets<br><br>Statistiques valides : Sum                                                                                                                                                                                                                                                                                                                                                                                          |
| DataWriteBytes     | <p>Nombre d'octets (E/S réseau) écrits sur le volume par les clients.</p> <p>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.</p> <p>Unités : octets</p> <p>Statistiques valides : Sum</p>                   |
| DataReadOperations | <p>Nombre d'opérations de lecture (E/S réseau) effectuées par les clients sur le volume.</p> <p>La Sum statistique représente le nombre total d'opérations de lecture pendant 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.</p> <p>Unités : nombre</p> <p>Statistiques valides : Sum</p> |

| Métrique            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DataWriteOperations | <p>Nombre d'opérations d'écriture (E/S réseau) effectuées par les clients sur le volume.</p> <p>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.</p> <p>Unités : nombre</p> <p>Statistiques valides : Sum</p>                          |
| MetadataOperations  | <p>Nombre d'opérations d'E/S (E/S réseau) entre les activités de métadonnées des clients et le volume.</p> <p>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.</p> <p>Unités : nombre</p> <p>Statistiques valides : Sum</p> |

| Métrique               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DataReadOperationTime  | <p>Somme du temps total passé dans le volume pour les opérations de lecture (E/S réseau) par les clients accédant aux données du volume.</p> <p>La Sum statistique représente le nombre total de secondes consacrées aux opérations de lecture au cours de 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.</p> <p>Unités : secondes</p> <p>Statistiques valides : Sum</p> |
| DataWriteOperationTime | <p>Somme du temps total passé dans le volume pour effectuer les opérations d'écriture (E/S réseau) des clients accédant aux données du volume.</p> <p>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.</p> <p>Unités : secondes</p> <p>Statistiques valides : Sum</p>            |



| Métrique              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MetadataOperationTime | <p>Somme du temps total passé dans le volume pour exécuter les opérations de métadonnées (E/S réseau) des clients accédant aux données du volume.</p> <p>La Sum statistique représente le nombre total de secondes consacrées aux opérations de lecture au cours de 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.</p> <p>Unités : secondes</p> <p>Statistiques valides : Sum</p>                                                                                                              |
| CapacityPoolReadBytes | <p>Nombre d'octets lus (E/S réseau) depuis le niveau du pool de capacité du volume.</p> <p>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.</p> <p>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.</p> <p>Unités : octets</p> <p>Statistiques valides : Sum</p> |

| Métrique                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CapacityPoolReadOperations | <p>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.</p> <p>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.</p> <p>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.</p> <p>Unités : nombre</p> <p>Statistiques valides : Sum</p> |

| Métrique               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CapacityPoolWriteBytes | <p>Nombre d'octets écrits (E/S réseau) dans le niveau du pool de capacités du volume.</p> <p>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.</p> <p>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.</p> <p>Unités : octets</p> <p>Statistiques valides : Sum</p> |

| Métrique                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CapacityPoolWriteOperations | <p>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.</p> <p>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.</p> <p>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.</p> <p>Unités : nombre</p> <p>Statistiques valides : Sum</p> |

## Indicateurs de capacité de stockage

Toutes ces mesures prennent deux dimensions, `FileSystemId` et `VolumeId`.

| Métrique        | Description                                                                                     |
|-----------------|-------------------------------------------------------------------------------------------------|
| StorageCapacity | <p>Taille du volume en octets.</p> <p>Unités : octets</p> <p>Statistiques valides : Maximum</p> |
| StorageUsed     | <p>Capacité de stockage logique utilisée par le volume.</p> <p>Unités : octets</p>              |

| Métrique                   | Description                                                                                                                               |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
|                            | Statistiques valides : Average                                                                                                            |
| StorageCapacityUtilization | <p>Utilisation de la capacité de stockage du volume.</p> <p>Unités : pourcentage</p> <p>Statistiques valides : Average</p>                |
| FilesUsed                  | <p>Les fichiers utilisés (nombre de fichiers ou d'inodes) sur le volume.</p> <p>Unités : nombre</p> <p>Statistiques valides : Average</p> |
| FilesCapacity              | <p>Nombre total d'inodes pouvant être créés sur le volume.</p> <p>Unités : nombre</p> <p>Statistiques valides : Maximum</p>               |

## 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 `FileSystemId`, `VolumeId`, `StorageTier`, et `DataType`.

- La `StorageTier` dimension indique le niveau de stockage mesuré par la métrique, avec les valeurs possibles de `AllSSD`, `etStandardCapacityPool`.
- 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                | <p>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 <code>StorageTier SSD</code> ou <code>StandardCapacityPool</code>, et que vous définissez <code>DataType</code> sur <code>All</code>, cette métrique mesure l'utilisation de l'espace logique pour ce volume pour les niveaux de votre SSD et de votre pool de capacité, respectivement. Lorsque vous définissez la <code>DataType</code> dimension sur <code>User SnapshotOther</code>, ou et sur <code>All</code>, cette métrique mesure l'utilisation de l'espace logique pour chaque type de données respectif. <code>StorageTier</code> La consommation de Snapshot données inclut la réserve d'instantanés, qui représente 5 % de la taille du volume par défaut.</p> <p>Unités : octets</p> <p>Statistiques valides : <code>AverageMinimum</code>, et <code>Maximum</code></p> |
| StorageCapacityUtilization | <p>Pourcentage d'espace disque physique utilisé par le volume.</p> <p>Unités : pourcentage</p> <p>Statistiques valides : <code>Maximum</code></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

# Surveillance FSx des événements ONTAP EMS

Vous pouvez surveiller FSx les événements du système de fichiers 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](#)
- [Affichage des événements EMS](#)
- [Transfert d'événements EMS vers un serveur Syslog](#)

## 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 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'-severityoption.
- 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. |



| Option d'événement                          | Description                                                                                                                                            |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-instance</code>                      | Affiche des informations détaillées sur tous les champs.                                                                                               |
| <code>-node <i>nodename</i>   local</code>  | Affiche la liste des événements pour le nœud que vous spécifiez. Utilisez cette option <code>-seqnum</code> pour afficher des informations détaillées. |
| <code>-seqnum <i>sequence_number</i></code> | Sélectionne les événements correspondant à ce numéro dans la séquence. Utilisez avec <code>-node</code> pour afficher des informations détaillées.     |

| Option d'événement                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-time <i>MM/DD/YYYY HH:MM:SS</i></code> | <p>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.</p> <div data-bbox="1073 632 1507 831"><pre>event log show -<br/>time "04/17/2023<br/>05:55:00".. "04/17/<br/>2023 06:10:00"</pre></div> <p>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 :</p> <div data-bbox="1073 1272 1507 1356"><pre>event log show -time &gt;1m</pre></div> <p>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.</p> |

| Option d'événement                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-severity <i>sev_level</i></code> | <p>Sélectionne les événements correspondant à la <i>sev_level</i> valeur, qui doit être l'une des suivantes :</p> <ul style="list-style-type: none"><li>• EMERGENCY — Perturbation</li><li>• ALERT— Point de défaillance unique</li><li>• ERROR— Dégradation</li><li>• NOTICE— Informations</li><li>• INFORMATIONAL — Informations</li><li>• DEBUG— Informations de débogage</li></ul> <p>Pour afficher tous les événements, spécifiez leur gravité comme suit :</p> <div><pre>event log show -severity &lt;=DEBUG</pre></div> |

| Option d'événement                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-ems-severity</code> <i>ems_sev_level</i> | <p>Sélectionne les événements correspondant à la <i>ems_sev_level</i> valeur, qui doit être l'une des suivantes :</p> <ul style="list-style-type: none"><li>• <code>NODE_FAULT</code> — Une corruption des données est détectée ou le nœud n'est pas en mesure de fournir un service client.</li><li>• <code>SVC_FAULT</code> — Une perte de service temporaire, généralement une défaillance logicielle transitoire, est détectée.</li><li>• <code>NODE_ERROR</code> — Une erreur matérielle qui n'est pas immédiatement fatale est détectée.</li><li>• <code>SVC_ERROR</code> — Une erreur logicielle qui n'est pas immédiatement fatale est détectée.</li><li>• <code>WARNING</code>— Un message hautement prioritaire qui n'indique aucun défaut.</li><li>• <code>NOTICE</code>— Un message de priorité normale qui n'indique aucun défaut.</li><li>• <code>INFO</code>— Un message de faible priorité qui n'indique aucun défaut.</li></ul> |

| Option d'événement                | Description                                                                                                                                                                                                                                                                                       |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                   | <ul style="list-style-type: none"><li>• DEBUG— Un message de débogage.</li><li>• VAR— Un message de gravité variable, sélectionné lors de l'exécution.</li></ul> <p>Pour afficher tous les événements, spécifiez leur gravité comme suit :</p> <pre>event log show -ems-severity &lt;=DEBUG</pre> |
| -source <i>text</i>               | Sélectionne les événements correspondant à la <i>text</i> valeur. La source est généralement un module logiciel.                                                                                                                                                                                  |
| -message-name <i>message_name</i> | Sélectionne les événements correspondant à la <i>message_name</i> valeur. 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 <i>text</i>                | Sélectionne les événements correspondant à la <i>text</i> valeur. Le event champ contient le texte intégral de l'événement, y compris les paramètres éventuels.                                                                                                                                   |

| Option d'événement                                 | Description                                                                                                                                                                                         |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-kernel-generation-num</code> <i>integer</i> | Sélectionne les événements correspondant à la <i>integer</i> valeur. Seuls les événements qui proviennent du noyau ont des numéros de génération du noyau.                                          |
| <code>-kernel-sequence-num</code> <i>integer</i>   | Sélectionne les événements correspondant à la <i>integer</i> valeur. Seuls les événements qui proviennent du noyau ont des numéros de séquence du noyau.                                            |
| <code>-action</code> <i>text</i>                   | Sélectionne les événements correspondant à la <i>text</i> valeur. Le <code>action</code> champ décrit les mesures correctives que vous devez prendre, le cas échéant, pour remédier à la situation. |
| <code>-description</code> <i>text</i>              | Sélectionne les événements correspondant à la <i>text</i> valeur. Le <code>description</code> champ décrit pourquoi l'événement s'est produit et ce que cela signifie.                              |
| <code>-filter-name</code> <i>filter_name</i>       | Sélectionne les événements correspondant à la <i>filter_name</i> valeur. Seuls les événements inclus par les filtres existants qui correspondent à cette valeur s'affichent.                        |

| Option d'événement                         | Description                                                                                                                                                                                  |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-fields <i>fieldname</i> ,...</code> | Indique que la sortie de commande inclut également le ou les champs spécifiés. Vous pouvez l'option <code>-fields</code> 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 NetApp ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#) section du guide de l'utilisateur d'Amazon FSx pour 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.

**Note**

Votre destination Syslog doit se trouver dans le sous-réseau principal utilisé par votre système de fichiers.

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 NetApp ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#) section du guide de l'utilisateur d'Amazon FSx pour 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, car FSx 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. Si vous avez sélectionné TCP*transport\_protocol*, vous pouvez utiliser 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 à l'aide d'informations sur l'infrastructure de données

NetApp Data Infrastructure Insights (anciennement 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 solutions NetApp de stockage. Avec Data Infrastructure 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 besoins futurs en matière

de performances et de 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

Data Infrastructure Insights n'est pas pris en charge pour les systèmes de fichiers de deuxième génération comportant plusieurs paires HA.

Data Infrastructure 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 ONTAP plus efficace FSx . 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, consultez la documentation [Data Infrastructure Insights dans la documentation](#) du produit NetApp ONTAP.

## Surveillance des systèmes FSx de fichiers 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 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 FSx pour mesurer les performances de votre système de fichiers ONTAP et l'utilisation de la capacité de stockage.

Vous pouvez surveiller votre système de fichiers Amazon FSx for NetApp ONTAP en utilisant Harvest and Grafana. NetApp Harvest moniteurs ONTAP centres de données en collectant des indicateurs de performance, de capacité et de matériel à partir FSx des systèmes de fichiers ONTAP. Grafana fournit un tableau de bord où les données collectées Harvest les métriques peuvent être affichées.

### Tableaux de bord Harvest pris en charge

Amazon FSx for NetApp ONTAP présente un ensemble de mesures différent de celui affiché sur site NetApp ONTAP. Par conséquent, seuls les éléments suivants out-of-the-box Harvest les tableaux de bord marqués avec fsx sont actuellement compatibles avec FSx ONTAP. Certains panneaux de ces tableaux de bord peuvent ne pas contenir des informations qui ne sont pas prises en charge.

- Récolte : métadonnées
- ONTAP : CDot
- ONTAP : Cluster
- ONTAP : Conformité
- ONTAP : Datacenter
- ONTAP : Instantanés de protection des données
- ONTAP : LUNE
- ONTAP : Nœud
- ONTAP : Arree
- ONTAP : Sécurité
- ONTAP : SnapMirror
- POINT DE CONTACT : SVM
- ONTAP : Volume

Procédez comme suit : Harvest les tableaux de bord sont pris en charge par FSx for ONTAP, mais ne sont pas activés par défaut dans Harvest.

- ONTAP : FlexCache

- ONTAP : FlexGroup
- ONTAP : Clients NFS
- ONTAP : Moniteurs NFSv4 Storepool
- ONTAP : Résolution des problèmes liés au NFS
- POINT DE CONTACT : SMB
- ONTAP : Charge de travail

## Non pris en charge Harvest tableaux de bord

Procédez comme suit : Harvest les tableaux de bord ne sont pas pris en charge par FSx for ONTAP.

- ONTAP : Agrégat
- ONTAP : Disque
- ONTAP : Fonctionnement du service externe
- ONTAP : Analyse des systèmes de fichiers (FSA)
- ONTAP : Health
- ONTAP : MetroCluster
- ONTAP : Alimentation
- ONTAP : Étagère
- ONTAP : Magasins d'objets S3

## AWS CloudFormation modèle

Pour commencer, vous pouvez déployer un AWS CloudFormation modèle qui lance automatiquement une EC2 instance Amazon exécutant Harvest et Grafana. En entrée dans le AWS CloudFormation modèle, vous spécifiez l'`fsxadmin` utilisateur et le point de terminaison de FSx gestion Amazon 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 Amazon EC2 Linux et installe les logiciels Harvest et Grafana. Pour utiliser cette solution, téléchargez le [fsx-ontap-harvest-grafana modèle AWS CloudFormation .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' EC2 instances Amazon

Lors de la configuration du modèle, vous indiquez le type d' EC2 instance Amazon. 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)

Vous trouverez ci-dessous quelques exemples de configurations et le type d'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' EC2 [instances Amazon](#), consultez la section [Instances à usage général](#) dans le guide de EC2 l'utilisateur Amazon.

## Règles relatives aux ports d'instance

Lorsque vous configurez votre EC2 instance Amazon, assurez-vous que les ports 3000 et 9090 sont ouverts au trafic entrant pour le groupe de sécurité dans lequel se trouve 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 AWS votre compte, ainsi que des informations sur les paramètres du modèle répertorié ci-dessous. Pour plus d'informations sur la création d'un système de fichiers, consultez [Création de systèmes de fichiers](#).

Pour lancer la suite de solutions Harvest/Grafana

1. Téléchargez le [fsx-ontap-harvest-grafana modèle AWS CloudFormation .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 [FSx Points de terminaison et quotas Amazon](#) 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   | Le type d' EC2 instance Amazon. Voici les types d'instances. <ul style="list-style-type: none"><li>• t3.micro</li><li>• t3.small</li><li>• t3.medium</li><li>• t3.large</li></ul> |

| Paramètre     | Par défaut               | Description                                                                                                                                                                                                                                               |
|---------------|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                          | <ul style="list-style-type: none"><li>• t3.xlarge</li><li>• t3.2xlarge</li></ul> <p>Pour obtenir la liste complète des valeurs de type d' EC2 instance Amazon autorisées pour ce paramètre, consultez le fsx-ontap-harvest-grafana fichier .template.</p> |
| KeyPair       | Aucune valeur par défaut | La paire de clés utilisée pour accéder à l' EC2 instance Amazon.                                                                                                                                                                                          |
| SecurityGroup | Aucune valeur par défaut | L'ID du groupe de sécurité pour l'instance Harvest/Grafana. 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.      |

| Paramètre           | Par défaut                                                                 | Description                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type de sous-réseau | Aucune valeur par défaut                                                   | Spécifiez le type de sous-réseau, <code>public</code> soit <code>private</code> . 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 <a href="#">Types de sous-réseaux</a> dans le guide de l'utilisateur Amazon VPC. |
| Sous-réseau         | Aucune valeur par défaut                                                   | Spécifiez le même sous-réseau que le sous-réseau préféré de votre système de fichiers Amazon FSx for NetApp ONTAP. Vous trouverez l'ID de sous-réseau préféré du système de fichiers dans la FSx console Amazon, dans l'onglet Réseau et sécurité de la page de détails du système FSx de fichiers ONTAP.                                                                                        |
| LatestLinuxAmild    | <code>/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2</code> | La dernière version de l'AMI Amazon Linux 2 est une donnée Région AWS.                                                                                                                                                                                                                                                                                                                           |



| Paramètre   | Par défaut               | Description                                                                                                                                                                                                                                                                  |
|-------------|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FSxEndPoint | 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 FSx console Amazon, dans l'onglet Administration de la FSx page de détails du système de fichiers ONTAP. |
| SecretName  | Aucune valeur par défaut | AWS Secrets Manager nom secret contenant le mot de passe de l'fsxadminutilisateur 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](#)
- [CloudFormation pile annulée après l'expiration du délai](#)

### 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' EC2 instance Amazon sur laquelle Harvest et Grafana sont déployés.

1. Connectez-vous par SSH à l' EC2 instance Amazon 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 l'expiration du délai

Si vous ne parvenez pas à déployer la CloudFormation pile avec succès et qu'elle est en train de revenir en arrière avec des erreurs, suivez la procédure ci-dessous pour résoudre le problème. Vous aurez besoin d'un accès SSH à l' EC2 instance 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' EC2 instance Amazon 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.

## Surveillance des FSx appels d'API ONTAP avec AWS CloudTrail

Amazon FSx est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service sur Amazon FSx. CloudTrail capture tous les appels d' FSx API Amazon pour Amazon FSx pour NetApp ONTAP sous forme d'événements. Les appels capturés incluent les appels provenant de la FSx console Amazon et les appels de code vers les opérations FSx d'API Amazon.

Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Amazon FSx. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été envoyée 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 CloudTrail, consultez le [guide de AWS CloudTrail l'utilisateur](#).

## FSx Informations Amazon dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité d'API a lieu sur Amazon FSx, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements

de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre AWS compte. Pour plus d'informations, consultez la section [Affichage des événements à l'aide de l'historique des CloudTrail événements](#).

Pour un enregistrement continu des événements de votre AWS compte, y compris des événements pour Amazon FSx, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un parcours dans la console, celui-ci s'applique à toutes les AWS régions. Le journal enregistre les événements de toutes les AWS régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les rubriques suivantes dans le AWS CloudTrail Guide de l'utilisateur :

- [Création d'un parcours pour votre Compte AWS](#)
- [AWS intégrations de services avec Logs CloudTrail](#)
- [Configuration des notifications Amazon SNS pour CloudTrail](#)
- [Réception de fichiers CloudTrail journaux de plusieurs régions](#) et [réception de fichiers CloudTrail journaux de plusieurs comptes](#)

Tous les [appels FSx d'API](#) Amazon sont enregistrés par CloudTrail. Par exemple, les appels aux TagResource opérations CreateFileSystem et génèrent des entrées dans les fichiers CloudTrail 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 faite avec les informations d'identification de l'utilisateur root 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 demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'[élément CloudTrail UserIdentity dans le Guide](#) de l'AWS CloudTrail utilisateur.

## Comprendre les entrées du fichier FSx journal Amazon

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut 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 trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal qui illustre le TagResource fonctionnement lors de la création d'une balise pour un système de fichiers à partir de 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 une entrée de CloudTrail journal qui illustre l'UntagResource action à effectuer lorsqu'une balise d'un système de fichiers est supprimée de 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"
}

```



# Utilisation de Microsoft Active Directory dans FSx ONTAP

Amazon FSx travaille 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 FSx de stockage ONTAP (SVMs) à votre domaine Active Directory pour fournir une authentification utilisateur et un contrôle d'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.

Si l'infrastructure de domaine Microsoft Active Directory n'est pas disponible, vous pouvez configurer un serveur SMB (Server Message Block) dans un groupe de travail sur une SVM au lieu de joindre une SVM à un Microsoft Active Directory. Pour de plus amples informations, veuillez consulter [Configuration d'un serveur SMB dans un groupe de travail](#).

Lorsque vous associez Amazon FSx for NetApp ONTAP à un Active Directory, vous associez les systèmes de fichiers SVMs à Active Directory de manière indépendante. Cela signifie que vous pouvez avoir un système de fichiers dont certains SVMs sont joints à un Active Directory, tandis que d'autres 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](#)
- [Bonnes pratiques d'utilisation d'Active Directory](#)
- [Comment fonctionne SVMs l'adhésion à Microsoft Active Directory](#)
- [Gestion des configurations Active Directory des SVM](#)

# 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](#)
- [Exigences en matière de configuration du réseau](#)
- [Exigences relatives aux comptes de service Active Directory](#)

## 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 FSx votre système de fichiers 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 utilisez AWS Directory Service, FSx car ONTAP ne prend pas en charge l'adhésion SVMs à 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.

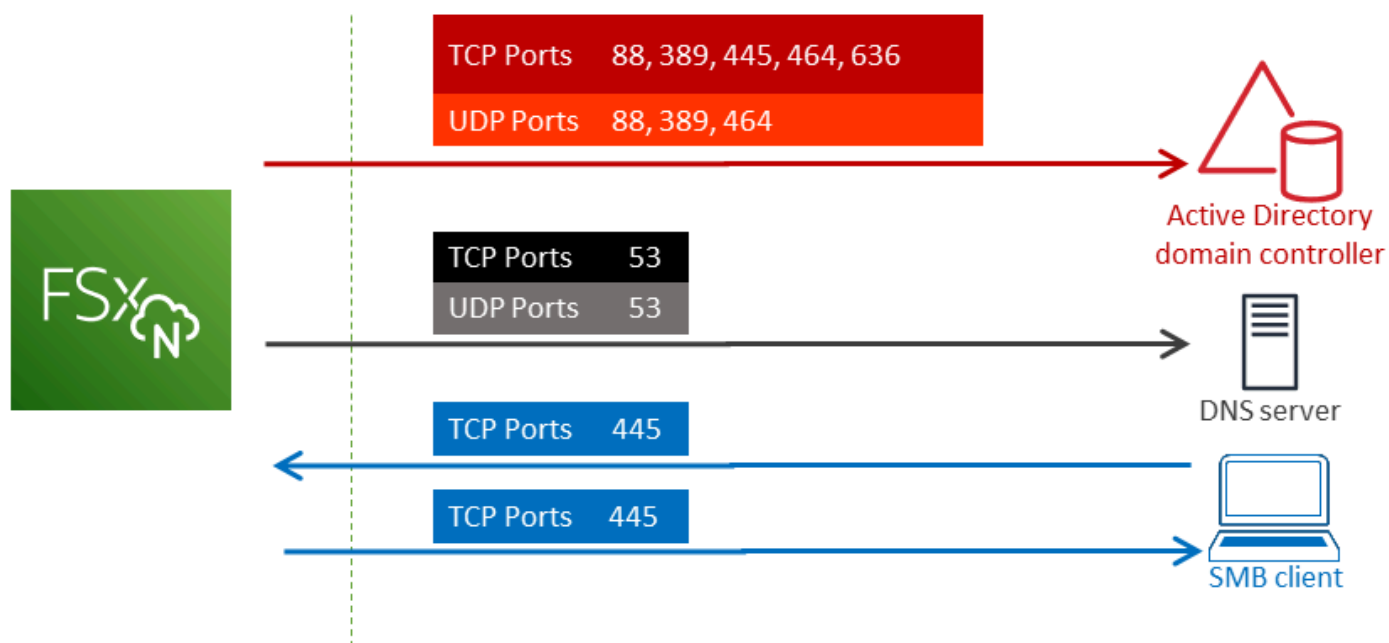
### ⚠ Important

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 ()) de la SVM. LIFs

- 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 VPN](#) ou [AWS Transit Gateway](#)
- Le groupe de sécurité et le réseau VPC ACLs des 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.

#### FSx for ONTAP File Server port requirements

Configure VPC security groups that you've associated with your Amazon FSx file system, along with any VPC Network ACLs and ONTAP firewalls to allow network traffic on the following ports:



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, serveurs DNS, FSx clients et administrateurs Active Directory. 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 réseaux VPC ACLs 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, consultez [Délégation d'autorisations à votre compte de FSx service Amazon](#).

 Important

Amazon a FSx besoin d'un compte de service valide pendant toute la durée de vie de votre système de FSx fichiers Amazon. 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, consultez [Maintenance à jour de votre configuration Active Directory avec Amazon FSx](#).

Si c'est la première fois que vous utilisez AWS et FSx pour ONTAP, assurez-vous de suivre les étapes de configuration initiales avant de commencer votre intégration à Active Directory. Pour de plus amples informations, veuillez consulter [Configuration d' FSx ONTAP](#).

 Important

Ne déplacez pas les objets informatiques FSx créés par Amazon dans l'unité d'organisation après votre SVMs création, et ne supprimez pas votre Active Directory alors que votre SVM y est jointe. Cela entraînera une mauvaise configuration SVMs de votre ordinateur.

# Bonnes pratiques d'utilisation d'Active Directory

Voici quelques suggestions et directives à prendre en compte lorsque vous rejoignez Amazon FSx for NetApp ONTAP sur SVMs 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 FSx service Amazon

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 Amazon FSx SVMs 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 FSx pour rejoindre ONTAP SVMs 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 votre SVMs création. Cela entraînera une mauvaise configuration SVMs de votre ordinateur.

## Maintien à jour de votre configuration Active Directory avec Amazon FSx

Pour une disponibilité ininterrompue de votre Amazon FSx SVMs, 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 auprès d'Amazon FSx. Pour ce faire, utilisez la FSx console Amazon, FSx l'API Amazon 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 auprès d'Amazon dès que le changement se produit FSx.

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, veuillez 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 [Mise à jour des configurations SVM Active Directory existantes à l'aide de l' AWS Management Console API 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, consultez [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 FSx fichiers Amazon. Pour en savoir plus, consultez [Contrôle d'accès au système de fichiers avec Amazon VPC](#).

## Comment fonctionne SVMs l'adhésion à 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 vous connecter SVMs directement à votre domaine Active Directory existant de la manière suivante :

- Ajouter un nouveau membre SVMs à un Active Directory lors de sa création :
  - En utilisant l'option de création standard de FSx la console Amazon pour créer un nouveau système de fichiers FSx pour 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 FSx console Amazon ou de FSx l'API Amazon pour créer une nouvelle SVM sur un système de fichiers FSx pour ONTAP existant. AWS CLI Pour de plus amples informations, veuillez consulter [Création de machines virtuelles de stockage \(SVM\)](#).



- Rejoindre un SVMs fichier existant 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 celles SVMs qui sont 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 [Mise à jour des configurations Active Directory de la SVM à l'aide de la CLI NetApp](#).

#### Important

- Amazon enregistre les enregistrements DNS pour une SVM FSx 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 votre Amazon FSx SVMs après les avoir créées.
- Si vous l'utilisez AWS Managed Microsoft AD, vous devez spécifier un groupe tel que FSx les administrateurs 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 choisissiez :

- 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, FSx à utiliser par Amazon pour joindre la SVM au domaine Active Directory. Pour plus d'informations sur les exigences relatives aux comptes de service, consultez [Exigences 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 située dans l'unité d'organisation par défaut qui AWS Directory Service crée pour les objets de répertoire auxquels ils sont 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' FSx API AWS Management Console, AWS CLI, 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
- Suppression SVMs d'un Active Directory

Pour supprimer une SVM d'un Active Directory, vous devez utiliser la NetApp CLI ONTAP.

## Rubriques

- [Connexion SVMs à Active Directory à l'aide de AWS Management Console l'API AWS CLI et](#)
- [Mise à jour des configurations SVM Active Directory existantes à l'aide de l' AWS Management Console API AWS CLI,, et](#)
- [Mise à jour des configurations Active Directory de la SVM à l'aide de la CLI NetApp](#)

## Connexion SVMs à 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 FSx console Amazon 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 options disponibles SVMs, dans le volet de navigation de gauche, développez ONTAP et choisissez Machines virtuelles de stockage. Une liste de tous SVMs les éléments 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 : IPv4 adresses 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, pourEXAMPLE\ADMIN, utiliser uniquementADMIN.
  - 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 FSx les administrateurs 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 estDomain 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-machine](#) CLI (ou une opération [UpdateStorageVirtualMachine](#) API 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",
 "IpAddresses": ["198.19.0.4"]
 },
 "Nfs": {
```

```

 "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com",
 "IpAddresses": ["198.19.0.4"],
 },
 "Smb": {
 "DnsName": "amznfsx12345",
 "IpAddresses": ["198.19.0.4"],
 },
 "SmbWindowsInterVpc": {
 "IpAddresses": ["198.19.0.5", "198.19.0.6"],
 },
 "Iscsi": {
 "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com",
 "IpAddresses": ["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": [],
}
}

```

## Mise à jour des configurations SVM Active Directory existantes à l'aide de l'AWS Management Console API 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 FSx console Amazon 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 options SVMs 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 : IPv4 adresses 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-machine](#)CLI (ou une opération [UpdateStorageVirtualMachine](#)API 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"]'
```

## Mise à jour des configurations Active Directory de la 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 un répertoire existant SVMs 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 au ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

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
```

| Vserver  | Name Server   | Name Server<br>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-OU, entrez le nom OUs auquel 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 au ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

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
```

| Vserver  | Name Server | Status | Status Details          |
|----------|-------------|--------|-------------------------|
| svmciaad | dns_ip_1    | up     | Response time (msec): 1 |
| svmciaad | 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 :
  - *computer\_name*, 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 au ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

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.AEXAMPLE.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'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'entrée dns en modifiant les 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
```

# Migrer vers Amazon FSx pour ONTAP NetApp

Les sections suivantes fournissent des informations sur la façon de migrer vos systèmes de fichiers NetApp ONTAP existants vers Amazon FSx for NetApp 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 for ONTAP à l'aide de NetApp SnapMirror](#)
- [Migration vers FSx for ONTAP à l'aide de AWS DataSync](#)

## Migration vers FSx for ONTAP à l'aide de NetApp SnapMirror

Vous pouvez migrer vos systèmes de fichiers NetApp ONTAP vers Amazon FSx for NetApp 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

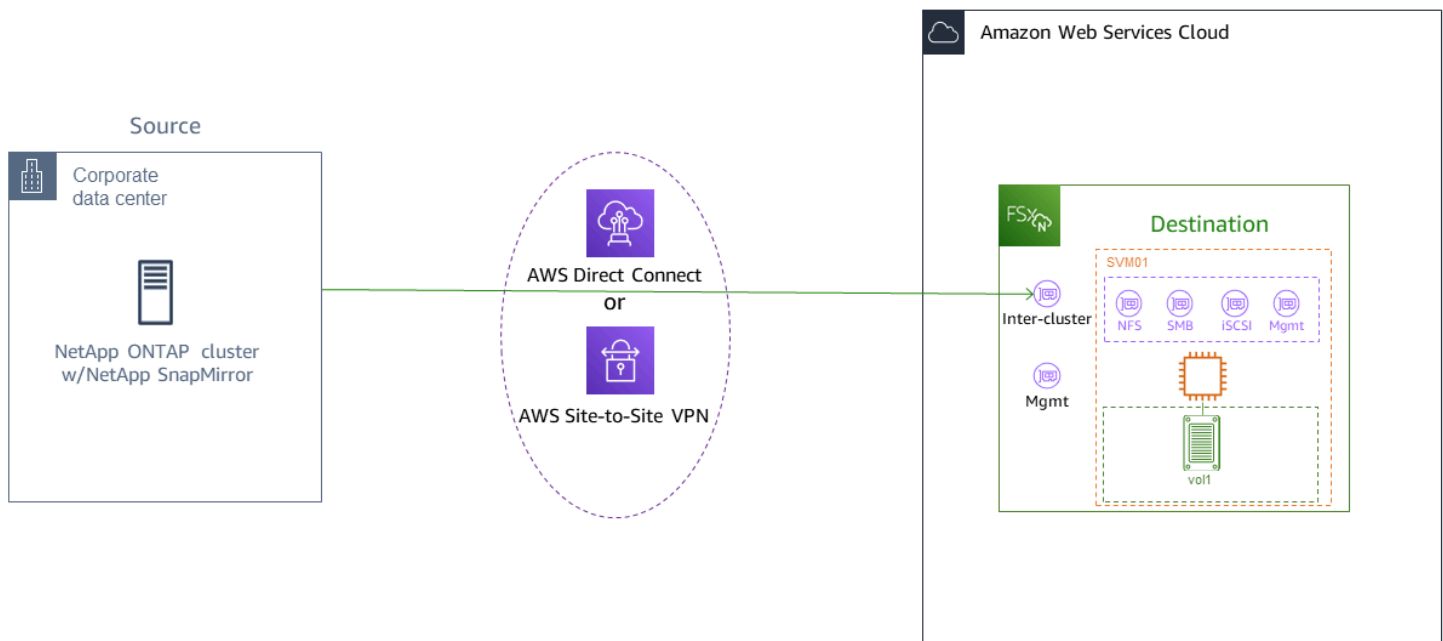
recommandons de l'utiliser SnapMirror pour migrer les systèmes de fichiers NetApp ONTAP sur site vers FSx ONTAP. NetApp SnapMirrorLa réplication au niveau des blocs est rapide et efficace, même pour les systèmes de fichiers dotés des caractéristiques suivantes :

- 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 ONTAP implique FSx les tâches de haut niveau suivantes :

1. Créez le volume de destination dans Amazon FSx.
2. Rassemblez les interfaces logiques source et destination (LIFs).
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 l'inter-cluster source et de destination LIFs](#)
- [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 FSx système de fichiers for ONTAP](#)
- [Passons 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 de plus amples informations, veuillez consulter [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 partir du principe d'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 le AWS Cloud](#) 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 l'ICMP ainsi que le TCP sur les ports 443, 10000, 11104 et 11105 pour vos points de terminaison inter-clusters (). LIFs
- 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 une destination FSx pour le système de fichiers ONTAP à l'aide d'une SVM, mais vous n'avez pas créé de volume de destination. Pour de plus amples informations, veuillez consulter [Création de systèmes de fichiers](#).

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 FSx IDABCDEF1234567890A).
- *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 vol11.

 Note

Un système de fichiers FSx pour 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 de plus amples informations, veuillez consulter [Utilisation de NetApp ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

## Créez le volume de destination

Vous pouvez créer un volume de destination pour la protection des données (DP) à l'aide de la FSx console Amazon, du AWS CLI, et de l' FSx API Amazon, en plus de la CLI NetApp ONTAP et de l'API REST. Pour plus d'informations sur la création d'un volume de destination à l'aide de FSx la console Amazon et AWS CLI consultez [Création de volumes](#).

 Note

ONTAP ne préserve pas les économies de compression après le traitement réalisées à la source dans le volume DP de destination lorsque la politique de hiérarchisation du volume de destination est définie. A11 Pour préserver les économies de compression après le traitement, vous devez définir la politique de hiérarchisation des volumes de destination inactive-data-compression sur le système de fichiers de destination Auto et autoriser le système de fichiers de destination à réappliquer les économies de compression après le traitement à la destination.

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 DPÀ 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 àauto.

#### 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 l'inter-cluster source et de destination LIFs

SnapMirror utilise des interfaces logiques inter-clusters (LIFs), chacune dotée d'une adresse IP unique, pour faciliter le transfert de données entre les clusters source et de destination.

1. Pour la destination FSx des systèmes de fichiers ONTAP, vous pouvez récupérer les adresses IP des points de terminaison inter-clusters depuis la FSx console Amazon 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<br>Vserver | Interface | Status | Network<br>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 mono-AZ de deuxième génération, 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 mono-AZ de deuxième génération, 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 mono-AZ de deuxième génération, 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 peering le. SVMs 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`— il s'agit du 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 la source et la destination de la SVM. SVMs

```
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'appariement 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 comparé la source et la destination SVMs, 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 FSx système de fichiers 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 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
```

## Passons 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 FSx de fichiers 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 Path | Destination Path | Mirror State | Relationship Status | Last Transfer End 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'utilisationsnapmirror show.

```
FSx-Dest::> snapmirror show
```

| Source Path     | Destination Path | Mirror State | Relationship 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, voir [Accès à vos données FSx for ONTAP](#).

## Migration vers FSx for ONTAP à l'aide de AWS DataSync

Nous vous recommandons de l'utiliser AWS DataSync FSx pour transférer des données entre des systèmes de fichiers ONTAP et des systèmes de fichiers non-ONTAP, notamment FSx pour Lustre, FSx pour OpenZFS, FSx pour Windows File Server, Amazon EFS, Amazon S3 et les serveurs de fichiers sur site. Si vous transférez des fichiers entre FSx for ONTAP et NetApp ONTAP, nous vous recommandons d'utiliser [NetApp SnapMirror](#). AWS DataSync est 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 ONTAP, et également FSx pour déplacer des données vers un système de fichiers appartenant à un autre AWS compte Région AWS OR. Vous pouvez également utiliser les systèmes de fichiers DataSync with 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 pour 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 MBps, une MBps accélération de 200 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 DataSync exigences. Pour en savoir plus, consultez la section [Conditions requises DataSync](#) dans le 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 deux Services 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 DataSync Guide de l'utilisateur :

- [Transfert de données entre le stockage autogéré et AWS](#)
- [Création d'un emplacement pour Amazon FSx pour NetApp ONTAP](#)

# Sécurité dans Amazon FSx pour NetApp ONTAP

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 pour NetApp ONTAP, consultez la section [AWS Services concernés par programme de conformitéAWS](#) .
- 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 pour répondre FSx 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 FSx ressources Amazon.

## Rubriques

- [Protection des données dans Amazon FSx pour NetApp ONTAP](#)
- [Gestion des identités et des accès pour Amazon FSx pour NetApp ONTAP](#)
- [AWS politiques gérées pour Amazon FSx pour OpenZFS](#)
- [Contrôle d'accès au système de fichiers avec Amazon VPC](#)
- [Validation de conformité pour Amazon FSx pour NetApp ONTAP](#)
- [Amazon FSx pour NetApp ONTAP et points de terminaison VPC d'interface \(\)AWS PrivateLink](#)
- [Résilience dans Amazon FSx pour NetApp ONTAP](#)
- [Sécurité de l'infrastructure dans Amazon FSx pour NetApp ONTAP](#)

- [Utiliser NetApp ONTAP Vscan avec FSx for ONTAP](#)
- [ONTAP rôles et utilisateurs](#)

## Protection des données dans Amazon FSx pour NetApp ONTAP

Le [modèle de responsabilité AWS partagée](#) s'applique à la protection des données dans Amazon FSx pour 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 sécurité AWS.

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.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section [Utilisation des CloudTrail sentiers](#) dans le guide de AWS CloudTrail l'utilisateur.
- 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 140-3 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 disponibles, consultez [Norme FIPS \(Federal Information Processing Standard\) 140-3](#).

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 Nom. Cela inclut lorsque vous travaillez avec Amazon FSx ou une autre entreprise Services AWS à l'aide de la console AWS CLI, de l'API ou AWS SDKs. 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 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 FSx fichiers Amazon. 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 protocole LDAP (Lightweight Directory Access Protocol).

### 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 pour NetApp ONTAP, consultez [Chiffrement de données au repos](#) et [chiffrement des données en transit](#).

## Chiffrement de données au repos

Tous les systèmes de fichiers et sauvegardes Amazon FSx for NetApp ONTAP sont chiffrés au repos à l'aide de clés gérées à l'aide de AWS Key Management Service (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. Toutes les sauvegardes sont automatiquement chiffrées lors de leur création et automatiquement déchiffrées lorsque la sauvegarde est restaurée sur un nouveau volume. Ces processus sont gérés de manière transparente par Amazon FSx, vous n'avez donc pas à modifier vos applications.

Amazon FSx utilise un algorithme de chiffrement AES-256 conforme aux normes du secteur pour chiffrer les FSx données et métadonnées Amazon 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 AWS KMS la gestion des clés. Amazon FSx utilise des clés KMS pour chiffrer votre système de fichiers et toutes les sauvegardes de volumes. Vous choisissez la clé KMS utilisée pour chiffrer et déchiffrer les systèmes de fichiers et les sauvegardes de volumes (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 quand 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 FSx clés d'Amazon 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 et les sauvegardes :

- 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 : GenerateDataKeyWithoutPlaintext — (Obligatoire) Renvoie une clé de chiffrement des données chiffrée sous une clé KMS. Cette autorisation est incluse dans la politique clé par défaut sous kms : GenerateDataKey \*.
- 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) Répertoire 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 FSx système de fichiers ONTAP et des 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 FSx systèmes de fichiers ONTAP et les clients connectés :

- Chiffrement automatique basé sur Nitro sur tous les protocoles et clients pris en charge s'exécutant sur les types d'instances Amazon EC2 [Linux](#) et [Windows](#) pris en charge.
- Chiffrement basé sur Kerberos via les protocoles NFS et SMB.
- IPsecchiffrement basé 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 grâce IPsec au chiffrement](#)
- [Activation du chiffrement des données en transit par les PME](#)
- [Configuration à IPsec l'aide de l'authentification PSK](#)
- [Configuration à IPsec 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 :

- Celui dans Région AWS le quel 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.
- Le protocole de données que vous souhaitez chiffrer.
- Si vous utilisez Microsoft Active Directory.

### Région AWS

Le système de fichiers dans Région AWS le quel s'exécute votre système de fichiers détermine si vous pouvez ou non utiliser le chiffrement basé sur Amazon Nitro. Pour de plus amples informations, veuillez consulter [Chiffrer les données en transit avec AWS Nitro System](#).

### Type d'instance client

Vous pouvez utiliser le chiffrement basé sur Amazon Nitro si le client accédant à votre système de fichiers fonctionne 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 Kerberos ou IPsec le chiffrement.

### 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 un environnement pair VPCs, 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 EC2 instances Amazon 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 de Kerberos ou du IPsec chiffrement 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.

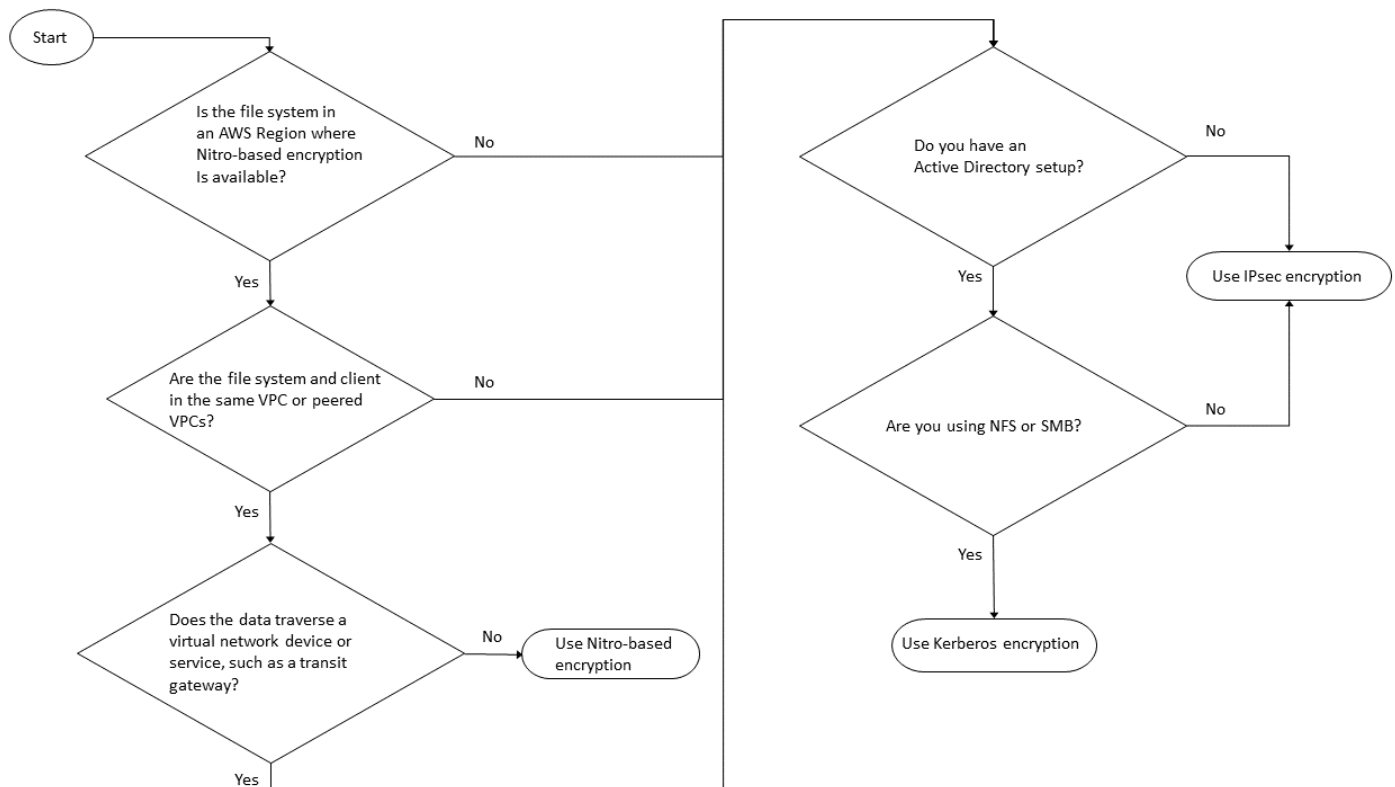
## Protocole de données

Vous pouvez utiliser le chiffrement et IPsec le chiffrement basés sur Amazon Nitro 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.



IPsec le chiffrement 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, Régions AWS là où elles sont disponibles sur ONTAP FSx .

L'utilisation du chiffrement basé sur Amazon Nitro n'a aucun impact sur les performances du réseau. Cela est dû au fait que les EC2 instances Amazon 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 EC2 l'utilisateur Amazon pour les types d'instances [Linux](#) ou [Windows](#).

Le tableau suivant indique dans quel format Régions AWS le chiffrement basé sur Nitro est disponible.

#### Support du chiffrement basé sur Nitro

| Génération                                    | Types de déploiement | Région AWS                                                                                                                                                    |
|-----------------------------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Systèmes de fichiers de première génération 1 | Mono-AZ 1 Multi-AZ 1 | USA Est (Virginie du Nord), USA Est (Ohio), USA Ouest (Oregon), Europe (Irlande)                                                                              |
| Systèmes de fichiers de deuxième génération   | Mono-AZ 2 Multi-AZ 2 | USA Est (Virginie du Nord), USA Est (Ohio), USA Ouest (Californie du Nord), USA Ouest (Oregon), Europe (Francfort), Europe (Irlande), Asie-Pacifique (Sydney) |

<sup>1</sup> Les systèmes de fichiers de première génération créés le 28 novembre 2022 ou après cette date prennent en charge le chiffrement en transit basé sur Nitro dans la liste. Régions AWS

Pour plus d'informations sur la disponibilité de Régions AWS Where FSx for ONTAP, consultez les tarifs [Amazon FSx for NetApp ONTAP](#).

Pour plus d'informations sur les spécifications de performance des systèmes FSx 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 basé sur Kerberos sur les protocoles NFS et SMB pour chiffrer les données en transit pour les volumes enfants qui [SVMs sont 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 pour NFSv3 et les protocoles. 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. Lorsque cette option est activée, 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 car ONTAP SMB prend en charge le chiffrement à 128 et 256 bits, 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 SMB FSx for ONTAP 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.

Vous utilisez la ONTAP CLI pour gérer le chiffrement dans les paramètres de transit FSx pour ONTAP SVMs et les volumes. 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. [Gérer SVMs avec le ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#)

Pour savoir comment activer le chiffrement SMB sur une SVM ou un volume, consultez. [Activation du chiffrement des données en transit par les PME](#)

## Chiffrement des données en transit grâce IPsec au chiffrement

FSx for ONTAP prend en charge l'utilisation IPsec du protocole en mode transport afin de garantir la sécurité et le chiffrement continu des données pendant leur transit. IPsec permet end-to-end le chiffrement des données en transit entre les clients et FSx pour les systèmes de fichiers ONTAP pour tout le trafic IP pris en charge (protocoles NFS, iSCSI et SMB). Avec IPsec le chiffrement, vous établissez un IPsec tunnel entre une SVM FSx pour ONTAP configurée avec IPsec Activé et un IPsec client exécuté sur le client connecté accédant aux données.

Nous vous recommandons de 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 n'est pas connecté à un Active Directory, ce qui est requis pour le chiffrement basé sur Kerberos. IPsec SVMs IPsec le chiffrement 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 IPsec l'authentification, vous pouvez utiliser des clés pré-partagées (PSKs) ou des certificats. Si vous utilisez un PSK, le IPsec client que vous utilisez doit prendre en charge Internet Key Exchange version 2 (IKEv2) avec un PSK. Les étapes de haut niveau pour configurer le IPsec chiffrement à la fois FSx pour ONTAP et pour le client sont les suivantes :

1. Activez et configurez IPsec sur votre système de fichiers.
2. Installation et configuration IPsec sur votre client
3. Configuration IPsec pour un accès client multiple

Pour plus d'informations sur la configuration à IPsec l'aide de PSK, voir [Configurer le chiffrement par fil de la sécurité IP \(IPsec\)](#) dans le centre de NetApp ONTAP documentation.

Pour plus d'informations sur la configuration à IPsec l'aide de certificats, consultez [Configuration à IPsec l'aide de l'authentification par certificat](#).

## Activation du 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 ONTAP CLI 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 ONTAP CLI :

```
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. [Gérer SVMs avec le ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#)
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 à IPsec l'aide de l'authentification PSK

Si vous utilisez PSK pour l'authentification, les étapes de configuration du IPsec chiffrement à la fois FSx pour ONTAP et pour le client sont les suivantes :

1. Activez et configurez IPsec sur votre système de fichiers.
2. Installation et configuration IPsec sur votre client
3. Configuration IPsec pour un accès client multiple

Pour plus de détails sur la configuration IPsec à l'aide de PSK, voir [Configurer la sécurité IP \(IPsec\) over wire encryption](#) dans le centre de NetApp ONTAP documentation.

## Configuration à IPsec l'aide de l'authentification par certificat

Les rubriques suivantes fournissent des instructions pour configurer le IPsec chiffrement à l'aide de l'authentification par certificat sur un système FSx de fichiers ONTAP et un client exécutant IPsec Libreswan. 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 IPsec chiffrement à l'aide de l'authentification par certificat activée 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-le IPsec sur l'instance cliente.
4. Installez le certificat et configurez-le 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 accéderont 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 racines et subordonnées (CAs) 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 [create-certificate-authority](#) AWS Private CA CLI pour créer une autorité de certification privée.

```
~/home > aws acm-pca create-certificate-authority \
 --certificate-authority-configuration file://ca_config.txt \
 --certificate-authority-type "R00T" \
 --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-----
MIICiCCAfICCQD6m7oRw0uX0jANBgkqhkiG9w0BAQUFADCBiDELMakGA1UEBhMC
VVMxCzAJBgNVBAGTAldBMRAwDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBA5TC0lBTSBDb25zb2x1MRIwEAYDVQQDEw1UZXRhbnQ21sYWMxH3Ad
BgkqhkiG9w0BCQEWEG5vb25lQGFTYXpvcjE5b20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI1MjA0NTIxWjCBiDELMakGA1UEBhMCVVMxCzAJBgNVBAGTAldBMRAwDgYD
VQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBA5TC0lBTSBDb25z
b2x1MRIwEAYDVQQDEw1UZXRhbnQ21sYWMxH3AdBgkqhkiG9w0BCQEWEG5vb25lQGFT
YXpvcjE5b20wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMak0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLygVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITx0USQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb30hjZnzcvcQAARHhd1QWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
```

```
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJI1J00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp3780D8uTs7fLvJx79LjSTb
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 EC2 instance Linux.

```
$ 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.

```
$ passphrase=$(cat passphrase.txt | base64)
cat exported_cert.json | jq -r .PrivateKey > prv.key

cat exported_cert.json | jq -r .Certificate > cert.pem
```

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 EC2 instance Amazon exécutant Amazon Linux 2.

Pour installer et configurer Libreswan

1. Connectez-vous à votre EC2 instance 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) IPsec Lors d'une vérification 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 IPsec configuration.



```
$ 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' EC2 instance. 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 IPsec de configuration 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 l'avoir configuré IPsec sur votre système de fichiers.

### Configuration 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 sa configuration 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 ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

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 CA utilisés lors de l'authentification mutuelle, y compris côté TAP et côté client, dans la gestion des certificats CAs, sauf s'ils sont déjà installés (comme c'est le cas d'une autorité de ONTAP 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 à utiliser par la SVM. L'autorité de certification émettrice de ce certificat doit déjà être installée ONTAP et ajoutée. 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'IPsec autorité de certification lors de l'authentification, ajoutez la gestion des ONTAP certificats au IPsec module CAs 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 IPsec politique 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 IPsec politique 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
```

Commencez par IPsec le client

Maintenant IPsec configuré à la fois sur le système FSx de fichiers ONTAP et sur le client, vous pouvez commencer par IPsec le client.

1. Connectez-vous à votre système client à l'aide de SSH.
2. Démarrez IPsec.

```
$ sudo ipsec start
```

3. Vérifiez le statut de 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 IPsec configuration 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
```

| Vserver | Policy Name        | Local Address | Remote Address | Initiator-SPI    | State       |
|---------|--------------------|---------------|----------------|------------------|-------------|
| dr      | <i>policy-name</i> | 198.19.254.13 | 172.31.77.6    | 551c55de57fe8976 | ESTABLISHED |
| fsx     | <i>policy-name</i> | 198.19.254.38 | 172.31.65.193  | 4fd3f22c993e60c5 | ESTABLISHED |

2 entries were displayed.

### Configuration IPsec pour plusieurs clients

Lorsqu'un petit nombre de clients ont besoin d'un effet de levier IPsec, il suffit d'utiliser une seule entrée SPD pour chaque client. Toutefois, lorsque des centaines, voire des milliers de clients ont besoin d'en tirer parti IPsec, nous vous recommandons d'utiliser une configuration client IPsec multiple.

FSx for ONTAP permet de connecter plusieurs clients sur de nombreux réseaux à une seule adresse IP SVM lorsque cette option est activée. IPsec 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**

Lors de 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 du certificat CAs installé sur son trust store local. FSx for ONTAP prend également en charge la vérification des listes de révocation de certificats (CRL).

1. Pour accéder à la ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

2. Utilisez la commande `security ipsec policy create` NetApp ONTAP CLI comme suit, en remplaçant les *sample* valeurs 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 IPsec activée par la SVM, utilisez le caractère générique `0.0.0.0/0` lorsque vous spécifiez le `remote-ip-subnets` champ.

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 ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

2. Utilisez la commande `security ipsec policy create` NetApp ONTAP CLI comme suit, en remplaçant les *sample* valeurs 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 pour NetApp ONTAP

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](#)
- [Authentification par des identités](#)
- [Gestion des accès à l'aide de politiques](#)
- [Comment Amazon FSx pour NetApp ONTAP fonctionne avec IAM](#)
- [Exemples de politiques basées sur l'identité pour Amazon FSx pour ONTAP NetApp](#)
- [Résolution des problèmes d'identité et d'accès à Amazon FSx for NetApp ONTAP](#)
- [Utilisation de rôles liés à un service pour Amazon FSx](#)

- [Utiliser des tags avec Amazon FSx](#)

## Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez sur Amazon FSx.

Utilisateur du service — Si vous utilisez le FSx service Amazon 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 FSx fonctionnalités Amazon dans le cadre de 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 parvenez pas à accéder à une fonctionnalité d'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 FSx ressources Amazon au sein de votre entreprise, vous avez probablement un accès complet à Amazon FSx. C'est à vous de déterminer à quelles FSx fonctionnalités et ressources Amazon les utilisateurs de vos services 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 souhaitez 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 FSx basées sur l'identité Amazon que vous pouvez utiliser dans IAM, consultez. [Exemples de politiques basées sur l'identité pour Amazon FSx pour 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 des demandes vous-même, consultez [AWS Signature Version 4 pour les demandes 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 plus d'informations, consultez [Authentification multifactorielle](#) dans le Guide de l'utilisateur AWS IAM Identity Center et [Authentification multifactorielle AWS dans IAM](#) 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 racine, consultez [Tâches nécessitant des informations d'identification d'utilisateur racine](#) 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 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 telles que des mots de passe et des 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 d'effectuer une rotation des 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 nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer les 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 plus d'informations, consultez [Cas d'utilisation pour les utilisateurs IAM](#) dans le Guide de l'utilisateur IAM.

## Rôles IAM

Un [rôle IAM](#) est une identité au sein de votre 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. Pour assumer temporairement un rôle IAM dans le AWS Management Console, vous pouvez [passer d'un rôle d'utilisateur à un rôle IAM \(console\)](#). 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 [Méthodes pour endosser un rôle](#) 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 [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 [Accès intercompte aux ressources dans IAM](#) 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 une politique lors de la formulation de demandes FAS, consultez [Transmission des sessions 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 un rôle de 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 EC2 instance et qui envoient des demandes AWS CLI d' AWS API. Cela est préférable au stockage des clés d'accès dans l' EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour 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 exécutés sur l' EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez [Utiliser un rôle IAM pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon](#) 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 [Définition d'autorisations IAM personnalisées avec des politiques gérées par le client](#) 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. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. 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 (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et AWS WAF Amazon VPC sont des exemples de services compatibles. ACLs Pour en savoir plus ACLs, consultez la [présentation de la liste 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 annule 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 (SCPs)** : SCPs 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 des politiques de contrôle des services (SCPs) 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 Organizations et consultez SCPs les [politiques de contrôle des services](#) dans le Guide de AWS Organizations l'utilisateur.

- **Politiques de contrôle des ressources (RCPs) :** RCPs politiques JSON que vous pouvez utiliser pour définir le maximum d'autorisations disponibles pour les ressources de vos comptes sans mettre à jour les politiques IAM associées à chaque ressource que vous possédez. Le RCP limite les autorisations pour les ressources des comptes membres et peut avoir un impact sur les autorisations effectives pour les identités, y compris Utilisateur racine d'un compte AWS, qu'elles appartiennent ou non à votre organisation. Pour plus d'informations sur les Organizations RCPs, y compris une liste de ces Services AWS supports RCPs, consultez la section [Resource control policies \(RCPs\)](#) dans le guide de AWS Organizations l'utilisateur.
- **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 session](#) 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 FSx pour ONTAP NetApp

| Fonctionnalité IAM                               | FSx Assistance Amazon |
|--------------------------------------------------|-----------------------|
| <a href="#">Politiques basées sur l'identité</a> | Oui                   |



| Fonctionnalité IAM                                        | FSx Assistance Amazon |
|-----------------------------------------------------------|-----------------------|
| <a href="#">Politiques basées sur les ressources</a>      | Non                   |
| <a href="#">Actions de politique</a>                      | Oui                   |
| <a href="#">Ressources de politique</a>                   | Oui                   |
| <a href="#">Clés de condition de politique</a>            | Oui                   |
| <a href="#">ACLs</a>                                      | Non                   |
| <a href="#">ABAC (étiquettes dans les politiques)</a>     | Oui                   |
| <a href="#">Informations d'identification temporaires</a> | Oui                   |
| <a href="#">Transmission des sessions d'accès (FAS)</a>   | Oui                   |
| <a href="#">Fonctions du service</a>                      | Non                   |
| <a href="#">Rôles liés à un service</a>                   | 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 [Définition d'autorisations IAM personnalisées avec des politiques gérées par le client](#) 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 FSx basées sur l'identité d'Amazon, consultez. [Exemples de politiques basées sur l'identité pour Amazon FSx pour 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 politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des FSx actions Amazon, consultez la section [Actions définies par Amazon FSx](#) dans le Service Authorization Reference.

Les actions politiques sur 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 FSx basées sur l'identité d'Amazon, consultez. [Exemples de politiques basées sur l'identité pour Amazon FSx pour 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 FSx ressources Amazon et leurs caractéristiques ARNs, 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 FSx basées sur l'identité d'Amazon, consultez. [Exemples de politiques basées sur l'identité pour Amazon FSx pour ONTAP NetApp](#)

## Clés relatives aux 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 FSx condition Amazon, 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 FSx basées sur l'identité d'Amazon, consultez. [Exemples de politiques basées sur l'identité pour Amazon FSx pour ONTAP NetApp](#)

## Listes de contrôle d'accès (ACLs) sur Amazon FSx

Supports ACLs : Non

## Contrôle d'accès basé sur les attributs (ABAC) avec Amazon FSx

Prise en charge d'ABAC (balises 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 ABAC, consultez [Définition d'autorisations avec l'autorisation 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 FSx ressources Amazon, consultez [Marquer les 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 FSx ressources Amazon](#).

## 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 [Passage d'un rôle utilisateur à un rôle IAM \(console\)](#) 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 rôles de service : Non

## Rôles liés à un service pour Amazon FSx

Prend en charge les rôles liés aux services : 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 en savoir plus sur la création ou la gestion des rôles FSx liés aux services Amazon, consultez.

[Utilisation de rôles liés à un service pour Amazon FSx](#)

## Exemples de politiques basées sur l'identité pour Amazon FSx pour ONTAP NetApp

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier FSx des ressources Amazon. 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 IAM \(console\)](#) 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 ARNs de chaque type de ressource, 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 FSx console Amazon](#)
- [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 FSx des ressources Amazon 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.

- Accordez 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 d'IAM pour appliquer des autorisations, consultez [politiques et autorisations dans IAM](#) dans le Guide de l'utilisateur IAM.
- Utilisez 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 l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM 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 politiques avec 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 la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez [Sécurisation de l'accès aux API avec 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 FSx console Amazon

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 FSx ressources Amazon présentes dans votre Compte AWS. Si vous

créez une politique 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 politique.

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 FSx console Amazon, 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 relatives `AmazonFSxConsoleReadOnlyAccess` aux services FSx gérés d'Amazon et les autres dans [AWS politiques gérées pour Amazon FSx pour OpenZFS](#).

## 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 sur Amazon FSx](#)
- [Je ne suis pas autorisé à effectuer iam : PassRole](#)
- [Je souhaite autoriser des personnes extérieures Compte AWS à moi à accéder à mes FSx ressources Amazon](#)

### Je ne suis pas autorisé à effectuer une action sur 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 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 sur 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 Compte AWS à moi à accéder à mes FSx ressources Amazon

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 (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, 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 en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.

## Utilisation de rôles liés à un service pour Amazon FSx

Amazon FSx utilise des rôles AWS Identity and Access Management liés à un [service](#) (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à Amazon. FSx Les rôles liés au 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 FSx ressources Amazon, 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 FSx ServiceRolePolicy](#).

Détails de l'autorisation

Détails de l'autorisation

Les autorisations de `AWSServiceRoleForAmazonFSx` sont définies par la politique `FSxServiceRolePolicy` AWS gérée par Amazon. `AWSServiceRoleForAmazonFSx` dispose des autorisations suivantes :

### Note

`AWSServiceRoleForAmazonFSx` est utilisé par tous les types de systèmes de FSx fichiers Amazon ; certaines des autorisations répertoriées ne s'appliquent pas FSx à ONTAP.

- `ds`— Permet FSx à Amazon de consulter, d'autoriser et d'annuler les applications de votre AWS Directory Service annuaire.
- `ec2`— Permet FSx à Amazon d'effectuer les opérations suivantes :
  - Affichez, créez et dissociez les interfaces réseau associées à un système de FSx fichiers Amazon.
  - Affichez une ou plusieurs adresses IP élastiques associées à un système de FSx fichiers Amazon.
  - Affichez Amazon VPCs, les groupes de sécurité et les sous-réseaux associés à un système de FSx fichiers Amazon.
  - 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 FSx à Amazon de publier des points de données métriques CloudWatch sous l'espace de FSx noms AWS/.

- **route53**— Permet FSx à Amazon d'associer un Amazon VPC à une zone hébergée privée.

```
{
 "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"
 }
 }
 }
]
```

Toute mise à jour de cette politique est décrite dans [Amazon FSx met à jour AWS ses politiques gérées](#).

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 IAM CLI 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 au service pour vous.

## Modification d'un rôle lié à un service pour Amazon FSx

Amazon FSx ne vous autorise pas à modifier le rôle AWSService RoleForAmazon FSx lié au 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 FSx service Amazon 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, l'interface de ligne de commande IAM ou l'API IAM pour supprimer le rôle lié à un service `AWSServiceRoleForAmazonFSx`. 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 FSx liés aux services Amazon

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](#).

## Utiliser des tags avec Amazon FSx

Vous pouvez utiliser des balises pour contrôler l'accès aux FSx ressources Amazon et pour implémenter le contrôle d'accès basé sur les attributs (ABAC). Pour appliquer des balises aux FSx ressources Amazon 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' FSx API Amazon 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'action `fsx:TagResource` 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 (SVMs) 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'action `fsx:TagResource` 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'action `fsx:TagResource` 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 FSx ressources Amazon, consultez [Marquer les ressources Amazon FSx](#). Pour plus d'informations sur l'utilisation de balises pour contrôler l'accès aux FSx ressources Amazon, consultez [Utilisation de balises pour contrôler l'accès à vos FSx ressources Amazon](#).

## Utilisation de balises pour contrôler l'accès à vos FSx ressources Amazon

Pour contrôler l'accès aux FSx ressources et aux actions Amazon, vous pouvez utiliser des politiques IAM basées sur des balises. Vous pouvez fournir le contrôle de deux manières :

- Vous pouvez contrôler l'accès aux FSx ressources Amazon 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 FSx ressources Amazon 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 [Marquer les 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 FSx ressource Amazon, 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.

#### Exemple 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"
 }
 }
}
```

#### Exemple 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 FSx pour les volumes ONTAP marqués avec la paire clé-valeur, `key=Department value=Finance`. La sauvegarde est créée avec le `tagDepartment=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"
 }
 }
 }
]
}

```

Exemple 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"
 }
 }
 }
]
}

```

### Exemple 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"
 }
 }
}
]
}

```

### Exemple 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"
 }
}
]
```

## AWS politiques gérées pour Amazon FSx pour OpenZFS

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 politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez [Politiques gérées par AWS](#) dans le Guide de l'utilisateur IAM.

### Amazon FSx ServiceRolePolicy

Permet FSx à Amazon 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 : Amazon FSx DeleteServiceLinkedRoleAccess

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 de plus amples informations, veuillez consulter [Utilisation de rôles liés à un service pour Amazon FSx](#).

Cette politique accorde des autorisations administratives qui permettent FSx à Amazon de supprimer son rôle lié au service pour l'accès à Amazon S3, utilisé uniquement par Amazon FSx pour Lustre.

#### Détails de l'autorisation

Cette politique inclut des autorisations permettant iam FSx à Amazon de consulter, de supprimer et de consulter le statut de suppression des rôles liés au FSx service pour l'accès à Amazon S3.

Pour consulter les autorisations associées à cette politique, consultez [Amazon FSx DeleteServiceLinkedRoleAccess](#) dans le AWS Managed Policy Reference Guide.

## AWS politique gérée : Amazon FSx FullAccess

Vous pouvez associer Amazon FSx FullAccess à vos entités IAM. Amazon associe FSx également cette politique à un rôle de service qui permet FSx à Amazon d'effectuer des actions en votre nom.

Fournit un accès complet à Amazon FSx et aux AWS services associés.

#### Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `fsx`— Permet aux principaux un accès complet pour effectuer toutes les FSx actions Amazon, à l'exception `BypassSnaplockEnterpriseRetention` de.
- `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 à un FSx service Amazon au nom de l'utilisateur. Cela est nécessaire pour qu'Amazon FSx puisse gérer les AWS ressources au nom de l'utilisateur.
- `firehose`— Permet aux directeurs d'écrire des enregistrements sur un Amazon Data Firehose. Cela est nécessaire FSx pour que les utilisateurs puissent surveiller l'accès au système de fichiers Windows File Server en envoyant des journaux d'accès d'audit à Firehose.
- `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 FSx pour que les utilisateurs puissent surveiller l'accès au système de fichiers Windows File Server en envoyant les journaux d'accès aux audits à CloudWatch Logs.



Pour consulter les autorisations associées à cette politique, consultez [Amazon FSx FullAccess](#) dans le AWS Managed Policy Reference Guide.

## AWS politique gérée : Amazon FSx ConsoleFullAccess

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 FSx gestion Amazon, à l'exception `BypassSnaplockEnterpriseRetention` de.
- `cloudwatch`— Permet aux principaux de consulter les CloudWatch alarmes et les statistiques dans la console FSx de gestion Amazon.
- `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.
  - Permet aux principaux de visualiser les interfaces réseau élastiques associées à un système de FSx fichiers Amazon.
- `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 FSx à Amazon d'effectuer des actions au nom de l'utilisateur.

Pour consulter les autorisations associées à cette politique, consultez [Amazon FSx ConsoleFullAccess](#) dans le AWS Managed Policy Reference Guide.

## AWS politique gérée : Amazon FSx ConsoleReadOnlyAccess

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 FSx fichiers Amazon, y compris toutes les balises, dans l'Amazon FSx Management Console.
- `cloudwatch`— Permet aux principaux de consulter les CloudWatch alarmes et les statistiques dans l'Amazon FSx Management Console.
- `ds`— Permet aux principaux de consulter les informations relatives à un AWS Directory Service annuaire dans Amazon FSx Management Console.
- `ec2`
  - Permet aux principaux de visualiser les interfaces réseau, les groupes de sécurité, les sous-réseaux et le VPC associé à un système de FSx fichiers Amazon dans l'Amazon Management Console. 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.
  - Permet aux principaux de visualiser les interfaces réseau élastiques associées à un système de FSx fichiers Amazon.
- `kms`— Permet aux principaux de consulter les alias des AWS Key Management Service clés dans l'Amazon FSx Management Console.
- `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 FSx pour un système de fichiers 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 FSx pour un système de fichiers Windows File Server.

Pour consulter les autorisations associées à cette politique, consultez [Amazon FSx ConsoleReadOnlyAccess](#) dans le AWS Managed Policy Reference Guide.

## AWS politique gérée : Amazon FSx ReadOnlyAccess

Vous pouvez associer la politique AmazonFSxReadOnlyAccess à vos identités IAM.

- `fsx`— Permet aux principaux de consulter les informations relatives aux systèmes de FSx fichiers Amazon, y compris toutes les balises, dans l'Amazon FSx Management Console.
- `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 [Amazon FSx ReadOnlyAccess](#) dans le AWS Managed Policy Reference Guide.

## Amazon FSx met à jour AWS ses politiques gérées

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 FSx [Historique du document pour Amazon FSx pour NetApp ONTAP](#) page Amazon.

| Modification                                                                         | Description                                                                                                                                                             | Date          |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Mise à jour d'une politique existante | Amazon FSx a ajouté une nouvelle autorisation, <code>fsx:CreateAndAttachS3AccessPoint</code> qui permet aux principaux de créer un S3 et de l'attacher à un FSx volume. | 14 avril 2025 |

| Modification                                                                         | Description                                                                                                                                                                         | Date          |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Mise à jour d'une politique existante | Amazon FSx a ajouté une nouvelle autorisation, <code>fsx:DescribeS3AccessPointAttachments</code> qui permet aux principaux de répertorier tous les S3 Compte AWS dans un Région AWS | 14 avril 2025 |
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Mise à jour d'une politique existante | Amazon FSx a ajouté une nouvelle autorisation, <code>fsx:UpdateS3AccessPointAttachments</code> qui permet aux principaux de modifier un S3 existant.                                | 14 avril 2025 |
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Mise à jour d'une politique existante | Amazon FSx a ajouté une nouvelle autorisation, <code>fsx:DetachAndDeleteS3AccessPoint</code> qui permet aux principaux de supprimer un S3.                                          | 14 avril 2025 |
| <a href="#">Amazon FSx FullAccess</a> — Mise à jour d'une politique existante        | Amazon FSx a ajouté une nouvelle autorisation, <code>fsx&gt;CreateAndAttachS3AccessPoint</code> qui permet aux principaux de créer un S3 et de l'attacher à un FSx volume.          | 14 avril 2025 |

| Modification                                                                             | Description                                                                                                                                                                                             | Date            |
|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <a href="#">Amazon FSx FullAccess</a> — Mise à jour d'une politique existante            | Amazon FSx a ajouté une nouvelle autorisation, <code>fsx:DescribeS3AccessPointAttachments</code> qui permet aux principaux de répertorier tous les S3 Compte AWS dans un Région AWS                     | 14 avril 2025   |
| <a href="#">Amazon FSx FullAccess</a> — Mise à jour d'une politique existante            | Amazon FSx a ajouté une nouvelle autorisation, <code>fsx:UpdateS3AccessPointAttachments</code> qui permet aux principaux de modifier un S3 existant.                                                    | 14 avril 2025   |
| <a href="#">Amazon FSx FullAccess</a> — Mise à jour d'une politique existante            | Amazon FSx a ajouté une nouvelle autorisation, <code>fsx:DetachAndDeleteS3AccessPoint</code> qui permet aux principaux de supprimer un S3.                                                              | 14 avril 2025   |
| <a href="#">Amazon FSx ConsoleReadOnlyAccess</a> — Mise à jour d'une politique existante | Amazon FSx a ajouté une nouvelle autorisation, <code>ec2:DescribeNetworkInterfaces</code> qui permet aux principaux de consulter les interfaces réseau élastiques associées à leur système de fichiers. | 25 février 2025 |

| Modification                                                                         | Description                                                                                                                                                                                                                                      | Date            |
|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Mise à jour d'une politique existante | Amazon FSx a ajouté une nouvelle autorisation, <code>ec2:DescribeNetworkInterfaces</code> qui permet aux principaux de consulter les interfaces réseau élastiques associées à leur système de fichiers.                                          | 07 février 2025 |
| <a href="#">Amazon FSx ServiceRolePolicy</a> — Mise à jour d'une politique existante | Amazon FSx a ajouté une nouvelle autorisation, <code>ec2:GetSecurityGroupsForVpc</code> 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  |
| <a href="#">Amazon FSx ReadOnlyAccess</a> — Mise à jour d'une politique existante    | Amazon FSx a ajouté une nouvelle autorisation, <code>ec2:GetSecurityGroupsForVpc</code> 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           |
|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <a href="#">Amazon FSx ConsoleReadOnlyAccess</a> — Mise à jour d'une politique existante | Amazon FSx a ajouté une nouvelle autorisation, <code>ec2:GetSecurityGroupsForVpc</code> 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 |
| <a href="#">Amazon FSx FullAccess</a> — Mise à jour d'une politique existante            | Amazon FSx a ajouté une nouvelle autorisation, <code>ec2:GetSecurityGroupsForVpc</code> 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 |
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Mise à jour d'une politique existante     | Amazon FSx a ajouté une nouvelle autorisation, <code>ec2:GetSecurityGroupsForVpc</code> 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             |
|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| <a href="#">Amazon FSx FullAccess</a> — 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 FSx pour les systèmes de fichiers OpenZFS. | 20 décembre 2023 |
| <a href="#">Amazon FSx ConsoleFullAccess</a> — 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 FSx pour les systèmes de fichiers OpenZFS. | 20 décembre 2023 |
| <a href="#">Amazon FSx FullAccess</a> — 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 FSx pour les systèmes de fichiers OpenZFS.                       | 26 novembre 2023 |
| <a href="#">Amazon FSx ConsoleFullAccess</a> — 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 FSx pour les systèmes de fichiers OpenZFS.                       | 26 novembre 2023 |



| Modification                                                                                               | Description                                                                                                                                                                                    | Date             |
|------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| <a href="#">Amazon FSx FullAccess</a> — 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 FSx pour les systèmes de fichiers ONTAP Multi-AZ. | 14 novembre 2023 |
| <a href="#">Amazon FSx ConsoleFullAccess</a> — 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 FSx pour les systèmes de fichiers ONTAP Multi-AZ. | 14 novembre 2023 |
| <a href="#">Amazon FSx FullAccess</a> — Mise à jour d'une politique existante                              | Amazon FSx a ajouté de nouvelles autorisations pour permettre FSx à Amazon de gérer les configurations réseau FSx pour les systèmes de fichiers OpenZFS Multi-AZ.                              | 9 août 2023      |
| <a href="#">AWS politique gérée : Amazon FSx ServiceRolePolicy</a> — Mise à jour d'une politique existante | Amazon a FSx modifié l' <code>cloudwatch:PutMetricData</code> autorisation existante afin qu'Amazon FSx publie CloudWatch les métriques dans l'espace de AWS/FSx noms.                         | 24 juillet 2023  |

| Modification                                                                             | Description                                                                                                                                                                                                                                        | Date              |
|------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| <a href="#">Amazon FSx FullAccess</a> — Mise à jour d'une politique existante            | Amazon a FSx mis à jour la politique afin de supprimer l'fsx : *autorisation et d'ajouter des fsx actions spécifiques.                                                                                                                             | 13 juillet 2023   |
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Mise à jour d'une politique existante     | Amazon a FSx mis à jour la politique afin de supprimer l'fsx : *autorisation et d'ajouter des fsx actions spécifiques.                                                                                                                             | 13 juillet 2023   |
| <a href="#">Amazon FSx ConsoleReadOnlyAccess</a> — 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 FSx pour les systèmes de fichiers Windows File Server dans la FSx console Amazon. | 21 septembre 2022 |
| <a href="#">Amazon FSx ConsoleFullAccess</a> — 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 FSx pour les systèmes de fichiers Windows File Server dans la FSx console Amazon. | 21 septembre 2022 |

| Modification                                                                                | Description                                                                                                                                                              | Date             |
|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| <a href="#">Amazon FSx ReadOnlyAccess</a> — Politique de suivi mise en place                | Cette politique accorde un accès en lecture seule à toutes les FSx ressources Amazon et à tous les tags qui leur sont associés.                                          | 4 février 2022   |
| <a href="#">Amazon FSx DeleteServiceLinkedRoleAccess</a> — Politique de suivi mise en place | Cette politique accorde des autorisations administratives qui permettent FSx à Amazon de supprimer son rôle lié au service pour accéder à Amazon S3.                     | 7 janvier 2022   |
| <a href="#">Amazon FSx ServiceRolePolicy</a> — Mise à jour d'une politique existante        | Amazon FSx a ajouté de nouvelles autorisations pour permettre FSx à Amazon de gérer les configurations réseau pour les systèmes de fichiers Amazon FSx for NetApp ONTAP. | 2 septembre 2021 |
| <a href="#">Amazon FSx FullAccess</a> — Mise à jour d'une politique existante               | Amazon FSx a ajouté de nouvelles autorisations pour permettre FSx à Amazon de créer des balises sur les tables de EC2 routage pour les appels délimités.                 | 2 septembre 2021 |
| <a href="#">Amazon FSx ConsoleFullAccess</a> — 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 NetApp ONTAP.                      | 2 septembre 2021 |

| Modification                                                                                             | Description                                                                                                                                                                                                                                                                                                                                               | Date             |
|----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| <a href="#">Amazon FSx ConsoleFu</a><br><a href="#">llAccess</a> — Mise à jour d'une politique existante | Amazon FSx a ajouté de nouvelles autorisations pour permettre FSx à Amazon de créer des balises sur les tables de EC2 routage pour les appels délimités.                                                                                                                                                                                                  | 2 septembre 2021 |
| <a href="#">Amazon FSx ServiceRo</a><br><a href="#">lePolicy</a> — Mise à jour d'une politique existante | Amazon FSx a ajouté de nouvelles autorisations pour permettre FSx à Amazon de décrire et d'écrire dans les flux de CloudWatch journaux Logs.<br><br>Cela est nécessaire pour que les utilisateurs puissent consulter les journaux d'audit d'accès aux fichiers FSx pour les systèmes de fichiers Windows File Server à l'aide CloudWatch des journaux.    | 8 juin 2021      |
| <a href="#">Amazon FSx ServiceRo</a><br><a href="#">lePolicy</a> — Mise à jour d'une politique existante | Amazon FSx a ajouté de nouvelles autorisations pour permettre FSx à Amazon de décrire et d'écrire dans les flux de diffusion Amazon Data Firehose.<br><br>Cela est nécessaire pour que les utilisateurs puissent consulter les journaux d'audit d'accès aux fichiers FSx pour un système de fichiers Windows File Server à l'aide d'Amazon Data Firehose. | 8 juin 2021      |

| Modification                                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                     | Date        |
|----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| <a href="#">Amazon FSx FullAccess</a> —<br>Mise à jour d'une politique existante | <p>Amazon FSx a ajouté de nouvelles autorisations pour permettre aux principaux de décrire et de créer des journaux, des groupes de CloudWatch journaux, des flux de journaux et d'écrire des événements dans des flux de journaux.</p> <p>Cela est nécessaire pour que les principaux puissent consulter les journaux d'audit d'accès aux fichiers FSx pour les systèmes de fichiers Windows File Server à l'aide des CloudWatch journaux.</p> | 8 juin 2021 |
| <a href="#">Amazon FSx FullAccess</a> —<br>Mise à jour d'une politique existante | <p>Amazon FSx a ajouté de nouvelles autorisations pour permettre aux principaux de décrire et d'écrire des enregistrements sur un Amazon Data Firehose.</p> <p>Cela est nécessaire pour que les utilisateurs puissent consulter les journaux d'audit d'accès aux fichiers FSx pour un système de fichiers Windows File Server à l'aide d'Amazon Data Firehose.</p>                                                                              | 8 juin 2021 |

| Modification                                                                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                  | Date        |
|----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| <a href="#">Amazon FSx ConsoleFu</a><br><a href="#">llAccess</a> — Mise à jour d'une politique existante | <p>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.</p> <p>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 FSx pour un système de fichiers Windows File Server.</p> | 8 juin 2021 |
| <a href="#">Amazon FSx ConsoleFu</a><br><a href="#">llAccess</a> — Mise à jour d'une politique existante | <p>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.</p> <p>Cela est nécessaire pour que les principaux puissent choisir un flux de diffusion Firehose existant lors de la configuration de l'audit d'accès aux fichiers pour FSx un système de fichiers Windows File Server.</p>             | 8 juin 2021 |

| Modification                                                                              | Description                                                                                                                                                                                                                                                                                                                                                                    | Date        |
|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| <a href="#">Amazon FSx ConsoleRe adOnlyAccess</a> — Mise à jour d'une politique existante | <p>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.</p> <p>Cela est nécessaire pour que les principaux puissent consulter la configuration d'audit d'accès aux fichiers existante FSx pour un système de fichiers Windows File Server.</p> | 8 juin 2021 |
| <a href="#">Amazon FSx ConsoleRe adOnlyAccess</a> — Mise à jour d'une politique existante | <p>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.</p> <p>Cela est nécessaire pour que les principaux puissent consulter la configuration d'audit d'accès aux fichiers existante FSx pour un système de fichiers Windows File Server.</p>     | 8 juin 2021 |

| Modification                                     | Description                                                                             | Date        |
|--------------------------------------------------|-----------------------------------------------------------------------------------------|-------------|
| Amazon FSx a commencé à suivre les modifications | Amazon FSx a commencé à suivre les modifications apportées AWS à ses politiques gérées. | 8 juin 2021 |

## Contrôle d'accès au système de fichiers avec Amazon VPC

Vous accédez à vos systèmes de fichiers Amazon FSx for NetApp ONTAP SVMs 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 des règles à chaque groupe de sécurité qui autorisent le trafic à destination ou en provenance de ses systèmes de fichiers associés et SVMs. 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 FSx fichiers Amazon, ajoutez des règles entrantes et sortantes. 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 FSx fichiers de votre système de fichiers Amazon 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 EC2 l'utilisateur Amazon.

## Création d'un groupe de sécurité VPC

Pour créer un groupe de sécurité pour Amazon FSx

1. Ouvrez la EC2 console Amazon 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 ou and/or macOS qui accèdent aux données de votre système de fichiers via NFS, SMB ou iSCSI.
  - Tout fichier ONTAP systems/clusters que vous allez associer à votre système de fichiers (par exemple, pour utiliser SnapMirror SnapVault, ou FlexCache).
  - Tous les clients que vous utiliserez pour accéder à l'API ONTAP REST, à la CLI ou ZAPIs (par exemple, une Harvest/Grafana instance, un NetApp connecteur ou NetApp BlueXP).

| 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 via 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 d'un intercluster LIFs                                       |
| 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 inbound/outbound règles.

## Validation de conformité pour Amazon FSx pour NetApp ONTAP

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 :

- [Conformité et gouvernance de la sécurité](#) : ces guides de mise en œuvre de solutions traitent des considérations architecturales et fournissent les étapes à suivre afin de déployer des fonctionnalités de sécurité et de conformité.
- [Référence des services éligibles HIPAA](#) : liste les services éligibles HIPAA. Tous ne Services AWS sont pas éligibles à la loi HIPAA.
- 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 qu'il utilise un point de terminaison VPC d'interface. Les points de terminaison VPC d'interface sont alimentés par [AWS PrivateLink](#) une technologie qui vous permet d'accéder à Amazon en privé FSx APIs sans passerelle Internet, appareil NAT, connexion VPN ou connexion. AWS Direct Connect Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec Amazon. FSx APIs Le trafic entre votre VPC et Amazon FSx ne quitte pas le AWS réseau.

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' FSx API Amazon. Amazon FSx prend en charge les points de terminaison VPC configurés avec des types d' IPv4 adresses IP Dualstack (IPv4 et IPv6). Pour plus d'informations, consultez la section [Création d'un point de terminaison VPC d'interface](#) dans le guide de l'utilisateur Amazon VPC.

## Considérations relatives aux points de terminaison FSx VPC de l'interface Amazon

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' FSx API Amazon 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 d'Amazon FSx APIs, consultez la section [Actions](#) du manuel Amazon FSx API Reference.

## Considérations relatives au peering VPC

Vous pouvez en connecter d'autres VPCs au VPC à l'aide de points de terminaison VPC d'interface à l'aide du peering VPC. Le peering VPC est une connexion réseau entre deux. VPCs Vous pouvez établir une connexion d'appariage VPC entre les vôtres ou avec un VPC dans un autre. VPCs Compte AWS Ils VPCs peuvent également être en deux versions différentes Régions AWS.

Le trafic entre pairs VPCs reste sur le AWS réseau et ne traverse pas l'Internet public. Une fois peered, VPCs les ressources telles que les instances Amazon Elastic Compute Cloud (Amazon EC2)

présentes dans les deux instances VPCs peuvent accéder à l' FSx API Amazon via les points de terminaison VPC de l'interface créés dans l'un des VPCs

## Création d'un point de terminaison VPC d'interface pour Amazon API FSx

Vous pouvez créer un point de terminaison VPC pour l' FSx API Amazon à l'aide de la console Amazon VPC ou du (). AWS Command Line Interface AWS CLI Pour plus d'informations, consultez la section [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 FSx d'API Amazon.
- **com.amazonaws.*region*.fsx-fips**— Crée un point de terminaison pour l' FSx API Amazon 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 le Région AWS, par exemple. `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' FSx API Amazon, 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 NetApp ONTAP

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 automatiques 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 de plus amples informations, veuillez consulter [Protection de vos données grâce à des sauvegardes en volume](#).

### Instantanés

Amazon FSx crée des copies instantanées des volumes Amazon FSx for NetApp ONTAP. Les copies instantanées offrent une protection contre la suppression ou la modification accidentelle de fichiers

de vos volumes par les utilisateurs finaux. Pour de plus amples informations, veuillez consulter [Protection de vos données grâce à 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 réplique FSx 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 pour 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 de plus amples informations, veuillez consulter [Disponibilité, durabilité et options de déploiement](#).

### 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 assurer 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 de plus amples informations, veuillez consulter [Disponibilité, durabilité et options de déploiement](#).

## Sécurité de l'infrastructure dans Amazon FSx pour NetApp ONTAP

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 for ONTAP

Vous pouvez utiliser la fonction NetApp ONTAP's Vscan pour exécuter un logiciel antivirus tiers compatible. Pour plus d'informations, consultez les ressources suivantes pour chacune des solutions prises en charge.

- Deep Instinct — [Solutions partenaires Vscan](#) et [documentation Deep Instinct 1](#)
- SentinelOne — [Solutions partenaires Vscan et sécurité des](#) données [SentinelOne Singularity Cloud](#)
- [Solutions partenaires Symantec — Vscan](#) et [Symantec](#) Protection Engine
- [Trellix \(anciennement McAfee\) — Solutions partenaires Vscan et documentation sur les produits Trellix](#)
- Trend Micro — [Solutions partenaires Vscan](#)

### Note

<sup>1</sup> Vous devez vous connecter au portail de Deep Instinct pour consulter leur documentation.

# ONTAP rôles et utilisateurs

NetApp ONTAP inclut une fonctionnalité de contrôle d'accès basé sur les rôles (RBAC) robuste et extensible. ONTAP les 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 ONTAP lors FSx de l'utilisation de l'ONTAP API REST et de la CLI. Des ONTAP rôles sont disponibles séparément FSx pour les utilisateurs du système de fichiers ONTAP et pour les utilisateurs de machines virtuelles de stockage (SVM).

Lorsque vous créez un système de fichiers FSx pour 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 FSx de fichiers 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 de plus amples informations, veuillez consulter [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                                                                                 |
|--------------------------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <code>fsxadmin</code>          | Tout             | Tous les répertoires de commandes disponibles dans FSx for ONTAP                                                                        |
| <code>fsxadmin-readonly</code> | Tout             | <code>security login password</code><br><br>Pour gérer le compte utilisateur, le mot de passe local et les informations clés uniquement |
|                                | none             | <code>security</code>                                                                                                                   |
|                                | en 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        | <ul style="list-style-type: none"> <li>• Gérez votre compte utilisateur, votre mot de passe local et vos informations clés</li> <li>• Gérez les volumes, à l'exception des déplacements de volumes</li> <li>• Gérez les quotas, les qtrees, les copies instantanées et les fichiers</li> <li>• Gérez LUNs</li> <li>• Effectuer des SnapLock opérations, à l'exception de la suppression privilégiée</li> <li>• Configuration des protocoles : NFS, SMB et iSCSI</li> <li>• Configuration des services : DNS, LDAP et NIS</li> <li>• Surveillance des tâches</li> <li>• Surveiller les connexions réseau et l'interface réseau</li> <li>• Surveillez l'état de santé de la SVM</li> </ul> |
| vsadmin-volume | <ul style="list-style-type: none"> <li>• Gérez votre compte utilisateur, votre mot de passe local et vos informations clés</li> <li>• Gérez les volumes, y compris les déplacements de volumes</li> <li>• Gérez les quotas, les qtrees, les copies instantanées et les fichiers</li> <li>• Gérez LUNs</li> <li>• Configuration des protocoles : NFS, SMB et iSCSI</li> <li>• Configuration des services : DNS, LDAP et NIS</li> <li>• Surveiller l'interface réseau</li> <li>• Surveillez l'état de santé de la SVM</li> </ul>                                                                                                                                                           |

| Nom du rôle      | Fonctionnalités                                                                                                                                                                                                                                                                                                                                                    |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsadmin-protocol | <ul style="list-style-type: none"><li>• Gérez votre compte utilisateur, votre mot de passe local et vos informations clés</li><li>• Gérez LUNs</li><li>• Configuration des protocoles : NFS, SMB et iSCSI</li><li>• Configuration des services : DNS, LDAP et NIS</li><li>• Surveiller l'interface réseau</li><li>• Surveillez l'état de santé de la SVM</li></ul> |
| vsadmin-backup   | <ul style="list-style-type: none"><li>• Gérez votre compte utilisateur, votre mot de passe local et vos informations clés</li><li>• Gestion des opérations NDMP</li><li>• Lecture et écriture d'un volume restauré</li><li>• Gérez SnapMirror les relations et les copies instantanées</li><li>• Afficher les volumes et les informations sur le réseau</li></ul>  |

| Nom du rôle      | Fonctionnalités                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsadmin-snaplock | <ul style="list-style-type: none"><li>• Gérez votre compte utilisateur, votre mot de passe local et vos informations clés</li><li>• Gérez les volumes, à l'exception des déplacements de volumes</li><li>• Gérez les quotas, les qtrees, les copies instantanées et les fichiers</li><li>• Effectuer des SnapLock opérations, y compris la suppression privilégiée</li><li>• Configuration des protocoles : NFS et SMB</li><li>• Configuration des services : DNS, LDAP et NIS</li><li>• Surveillance des tâches</li><li>• Surveiller les connexions réseau et l'interface réseau</li></ul> |
| vsadmin-readonly | <ul style="list-style-type: none"><li>• Gérez votre compte utilisateur, votre mot de passe local et vos informations clés</li><li>• Surveillez l'état de santé de la SVM</li><li>• Surveiller l'interface réseau</li><li>• Afficher les volumes et LUNs</li><li>• Afficher les services et les protocoles</li></ul>                                                                                                                                                                                                                                                                         |

Pour plus d'informations sur la création d'un nouveau rôle de SVM, consultez [Création de rôles de SVM](#).

## Utiliser Active Directory pour ONTAP authentifier les utilisateurs

Vous pouvez authentifier l'accès des utilisateurs du domaine Windows Active Directory à un système de fichiers et à une SVM FSx for ONTAP. 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 de plus amples informations, veuillez consulter [Comment fonctionne SVMs l'adhésion à 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, voir [Configuration de l'authentification Active Directory pour ONTAP les utilisateurs](#).

## 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 procédure de création d'un nouvel ONTAP utilisateur, consultez [Création d'utilisateurs ONTAP](#).

### Rubriques

- [Création d'utilisateurs ONTAP](#)

- [Création de rôles 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'utilisateurs 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 ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

2. Utilisez la commande `security login create` ONTAP CLI pour créer un nouveau compte utilisateur sur votre système de fichiers ou SVM FSx for ONTAP.

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 attribué, 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 de plus amples informations, veuillez consulter [Surveillance des systèmes FSx de fichiers 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 SVMs.

```
Fsx0123456::> security login show
```

```
Vserver: Fsx0123456
```

| User/Group<br>Name | Application | Authentication<br>Method | Role Name   | Acct<br>Locked | Second<br>Authentication<br>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

User/Group Authentication Acct Second
Name Method Locked Authentication

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 de rôles 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 -vserver vs1.example.com -role vol_role -
cmddirname volume

```

2. Spécifiez les paramètres obligatoires suivants dans la commande :
  - `-vserver` le nom de la SVM
  - `-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`, `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 ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

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. `svm_name` Remplacez-le 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 d'utilisateurs de domaine Active Directory qui accéderont 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 fichiers `filesystem1`.

```
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'utilisateur CORP\Admin 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                                                                                                                                                                                                                                |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-vserver</code> (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 <code>-vserver</code> pas.                                                |
| <code>-username</code>             | Le nom d'utilisateur du compte. La valeur par défaut <code>admin</code> , est le nom par défaut de l'administrateur du cluster.                                                                                                            |
| <code>-index</code>                | 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. |
| <code>-publickey</code>            | La clé publique OpenSSH. Placez la clé entre guillemets doubles.                                                                                                                                                                           |
| <code>-role</code>                 | Rôle de contrôle d'accès attribué au compte.                                                                                                                                                                                               |
| <code>-comment</code> (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 publique5.

```
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 ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

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                        | 0                  | 0                          | 0                          | 0                 | 0                       |

# 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](#)
- [Quotas de ressources pour chaque système de fichiers](#)

## Les quotas que vous pouvez augmenter

Vous trouverez ci-dessous les quotas d'Amazon FSx pour NetApp ONTAP que vous pouvez augmenter pour chacun Compte AWS d'entre eux. Région AWS

| Ressource                      | Par défaut | Description                                                                                                                                    |
|--------------------------------|------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| ONTAP systèmes de fichiers     | 100        | Le nombre maximum de systèmes de fichiers Amazon FSx for NetApp ONTAP que vous pouvez créer dans ce compte.                                    |
| ONTAP Capacité 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. |
| ONTAP capacité de débit        | 10 240     | Capacité de débit maximale (in MBps) pour tous les systèmes de fichiers Amazon FSx for NetApp ONTAP que vous pouvez avoir sur ce compte.       |

| Ressource         | Par défaut | Description                                                                                                                                                                     |
|-------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ONTAP SSD IOPS    | 1 000 000  | Le nombre maximal d'IOPS SSD pour tous les systèmes de fichiers Amazon FSx for NetApp ONTAP que vous pouvez avoir sur ce compte.                                                |
| ONTAP sauvegardes | 10 000     | Le nombre maximum de sauvegardes de volumes initiées par l'utilisateur pour tous les systèmes de fichiers Amazon FSx for NetApp ONTAP que vous pouvez avoir dans un. Compte AWS |

Pour demander une augmentation de quota

- Ouvrez la page [AWS Support](#), connectez-vous (si nécessaire), puis choisissez Create case (Créer une demande de support).
- Pour Créer un dossier, choisissez Compte et assistance à la facturation.
- Dans le panneau Détails du dossier, saisissez les informations suivantes :
  - Pour Type, choisissez Compte.
  - Dans Catégorie, sélectionnez 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 FSx quota 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.
- 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 | <ul style="list-style-type: none"> <li>• Systèmes de fichiers mono-AZ de deuxième génération : 512 TiB par paire HA, jusqu'à 1 PiB</li> <li>• Systèmes de fichiers multi-AZ de deuxième génération : 512 TiB</li> <li>• Systèmes de fichiers de première génération : 192 TiB</li> </ul>                                                                                                                                                                                                                                             |
| Nombre maximal d'IOPS sur SSD     | <p>Systèmes de fichiers de deuxième génération :</p> <ul style="list-style-type: none"> <li>• 200 000 par paire HA (jusqu'à 12 paires) pour un seul AZ</li> <li>• 200 000 au total pour Multi-AZ</li> </ul> <p>Systèmes de fichiers de première génération :</p> <ul style="list-style-type: none"> <li>• 160 000 dans les régions USA Est (Ohio), USA Est (Virginie du Nord), USA Ouest (Oregon) et Europe (Irlande)</li> <li>• 80 000 <a href="#">dans tous les autres Régions AWS pays où FSx ONTAP est disponible</a></li> </ul> |

| Ressource                  | Limite par système de fichiers                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Capacité de débit minimale | <ul style="list-style-type: none"> <li>• Systèmes de fichiers de deuxième génération (1 paire HA) : 384 MBps</li> <li>• Systèmes de fichiers de deuxième génération (2 paires HA ou plus) : 1 536 MBps par paire HA</li> <li>• Systèmes de fichiers de première génération : 128 MBps</li> </ul>                                                                                                                                                                                                                                  |
| Capacité de débit maximale | <p>Systèmes de fichiers de deuxième génération :</p> <ul style="list-style-type: none"> <li>• 73 728 MBps <sup>1</sup> pour Single-AZ</li> <li>• 6 144 MBps pour Multi-AZ</li> </ul> <p>Systèmes de fichiers de première génération :</p> <ul style="list-style-type: none"> <li>• 4 096 MBps <sup>2</sup> dans les régions USA Est (Ohio), USA Est (Virginie du Nord), USA Ouest (Oregon) et Europe (Irlande)</li> <li>• 2 048 MBps <a href="#">dans tous les autres pays Régions AWS où FSx ONTAP est disponible</a></li> </ul> |
| Nombre maximum de volumes  | <ul style="list-style-type: none"> <li>• Systèmes de fichiers de deuxième génération (1 paire HA) : 500</li> <li>• Systèmes de fichiers de deuxième génération (2 paires HA ou plus) : 1 000</li> <li>• Systèmes de fichiers de première génération : 500</li> </ul>                                                                                                                                                                                                                                                              |

| Ressource                     | Limite par système de fichiers |
|-------------------------------|--------------------------------|
| Nombre maximum d'instantanés  | 1 023 par volume 3             |
| Nombre maximum de sauvegardes | 4 091 par volume 4             |

| Ressource              | Limite par système de fichiers                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nombre maximum de SVMs | <p>Systèmes de fichiers de deuxième génération avec une paire HA :</p> <ul style="list-style-type: none"> <li>• 6 (384 MBps de capacité de débit)</li> <li>• 6 (768 MBps de capacité de débit)</li> <li>• 14 (1 536 MBps de capacité de débit)</li> <li>• 14 (3 072 MBps de capacité de débit)</li> <li>• 24 (6 144 MBps de capacité de débit)</li> </ul> <p>Systèmes de fichiers de deuxième génération avec 2 à 12 paires HA :</p> <ul style="list-style-type: none"> <li>• 5</li> </ul> <p>Systèmes de fichiers de première génération :</p> <ul style="list-style-type: none"> <li>• 6 (capacité de MBps débit de 128)</li> <li>• 6 (capacité de MBps débit de 256)</li> <li>• 14 (capacité de MBps débit de 512)</li> <li>• 14 (capacité de MBps débit de 1 024)</li> <li>• 24 (capacité de MBps débit de 2 048)</li> <li>• 24 (capacité de MBps débit de 4 096)</li> </ul> |
| 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 <sup>5</sup>                |
| Nombre maximum de connexions client par serveur de fichiers <sup>6</sup>       | 100 000                        |

### Note

<sup>1</sup> Sur un système de fichiers mono-AZ de deuxième génération avec 12 paires HA (6 144 MBps par paire HA). Pour de plus amples informations, veuillez consulter [Gestion des paires de haute disponibilité \(HA\)](#).

<sup>2</sup> Pour fournir 4 % GBps de capacité de débit, votre système de fichiers de première génération FSx pour ONTAP nécessite une configuration du maximum d'IOPS sur SSD (160 000) et un minimum de 5 120 GiB de capacité de stockage SSD dans un environnement compatible. Région AWS Pour plus d'informations sur ceux qui Régions AWS prennent en charge 4 096 % MBps de capacité de débit, consultez. [Impact de la capacité de débit sur les performances](#)

<sup>3</sup> 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.

<sup>4</sup> 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.

<sup>5</sup> 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 routes SVMs qu'il possède et par le nombre de tables de routage qui lui sont associées. Vous pouvez déterminer le nombre existant de routes vers un système de fichiers

à l'aide de l'équation suivante :  $(1 + \text{nombre de routes SVMs dans le système de fichiers})^*$   
(tables de routage associées au système de fichiers).

<sup>6</sup> Une connexion client est définie comme une connexion TCP unique à un serveur de fichiers donné. Il existe un serveur de fichiers actif par paire HA dans un système de fichiers. Un client peut avoir plusieurs connexions TCP à un serveur de fichiers. Par exemple, si un client utilise le multiacheminement.

# Résolution des problèmes liés à Amazon FSx pour NetApp ONTAP

Utilisez les sections suivantes pour résoudre les problèmes liés aux systèmes FSx de fichiers ONTAP.

## Rubriques

- [Votre système de fichiers est dans un MISCONFIGURED état](#)
- [Vous ne pouvez pas accéder à votre système de fichiers](#)
- [Votre machine virtuelle de stockage \(SVM\) est en état MISCONFIGURED](#)
- [Impossible de joindre une machine virtuelle de stockage \(SVM\) à Active Directory](#)
- [Impossible de supprimer une machine virtuelle ou un volume de stockage](#)
- [Votre volume est dans un MISCONFIGURED état](#)
- [La capacité de stockage de votre volume est insuffisante](#)
- [Vos sauvegardes échouent en raison d'une capacité de volume insuffisante](#)
- [Résolution des problèmes de réseau](#)

## Votre système de fichiers est dans un **MISCONFIGURED** état

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](#)
- [Impossible de créer une nouvelle SVM sur un système de fichiers multi-AZ](#)
- [Le niveau de stockage SSD de votre système de fichiers est plein à plus de 90 %](#)

## 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 ONTAP. FSx
- Le compte propriétaire a cessé de partager le sous-réseau VPC.

Si le compte propriétaire a cessé de partager le sous-réseau VPC, le message suivant s'affichera dans la console pour ce système de fichiers :

```
The vpc ID vpc-012345abcde does not exist
```

Pour résoudre le problème, vous devez contacter le compte propriétaire qui a partagé le sous-réseau VPC avec vous. 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 ONTAP. FSx
- Le compte propriétaire a cessé de partager le sous-réseau VPC.

Pour résoudre le problème, vous devez contacter le compte propriétaire qui a partagé le sous-réseau VPC avec vous. Pour plus d'informations, voir [Création de systèmes de fichiers FSx pour ONTAP dans des sous-réseaux partagés](#) pour plus d'informations.

## Le niveau de stockage SSD de votre système de fichiers est plein à plus de 90 %

Le niveau de stockage SSD de votre système de fichiers mono-AZ ou multi-AZ est actuellement plein à plus de 90 %. Nous vous recommandons de ne pas dépasser 80 % d'utilisation du niveau de stockage de votre SSD sur une base continue. Si vous ne libérez pas d'espace dans le niveau de stockage SSD avant la prochaine fenêtre de maintenance de votre système de fichiers, FSx ONTAP réduira temporairement le débit de votre système de fichiers pendant la durée de l'opération de correction. Ceci est fait pour garantir que les processus de maintenance en arrière-plan peuvent être achevés dans un délai raisonnable. Pour éviter cela, réduisez le taux d'utilisation de votre niveau de

stockage SSD à moins de 90 %. Vous pouvez réduire l'utilisation des SSD de plusieurs manières, notamment :

- Augmenter la capacité de stockage SSD de votre système de fichiers.
- En supprimant les données inutiles.
- En supprimant les instantanés de volume inutiles.

Pour de plus amples informations, veuillez consulter [Gestion de la capacité de stockage](#).

## Vous ne pouvez pas accéder à votre système de fichiers

Cette section décrit les problèmes et les solutions liés à l'impossibilité d'accéder à votre système de fichiers.

### Rubriques

- [Des balises de table de routage sont manquantes dans votre système de fichiers multi-AZ](#)
- [Votre système de fichiers comporte plus de 50 itinéraires](#)
- [Votre système de fichiers ne dispose pas de routes vers un ou plusieurs serveurs de fichiers](#)
- [L'interface Elastic Network du système de fichiers a été modifiée ou supprimée](#)
- [L'adresse IP Elastic attachée à l'interface Elastic Network du système de fichiers a été supprimée](#)
- [Le groupe de sécurité VPC du système de fichiers ne dispose pas des règles entrantes requises](#)
- [Le groupe de sécurité VPC de l'instance de calcul ne dispose pas des règles de sortie requises](#)
- [Le sous-réseau de l'instance de calcul n'utilise aucune des tables de routage associées à votre système de fichiers](#)
- [Amazon ne FSx 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 cessé de partager le 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](#)

## Des balises de table de routage sont manquantes dans votre système de fichiers multi-AZ

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 balises de table de routage sont actuellement absentes d'une ou de plusieurs tables de routage associées à votre système de fichiers. Ces tables de routage sont étiquetées avec `Key: AmazonFSx; Value: ManagedByAmazonFSx`. Si vous n'ajoutez pas manuellement ces balises avant la prochaine fenêtre de maintenance, les clients des sous-réseaux associés aux tables de routage auxquels les balises sont absentes perdront temporairement l'accès au système de fichiers pendant la durée de l'opération de correction. Pour éviter cela, veuillez ajouter manuellement les balises de table de routage manquantes.

Pour de plus amples informations, veuillez consulter [Mise à jour des systèmes de fichiers](#).

## Votre système de fichiers comporte plus de 50 itinéraires

Plus de 50 itinéraires sont actuellement associés à votre système de fichiers. Si vous ne supprimez pas certaines de ces routes avant la prochaine fenêtre de maintenance planifiée de votre système de fichiers, le processus de basculement peut prendre plus de temps que d'habitude. Pour éviter cela, veuillez réduire le nombre de lignes à moins de 50. Vous pouvez suivre les étapes suivantes pour réduire le nombre de routes associées à votre système de fichiers :

- Supprimer les itinéraires excédentaires
- Réduction du nombre de fichiers SVMs associés au système de fichiers
- Réduction du nombre de tables de routage associées au système de fichiers

Pour plus d'informations, consultez [Mise à jour des systèmes de fichiers](#) et [Suppression de machines virtuelles de stockage \(SVM\)](#).

## Votre système de fichiers ne dispose pas de routes vers un ou plusieurs serveurs de fichiers

Il manque actuellement des routes vers un ou plusieurs serveurs de fichiers dans votre système de fichiers, et les tables de routage existantes ne disposent pas de suffisamment d'espace pour ajouter de nouvelles entrées de table de routage. Si vous n'ajoutez pas les routes manquantes avant la prochaine fenêtre de maintenance planifiée de votre système de fichiers, tous les clients connectés

seront déconnectés pendant la durée de l'opération de correction. Pour éviter cela, veuillez ajouter les itinéraires manquants.

Pour plus d'informations, consultez [Mise à jour des systèmes de fichiers](#) et [Quotas](#).

## 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 FSx réseau Amazon. Pour de plus amples informations, veuillez consulter [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 détache FSx automatiquement toute adresse IP élastique qui est une adresse IP publique accessible depuis Internet et attachée à l'interface Elastic Network d'un système de fichiers. Pour de plus amples informations, veuillez consulter [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 pour 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 FSx à utiliser par Amazon 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 [Mise à jour des systèmes de fichiers](#)

## Amazon ne FSx 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`. Lorsque vous créez ou mettez à jour FSx des systèmes de fichiers ONTAP Multi-AZ, AWS CloudFormation nous vous recommandons d'ajouter la `Key: AmazonFSx; Value: ManagedByAmazonFSx` balise manuellement.

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 [Mise à jour des systèmes 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 cessé de partager le 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 cessé de partager le sous-réseau VPC.

Si le compte propriétaire a cessé de partager le 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 de plus amples informations, veuillez consulter [Accès à vos données FSx for ONTAP](#).

## Votre machine virtuelle de stockage (SVM) est en état **MISCONFIGURED**

Il existe un certain nombre de causes potentielles pour lesquelles une machine virtuelle de stockage passe dans un MISCONFIGURED état, chacune ayant sa propre résolution, comme suit.

## Votre SVM possède un volume hors ligne

Votre système de fichiers contient un volume qui est hors ligne. Nous vous recommandons de maintenir les volumes en ligne de manière continue. Si vous ne mettez pas en ligne ce volume avant la prochaine fenêtre de maintenance de votre système de fichiers, Amazon FSx mettra temporairement ce volume en ligne pendant la durée de l'opération de correction. Pour éviter cela, connectez-vous ou supprimez le volume.

Pour remettre en ligne un volume hors ligne, utilisez [volume online](#) ONTAP Commande CLI, comme indiqué dans l'exemple suivant. S'il n'existe qu'une seule SVM (Vserver), il n'est pas nécessaire de spécifier le `-vserver` paramètre.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

## Votre SVM possède un volume hors ligne doté d'un LUN iSCSI ou d'un espace de noms /TCP NVMe

Votre système de fichiers contient un volume dont l'état est restreint. Nous vous recommandons de maintenir les volumes en ligne de manière continue. Si vous ne mettez pas en ligne ce volume avant la prochaine fenêtre de maintenance de votre système de fichiers, Amazon FSx mettra temporairement ce volume en ligne pendant la durée de l'opération de correction. Pour éviter cela, connectez-vous ou supprimez le volume.

Pour remettre en ligne un volume hors ligne, utilisez [volume online](#) ONTAP Commande CLI, comme indiqué dans l'exemple suivant. S'il n'existe qu'une seule SVM (Vserver), il n'est pas nécessaire de spécifier le `-vserver` paramètre.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

## 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 [Comment fonctionne SVMs l'adhésion à 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 SVM est déjà jointe à un autre Active Directory](#)
- [Amazon ne FSx peut pas se connecter à vos contrôleurs de domaine Active Directory car le nom NetBIOS de la SVM est déjà utilisé](#)
- [Amazon ne FSx peut pas communiquer avec vos contrôleurs de domaine Active Directory](#)
- [Amazon ne FSx peut pas se connecter à votre Active Directory en raison d'exigences de port ou d'autorisations de compte de service non satisfaites](#)
- [Amazon ne FSx peut pas se connecter à vos contrôleurs de domaine Active Directory car les informations d'identification du compte de service ne sont pas valides](#)
- [Amazon ne FSx peut pas se connecter à vos contrôleurs de domaine Active Directory en raison d'identifiants de compte de service insuffisants](#)
- [Amazon ne FSx peut pas communiquer avec vos serveurs DNS ou contrôleurs de domaine Active Directory](#)
- [Amazon ne FSx peut pas communiquer avec votre Active Directory en raison d'un nom de domaine Active Directory non valide.](#)
- [Le compte de service ne peut pas accéder au groupe d'administrateurs spécifié dans la configuration Active Directory de la SVM](#)
- [Amazon ne FSx peut pas se connecter aux contrôleurs de domaine Active Directory car l'unité organisationnelle spécifiée n'existe pas ou n'est pas accessible](#)

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 n' FSx est pas en mesure d'établir une 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 [Connexion SVMs à 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 n' FSx est pas en mesure d'établir une 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 de plus amples informations, veuillez consulter [Dissocier un Active Directory de votre SVM à l'aide de la NetApp CLI ONTAP](#).
2. Suivez la procédure décrite dans la section [Connexion SVMs à Active Directory à l'aide de AWS Management Console l'API AWS CLI et](#) pour réessayer de joindre votre SVM au nouvel AD.

## Amazon ne FSx 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 n' FSx est pas en mesure d'établir une 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 [Connexion SVMs à 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 ne FSx 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 ne FSx est pas en mesure de 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 [Connexion SVMs à Active Directory à l'aide de AWS Management Console l'API AWS CLI et](#) et réessayez de joindre votre SVM à votre AD.

## Amazon ne FSx 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 ne FSx est pas en mesure d'établir une 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 tout problème d'autorisation lié aux ports et aux comptes de service, comme recommandé dans le guide de FSx l'utilisateur Amazon.

Pour résoudre ce problème, procédez comme suit :

1. Passez en revue les exigences décrites dans [Exigences 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 dans [Exigences 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 [Connexion SVMs à Active Directory à l'aide de AWS Management Console l'API AWS CLI et](#) et réessayez de joindre votre SVM à votre AD.

## Amazon ne FSx 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 n' FSx est pas en mesure d'établir une 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 [Mise à jour des configurations SVM Active Directory existantes à l'aide de l' AWS Management Console API 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 ne FSx peut pas se connecter à vos contrôleurs de domaine Active Directory en raison d'identifiants de compte de service insuffisants

La connexion d'une SVM à votre Active Directory autogéré échoue avec le message d'erreur suivant :

Amazon n' FSx est pas en mesure d'établir une connexion avec vos contrôleurs de domaine Active Directory. Cela est dû soit aux exigences de port non satisfaites pour Active Directory, soit au fait 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](#) et [Délégation d'autorisations à votre compte de FSx service Amazon](#).

## Amazon ne FSx 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 n' FSx est pas en mesure de communiquer avec votre Active Directory. Cela est dû au fait qu'Amazon ne FSx 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 au ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

- b. Entrez la commande suivante, où :

  - `-vserver vs_server_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::> vs_server cifs domain preferred-dc add -vserver vs_server_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::> vs_server 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 [vs\\_server 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 au ONTAP CLI, établissez une session SSH sur le port de gestion du système de fichiers Amazon FSx for NetApp ONTAP ou de la SVM 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 du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

- 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 vservice_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::> vservice services access-check dns forward-lookup \
-vserver vservice_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 ne FSx 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 [Connexion SVMs à 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 [Connexion SVMs à Active Directory à l'aide de AWS Management Console l'API AWS CLI et](#) et réessayez de joindre votre SVM à un AD.

## Amazon ne FSx 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 n' FSx est pas en mesure d'établir une 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 pour ONTAP peut contenir une ou plusieurs machines virtuelles de stockage (SVMs), 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 FSx console, de l'API et de la CLI Amazon. Vous ne pouvez supprimer des volumes à l'aide de la FSx console, de l'API ou de la CLI Amazon que si les FSx sauvegardes Amazon sont activées sur le volume.

Pour protéger vos données et votre configuration, Amazon FSx empêche la suppression de volumes SVMs et de volumes dans certaines circonstances. Si vous tentez de supprimer une SVM ou un volume et que votre demande de suppression n'aboutit pas, Amazon vous FSx fournit des informations dans la AWS 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](#)
- [Suppression de la SVM : les tables de routage sont inaccessibles](#)
- [Suppression de la SVM : relation avec les pairs](#)
- [Suppression d'une SVM ou d'un volume : SnapMirror](#)
- [Suppression de la SVM : LIF compatible avec Kerberos](#)
- [Suppression de la SVM : autre raison](#)
- [Suppression d'un volume : FlexCache relation](#)

## Identification des suppressions échouées

Lorsque vous supprimez une FSx SVM ou un volume Amazon, l'`Lifecycle` état de la ressource passe généralement jusqu'à `DELETING` quelques minutes avant qu'elle ne disparaisse de la FSx console, de la CLI et de l'API Amazon.

Si vous tentez de supprimer une ressource et que son `Lifecycle` état passe de `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.

## Lifecycle state

 Created 

## Lifecycle transition message

**Cannot delete storage virtual machine while it has non-root volumes.**

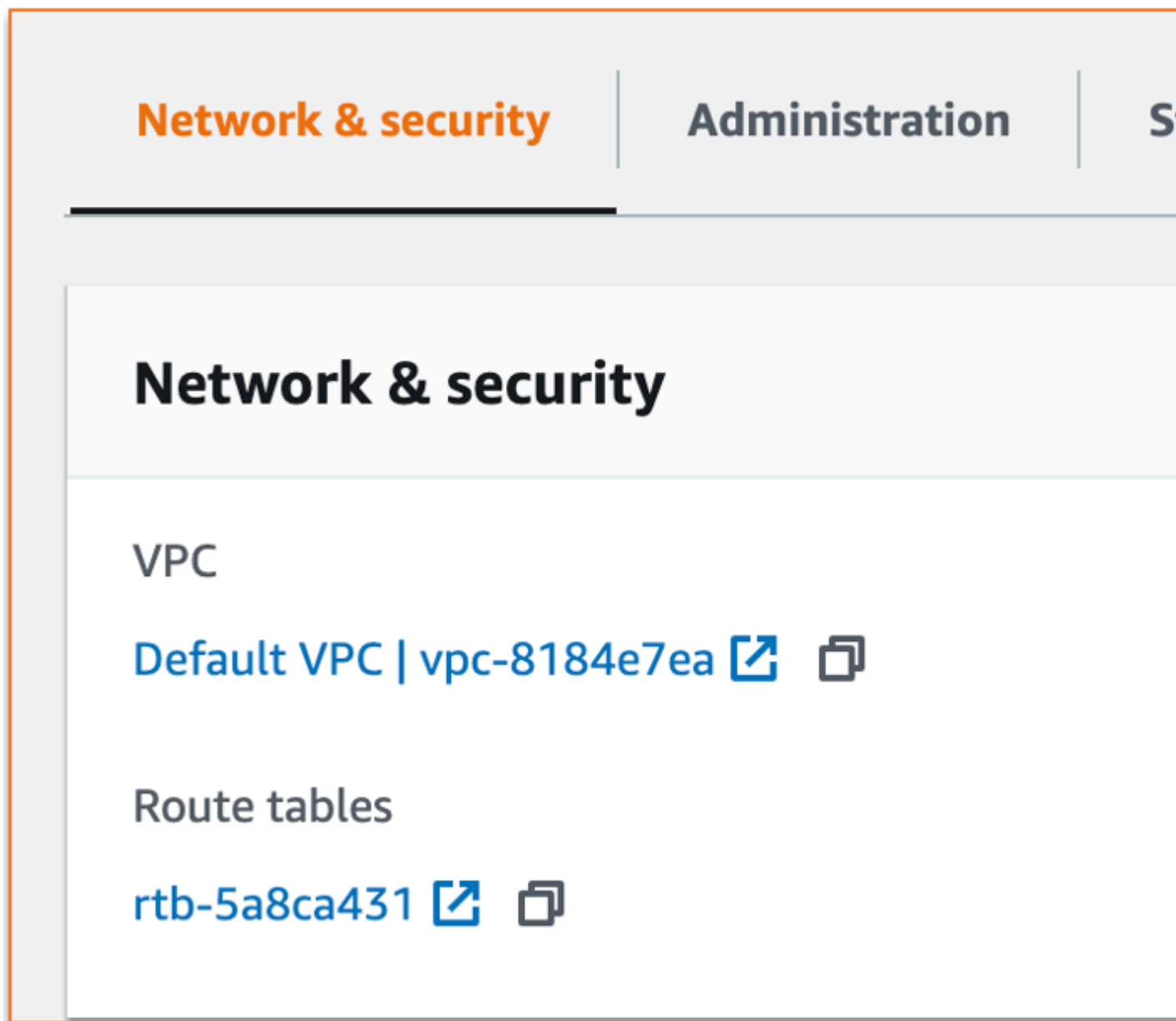
Les raisons les plus courantes pour lesquelles Amazon FSx empêche la suppression des SVM et des volumes sont indiquées dans les sections suivantes, avec des step-by-step instructions sur la manière de résoudre ces problèmes.

## Suppression de la SVM : les tables de routage sont inaccessibles

Chaque système de fichiers FSx pour ONTAP crée une ou plusieurs entrées de table de routage pour permettre un basculement automatique et un retour en arrière 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 FSx des interfaces 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 FSx empêcher Amazon 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 Support.

Vous pouvez trouver les tables de routage de votre système de fichiers dans la FSx console Amazon 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

| Tags                             |                    |
|----------------------------------|--------------------|
| <input type="text"/> Search tags |                    |
| Key                              | Value              |
| Name                             | Default            |
| AmazonFSx                        | 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 empêche le pair SVMs de devenir malsain. Si votre SVM ne peut pas être supprimée en raison d'une relation entre pairs, vous pouvez voir ce qui suit : LifecycleTransitionReason

Amazon n' FSx 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 dans [Gestion des systèmes de fichiers à l'aide du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#). 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 :

| Vserver         | Peer Vserver | Peer State | Peer Cluster           | Peering Applications | Remote Vserver |
|-----------------|--------------|------------|------------------------|----------------------|----------------|
| <i>svm_name</i> | test2        | peered     | FsxId02d81fef0d84734b6 | snamirror            | 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 (voir [Suppression 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 dans [Gestion des systèmes de fichiers à l'aide du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

### Note

FSx Les sauvegardes Amazon permettent SnapMirror de 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 via la AWS CLI, l'API ou 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 Path         | Type | Destination Path | Mirror State | Relationship Status | Total Progress | Healthy | Last 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 dans [Gestion des systèmes de fichiers à l'aide du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

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 |
|---------------------------|----------------------|--------------|----------|-----|
| -----                     |                      |              |          |     |
| <i>svm_name</i>           | nfs_smb_management_1 | 10.19.153.48 | disabled |     |
| 5 entries were displayed. |                      |              |          |     |

- 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

FSx pour ONTAP, SVMs créez un objet informatique dans votre Active Directory lorsqu'ils rejoignent votre Active Directory. Dans certains cas, vous souhaitez 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 décrites [Gestion des systèmes de fichiers à l'aide du ONTAP INTERFACE DE LIGNE DE](#)

[COMMANDE \(CLI\)](#), 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 dans [Gestion des systèmes de fichiers à l'aide du ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#).

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.

## Votre volume est dans un **MISCONFIGURED** état

Un volume ONTAP peut avoir plusieurs causes possibles pour lesquelles un volume ONTAP passe dans un MISCONFIGURED état, comme indiqué dans les rubriques suivantes.

### Votre volume est plein à plus de 98 %

Votre système de fichiers contient actuellement un volume plein à plus de 98 %. Nous vous recommandons de ne pas dépasser 95 % d'utilisation de votre volume sur une base continue. Si vous ne libérez pas d'espace dans le volume avant la prochaine fenêtre de maintenance de votre système de fichiers, Amazon FSx désactivera le verrouillage opportuniste du volume, brisant ainsi tous les « oplocks » existants. Amazon FSx réactivera les oplocks sur le volume une fois le processus d'application des correctifs terminé. Pour éviter cela, réduisez le taux d'utilisation de la capacité de stockage du volume à moins de 98 %. Parmi les moyens d'y parvenir, on peut citer :

- Augmenter la taille du volume.
- Suppression des données inutiles.
- Suppression des instantanés inutiles.

Pour plus d'informations, consultez [Mettre à jour la capacité de stockage](#) et [Suppression d'instantanés](#).

### Votre volume hors ligne possède un LUN iSCSI ou un espace de noms / TCP NVMe

Votre système de fichiers héberge actuellement un volume qui est hors ligne et ce volume contient un LUN iSCSI, un espace de noms NVMe /TCP, ou les deux. Nous vous recommandons de maintenir les volumes en ligne de manière continue. Si vous ne mettez pas en ligne ce volume avant la prochaine fenêtre de maintenance de votre système de fichiers, Amazon FSx mettra temporairement

ce volume en ligne pendant la durée de l'opération de correction. Pour éviter cela, connectez-vous ou supprimez le volume.

Pour remettre en ligne un volume hors ligne, utilisez [volume online](#) ONTAP Commande CLI, comme indiqué dans l'exemple suivant. S'il n'existe qu'une seule SVM (Vserver), il n'est pas nécessaire de spécifier le `-vserver` paramètre.

```
FsxID-abcdef123456:> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

## Votre volume hors ligne est un FlexCache origine

Votre système de fichiers contient un volume FlexCache d'origine qui est hors ligne. Nous vous recommandons de maintenir les volumes en ligne de manière continue. Si vous ne mettez pas en ligne ce volume avant la prochaine fenêtre de maintenance de votre système de fichiers, Amazon FSx mettra temporairement ce volume en ligne pendant la durée de l'opération de correction. Pendant ce temps, il est possible que les données soient réécrites sur le volume FlexCache d'origine avec les données du volume de cache. Pour éviter cela, connectez-vous ou supprimez le volume.

Pour remettre en ligne un volume hors ligne, utilisez [volume online](#) ONTAP Commande CLI, comme indiqué dans l'exemple suivant. S'il n'existe qu'une seule SVM (Vserver), il n'est pas nécessaire de spécifier le `-vserver` paramètre.

```
FsxID-abcdef123456:> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

## Votre volume hors ligne fait partie d'un SnapMirror relation

Votre système de fichiers héberge actuellement un volume en mode hors connexion, et ce volume est un SnapMirror source ou destination. Nous vous recommandons de maintenir les volumes en ligne de manière continue. Si vous ne mettez pas en ligne ce volume avant la prochaine fenêtre de maintenance de votre système de fichiers, Amazon FSx mettra temporairement ce volume en ligne pendant la durée de l'opération de correction et interrompra le SnapMirror relation. Pendant ce temps, il est possible que les données soient écrites dans SnapMirror volume de destination avec des données provenant du SnapMirror volume de la source. Pour éviter cela, connectez-vous ou supprimez le volume.

Pour remettre en ligne un volume hors ligne, utilisez [volume online](#) ONTAP Commande CLI, comme indiqué dans l'exemple suivant. S'il n'existe qu'une seule SVM (Vserver), il n'est pas nécessaire de spécifier le `-vserver` paramètre.

```
FsxID-abcdef123456:> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

## Votre volume restreint contient un LUN iSCSI ou un espace de noms /TCP NVMe

Votre système de fichiers héberge actuellement un volume dont l'état est restreint et ce volume contient un LUN iSCSI, un espace de noms NVMe /TCP, ou les deux. Nous vous recommandons de maintenir les volumes en ligne de manière continue. Si vous ne mettez pas en ligne ce volume avant la prochaine fenêtre de maintenance de votre système de fichiers, Amazon FSx mettra temporairement ce volume en ligne pendant la durée de l'opération de correction. Pour éviter cela, connectez-vous ou supprimez le volume.

Pour remettre en ligne un volume hors ligne, utilisez [volume online](#) ONTAP Commande CLI, comme indiqué dans l'exemple suivant. S'il n'existe qu'une seule SVM (Vserver), il n'est pas nécessaire de spécifier le `-vserver` paramètre.

```
FsxID-abcdef123456:> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

## Votre volume restreint est une FlexCache origine

Votre système de fichiers contient un volume FlexCache d'origine dont l'état est restreint. Nous vous recommandons de maintenir les volumes en ligne de manière continue. Si vous ne mettez pas en ligne ce volume avant la prochaine fenêtre de maintenance de votre système de fichiers, Amazon FSx mettra temporairement ce volume en ligne pendant la durée de l'opération de correction. Pendant ce temps, il est possible que les données soient réécrites sur le volume FlexCache d'origine avec les données du volume de cache. Pour éviter cela, connectez-vous ou supprimez le volume.

Pour remettre en ligne un volume hors ligne, utilisez [volume online](#) ONTAP Commande CLI, comme indiqué dans l'exemple suivant. S'il n'existe qu'une seule SVM (Vserver), il n'est pas nécessaire de spécifier le `-vserver` paramètre.



```
FsxID-abcdef123456:> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

## Votre volume restreint fait partie d'un SnapMirror relation

Votre système de fichiers héberge actuellement un volume dont l'état est restreint, et ce volume est SnapMirror source ou destination. Nous vous recommandons de maintenir les volumes en ligne de manière continue. Si vous ne mettez pas en ligne ce volume avant la prochaine fenêtre de maintenance de votre système de fichiers, Amazon FSx mettra temporairement ce volume en ligne pendant la durée de l'opération de correction et interrompra le SnapMirror relation. Pendant ce temps, il est possible que les données soient écrites dans SnapMirror volume de destination avec des données provenant du SnapMirror volume de la source. Pour éviter cela, connectez-vous ou supprimez le volume.

Pour remettre en ligne un volume hors ligne, utilisez [volume online](#) ONTAP Commande CLI, comme indiqué dans l'exemple suivant. S'il n'existe qu'une seule SVM (Vserver), il n'est pas nécessaire de spécifier le `-vserver` paramètre.

```
FsxID-abcdef123456:> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

## La capacité de stockage de votre 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 de plus amples informations, veuillez consulter [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 FSx console Amazon et de FSx l'API Amazon. AWS CLI Pour plus d'informations sur la mise à jour d'un volume avec une capacité accrue, consultez [Mise à jour des volumes](#).

Vous pouvez également augmenter la capacité de stockage d'un volume à l'aide de la commande `volume modify` NetApp ONTAP CLI. Pour de plus amples informations, veuillez consulter [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 FSx pour ONTAP, à l'aide de la `volume autosize` NetApp commande ONTAP CLI. Pour de plus amples informations, veuillez consulter [Activation du dimensionnement automatique](#).

## Le stockage principal de votre système de fichiers est plein

Si le stockage principal FSx de votre système de fichiers 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 FSx console Amazon. Pour de plus amples 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 de plus amples informations, veuillez consulter [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.

Lorsque vous supprimez un instantané, vous ne récupérez pas une quantité de stockage égale à la taille de l'instantané que vous supprimez. Vous pouvez voir la quantité d'espace de stockage que vous pouvez récupérer lors de la suppression d'un instantané en utilisant le [volume snapshot compute-reclaimable](#) -vserver ONTAP Commande CLI, utilisant vos données pour remplacer `svm_namevol_name`, et `snapshot_name`.

```
fsid8970abc52::> volume snapshot compute-reclaimable -vserver svm_name -volume vol_name
-snapshot snapshot_name
A total of 667648 bytes can be reclaimed.
```

Pour plus d'informations sur la suppression des instantanés et la gestion des politiques relatives aux instantanés afin de préserver la capacité de stockage, consultez [Suppression 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 de plus amples informations, veuillez consulter [Capacité du fichier de volume](#).

Le nombre d'inodes dans un volume augmente proportionnellement à sa capacité de stockage, 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, consultez [Surveillance de la capacité de fichiers 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 de plus amples informations, veuillez consulter [Pour augmenter le nombre maximum de fichiers sur un volume \(ONTAPCLI\)](#).

## Vos sauvegardes 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](#)

## 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 avec les méthodes suivantes NetApp ONTAP Commandes CLI :

- `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 par SSH au NetApp ONTAP CLI de votre système de fichiers, suivez les étapes décrites dans la [Utilisation de NetApp ONTAP INTERFACE DE LIGNE DE COMMANDE \(CLI\)](#) 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, entrez y.

```
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, `FsxD01234567890abcdef-01`).

- *svm\_name* Remplacez-le 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'e0einterface et dans l'espace Default IP. Dans FSx ONTAP, tout le trafic réseau utilise l'e0einterface.

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 : *svm\_name* / clus//*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 : *node-name* \_\_ *port-name* .trc *yyyymmdd\_hhmmss*
- 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 -ip space 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 [Comment utiliser le vidage réseau de débogage dans ONTAP 9.10+](#) dans le NetApp Knowledge Base.

# Historique du document pour Amazon FSx pour NetApp ONTAP

- Version de l'API : 01/03/2018
- Dernière mise à jour de la documentation : 9 juin 2025

Le tableau suivant décrit les modifications importantes apportées au guide de l'utilisateur 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        |
|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| <a href="#">FSx pour ONTAP prend en charge Amazon Elastic Service VMware</a> | FSx for ONTAP peut désormais être utilisé comme banque de données externe pour Amazon EVS. Pour plus d'informations, consultez la section <a href="#">Utilisation d'Amazon Elastic VMware Service avec FSx for ONTAP</a> .                                                 | 9 juin 2025 |
| <a href="#">Région AWS Support supplémentaire ajouté</a>                     | La deuxième génération (Multi-AZ 2 et Single-AZ 2) FSx pour les systèmes de fichiers ONTAP est désormais disponible en Asie-Pacifique (Tokyo) et en Asie-Pacifique (Mumbai). Pour plus d'informations, consultez <a href="#">la section Disponibilité par Région AWS</a> . | 2 juin 2025 |
| <a href="#">Support ajouté pour le mode FlexCache écriture différée</a>      | FSx pour les volumes ONTAP, le mode FlexCache écriture différée est désormais compatible. Pour plus                                                                                                                                                                        | 28 mai 2025 |



d'informations, consultez la section [Réplication de vos données avec FlexCache](#).

[Amazon a FSx mis à jour la politique FSx FullAccess AWS gérée par Amazon](#)

La politique FSx FullAccess gérée par [Amazon](#) a été mise à jour pour ajouter les `fsx:DetachAndDeleteS3AccessPoint` autorisations `fsx:CreateAndAttachS3AccessPoint` `fsx:DescribeS3AccessPointAttachments` , `fsx:UpdateS3AccessPointAttachments` , et.

28 mai 2025

[Amazon a FSx mis à jour la politique FSx ConsoleFullAccess AWS gérée par Amazon](#)

La politique FSx ConsoleFullAccess gérée par [Amazon](#) a été mise à jour pour ajouter les `fsx:DetachAndDeleteS3AccessPoint` autorisations `fsx:CreateAndAttachS3AccessPoint` `fsx:DescribeS3AccessPointAttachments` , `fsx:UpdateS3AccessPointAttachments` , et.

28 mai 2025

[Région AWS Support  
supplémentaire ajouté](#)

FSx pour les systèmes de fichiers ONTAP sont désormais disponibles en Asie-Pacifique (Thaïlande) et au Mexique (centre). Pour plus d'informations, consultez [la section Disponibilité par Région AWS](#).

8 mai 2025

[La protection autonome contre les ransomwares \(ARP\) est désormais prise en charge](#)

L'ARP, une fonctionnalité NetApp basée sur l'IA qui surveille et protège contre les attaques de ransomwares et de logiciels malveillants, est désormais prise en charge par FSx for ONTAP. Pour plus d'informations, voir [Protection de vos données grâce à une protection autonome contre les ransomwares](#)

7 avril 2025

[Une nouvelle rubrique du guide de l'utilisateur FSx pour ONTAP explique comment configurer un serveur SMB dans un groupe de travail](#)

[Configuration de serveurs SMB dans un groupe de travail](#) décrit comment configurer un serveur SMB dans un groupe de travail sur une SVM au lieu de joindre une SVM à un Microsoft Active Directory.

4 mars 2025

[Amazon a FSx mis à jour la politique FSx ConsoleReadOnlyAccess AWS gérée par Amazon](#)

Amazon a FSx mis à jour la FSx ConsoleReadOnlyAccess politique d'Amazon pour ajouter l'ec2:DescribeNetworkInterfaces autorisation. Pour plus d'informations, consultez la FSx ConsoleReadOnlyAccess politique [d'Amazon](#).

25 février 2025

[Des Harvest tableaux de bord supplémentaires sont désormais pris en charge](#)

Des Harvest tableaux de bord supplémentaires sont désormais pris en charge par FSx for ONTAP, y compris les tableaux de bord qui ne sont pas activés par défaut. Une liste de tableaux de bord non compatibles avec ONTAP a également été ajoutée. FSx Pour plus d'informations, voir [Surveillance des systèmes FSx de fichiers ONTAP à l'aide de Harvest et Grafana](#).

18 février 2025

[Nouveau sujet FSx relatif à la facturation et aux rapports d'utilisation d'ONTAP ajouté au guide de l' FSx utilisateur d'ONTAP](#)

La rubrique [Rapports AWS de facturation et d'utilisation FSx pour ONTAP](#) explique comment accéder aux rapports de facturation et d'utilisation FSx pour les systèmes de fichiers ONTAP dans la AWS Billing and Cost Management console. Il fournit également tous les types d'utilisation dans les deux rapports spécifiques FSx à ONTAP.

13 février 2025

[Support ajouté pour les points de terminaison d'interface VPC à double pile pour Amazon FSx](#)

Vous pouvez désormais créer des points de terminaison d'interface VPC à double pile pour FSx Amazon IPv4 avec à la IPv6 fois des adresses IP et des noms DNS. Pour plus d'informations, consultez la section relative [FSx aux points de terminaison ONTAP et VPC d'interface](#).

7 février 2025

[Support ajouté pour les points de terminaison d'API à double pile](#)

L'API du FSx service Amazon pour la création et la gestion des systèmes de fichiers possède de nouveaux points de terminaison à double pile. Pour plus d'informations, consultez la section [Points de terminaison des API](#) dans le Amazon FSx API Reference.

7 février 2025

[Amazon a FSx mis à jour la politique FSx ConsoleFullAccess AWS gérée par Amazon](#)

Amazon a FSx mis à jour la FSx ConsoleFullAccess politique d'Amazon pour ajouter l'ec2:DescribeNetworkInterfaces autorisation. Pour plus d'informations, consultez la FSx ConsoleFullAccess politique [d'Amazon](#).

7 février 2025

[Nouveau sujet publié, Réplication de données avec FlexCache](#)

Publication d'une nouvelle rubrique décrivant comment répliquer les données d'un système de fichiers ONTAP local vers un système de fichiers ONTAP à l'aide d'un système FSx de fichiers ONTAP a été publiée. FlexCache Pour plus d'informations, consultez la section [Réplication de données avec FlexCache](#).

19 décembre 2024

[Support ajouté pour les systèmes de fichiers de deuxième génération](#)

Vous pouvez désormais créer des systèmes de fichiers mono-AZ et multi-AZ de deuxième génération. Une seule paire de haute disponibilité (HA) fournit désormais jusqu'à 6 % de capacité GBps de débit et 200 000 IOPS sur SSD. Pour plus d'informations, consultez la section [Paires à haute disponibilité \(HA\)](#).

9 juillet 2024

[Support ajouté pour lire les données d'un volume lors de sa restauration à partir d'une sauvegarde](#)

Vous pouvez désormais monter un volume avec un accès en lecture seule aux données du fichier pendant sa restauration à partir d'une sauvegarde sur des systèmes de fichiers de deuxième génération. Pour plus d'informations, consultez [la section Restauration des sauvegardes sur un nouveau volume](#).

9 juillet 2024

[Support ajouté pour ajuster la capacité de débit sur les systèmes de fichiers de deuxième génération](#)

Vous pouvez désormais ajuster la capacité de débit de vos systèmes de fichiers de deuxième génération après leur création. Pour plus d'informations, consultez la section [Gestion de la capacité de débit](#).

9 juillet 2024

[Support ajouté pour l'ajout de paires HA aux systèmes de fichiers mono-AZ de deuxième génération](#)

Vous pouvez désormais ajouter des paires HA aux systèmes de fichiers mono-AZ de deuxième génération après leur création. Vous pouvez disposer de 12 paires HA au total sur un système de fichiers mono-AZ de deuxième génération. Pour plus d'informations, consultez la section [Ajout de paires à haute disponibilité \(HA\)](#).

9 juillet 2024

[Support ajouté pour le protocole Non-Volatile Memory Express over TCP \(NVMe/TCP\)](#)

Vous pouvez désormais utiliser le NVMe/TCP protocole pour le transport de données sur Amazon FSx pour les systèmes de fichiers NetApp ONTAP. Pour plus d'informations, voir [Utilisation des protocoles de stockage par blocs](#)

9 juillet 2024

[Support ajouté pour le fsxadmin-readonly rôle des utilisateurs administratifs du système de fichiers](#)

Le fsxadmin-readonly rôle est désormais disponible pour les utilisateurs administratifs du système de ONTAP fichiers et peut être utilisé pour les applications de surveillance du système de fichiers telles que NetApp Harvest. Pour plus d'informations, consultez la section [Rôles et utilisateurs des administrateurs de systèmes de fichiers](#).

30 avril 2024

[Support ajouté pour l'authentification par clé publique SSH pour les utilisateurs administratifs 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, voir [Configuration de l'authentification Active Directory pour ONTAP les utilisateurs](#).

30 avril 2024

[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 jusqu'à 72 % GBps de capacité de débit et 2 400 000 IOPS sur SSD sur 12 paires de haute disponibilité (HA). Pour plus d'informations, consultez les [paires de haute disponibilité \(HA\)](#) et [Amazon FSx pour les performances NetApp 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 la section [Utilisation AWS Backup avec Amazon FSx](#).

11 janvier 2024



[Amazon FSx FullAccess a FSx mis à jour les politiques FSx ServiceRolePolicy AWS gérées par Amazon FSx ConsoleFullAccess FSxReadOnlyAccess, Amazon FSxConsoleReadOnlyAccess, Amazon, Amazon et Amazon](#)

Amazon a FSx mis à jour les FSx ServiceRolePolicy politiques d'Amazon FSx FullAccess FSx ConsoleFullAccess FSxReadOnlyAccess, Amazon FSxConsoleReadOnlyAccess, Amazon, Amazon et Amazon pour ajouter l'ec2:GetSecurityGroupsForVpc autorisation. Pour plus d'informations, consultez les [FSx mises à jour des politiques AWS gérées par Amazon](#).

9 janvier 2024

[Amazon a FSx mis à jour FSx FullAccess les politiques FSx ConsoleFullAccess AWS gérées par Amazon et Amazon](#)

Amazon a FSx mis à jour les FSx ConsoleFullAccess politiques d'Amazon FSx FullAccess et d'Amazon pour ajouter ManageCrossAccountDataReplication cette action. Pour plus d'informations, consultez les [FSx mises à jour des politiques AWS gérées par Amazon](#).

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 jusqu'à 36 % de capacité GBps de débit et 1 200 000 IOPS sur SSD sur six paires de haute disponibilité (HA). Pour plus d'informations, consultez les [paires de haute disponibilité \(HA\)](#) et [Amazon FSx pour les performances NetApp ONTAP](#).

26 novembre 2023

### [Support ajouté pour les FlexGroup volumes](#)

Amazon FSx for NetApp ONTAP a ajouté la prise en charge des FlexGroup volumes. 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 FSx console, la CLI et l'API Amazon. Pour plus d'informations, voir [Création de systèmes FSx de fichiers ONTAP dans des sous-réseaux partagés](#)

26 novembre 2023

[Amazon a FSx mis à jour FSx FullAccess les politiques FSx ConsoleFullAccess AWS gérées par Amazon et Amazon](#)

Amazon a FSx mis à jour les FSx ConsoleFullAccess politiques d'Amazon FSx FullAccess et d'Amazon pour ajouter l'fsx:CopySnapshotAndUpdateVolume autorisation. Pour plus d'informations, consultez les [FSx mises à jour des politiques AWS gérées par Amazon](#).

26 novembre 2023

[Amazon a FSx mis à jour FSx FullAccess les politiques FSx ConsoleFullAccess AWS gérées par Amazon et Amazon](#)

Amazon a FSx mis à jour les FSx ConsoleFullAccess politiques d'Amazon FSx FullAccess et d'Amazon pour ajouter les fsx:UpdateSharedVPCConfiguration autorisations fsx:DescribeSharedVPCConfiguration et. Pour plus d'informations, consultez les [FSx mises à jour des politiques AWS gérées par Amazon](#).

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 privilèges 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 pour 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 supplémentaires 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 a FSx mis à jour la politique FSx ServiceRolePolicy AWS gérée par Amazon](#)

Amazon a FSx mis à jour l'`cloudwatch:PutMetricData` autorisation dans Amazon FSxServiceRolePolicy. Pour plus d'informations, consultez les [FSx mises à jour des politiques AWS gérées par Amazon](#).

24 juillet 2023

### [Support ajouté pour l'utilisation directe de NetApp System Manager](#)

Vous pouvez gérer vos systèmes de fichiers FSx pour ONTAP en utilisant System Manager directement depuis 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 FSx les événements du système de fichiers 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 FSx des événements ONTAP EMS.](#)

13 juillet 2023

### Support ajouté pour SnapLock

FSx for ONTAP prend désormais en charge les SnapLock volumes. SnapLock 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. 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 IPsec le chiffrement des données en transit

FSx for ONTAP prend désormais en charge l'utilisation du IPsec chiffrement pour chiffrer les données en transit entre les systèmes de fichiers et les clients connectés. Pour plus d'informations, voir [Configuration à IPsec l'aide de l'authentification PSK](#) et [Configuration à IPsec l'aide de l'authentification par certificat](#).

13 juillet 2023

[La taille maximale du volume a augmenté](#)

FSx pour ONTAP, la taille maximale d'un volume a été mise à jour de 100 To à 300 To. Pour plus d'informations, voir [Activer le dimensionnement automatique du volume](#).

13 juillet 2023

[Amazon a FSx mis à jour la politique FSx FullAccess AWS gérée par Amazon](#)

Amazon a FSx mis à jour la FSx FullAccess politique d'Amazon pour supprimer l'fsx : \*autorisation et ajouter des fsx actions spécifiques. Pour plus d'informations, consultez la FSx FullAccess politique [d'Amazon](#).

13 juillet 2023

[Amazon a FSx mis à jour la politique FSx ConsoleFullAccess AWS gérée par Amazon](#)

Amazon a FSx mis à jour la FSx ConsoleFullAccess politique d'Amazon pour supprimer l'fsx : \*autorisation et ajouter des fsx actions spécifiques. Pour plus d'informations, consultez la FSx ConsoleFullAccess politique [d'Amazon](#).

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 NVMe  
lecture ajouté pour les  
systèmes de fichiers mono-AZ](#)

NVMe le cache de lecture est désormais pris en charge pour les systèmes de fichiers mono-AZ créés après le 28 novembre 2022 avec une capacité GBps de débit d'au moins 2 % 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'utilisa  
tion de plages d'adresses IP  
intégrées au VPC pour créer  
des systèmes de fichiers multi-  
AZ](#)

Vous pouvez désormais créer des systèmes de fichiers FSx Multi-AZ pour ONTAP en spécifiant des points de terminaison situés dans la plage d'adresses IP de votre VPC. Pour plus d'informations, voir [Création 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 Multi-AZ FSx pour ONTAP existant ou dissocier (supprimer) une table de routage VPC existante d'un système de fichiers Multi-AZ pour ONTAP existant. FSx 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' EC2 instances Amazon prises en charge dans les régions USA Est (Ohio), USA Est (Virginie du Nord), USA Ouest (Oregon) et Europe (Irlande). Pour plus d'informations, 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 FSx console Amazon ou de FSx l'API Amazon. AWS CLI 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' FSx API AWS CLI ou Amazon 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 l'une des trois politiques intégrées relatives aux instantanés lorsque vous créez ou mettez à jour un volume à l'aide de la FSx console Amazon ou de FSx l'API Amazon. AWS CLI 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 MBps de débit de 4 096 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 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 FSx pour l'utilisation d'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 le VMware cloud sur des centres de données AWS définis par logiciel (SDDCs). Cette prise en charge supplémentaire offre la flexibilité nécessaire pour augmenter ou diminuer le stockage indépendamment des ressources de calcul pour le VMware Cloud sur les AWS charges de travail. Pour plus d'informations, consultez la section [Utilisation du 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 utiliser AWS Backup pour sauvegarder et restaurer vos systèmes de FSx fichiers en plus d'utiliser les FSx sauvegardes natives d'Amazon. Pour plus d'informations, consultez la section [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 une zone de disponibilité unique FSx pour les systèmes de fichiers ONTAP, conçus pour garantir 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 terminais on VPC d'interface](#)

Vous pouvez désormais utiliser les points de terminais on VPC de l'interface pour accéder à l' FSx API Amazon 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 le dimensionnement des IOPS provisionnés](#)

Vous pouvez désormais augmenter la capacité de stockage SSD et les IOPS provisionnées pour les systèmes de fichiers ONTAP existants FSx 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 provisionnés](#).

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 supplémen  
taires du système de fichiers](#)

FSx for ONTAP prend désormais en charge les MBps options 128 MBps et 256 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 capacités APIs 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.