Guide de l'utilisateur Windows

Amazon FSx for Windows File Server

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon FSx for Windows File Server: Guide de l'utilisateur Windows

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d’Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n’est pas d’Amazon, d’une manière susceptible de créer une confusion parmi 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 que FSx for Windows File Server ?

Amazon FSx for Windows File Server fournit des serveurs de fichiers Microsoft Windows entièrement gérés, sécurisés par un système de fichiers Windows entièrement natif. FSx for Windows File Server possède les fonctionnalités, les performances et la compatibilité nécessaires pour transférer et transférer facilement les applications d'entreprise vers le. AWS Cloud

Amazon FSx prend en charge un large éventail de charges de travail Windows d'entreprise avec un stockage de fichiers entièrement géré basé sur Microsoft Windows Server. Amazon FSx prend en charge nativement les fonctionnalités du système de fichiers Windows et le protocole SMB (Server Message Block) standard pour accéder au stockage de fichiers via un réseau. Amazon FSx est optimisé pour les applications d'entreprise dans le monde, avec une compatibilité native avec Windows AWS Cloud, des performances et des fonctionnalités d'entreprise, ainsi que des latences constantes inférieures à la milliseconde.

Grâce au stockage de fichiers sur Amazon FSx, le fonctionnement du code, des applications et des outils actuellement utilisés par les développeurs et administrateurs Windows reste inchangé. Les applications et charges de travail Windows idéales pour Amazon FSx incluent les applications professionnelles, les annuaires personnels, le service Web, la gestion de contenu, l'analyse des données, les configurations de développement de logiciels et les charges de travail de traitement multimédia.

En tant que service entièrement géré, FSx for Windows File Server élimine la surcharge administrative liée à la configuration et à l'approvisionnement des serveurs de fichiers et des volumes de stockage. En outre, Amazon FSx met à jour les logiciels Windows, détecte et corrige les défaillances matérielles, et effectue des sauvegardes. Il fournit également une intégration riche avec d'autres AWS services tels que AWS IAM AWS Directory Service for Microsoft Active Directory WorkSpacesAWS Key Management Service, Amazon et AWS CloudTrail.

Ressources de FSx for Windows File Server : systèmes de fichiers, sauvegardes et partages de fichiers

Les principales ressources d'Amazon FSx sont les systèmes de fichiers et les sauvegardes. Un système de fichiers est l'endroit où vous stockez et accédez à vos fichiers et dossiers. Un système de fichiers est composé d'un ou de plusieurs serveurs de fichiers et volumes de stockage Windows. Lorsque vous créez un système de fichiers, vous spécifiez la capacité de stockage

(en GiB), le nombre d'IOPS du SSD et la capacité de débit (en Mo/s). Vous pouvez modifier ces propriétés en fonction de l'évolution de vos besoins après avoir créé le système de fichiers. Pour plus d'informations, consultez Gestion de la capacité de stockage, Gestion des IOPS sur SSD et Gestion de la capacité de débit.

Les sauvegardes de FSx for Windows File Server file-system-consistent sont extrêmement durables et incrémentielles. Pour garantir la cohérence du système de fichiers, Amazon FSx utilise le Volume Shadow Copy Service (VSS) sous Microsoft Windows. Les sauvegardes quotidiennes automatiques sont activées par défaut lorsque vous créez un système de fichiers, et vous pouvez également effectuer des sauvegardes manuelles supplémentaires à tout moment. Pour plus d'informations, consultez Utilisation des sauvegardes.

Un partage de fichiers Windows est un dossier spécifique (et ses sous-dossiers) de votre système de fichiers que vous rendez accessible à vos instances de calcul avec SMB. Votre système de fichiers est déjà fourni avec un partage de fichiers Windows par défaut appelé`\share`. Vous pouvez créer et gérer autant d'autres partages de fichiers Windows que vous le souhaitez à l'aide de l'outil d'interface utilisateur graphique (GUI) des dossiers partagés sous Windows. Pour plus d'informations, consultez Utilisation des partages de fichiers Microsoft Windows.

Les partages de fichiers sont accessibles à l'aide du nom DNS du système de fichiers ou des alias DNS que vous associez au système de fichiers. Pour plus d'informations, consultez Gestion des alias DNS.

Accès aux partages de fichiers

Amazon FSx est accessible à partir d'instances de calcul avec le protocole SMB (compatible avec les versions 2.0 à 3.1.1). Vous pouvez accéder à vos partages depuis toutes les versions de Windows, à partir de Windows Server 2008 et Windows 7, ainsi que depuis les versions actuelles de Linux. Vous pouvez mapper vos partages de fichiers Amazon FSx sur des instances Amazon Elastic Compute Cloud (Amazon EC2), ainsi que sur des instances, des WorkSpaces instances AppStream Amazon 2.0 et VMware Cloud sur des machines virtuelles. AWS

Vous pouvez accéder à vos partages de fichiers à partir d'instances de calcul locales à l'aide de AWS Direct Connect ou AWS VPN. Outre l'accès aux partages de fichiers qui se trouvent dans le même VPC, le même AWS compte et la même AWS région que le système de fichiers, vous pouvez également accéder à vos partages sur des instances de calcul situées dans un VPC, un compte ou une région Amazon différents. Pour ce faire, utilisez le peering VPC ou les passerelles de transit. Pour plus d'informations, consultez Moyens d'accès acceptés.

Sécurité et protection des données

Amazon FSx fournit plusieurs niveaux de sécurité et de conformité pour garantir la protection de vos données. Il chiffre automatiquement les données au repos (pour les systèmes de fichiers et les sauvegardes) à l'aide de clés que vous gérez dans AWS Key Management Service (AWS KMS). Les données en transit sont également automatiquement chiffrées à l'aide des clés de session SMB Kerberos. Il a été évalué pour être conforme aux certifications ISO, PCI-DSS et SOC, et est éligible à la loi HIPAA.

Amazon FSx fournit un contrôle d'accès au niveau des fichiers et des dossiers avec des listes de contrôle d'accès (ACL) Windows. Il fournit un contrôle d'accès au niveau du système de fichiers à l'aide des groupes de sécurité Amazon Virtual Private Cloud (Amazon VPC). En outre, il fournit un contrôle d'accès au niveau de l'API à l'aide de politiques d'accès AWS Identity and Access Management (IAM). Les utilisateurs qui accèdent aux systèmes de fichiers sont authentifiés auprès de Microsoft Active Directory. Amazon FSx s'intègre AWS CloudTrail à Amazon FSx pour surveiller et consigner vos appels d'API, ce qui vous permet de voir les actions entreprises par les utilisateurs sur vos ressources Amazon FSx.

En outre, il protège vos données en effectuant automatiquement des sauvegardes hautement durables de votre système de fichiers sur une base quotidienne et vous permet d'effectuer des sauvegardes supplémentaires à tout moment. Pour plus d’informations, consultez Sécurité dans Amazon FSx.

Disponibilité et durabilité

FSx for Windows File Server propose des systèmes de fichiers dotés de deux niveaux de disponibilité et de durabilité. Les fichiers mono-AZ garantissent une haute disponibilité au sein d'une seule zone de disponibilité (AZ) en détectant et en corrigeant automatiquement les défaillances des composants. En outre, les systèmes de fichiers multi-AZ fournissent une haute disponibilité et une prise en charge du basculement sur plusieurs zones de disponibilité en provisionnant et en gérant un serveur de fichiers de secours dans une zone de disponibilité distincte au sein d'une région. AWS Pour en savoir plus sur les déploiements de systèmes de fichiers mono-AZ et multi-AZ, consultez. Disponibilité et durabilité : systèmes de fichiers mono-AZ et multi-AZ

Gestion des systèmes de fichiers

Vous pouvez administrer vos systèmes de fichiers FSx for Windows File Server à l'aide de commandes de PowerShell gestion à distance personnalisées ou à l'aide de l'interface graphique

native de Windows dans certains cas. Pour en savoir plus sur la gestion des systèmes de fichiers Amazon FSx, consultez. Administration des systèmes de fichiers

Flexibilité des prix et des performances

FSx for Windows File Server vous offre une flexibilité en termes de prix et de performances en proposant à la fois des types de stockage sur disque SSD et sur disque dur (HDD). Le stockage sur disque dur est conçu pour un large éventail de charges de travail, notamment les répertoires personnels, les partages entre utilisateurs et départements et les systèmes de gestion de contenu. Le stockage SSD est conçu pour les charges de travail les plus performantes et les plus sensibles à la latence, notamment les bases de données, les charges de travail de traitement multimédia et les applications d'analyse de données.

Avec FSx for Windows File Server, vous pouvez provisionner le stockage du système de fichiers, les IOPS SSD et le débit indépendamment pour obtenir le bon équilibre entre coûts et performances. Vous pouvez modifier le stockage, les IOPS des SSD et les capacités de débit de votre système de fichiers pour répondre à l'évolution des besoins en matière de charge de travail, afin de ne payer que pour ce dont vous avez besoin. Pour plus d'informations, consultez Optimisation des coûts avec Amazon FSx.

Tarification pour Amazon FSx

Avec Amazon FSx, il n'y a aucun coût initial lié au matériel ou aux logiciels. Vous ne payez que pour les ressources utilisées, sans engagement minimum, frais d'installation ou frais supplémentaires. Pour plus d'informations sur la tarification et les frais associés à ce service, consultez la section Tarification d'Amazon FSx for Windows File Server.

Hypothèses

Pour utiliser Amazon FSx, vous devez disposer d'un AWS compte avec une instance, une instance WorkSpaces , une instance 2.0 ou une machine virtuelle Amazon EC2 exécutée dans VMware Cloud AWS sur des environnements du type pris en charge. AppStream

Dans ce guide, nous formulons les hypothèses suivantes :

- Si vous utilisez Amazon EC2, nous supposons que vous connaissez Amazon EC2. Pour plus d'informations sur l'utilisation d'Amazon EC2, consultez la documentation Amazon Elastic Compute Cloud.

- Si vous utilisez WorkSpaces, nous supposons que vous le connaissez WorkSpaces. Pour plus d'informations sur l'utilisation WorkSpaces, consultez le guide de WorkSpaces l'utilisateur Amazon.
- Si vous utilisez VMware Cloud sur VMware Cloud AWS, nous supposons que vous le connaissez bien. Pour plus d'informations, consultez la section VMware Cloud on AWS.
- Nous supposons que vous connaissez les concepts de Microsoft Active Directory.

Prérequis

Pour créer un système de fichiers Amazon FSx, vous avez besoin des éléments suivants :

- Un AWS compte disposant des autorisations nécessaires pour créer un système de fichiers Amazon FSx et une instance Amazon EC2. Pour plus d'informations, consultez Configuration de votre Compte AWS.
- Une instance Amazon EC2 exécutant Microsoft Windows Server dans le cloud privé virtuel (VPC) basée sur le service Amazon VPC que vous souhaitez associer à votre système de fichiers Amazon FSx. Pour plus d'informations sur la façon d'en créer une, consultez Getting Started with Amazon EC2 Windows Instances dans le guide de l'utilisateur Amazon EC2.
- Amazon FSx fonctionne avec Microsoft Active Directory pour effectuer l'authentification des utilisateurs et le contrôle d'accès. Vous associez votre système de fichiers Amazon FSx à un Microsoft Active Directory lors de sa création. Pour plus d'informations, consultez Utilisation de Microsoft Active Directory dans FSx for Windows File Server.
- Ce guide part du principe que vous n'avez pas modifié les règles du groupe de sécurité par défaut de votre VPC en fonction du service Amazon VPC. Si c'est le cas, vous devez vous assurer d'ajouter les règles nécessaires pour autoriser le trafic réseau de votre instance Amazon EC2 vers votre système de fichiers Amazon FSx. Pour en savoir plus, consultez Sécurité dans Amazon FSx.
- Installez et configurez le AWS Command Line Interface (AWS CLI). Les versions prises en charge sont la 1.9.12 et les versions ultérieures. Pour plus d'informations, consultez la section Installation, mise à jour et désinstallation du AWS CLI dans le guide de l'AWS Command Line Interface utilisateur.

> **Note**
>
> Vous pouvez vérifier la version AWS CLI que vous utilisez à l'aide de la `aws --version` commande.

Forums Amazon FSx pour Windows File Server

Si vous rencontrez des problèmes lors de l'utilisation d'Amazon FSx, utilisez les forums.

Utilisez-vous Amazon FSx pour la première fois ?

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

1. Si vous êtes prêt à créer votre premier système de fichiers Amazon FSx, essayez le. Commencer à utiliser Amazon FSx for Windows File Server
2. Pour plus d'informations sur les performances, consultez Performances de FSx for Windows File Server.
3. Pour plus d'informations sur la sécurité d'Amazon FSx, consultez. Sécurité dans Amazon FSx
4. Pour plus d'informations sur l'API Amazon FSx, consultez le manuel de référence des API Amazon FSx.

Bonnes pratiques pour FSx for Windows File Server

Nous vous recommandons de suivre ces bonnes pratiques lorsque vous travaillez avec Amazon FSx for Windows File Server. Suivez les liens ci-dessous pour en savoir plus sur les sujets abordés.

Rubriques

Bonnes pratiques d'ordre général

Tester vos charges de travail avant de passer à la production

Nous vous recommandons d'utiliser un environnement intermédiaire avec la même configuration que votre environnement de production pour tester vos charges de travail. Par exemple, utilisez les mêmes configurations Active Directory (AD) et réseau, la même taille et la même configuration du système de fichiers, ainsi que les mêmes fonctionnalités Windows, telles que la déduplication des données et les clichés instantanés. L'exécution de charges de travail de test dans un environnement intermédiaire qui simule le trafic de production souhaité permet de garantir le bon déroulement du processus.

Nous vous recommandons également de revoir le modèle de disponibilité de votre système de fichiers et de vous assurer que votre charge de travail résiste au comportement de restauration attendu pour votre type de système de fichiers lors d'événements tels que la maintenance du système de fichiers, les modifications de capacité de débit et les interruptions de service imprévues. Pour plus d’informations, consultez Disponibilité et durabilité : systèmes de fichiers mono-AZ et multi-AZ.

Création d'un plan de surveillance

Vous pouvez utiliser les métriques du système de fichiers pour surveiller l'utilisation de votre stockage et des performances, comprendre vos habitudes d'utilisation et déclencher des notifications lorsque votre utilisation approche les limites de stockage ou de performance de votre système de fichiers. La surveillance de vos systèmes de fichiers Amazon FSx ainsi que du reste de votre environnement

d'applications vous permet de résoudre rapidement tout problème susceptible d'avoir un impact sur les performances.

Veiller à ce que vos systèmes de fichiers disposent de ressources suffisantes

L'insuffisance des ressources peut entraîner une augmentation de la latence et de la mise en file d'attente pour les demandes d'E/S, ce qui peut apparaître comme une indisponibilité totale ou partielle de votre système de fichiers. Pour plus d'informations sur la surveillance des performances et l'accès aux avertissements et recommandations en matière de performances, consultezSurveillance du serveur de fichiers FSx for Windows.

Sauvegarde régulière de vos systèmes de fichiers

Les sauvegardes régulières vous permettent de répondre à vos besoins en matière de conservation des données, d'activité et de conformité. Nous vous recommandons d'utiliser les sauvegardes quotidiennes automatiques activées par défaut pour votre système de fichiers et de les utiliser comme solution de sauvegarde centralisée AWS Backup pour l'ensemble de votre système Services AWS. AWS Backup vous permet de configurer des plans de sauvegarde supplémentaires avec des fréquences différentes (par exemple, plusieurs fois par jour, quotidiennement ou chaque semaine) et des périodes de conservation différentes.

Bonnes pratiques de sécurité

Nous vous recommandons de suivre ces bonnes pratiques pour administrer la sécurité et les contrôles d'accès de votre système de fichiers. Pour des informations plus détaillées sur la configuration d'Amazon FSx afin de répondre à vos objectifs de sécurité et de conformité, consultez. Sécurité dans Amazon FSx

Sécurité du réseau

Ne modifiez ni ne supprimez l'ENI associé à votre système de fichiers

Votre système de fichiers Amazon FSx est accessible via une interface ELASTIC (ENI) qui réside dans le cloud privé virtuel (VPC) associé 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.

Utilisation de groupes de sécurité et de listes ACL réseau

Vous pouvez utiliser des groupes de sécurité et des listes de contrôle d'accès réseau (ACL) pour limiter l'accès à vos systèmes de fichiers. Pour les groupes de sécurité VPC, le groupe de sécurité par défaut est déjà ajouté à votre système de fichiers dans la console. Assurez-vous que le groupe de sécurité et les ACL réseau des sous-réseaux sur lesquels vous créez votre système de fichiers autorisent le trafic sur les ports. Pour plus d'informations, consultez Groupes de sécurité Amazon VPC.

Active Directory

Lorsque vous créez un système de fichiers Amazon FSx, vous pouvez le joindre à votre domaine Microsoft AD pour authentifier les utilisateurs et autoriser le contrôle d'accès au niveau du partage, du fichier et du dossier. Vos utilisateurs peuvent utiliser leurs comptes AD existants pour se connecter aux partages de fichiers et accéder aux fichiers et dossiers qu'ils contiennent. En outre, vous pouvez migrer la configuration ACL de sécurité existante vers Amazon FSx sans aucune modification. Amazon FSx vous propose deux options pour Active Directory : AWS Microsoft AD géré ou Microsoft AD autogéré.

Si vous utilisez un Microsoft AD AWS géré, nous vous recommandons de conserver les paramètres par défaut de votre groupe de sécurité AD. Si vous modifiez ces paramètres, assurez-vous de conserver une configuration réseau qui répond aux exigences du réseau. Pour plus d'informations, consultez Conditions préalables à la mise en réseau.

Si vous utilisez un Microsoft AD autogéré, vous disposez d'options supplémentaires pour configurer votre système de fichiers. Nous recommandons les meilleures pratiques suivantes pour la configuration initiale lorsque vous utilisez Amazon FSx avec votre Microsoft AD autogéré :

- Attribuez des sous-réseaux à un seul site AD : si votre environnement AD comporte un grand nombre de contrôleurs de domaine, utilisez Active Directory Sites and Services pour attribuer les sous-réseaux utilisés par vos systèmes de fichiers Amazon FSx à un seul site AD offrant une disponibilité et une fiabilité optimales. Assurez-vous que le groupe de sécurité VPC, l'ACL du réseau VPC, les règles de pare-feu Windows sur vos contrôleurs de domaine et tous les autres contrôles de routage réseau présents dans votre infrastructure AD autorisent les communications depuis Amazon FSx sur les ports requis. Cela permet à Windows de revenir à d'autres contrôleurs de domaine s'il ne peut pas utiliser le site AD attribué. Pour plus d'informations, consultez Contrôle d'accès au système de fichiers avec Amazon VPC.

- Utiliser une unité organisationnelle (UO) distincte : utilisez une unité organisationnelle distincte de toutes les autres unités organisationnelles que vous pourriez avoir pour vos systèmes de fichiers Amazon FSx.
- Configurez votre compte de service avec les privilèges minimaux requis : configurez ou déléguez le compte de service que vous fournissez à Amazon FSx avec les privilèges minimaux requis. Pour plus d'informations, consultez Conditions préalables à l'utilisation d'un Microsoft Active Directory autogéré et Délégation de privilèges à votre compte de service Amazon FSx .
- Vérifiez en permanence votre configuration AD : exécutez l'outil de validation Amazon FSx Active Directory par rapport à votre configuration AD avant de créer votre système de fichiers Amazon FSx afin de vérifier que votre configuration est valide pour une utilisation avec Amazon FSx et pour découvrir les éventuels avertissements et erreurs que l'outil pourrait révéler.

Évitez de perdre la disponibilité en raison d'une mauvaise configuration d'AD

Lorsque vous utilisez Amazon FSx avec votre Microsoft AD autogéré, il est important de disposer d'une configuration AD valide, non seulement lors de la création de votre système de fichiers, mais également pour garantir les opérations et la disponibilité continues. Lors d'événements de reprise après défaillance, d'événements de maintenance de routine et d'actions de mise à jour de la capacité de débit, Amazon FSx intègre les ressources du serveur de fichiers à votre Active Directory. Si la configuration AD n'est pas valide lors d'un événement, votre système de fichiers passe à l'état Mal configuré et risque de devenir indisponible. Voici quelques moyens d'éviter de perdre la disponibilité :

- Maintenez votre configuration AD à jour avec Amazon FSx : si vous apportez des modifications, telles que la réinitialisation du mot de passe de votre compte de service, assurez-vous de mettre à jour la configuration de tous les systèmes de fichiers utilisant ce compte de service.
- Surveillez les erreurs de configuration d'AD : définissez vous-même des notifications d'état mal configurées afin de pouvoir réinitialiser la configuration AD de votre système de fichiers, si nécessaire. Pour un exemple utilisant une solution basée sur Lambda pour y parvenir, consultez la section Surveillance de l'état des systèmes de fichiers Amazon FSx à l'aide d'Amazon et. EventBridge AWS Lambda
- Validez régulièrement votre configuration AD : si vous souhaitez détecter de manière proactive les erreurs de configuration AD, nous vous recommandons d'exécuter régulièrement l'outil de validation Active Directory par rapport à votre configuration AD. Si vous recevez des avertissements ou des erreurs lors de l'exécution de l'outil de validation, cela signifie que votre système de fichiers risque d'être mal configuré.

- Ne déplacez ni ne modifiez les objets informatiques créés par FSx : Amazon FSx crée et gère les objets informatiques dans votre AD, à l'aide du compte de service et des autorisations que vous fournissez. Le déplacement ou la modification de ces objets informatiques peut entraîner une mauvaise configuration de votre système de fichiers.

ACL Windows

Avec Amazon FSx, vous utilisez des listes de contrôle d'accès (ACL) Windows standard pour un contrôle d'accès précis au niveau des partages, des fichiers et des dossiers. Les systèmes de fichiers Amazon FSx vérifient automatiquement les informations d'identification des utilisateurs qui accèdent aux données du système de fichiers pour appliquer ces ACL Windows.

- Ne modifiez pas les autorisations ACL NTFS pour l'utilisateur du SYSTÈME : Amazon FSx exige que l'utilisateur du SYSTÈME dispose du contrôle total des autorisations ACL NTFS sur tous les dossiers de votre système de fichiers. La modification des autorisations ACL NTFS pour l'utilisateur du SYSTÈME peut rendre votre système de fichiers inaccessible et les futures sauvegardes du système de fichiers peuvent devenir inutilisables.

Configuration et dimensionnement appropriés de votre système de fichiers

Sélection d'un type de déploiement

Amazon FSx propose deux options de déploiement : mono-AZ et multi-AZ. Nous recommandons d'utiliser des systèmes de fichiers multi-AZ pour la plupart des charges de travail de production qui nécessitent une haute disponibilité des données de fichiers Windows partagées. Pour plus d'informations, consultez Disponibilité et durabilité : systèmes de fichiers mono-AZ et multi-AZ.

Sélection d'un type de stockage

Le stockage SSD convient à la plupart des charges de travail de production soumises à des exigences de performances élevées et à une sensibilité à la latence. Des exemples de ces charges de travail incluent les bases de données, l'analyse des données, le traitement multimédia et les applications commerciales. Nous recommandons également le SSD pour les cas d'utilisation impliquant un grand nombre d'utilisateurs finaux, des niveaux élevés d'E/S ou des ensembles de données contenant un grand nombre de petits fichiers. Enfin, nous vous recommandons d'utiliser

le stockage SSD si vous prévoyez d'activer les copies instantanées. Vous pouvez configurer et dimensionner les IOPS SSD pour les systèmes de fichiers dotés d'un stockage SSD, mais pas d'un stockage sur disque dur.

Si vous décidez d'utiliser le stockage sur disque dur, testez votre système de fichiers pour vous assurer qu'il répond à vos exigences de performance. Le stockage sur disque dur est moins coûteux que le stockage SSD, mais avec des latences plus élevées et des niveaux inférieurs de débit et d'IOPS par unité de stockage. Il peut convenir aux partages utilisateur à usage général et aux répertoires personnels nécessitant peu d'E/S, aux grands systèmes de gestion de contenu (CMS) dans lesquels les données sont rarement récupérées, ou aux ensembles de données contenant un petit nombre de fichiers volumineux. Pour plus d'informations, consultez Configuration et performances du stockage.

Vous pouvez mettre à niveau votre type de stockage du disque dur au SSD à tout moment à l'aide de la console Amazon FSx ou de l'API Amazon FSx. Pour plus d'informations, consultez Gestion du type de stockage.

Sélection d'une capacité de débit

Configurez votre système de fichiers avec une capacité de débit suffisante pour répondre non seulement au trafic attendu de votre charge de travail, mais également aux ressources de performance supplémentaires nécessaires pour prendre en charge les fonctionnalités que vous souhaitez activer sur votre système de fichiers. Par exemple, si vous exécutez la déduplication des données, la capacité de débit que vous sélectionnez doit fournir suffisamment de mémoire pour exécuter la déduplication en fonction de l'espace de stockage dont vous disposez. Si vous utilisez des clichés instantanés, augmentez la capacité de débit à une valeur au moins trois fois supérieure à la valeur censée être déterminée par votre charge de travail afin d'éviter que Windows Server ne supprime vos clichés instantanés. Pour plus d'informations, consultez Impact de la capacité de débit sur les performances.

Augmenter votre capacité de stockage et votre capacité de débit

Augmentez la capacité de stockage de votre système de fichiers lorsque l'espace de stockage disponible est insuffisant ou lorsque vous prévoyez que vos besoins de stockage dépasseront la limite de stockage actuelle. Nous vous recommandons de conserver à tout moment au moins 10 % de la capacité de stockage disponible sur votre système de fichiers. Nous recommandons également d'augmenter la capacité de stockage d'au moins 20 % avant le dimensionnement du stockage, car vous ne pourrez pas l'augmenter tant que le processus est en cours. Vous pouvez

utiliser l' CloudWatch indicateur de FreeStoragecapacité pour surveiller la quantité de stockage gratuit disponible et comprendre ses tendances. Pour plus d'informations, consultez Gestion de la capacité de stockage.

Vous devez également augmenter la capacité de débit de votre système de fichiers si votre charge de travail est limitée par les limites de performances actuelles. Vous pouvez utiliser la page Surveillance et performances de la console FSx pour voir quand les demandes de charge de travail ont atteint ou dépassé les limites de performances afin de déterminer si votre système de fichiers est sous-provisionné pour votre charge de travail.

Pour minimiser la durée du dimensionnement du stockage et éviter de réduire les performances d'écriture, nous vous recommandons d'augmenter la capacité de débit de votre système de fichiers avant d'augmenter la capacité de stockage, puis de réduire la capacité de débit une fois l'augmentation de capacité de stockage terminée. La plupart des charges de travail ont un impact minimal sur les performances lors de la mise à l'échelle du stockage, mais les applications gourmandes en écriture avec de grands ensembles de données actifs peuvent temporairement voir leurs performances d'écriture réduites de moitié.

Modification de la capacité de débit pendant les périodes d'inactivité

La mise à jour de la capacité de débit interrompt la disponibilité pendant quelques minutes pour les systèmes de fichiers mono-AZ et entraîne un basculement et un retour en arrière pour les systèmes de fichiers multi-AZ. Pour les systèmes de fichiers multi-AZ, si le trafic est permanent pendant le basculement et le retour en arrière, toutes les modifications de données effectuées pendant cette période devront être synchronisées entre les serveurs de fichiers. Le processus de synchronisation des données peut prendre plusieurs heures pour les charges de travail exigeantes en écriture et en IOPS. Même si votre système de fichiers restera disponible pendant cette période, nous vous recommandons de planifier des fenêtres de maintenance et d'effectuer des mises à jour de la capacité de débit pendant les périodes d'inactivité, lorsque la charge de votre système de fichiers est minimale, afin de réduire la durée de synchronisation des données. Pour en savoir plus, veuillez consulter la section Gestion de la capacité de débit.

Commencer à utiliser Amazon FSx for Windows File Server

Vous découvrirez ci-dessous comment commencer à utiliser FSx for Windows File Server. 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 répertoire Microsoft AD Active Directory AWS géré à l'aide du AWS Directory Service. Vous allez joindre votre système de fichiers et votre instance de calcul à Active Directory.
3. Créez une instance de calcul Amazon Elastic Compute Cloud exécutant Microsoft Windows Server. Vous allez utiliser cette instance pour accéder à votre système de fichiers.
4. Créez un système de fichiers Amazon FSx for Windows File Server à l'aide de la console Amazon FSx.
5. Mappez votre système de fichiers à votre instance EC2
6. Écrivez des données dans votre système de fichiers.
7. Sauvegardez votre système de fichiers.
8. Nettoyez les ressources que vous avez créées.

Rubriques

Configuration de votre Compte AWS

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

Inscrivez-vous pour un Compte AWS

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

Pour vous inscrire à un Compte AWS

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

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

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

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

Création d'un utilisateur doté d'un accès administratif

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

Sécurisez votre Utilisateur racine d'un compte AWS

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

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .

2. Activez l‘authentification multifactorielle (MFA) pour votre utilisateur racine.

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

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d’ AWS IAM Identity Center dans le Guide de l’utilisateur AWS IAM Identity Center .

2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

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

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

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

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

Attribuer l'accès à des utilisateurs supplémentaires

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

   Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.

2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

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

Créez votre système de fichiers

Pour créer votre système de fichiers Amazon FSx, vous devez créer votre instance Windows Amazon Elastic Compute Cloud (Amazon EC2) et le répertoire. AWS Directory Service Si vous n'avez pas encore cette configuration, consultezProcédure 1 : Conditions préalables à la prise en main.

Pour créer votre système de fichiers (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans Sur le tableau de bord, choisissez Create file system (Créer un système de fichiers) pour ouvrir l'assistant de création de système de fichiers.
3. Sur la page Select file system type (Sélectionner le type de système de fichiers), choisissez FSx for Windows File Server, puis Next (Suivant). La page Create file system (Créer un système de fichiers) s'affiche.
4. Pour Méthode de création, choisissez Création standard.

Détails du système de fichiers

1. Dans la section File system details (Informations du système de fichiers), indiquez un nom pour 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 + - =. _ :/
2. Pour le type de déploiement, choisissez Multi-AZ ou Single-AZ.

   - Choisissez Multi-AZ pour déployer un système de fichiers tolérant à l'indisponibilité de la zone de disponibilité. Cette option prend en charge le stockage SSD et HDD.
   - Choisissez Single-AZ pour déployer un système de fichiers déployé dans une seule zone de disponibilité. Mono-AZ 2 est la dernière génération de systèmes de fichiers de zone de disponibilité unique et prend en charge le stockage SSD et HDD.

   Pour plus d'informations, consultez Disponibilité et durabilité : systèmes de fichiers mono-AZ et multi-AZ.
3. Pour le type de stockage, vous pouvez choisir SSD ou HDD.

   FSx for Windows File Server propose des types de stockage sur disque SSD (Solid State Drive) et sur disque dur (HDD). Le stockage SSD est conçu pour les charges de travail les plus

performantes et les plus sensibles à la latence, notamment les bases de données, les charges de travail de traitement multimédia et les applications d'analyse de données. Le stockage sur disque dur est conçu pour un large éventail de charges de travail, notamment les répertoires personnels, les partages de fichiers entre utilisateurs et départements et les systèmes de gestion de contenu. Pour plus d'informations, consultez Optimisation des coûts à l'aide des types de stockage.

4. Pour les IOPS SSD provisionnées, vous pouvez choisir le mode automatique ou le mode provisionné par l'utilisateur.

   Si vous choisissez le mode automatique, FSx for Windows File Server adapte automatiquement le nombre d'E/S par seconde de votre SSD afin de maintenir 3 E/S par seconde par GiB de capacité de stockage. Si vous choisissez le mode provisionné par l'utilisateur, entrez un nombre entier compris entre 96 et 400 000. L'augmentation des IOPS sur SSD au-dessus de 80 000 est disponible dans l'est des États-Unis (Virginie du Nord), dans l'ouest des États-Unis (Oregon), dans l'est des États-Unis (Ohio), en Europe (Irlande), en Asie-Pacifique (Tokyo) et en Asie-Pacifique (Singapour). Pour plus d'informations, consultez Gestion des IOPS sur SSD.

5. Pour Capacité de stockage, entrez la capacité de stockage de votre système de fichiers, en GiB. Si vous utilisez un stockage SSD, entrez un nombre entier compris entre 32 et 65 536. Si vous utilisez un espace de stockage sur disque dur, entrez un nombre entier compris entre 2 000 et 65 536. Vous pouvez augmenter la capacité de stockage selon vos besoins à tout moment après avoir créé le système de fichiers. Pour plus d'informations, consultez Gestion de la capacité de stockage.

6. Conservez la valeur par défaut de Throughput capacity (Capacité de débit). La capacité de débit est la vitesse soutenue à laquelle le serveur de fichiers hébergeant votre système de fichiers peut traiter les données. Le paramètre de capacité de débit recommandée est basé sur la quantité de capacité de stockage que vous choisissez. Si vous avez besoin d'une capacité de débit supérieure à la capacité de débit recommandée, choisissez Spécifier la capacité de débit, puis choisissez une valeur. Pour plus d'informations, consultez Performances de FSx for Windows File Server.

> **Note**
>
> Si vous souhaitez activer l'audit d'accès aux fichiers, vous devez choisir une capacité de débit de 32 Mo/s ou plus. Pour plus d'informations, consultez Audit de l'accès aux fichiers.

Vous pouvez modifier la capacité de débit selon vos besoins à tout moment après avoir créé le système de fichiers. Pour plus d'informations, consultez Gestion de la capacité de débit.

Réseau et sécurité

1. Dans la section Réseau et sécurité, choisissez le VPC Amazon que vous souhaitez associer à votre système de fichiers. Pour cet exercice de mise en route, choisissez le même Amazon VPC que celui que vous avez choisi pour votre AWS Directory Service répertoire et votre instance Amazon EC2.
2. Pour les groupes de sécurité VPC, le groupe de sécurité par défaut pour votre Amazon VPC par défaut est déjà ajouté à votre système de fichiers dans la console. Si vous n'utilisez pas le groupe de sécurité par défaut, assurez-vous que le groupe de sécurité que vous choisissez est Région AWS identique à celui de votre système de fichiers. Pour vous assurer de pouvoir connecter une instance EC2 à votre système de fichiers, vous devez ajouter les règles suivantes au groupe de sécurité que vous avez choisi :

   a. Ajoutez les règles entrantes et sortantes suivantes pour autoriser les ports suivants.

Règles	Ports
UDP	53, 88, 123, 389, 464
TCP	53, 88, 135, 389, 445, 464, 636, 3268, 3269, 5985, 9389, 49152-65535

   Ajoutez des adresses IP de et vers ou des identifiants de groupes de sécurité associés aux instances de calcul clientes à partir desquelles vous souhaitez accéder à votre système de fichiers.

   b. Ajoutez des règles de sortie pour autoriser tout le trafic vers l'Active Directory auquel vous rejoignez votre système de fichiers. Pour ce faire, optez pour l'une des solutions suivantes :

      - Autorisez le trafic sortant vers l'ID du groupe de sécurité associé à votre annuaire AWS Managed AD.

- Autorisez le trafic sortant vers les adresses IP associées à vos contrôleurs de domaine Active Directory autogérés.

> **Note**
>
> Dans certains cas, vous avez peut-être modifié les règles de votre groupe de AWS Managed Microsoft AD sécurité par rapport aux paramètres par défaut. Si tel est le cas, assurez-vous que ce groupe de sécurité dispose des règles entrantes requises pour autoriser le trafic provenant de votre système de fichiers Amazon FSx. Pour plus d'informations sur les règles de trafic entrant requises, consultez la section AWS Managed Microsoft AD Conditions préalables du Guide d'AWS Directory Service administration.

Pour plus d'informations, consultez Contrôle d'accès au système de fichiers avec Amazon VPC.

3. Les systèmes de fichiers multi-AZ possèdent un serveur de fichiers principal et un serveur de secours, chacun dans sa propre zone de disponibilité et son propre sous-réseau. Si vous créez un système de fichiers multi-AZ (voir étape 5), choisissez une valeur de sous-réseau préféré pour le serveur de fichiers principal et une valeur de sous-réseau de secours pour le serveur de fichiers de secours.

   Si vous créez un système de fichiers mono-AZ, choisissez le sous-réseau correspondant à votre système de fichiers.

Authentification Windows

- Pour l'authentification Windows, vous disposez des options suivantes :

  Choisissez AWS Managed Microsoft Active Directory si vous souhaitez associer votre système de fichiers à un domaine Microsoft Active Directory géré par AWS, puis choisissez votre AWS Directory Service répertoire dans la liste. Pour plus d'informations, consultez Utilisation de Microsoft Active Directory dans FSx for Windows File Server.

  Choisissez Microsoft Active Directory autogéré si vous souhaitez associer votre système de fichiers à un domaine Microsoft Active Directory autogéré, et fournissez les informations suivantes pour votre Active Directory. Pour plus d'informations, consultez Utilisation d'Amazon FSx avec votre Microsoft Active Directory autogéré.

- Le nom de domaine complet de votre Active Directory.

  > **Important**
  >
  > Pour les systèmes de fichiers mono-AZ 2 et tous les systèmes de fichiers multi-AZ, le nom de domaine Active Directory ne peut pas dépasser 47 caractères. Cette limitation s'applique à la fois AWS Directory Service aux noms de domaine Active Directory autogérés.
  > Amazon FSx nécessite une connexion directe à votre adresse IP DNS pour le trafic interne. La connexion via une passerelle Internet n'est pas prise en charge. Utilisez plutôt l' AWS Virtual Private Network appairage VPC ou l'association AWS Direct Connect. AWS Transit Gateway

- Adresses IP des serveurs DNS : adresses IPv4 des serveurs DNS de votre domaine

  > **Note**
  >
  > L'EDNS (Extension Mechanisms for DNS) doit être activé sur votre serveur DNS. Si EDNS est désactivé, il se peut que la création de votre système de fichiers échoue.

- 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.
- (Facultatif) Unité organisationnelle (OU) : nom du chemin unique de l'unité organisationnelle à laquelle vous souhaitez rejoindre votre système de fichiers.
- (Facultatif) Groupe d'administrateurs de système de fichiers délégués : nom du groupe de votre Active Directory qui peut administrer votre système de fichiers. Le groupe par défaut est « Administrateurs de domaine ». Pour plus d'informations, consultez Délégation de privilèges à votre compte de service Amazon FSx .

Chiffrement, audit et accès (alias DNS)

1. Pour le chiffrement, choisissez la clé de AWS KMS key chiffrement utilisée pour chiffrer les données de votre système de fichiers au repos. Vous pouvez choisir l'aws/fsx (par défaut) géré par AWS KMS, une clé existante ou une clé gérée par le client en spécifiant l'ARN de la clé. Pour plus d'informations, consultez Chiffrement au repos.

2. Pour l'audit (facultatif), l'audit de l'accès aux fichiers est désactivé par défaut. Pour plus d'informations sur l'activation et la configuration de l'audit d'accès aux fichiers, consultezPour activer l'audit de l'accès aux fichiers lors de la création d'un système de fichiers (console).
3. Pour Accès (facultatif), entrez les alias DNS que vous souhaitez associer au système de fichiers. Chaque nom d'alias doit être formaté en tant que nom de domaine complet (FQDN). Pour plus d'informations, consultez Gestion des alias DNS.

Backup et maintenance

Pour plus d'informations sur les sauvegardes quotidiennes automatiques et les paramètres de cette section, consultezUtilisation des sauvegardes.

1. Pour la sauvegarde automatique quotidienne, elle est activée par défaut. Vous pouvez désactiver ce paramètre si vous ne souhaitez pas qu'Amazon FSx effectue des sauvegardes de votre système de fichiers automatiquement sur une base quotidienne.
2. Si les sauvegardes automatiques sont activées, elles ont lieu au cours d'une période connue sous le nom de fenêtre de sauvegarde. Vous pouvez utiliser la fenêtre par défaut ou choisir une heure de début de fenêtre de sauvegarde automatique.
3. Pour la période de conservation automatique des sauvegardes, vous pouvez utiliser le paramètre par défaut de 30 jours ou définir une valeur comprise entre 1 et 90 jours pendant lesquels Amazon FSx conservera les sauvegardes quotidiennes automatiques de votre système de fichiers. Ce paramètre ne s'applique pas aux sauvegardes initiées par l'utilisateur ou aux sauvegardes effectuées par AWS Backup.
4. Pour les balises (facultatif), entrez 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. Pour plus d'informations, consultez Baliser vos ressources Amazon FSx.

   Choisissez Suivant.

Vérifiez votre configuration et créez

1. 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, vous pouvez voir quels paramètres du système de fichiers vous pouvez et ne pouvez pas modifier une fois le système de fichiers créé. Choisissez Create file system (Créer un système de fichiers).

2. Une fois qu'Amazon FSx a créé le système de fichiers, choisissez l'ID du système de fichiers dans la liste du tableau de bord des systèmes de fichiers pour afficher les détails. Choisissez Joindre, puis notez le nom DNS de votre système de fichiers dans l'onglet Réseau et sécurité. Vous en aurez besoin dans la procédure suivante pour mapper un partage à une instance EC2.

Mappez votre partage de fichiers à une instance EC2 exécutant Windows Server

Vous pouvez désormais monter votre système de fichiers Amazon FSx sur votre instance Amazon EC2 basée sur Microsoft Windows jointe à votre répertoire. AWS Directory Service Le nom de votre partage de fichiers n'est pas le même que le nom de votre système de fichiers.

Pour mapper un partage de fichiers sur une instance Windows Amazon EC2 à l'aide de l'interface graphique

1. Avant de monter un partage de fichiers sur une instance Windows, vous devez lancer l'instance EC2 et la joindre à un AWS Directory Service for Microsoft Active Directory. Pour effectuer cette action, choisissez l'une des procédures suivantes dans le Guide d'AWS Directory Service administration :

   - Jonction facile d'une instance EC2 Windows
   - Jonction manuelle d'une instance Windows
2. Connectez-vous à votre instance. Pour plus d'informations, consultez la section Connexion à votre instance Windows dans le guide de l'utilisateur Amazon EC2.
3. Lorsque vous êtes connecté, ouvrez l'Explorateur de fichiers.
4. Dans le volet de navigation, ouvrez le menu contextuel (clic droit) de Network et choisissez Map Network Drive.
5. Choisissez la lettre de votre choix pour Drive.
6. Vous pouvez mapper votre système de fichiers en utilisant son nom DNS par défaut attribué par Amazon FSx ou en utilisant un alias DNS de votre choix. Cette procédure décrit le mappage d'un partage de fichiers à l'aide du nom DNS par défaut. Si vous souhaitez mapper un partage de fichiers à l'aide d'un alias DNS, consultezProcédure pas à pas 5 : Utilisation d'alias DNS pour accéder à votre système de fichiers.

   Pour Dossier, entrez le nom DNS du système de fichiers et le nom du partage. Le partage Amazon FSx par défaut est appelé. `\share` Vous pouvez trouver le nom DNS

dans la console Amazon FSx, à l'adresse https://console.aws.amazon.com/fsx/, dans la section Windows File Server > Network & Security, ou dans la réponse à une commande d'CreateFileSystemDescribeFileSystemsAPI.

- Pour un système de fichiers mono-AZ joint à un Microsoft Active Directory AWS géré, le nom DNS est le suivant.

```
fs-0123456789abcdef0.ad-domain.com
```

- Pour un système de fichiers mono-AZ joint à un Active Directory autogéré, et pour tout système de fichiers multi-AZ, le nom DNS est le suivant.

```
amznfsxaa11bb22.ad-domain.com
```

Par exemple, saisissez `\\fs-0123456789abcdef0.ad-domain.com\share`.

7. Choisissez si le partage de fichiers doit se reconnecter lors de la connexion, puis choisissez Terminer.

Écrire des données dans votre partage de fichiers

Maintenant que vous avez mappé votre partage de fichiers à votre instance, vous pouvez utiliser ce partage de fichiers comme n'importe quel autre répertoire de votre environnement Windows.

Pour écrire des données dans votre partage de fichiers

1. Ouvrez l'éditeur de texte du Bloc-notes.
2. Rédigez du contenu dans l'éditeur de texte. Par exemple : *Hello, World !*
3. Enregistrez le fichier dans la lettre de lecteur de votre partage de fichiers.
4. À l'aide de l'Explorateur de fichiers, accédez à votre partage de fichiers et recherchez le fichier texte que vous venez d'enregistrer.

Sauvegardez votre système de fichiers

Maintenant que vous avez eu l'occasion d'utiliser votre système de fichiers Amazon FSx et ses partages de fichiers, vous pouvez le sauvegarder. Par défaut, les sauvegardes quotidiennes sont créées automatiquement pendant la fenêtre de sauvegarde de 30 minutes de votre système de

fichiers. Vous pouvez toutefois créer une sauvegarde initiée par l'utilisateur à tout moment. Les sauvegardes entraînent des coûts supplémentaires. Pour plus d'informations sur la tarification des sauvegardes, consultez la section Tarification.

Pour créer une sauvegarde de votre système de fichiers depuis la console

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le tableau de bord de la console, choisissez le nom du système de fichiers que vous avez créé pour cet exercice.
3. Dans l'onglet Vue d'ensemble de votre système de fichiers, sélectionnez Créer une sauvegarde.
4. Dans la boîte de dialogue Créer une sauvegarde qui s'ouvre, donnez un nom à votre sauvegarde. Ce nom peut contenir un maximum de 256 lettres Unicode et inclure des espaces blancs, des chiffres et les caractères spéciaux suivants : + - =. _ :/
5. Choisissez Créer une sauvegarde.
6. Pour afficher toutes vos sauvegardes dans une liste afin de restaurer votre système de fichiers ou de supprimer la sauvegarde, choisissez Sauvegardes.

Lorsque vous créez une nouvelle sauvegarde, son statut est défini sur CRÉATION lors de sa création. Cette opération peut prendre quelques minutes. Lorsque la sauvegarde est prête à être utilisée, son statut passe à DISPONIBLE.

Nettoyage des ressources

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

Pour nettoyer des ressources

1. Sur la console Amazon EC2, mettez fin à votre instance. Pour plus d'informations, consultez la section Résiliation de votre instance dans le guide de l'utilisateur Amazon EC2.
2. Sur la console Amazon FSx, supprimez votre 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. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
    b. Dans le tableau de bord de la console, choisissez le nom du système de fichiers que vous avez créé pour cet exercice.

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

d. Dans la boîte de dialogue Supprimer le système de fichiers qui s'ouvre, décidez si vous souhaitez créer une sauvegarde finale. Si c'est le cas, attribuez un nom à la sauvegarde finale. Toutes les sauvegardes créées automatiquement sont également supprimées.

> **Important**
>
> De nouveaux systèmes de fichiers peuvent être créés à partir de sauvegardes. Nous vous recommandons de créer une sauvegarde finale en tant que bonne pratique. Si vous n'en avez plus besoin au bout d'un certain temps, vous pouvez supprimer cette sauvegarde ainsi que les autres sauvegardes créées manuellement.

e. Entrez l'ID du système de fichiers que vous souhaitez supprimer dans le champ ID du système de fichiers.

f. Choisissez Supprimer le système de fichiers.

g. Le système de fichiers est en cours de suppression et son statut dans le tableau de bord passe à DELETING. Lorsque le système de fichiers a été supprimé, il n'apparaît plus dans le tableau de bord.

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

i. 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.

j. La boîte de dialogue Supprimer les sauvegardes s'ouvre. Laissez la case cochée pour l'ID de la sauvegarde que vous avez sélectionnée, puis choisissez Supprimer les sauvegardes.

Votre système de fichiers Amazon FSx et les sauvegardes automatiques associées sont désormais supprimés.

3. Si vous avez créé un AWS Directory Service répertoire pour cet exercice dansProcédure 1 : Conditions préalables à la prise en main, vous pouvez le supprimer maintenant. Pour plus d'informations, voir Supprimer votre répertoire dans le Guide AWS Directory Service d'administration.

État du système de fichiers Amazon FSx

Vous pouvez consulter l'état d'un système de fichiers Amazon FSx à l'aide de la console Amazon FSx, de la AWS CLI commande describe-file-systems ou des systèmes d'exploitation des API. DescribeFile

État du système de fichiers	Description
DISPONIBLE	Le système de fichiers est en bon état, accessible et prêt à être utilisé.
CREAtioN	Amazon FSx est en train de créer un nouveau système de fichiers.
SUPPRESSION	Amazon FSx est en train de supprimer un système de fichiers existant.
MISE À JOUR	Le système de fichiers est en cours de mise à jour à l'initiative du client.
MAL CONFIGURÉ	Le système de fichiers est dans un état altéré en raison d'une modification de votre environnement Active Directory. Votre système de fichiers est actuellement indisponible ou risque de perdre sa disponibilité, et les sauvegardes risquent d'échouer. Pour plus d'informations sur le rétablissement de la disponibilité, consultez Le système de fichiers est mal configuré.
MAL CONFIGURÉ_INDISPONIBLE	Le système de fichiers est actuellement indisponible en raison d'une modification de votre environnement Active Directory. Pour plus d'informations sur le rétablissement de la disponibilité, consultezLe système de fichiers est mal configuré.

État du système de fichiers	Description
ÉCHEC	• Lors de la création d'un nouveau système de fichiers, Amazon FSx n'a pas pu créer le nouveau système de fichiers. • Le système de fichiers n'est pas disponible. • Le système de fichiers est défaillant et Amazon FSx ne parvient pas à le récupérer. • Amazon FSx n'est pas en mesure de créer des sauvegardes.

Clients, méthodes d'accès et environnements pris en charge pour Amazon FSx for Windows File Server

Vous pouvez accéder à vos systèmes de fichiers Amazon FSx à l'aide d'une variété de clients et de méthodes compatibles provenant des deuxAWSet des environnements sur site.

Rubriques

Clients pris en charge

Amazon FSx prend en charge la connexion à votre système de fichiers 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 Server Message Block (SMB), versions 2.0 à 3.1.1.

Les suivantes :AWSles instances de calcul sont prises en charge pour une utilisation avec Amazon FSx :

- Instances Amazon Elastic Compute Cloud (Amazon EC2), y compris les instances Microsoft Windows, Amazon Linux et Amazon Linux. Pour plus d'informations, consultez Accès aux partages de fichiers.
- Conteneurs Amazon Elastic Container Service (Amazon ECS). Pour plus d'informations, veuillez consulter la rubriqueVolumes FSx for Windows File Serverdans leGuide du développeur Amazon Elastic Container Service.
- WorkSpaces instances — Pour en savoir plus, consultez leAWSbillet de blogUtilisation de FSx for Windows File Server avec Amazon WorkSpaces.
- Amazon AppStream Instances 2.0 : pour en savoir plus, consultez leAWSbillet de blogUtilisation d'Amazon FSx avec Amazon AppStream 2.0.
- Machines virtuelles s'exécutant dans VMware Cloud surAWSenvironnements — Pour en savoir plus, consultez leAWSbillet de blogStockage et partage de fichiers avec FSx for Windows File Server dans un cloud VMware surAWSEnvironnement.

Les systèmes d'exploitation suivants sont pris en charge pour une utilisation avec Amazon FSx :

- Windows Server 2012 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2012 R2, Windows Server 2012 R2, Windows Server 2016, Windows Server 2016, Windows Server 2012, Windows Server 2012, Windows Server 2012, Windows Server 2012
- Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10 (y compris les expériences de bureau Windows 7 et Windows 10 de WorkSpaces) et Windows 11.
- Linux, à l'aide du `cifs-utils` outil.
- macOS

Moyens d'accès acceptés

Vous pouvez utiliser les méthodes et les approches d'accès suivantes avec Amazon FSx.

Accès aux systèmes de fichiers en utilisant leurs noms DNS par défaut

FSx for Windows File Server fournit un nom de système de noms de domaine (DNS) pour chaque système de fichiers. Vous accédez à votre système de fichiers FSx for Windows File Server en mappant une lettre de lecteur sur votre instance de calcul à votre partage de fichiers Amazon FSx à l'aide de ce nom DNS. Pour en savoir plus, veuillez consulter la section Utilisation des partages de fichiers Microsoft Windows.

> **Important**
>
> Amazon FSx enregistre uniquement les enregistrements DNS d'un système de fichiers si vous utilisez Microsoft DNS comme DNS par défaut. Si vous utilisez un DNS tiers, vous devez configurer manuellement les entrées DNS pour vos systèmes de fichiers Amazon FSx. Pour plus d'informations sur le choix des adresses IP correctes à utiliser pour le système de fichiers, consultezObtention des adresses IP de système de fichiers correctes à utiliser pour le DNS.

Pour trouver le nom DNS :

- Dans la console Amazon FSx, choisissezSystèmes de fichiers, puis choisissezDétails. Afficher le nom DNS dansRéseau et sécuritésection.

- Vous pouvez également le consulter dans la réponse duCreateFileSystemouDescribeFileSystemsCommande d'API.

Pour tous les systèmes de fichiers mono-AZ joints à unAWSMicrosoft Active Directory géré, le nom DNS ressemble à ce qui suit :`fs-0123456789abcdef0.ad-dns-domain-name`

Pour tous les systèmes de fichiers mono-AZ joints à un Active Directory autogéré, et pour tout système de fichiers multi-AZ, le nom DNS se présente comme suit :`amznfsxaa11bb22.ad-domain.com`

Utilisation de noms DNS avec l'authentification Kerberos

Nous vous recommandons d'utiliser l'authentification et le chiffrement basés sur Kerberos lors du transit avec Amazon FSx. Kerberos fournit l'authentification la plus sécurisée pour les clients qui accèdent à votre système de fichiers. Pour activer l'authentification basée sur Kerberos et le chiffrement des données en transit pour vos sessions SMB, utilisez le nom DNS du système de fichiers fourni par Amazon FSx pour accéder à votre système de fichiers.

Si vous avez configuré une relation de confiance externe entre votreAWSGestion de Microsoft Active Directory et de votre Active Directory sur site, pour utiliser Amazon FSx Remote PowerShell avec l'authentification Kerberos, vous devez configurer une politique de groupe locale sur le client pour l'ordre de recherche forestière. Pour plus d'informations, veuillez consulter la rubriqueConfigurer l'ordre de recherche dans la forêt Kerberos (KFSO)dans la documentation Microsoft.

Accès aux systèmes de fichiers à l'aide d'alias DNS

FSx for Windows File Server fournit un nom DNS pour chaque système de fichiers que vous pouvez utiliser pour accéder à vos partages de fichiers. Vous pouvez également activer l'accès à Amazon FSx à partir de noms DNS autres que le nom DNS par défaut créé par Amazon FSx en enregistrant des alias pour vos systèmes de fichiers FSx for Windows File Server.

À l'aide d'alias DNS, vous pouvez déplacer vos données de partage de fichiers Windows vers Amazon FSx et continuer à utiliser vos noms DNS existants pour accéder aux données sur Amazon FSx. Les alias DNS vous permettent également d'utiliser des noms significatifs qui facilitent l'administration des outils et des applications pour vous connecter à vos systèmes de fichiers Amazon FSx. Pour plus d'informations, consultez Gestion des alias DNS.

Utilisation d'alias DNS avec l'authentification Kerberos

Nous vous recommandons d'utiliser l'authentification et le chiffrement basés sur Kerberos lors du transit avec Amazon FSx. Kerberos fournit l'authentification la plus sécurisée pour les clients qui accèdent à votre système de fichiers. Pour activer l'authentification Kerberos pour les clients qui accèdent à Amazon FSx à l'aide d'un alias DNS, vous devez ajouter des noms principaux de service (SPN) qui correspondent à l'alias DNS sur l'objet informatique Active Directory de votre système de fichiers Amazon FSx.

Vous pouvez éventuellement obliger les clients qui accèdent au système de fichiers à l'aide d'un alias DNS à utiliser l'authentification et le chiffrement Kerberos en définissant les objets de stratégie de groupe (GPO) suivants dans votre Active Directory :

- Restriction de NTLM : Trafic NTLM sortant vers des serveurs distants- Utilisez ce paramètre de stratégie pour refuser ou auditer le trafic NTLM sortant d'un ordinateur vers tout serveur distant exécutant le système d'exploitation Windows.
- Restriction de NTLM : Ajouter des exceptions de serveur distant pour l'authentification NTLM- Utilisez ce paramètre de stratégie pour créer une liste d'exceptions de serveurs distants sur lesquels les appareils clients sont autorisés à utiliser l'authentification NTLM siSécurité du réseau : Restriction de NTLM : Trafic NTLM sortant vers des serveurs distantsle paramètre de stratégie est configuré.

Pour plus d'informations, consultez Procédure pas à pas 5 : Utilisation d'alias DNS pour accéder à votre système de fichiers.

Utilisation de FSx for Windows File Server avec les systèmes de fichiers FSx for Windows File Server

FSx for Windows File Server prend en charge l'utilisation des espaces de noms Microsoft Distributed File System (DFS). Vous pouvez utiliser les espaces de noms DFS pour organiser les partages de fichiers sur plusieurs systèmes de fichiers dans une structure de dossiers commune (un espace de noms) que vous utilisez pour accéder à l'ensemble de données de fichiers. Vous pouvez utiliser un nom dans votre espace de noms DFS pour accéder à votre système de fichiers Amazon FSx en configurant sa cible de lien comme étant le nom DNS du système de fichiers. Pour plus d'informations, consultez Regroupement de plusieurs systèmes de fichiers avec des espaces de noms DFS.

Environnements compatibles

Vous pouvez accéder à votre système de fichiers à partir de ressources qui se trouvent dans le même VPC que votre système de fichiers. Pour plus d'informations et des instructions détaillées, consultezProcédure 1 : Conditions préalables à la prise en main.

Vous pouvez également accéder aux systèmes de fichiers créés après le 22 février 2019 à partir de ressources locales et de ressources situées dans un autre VPC,AWSCompte, ouAWSRégion. Le tableau suivant illustre les environnements à partir desquels Amazon FSx prend en charge l'accès depuis les clients dans chacun des environnements pris en charge, en fonction de la date de création du système de fichiers.

Clients situés à...	Accès aux systèmes de fichiers créés avant le 22 février 2019	Accès aux systèmes de fichiers créés avant le 17 décembre 2020	Accès aux systèmes de fichiers créés après le 17 décembre 2020
Sous-réseaux dans lesquels le système de fichiers est créé	✓	✓	✓
Blocs d'adresse CIDR principaux du VPC dans lequel le système de fichiers a été créé	✓	✓	✓
CIDR secondaires du VPC dans lequel le système de fichiers a été créé		Clients dont les adresses IP se trouvent dans unRFC 1918plage d'adresses IP privées :	Clients dont les adresses IP se situent en dehors de la plage de blocs CIDR suivante : 198.19.0.0/16

Clients situés à...	Accès aux systèmes de fichiers créés avant le 22 février 2019	Accès aux systèmes de fichiers créés avant le 17 décembre 2020	Accès aux systèmes de fichiers créés après le 17 décembre 2020
Autres réseaux CIDR ou homologues		• 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	

> **Note**
>
> Dans certains cas, vous souhaiterez peut-être accéder à un système de fichiers créé avant le 17 décembre 2020 à partir d'un site local à l'aide d'une plage d'adresses IP non privées. Pour ce faire, créez un nouveau système de fichiers à partir d'une sauvegarde du système de fichiers. Pour plus d'informations, consultez Utilisation des sauvegardes.

Vous trouverez ci-dessous des informations sur la manière d'accéder à vos systèmes de fichiers FSx for Windows File Server à partir de locaux et de différents VPC,AWSdes comptes, ouAWSRégions.

Accès aux systèmes de fichiers FSx for Windows File Server à partir de l'environnement

FSx for Windows File Server prend en charge l'utilisation deAWS Direct ConnectouAWS VPNpour accéder à vos systèmes de fichiers à partir de vos instances de calcul sur site. Avec prise en charge deAWS Direct Connect, FSx for Windows File Server vous permet d'accéder à votre système de fichiers via une connexion réseau dédiée depuis votre environnement sur site. Avec prise en charge deAWS VPN, FSx for Windows File Server vous permet d'accéder à votre système de fichiers depuis vos appareils locaux via un tunnel privé et sécurisé.

Après avoir connecté votre environnement local au VPC associé à votre système de fichiers Amazon FSx, vous pouvez accéder à votre système de fichiers à l'aide de son nom DNS ou d'un alias DNS. Vous le faites de la même manière que vous le faites à partir d'instances de calcul au sein du VPC. Pour plus d'informations sur AWS Direct Connect, consultez le Guide de l'utilisateur AWS Direct

Connect. Pour plus d'informations sur la configurationAWS VPNconnexions, consultezConnexions VPNdans leAmazon VPC User Guide.

FSx for Windows File Server prend également en charge l'utilisation d'Amazon FSx File Gateway pour fournir un accès fluide et à faible latence à vos partages de fichiers FSx for Windows File Server dans le cloud à partir de vos instances de calcul sur site. Pour de plus amples informations, veuillez consulter le .Guide de l'utilisateur d'Amazon FSx File Gateway.

accédant aux systèmes de fichiers FSx for Windows File Server à partir d'un autre VPC, d'un autre compte ouRégion AWS

Vous pouvez accéder à votre système de fichiers FSx for Windows File Server à partir d'instances de calcul d'un VPC différent,AWSCompte, ouAWSRégion à partir de celle associée à votre système de fichiers. Pour ce faire, vous pouvez utiliser l'appairage VPC ou les passerelles de transit. Lorsque vous utilisez une connexion d'appairage ou une passerelle de transit d'un VPC pour connecter des VPC, les instances de calcul qui se trouvent dans un VPC peuvent accéder aux systèmes de fichiers Amazon FSx d'un autre VPC. Cet accès est possible même si les VPC appartiennent à des comptes différents, et même si les VPC résident sur des comptes différentsAWSRégions.

UNConnexion d'appairage de VPCest une connexion de mise en réseau entre deux VPC qui permet d'acheminer le trafic entre ces derniers à l'aide d'adresses IPv4 privées ou d'adresses IP IPv4 ou d'adresses IP IPv4 privées ou d'adresses IP Vous pouvez utiliser l'appairage de VPC pour connecter des VPC au sein d'un même réseauAWSRégion ou entreAWSRégions. Pour plus d'informations sur l'appairage de VPC, consultezQu'est-ce que l'appairage de VPC ?dans leAmazon VPC Peering Guide.

Une passerelle de transit est un hub de transit de réseau que vous pouvez utiliser pour relier votre VPC et vos réseaux sur site. Pour plus d'informations sur l'utilisation des passerelles de transit de VPC, consultezDémarrez avec les passerelles de transitdans lePasserelles de transit Amazon VPC.

Après avoir configuré une connexion de passerelle d'appairage ou de transit d'un VPC, vous pouvez accéder à votre système de fichiers à l'aide de son nom DNS. Vous le faites de la même manière que vous le faites à partir d'instances de calcul au sein du VPC associé.

Disponibilité et durabilité : systèmes de fichiers mono-AZ et multi-AZ

Amazon FSx for Windows File Server propose deux types de déploiement de systèmes de fichiers : mono-AZ et multi-AZ. Les sections suivantes fournissent des informations qui vous aideront à choisir le type de déploiement adapté à vos charges de travail. Pour plus d'informations sur le SLA (Service Level Agreement) de disponibilité du service, consultez l'accord de niveau de service Amazon FSx.

Les systèmes de fichiers mono-AZ sont composés d'une seule instance de serveur de fichiers Windows et d'un ensemble de volumes de stockage au sein d'une seule zone de disponibilité (AZ). Avec les systèmes de fichiers mono-AZ, les données sont automatiquement répliquées afin de les protéger contre la défaillance d'un seul composant dans la plupart des cas. Amazon FSx surveille en permanence les défaillances matérielles et se rétablit automatiquement en cas de défaillance en remplaçant le composant d'infrastructure défaillant. Les systèmes de fichiers mono-AZ sont hors ligne, généralement pendant moins de 20 minutes, pendant ces événements de reprise en cas de panne et pendant la maintenance planifiée du système de fichiers pendant la période de maintenance que vous configurez pour votre système de fichiers. Avec les systèmes de fichiers mono-AZ, une défaillance du système de fichiers peut être irréparable dans de rares cas, par exemple en raison de défaillances de plusieurs composants ou d'une défaillance involontaire du serveur de fichiers unique qui laisse le système de fichiers dans un état incohérent. Dans ce cas, vous pouvez récupérer votre système de fichiers à partir de la sauvegarde la plus récente.

Les systèmes de fichiers multi-AZ sont composés d'un cluster à haute disponibilité de serveurs de fichiers Windows répartis sur deux AZ (une AZ préférée et une AZ de secours), tirant parti de la technologie Windows Server Failover Clustering (WSFC) et d'un ensemble de volumes de stockage sur chacune des deux AZ. Les données sont répliquées de manière synchrone au sein de chaque AZ individuel et entre les deux AZ. Par rapport au déploiement mono-AZ, les déploiements multi-AZ offrent une durabilité accrue en répliquant davantage les données entre les zones de disponibilité, ainsi qu'une disponibilité accrue lors de la maintenance planifiée du système et des interruptions de service imprévues en basculant automatiquement vers la zone de secours. Cela vous permet de continuer à accéder à vos données et de les protéger contre les défaillances d'instance et les perturbations de l'AZ.

Choix du déploiement d'un système de fichiers mono-AZ ou multi-AZ

Nous recommandons d'utiliser des systèmes de fichiers multi-AZ pour la plupart des charges de travail de production étant donné le modèle de haute disponibilité et de durabilité qu'ils offrent. Le déploiement mono-AZ est conçu comme une solution rentable pour les charges de travail de test et de développement, certaines charges de travail de production dont la réplication est intégrée à la couche applicative et ne nécessitent pas de redondance supplémentaire au niveau du stockage, et les charges de travail de production qui ont assoupli les exigences en matière de disponibilité et d'objectifs de point de restauration (RPO). Les charges de travail présentant des besoins de disponibilité souples peuvent tolérer une perte de disponibilité temporaire pouvant aller jusqu'à 20 minutes en cas de maintenance planifiée du système de fichiers ou d'interruption de service imprévue, tandis que les charges de travail présentant des exigences de RPO assouplies peuvent tolérer, dans de rares cas, la perte de mises à jour des données depuis la dernière sauvegarde.

Support des fonctionnalités par type de déploiement

Le tableau suivant récapitule les fonctionnalités prises en charge par les types de déploiement du système de fichiers FSx for Windows File Server :

Type de déploiement	Stockage SSD	Stockage sur disque dur	Espaces de noms DFS	réplication DFS	Noms DNS personnalisés	Actions CA
Mono-AZ 1	✓		✓	✓	✓	
Mono-AZ 2	✓	✓	✓		✓	✓*
Multi-AZ	✓	✓	✓		✓	✓*

> **Note**
>
> * Bien que vous puissiez créer des partages disponibles en continu (CA) sur des systèmes de fichiers mono-AZ 2, vous devez utiliser des partages CA sur des systèmes de fichiers multi-AZ pour les déploiements SQL Server HA.

Processus de basculement pour FSx for Windows File Server

Les systèmes de fichiers multi-AZ basculent automatiquement du serveur de fichiers préféré vers le serveur de fichiers de secours si l'une des conditions suivantes se produit :

- Une panne de zone de disponibilité se produit.
- Le serveur de fichiers préféré devient indisponible.
- Le serveur de fichiers préféré fait l'objet d'une maintenance planifiée.

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. Lorsque les ressources du sous-réseau préféré sont disponibles, Amazon FSx revient automatiquement au serveur de fichiers préféré dans le sous-réseau préféré. Un basculement s'effectue généralement en moins de 30 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. Le retour à la configuration multi-AZ d'origine s'effectue également en moins de 30 secondes et ne se produit qu'une fois que le serveur de fichiers du sous-réseau préféré est complètement restauré.

Pendant la brève période au cours de laquelle votre système de fichiers bascule puis retombe en panne, les E/S peuvent être interrompues et les CloudWatch métriques Amazon peuvent être temporairement indisponibles.

Pour les systèmes de fichiers multi-AZ, si le trafic est permanent pendant le basculement et le retour en arrière, toutes les modifications de données effectuées pendant cette période devront être synchronisées entre les serveurs de fichiers. Ce processus peut prendre plusieurs heures pour les charges de travail exigeantes en écriture et en IOPS. Nous vous recommandons de tester l'impact des basculements sur votre application lorsque votre système de fichiers est moins chargé.

Expérience de basculement sur les clients Windows

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. Une fois que les ressources du sous-réseau préféré sont disponibles, Amazon FSx revient automatiquement au serveur de fichiers préféré dans le sous-réseau préféré. Le nom DNS du système de fichiers restant le même, les basculements sont transparents pour les applications Windows, qui reprennent les opérations du système de fichiers sans intervention manuelle. Un basculement s'effectue généralement en moins de 30 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. Le retour à la configuration multi-AZ d'origine s'effectue également en moins de 30 secondes et ne se produit qu'après la restauration complète du serveur de fichiers du sous-réseau préféré.

Expérience de basculement sur les clients Linux

Les clients Linux ne prennent pas en charge le basculement automatique basé sur le DNS. Ils ne se connectent donc pas automatiquement au serveur de fichiers de secours lors d'un basculement. Ils reprendront automatiquement les opérations du système de fichiers une fois que le système de fichiers multi-AZ aura échoué sur le serveur de fichiers du sous-réseau préféré.

Test du basculement sur un système de fichiers

Vous pouvez tester le basculement de votre système de fichiers multi-AZ en modifiant sa capacité de débit. Lorsque vous modifiez la capacité de débit de votre système de fichiers, Amazon FSx remplace le serveur de fichiers du système de fichiers. Les systèmes de fichiers multi-AZ basculent automatiquement vers le serveur secondaire tandis qu'Amazon FSx remplace d'abord le serveur de fichiers du serveur préféré. Ensuite, le système de fichiers revient automatiquement sur le nouveau serveur principal et Amazon FSx remplace le serveur de fichiers secondaire.

Vous pouvez suivre la progression de la demande de mise à jour de la capacité de débit dans la console Amazon FSx, la CLI et l'API. Une fois la mise à jour terminée avec succès, votre système de fichiers est redirigé vers le serveur secondaire, puis de nouveau vers le serveur principal. Pour plus d'informations sur la modification de la capacité de débit de votre système de fichiers et le suivi de la progression de la demande, consultezGestion de la capacité de débit.

Utilisation des ressources d'un système de fichiers mono-AZ ou multi-AZ

Sous-réseaux

Lorsque vous créez un VPC, il couvre toutes les zones de disponibilité (AZ) de la région. Les zones de disponibilité sont des emplacements distincts conçus pour être isolés des défaillances dans d'autres zones de disponibilité. Après avoir créé un VPC, vous pouvez ajouter un ou plusieurs sous-réseaux dans chaque zone de disponibilité. Le VPC par défaut possède un sous-réseau dans chaque zone de disponibilité. Chaque sous-réseau doit résider entièrement dans une zone de disponibilité et ne peut pas s'étendre sur plusieurs zones. Lorsque vous créez un système de fichiers Amazon FSx

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 AWS région.

Pour les AWS applications intégrées, nous vous recommandons de lancer vos clients dans la même zone de disponibilité que votre serveur de fichiers préféré afin de minimiser le temps de latence.

Interfaces réseau élastiques pour systèmes de fichiers

Lorsque vous créez un système de fichiers Amazon FSx, Amazon FSx fournit une ou plusieurs interfaces réseau élastiques dans l'Amazon Virtual Private Cloud (VPC) que vous associez à votre système de fichiers. L'interface réseau permet à votre client de communiquer avec le système de fichiers FSx for Windows File Server. L'interface réseau est considérée comme faisant partie du périmètre de service d'Amazon FSx, bien qu'elle fasse partie du VPC de votre compte. Les systèmes de fichiers multi-AZ disposent de deux interfaces réseau élastiques, une pour chaque serveur de fichiers. Les systèmes de fichiers mono-AZ possèdent une interface Elastic Network.

> **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.

Le tableau suivant récapitule les ressources relatives au sous-réseau, à l'interface Elastic Network et aux adresses IP pour les types de déploiement de systèmes de fichiers FSx for Windows File Server :

Type de déploiement du système de fichiers	Nombre de sous-réseaux	Nombre d'interfaces réseau élastiques	Nombre d'adresses IP
Mono-AZ 2	1	1	2
Mono-AZ 1	1	1	1
Multi-AZ	2	2	4

Une fois qu'un système de fichiers 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. Si une adresse IP élastique, qui est une adresse IP publique accessible depuis Internet, est attachée à l'interface réseau Elastic d'un système de fichiers, Amazon FSx la détache automatiquement.

Optimisation des coûts avec Amazon FSx

Le serveur de fichiers FSx pour Windows fournit plusieurs fonctionnalités qui vous aident à optimiser votre coût total de possession (TCO) en fonction des besoins de votre application. Vous pouvez choisir le type de stockage (disque dur ou SSD) afin de trouver le juste équilibre entre les coûts et les besoins de performance de votre application. Vous avez la possibilité de sélectionner la capacité de débit séparément de la capacité de stockage afin d'optimiser vos coûts. Vous pouvez également utiliser la déduplication des données pour optimiser les coûts de stockage en éliminant les données redondantes sur votre système de fichiers.

Rubriques

Flexibilité permettant de choisir indépendamment le stockage et le débit

Avec FSx pour Windows File Server, vous pouvez configurer le stockage, les IOPS SSD et les capacités de débit de votre système de fichiers de manière indépendante. Cela vous donne la flexibilité nécessaire pour trouver le bon équilibre entre coûts et performances. Par exemple, vous pouvez choisir de disposer d'une grande quantité de stockage avec une capacité de débit relativement faible pour les charges de travail froides (généralement inactives) afin de réduire les coûts de débit inutiles. Ou, comme autre exemple, vous pouvez choisir de disposer d'une grande capacité de débit pour une capacité de stockage relativement faible. Une capacité de débit plus élevée s'accompagne d'une plus grande quantité de mémoire pour la mise en cache sur le serveur de fichiers. Vous pouvez tirer parti de la mise en cache rapide sur le serveur de fichiers pour optimiser les performances des données auxquelles vous accédez activement. Pour plus d'informations, veuillez consulter Performances de FSx for Windows File Server.

Vous pouvez augmenter la capacité de stockage à tout moment après avoir créé un système de fichiers. Pour plus d'informations, veuillez consulter Gestion de la capacité de stockage. Vous pouvez ajuster les IOPS du SSD indépendamment de la capacité de stockage à tout moment après avoir créé un système de fichiers. Pour plus d'informations, veuillez consulter Gestion des IOPS sur SSD. Vous pouvez augmenter ou diminuer la capacité de débit à tout moment, ce qui offre la

flexibilité nécessaire pour répondre à l'évolution des besoins en matière de performances. Pour plus d'informations, veuillez consulter Gestion de la capacité de débit.

Optimisation des coûts de stockage

Vous pouvez optimiser vos coûts de stockage avec Amazon FSx de différentes manières, décrites ci-dessous.

Optimisation des coûts à l'aide des types de stockage

Le serveur de fichiers FSx pour Windows fournit deux types de stockage, les disques durs (HDD) et les disques SSD, pour vous permettre d'optimiser les coûts et les performances en fonction de vos besoins en matière de charge de travail. Le stockage sur disque dur est conçu pour un large éventail de charges de travail, notamment les répertoires personnels, les partages entre utilisateurs et services, ainsi que les systèmes de gestion de contenu. Le stockage SSD est conçu pour les charges de travail les plus performantes et les plus sensibles à la latence, notamment les bases de données, les charges de travail de traitement multimédia et les applications d'analyse de données. Pour plus d'informations, voirLatenceetTarification des serveurs de fichiers Amazon FSx pour Windows.

Optimisation des coûts de stockage grâce à la déduplication des données

Les grands ensembles de données contiennent souvent des données redondantes, ce qui augmente les coûts de stockage des données. Par exemple, les partages de fichiers utilisateur peuvent contenir plusieurs copies du même fichier, stockées par plusieurs utilisateurs. Les partages de développement logiciel peuvent contenir de nombreux fichiers binaires qui restent inchangés d'une version à l'autre. Vous pouvez réduire vos coûts de stockage de données en activantdéduplication des donnéespour votre système de fichiers. Lorsqu'elle est activée, la déduplication des données réduit ou élimine automatiquement les données redondantes en ne stockant qu'une seule fois les parties dupliquées du jeu de données. Pour plus d'informations sur la déduplication des données et sur la façon de l'activer facilement pour votre système de fichiers Amazon FSx, consultezDéduplication des données.

Révision de l'utilisation et de la facturation

Vous pouvez consulter l'utilisation de votre système de fichiers, notamment votre capacité de stockage, votre capacité de débit, vos sauvegardes et votre transfert de données, à l'aide duAWS BillingTableau de bord ouAWS Cost Explorer. Ces outils vous permettent d'examiner l'utilisation de vos ressources, de filtrer et de regrouper par type d'utilisation, région et autres critères pertinents.

Notez que pour visualiser l'utilisation d'un seul système de fichiers ou d'une sauvegarde de système de fichiers unique, vous devez activer les balises pour cette ressource spécifique et activer les rapports de facturation basés sur des balises. Pour plus d'informations, voirEn utilisantAWSbalises de répartition des coûtsdans leAWS Billingguide de l'utilisateur.

Utilisation de Microsoft Active Directory dans FSx for Windows File Server

Amazon FSx fonctionne avec Microsoft Active Directory pour s'intégrer à vos environnements Microsoft Windows existants. Active Directory est le service d'annuaire Microsoft utilisé pour stocker des informations sur les objets du réseau et faciliter la recherche et l'utilisation de ces informations par les administrateurs et les utilisateurs. Ces objets incluent généralement des ressources partagées telles que des serveurs de fichiers, des comptes d'utilisateurs et d'ordinateurs du réseau.

Lorsque vous créez un système de fichiers avec Amazon FSx, vous le joignez à votre domaine Active Directory pour permettre l'authentification des utilisateurs et le contrôle d'accès au niveau des fichiers et des dossiers. Vos utilisateurs peuvent ensuite utiliser leurs identités utilisateur existantes dans Active Directory pour s'authentifier et accéder au système de fichiers Amazon FSx. Les utilisateurs peuvent également 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 la configuration de la liste de contrôle d'accès (ACL) de ces éléments vers Amazon FSx sans aucune modification.

Amazon FSx vous propose deux options pour utiliser votre système de fichiers FSx for Windows File Server avec Active Directory : et. Utilisation d'Amazon FSx avec AWS Directory Service for Microsoft Active Directory Utilisation d'Amazon FSx avec votre Microsoft Active Directory autogéré

> **Note**
>
> Amazon FSx prend en charge les services de domaine Microsoft Azure Active Directory, que vous pouvez joindre à un répertoire Microsoft Azure Active Directory.

Après avoir créé une configuration Active Directory jointe pour un système de fichiers, vous ne pouvez mettre à jour que les propriétés suivantes :

- Informations d'identification des utilisateurs du service
- Adresses IP des serveurs DNS

Vous ne pouvez pas modifier les propriétés suivantes pour Microsoft AD que vous avez rejoint une fois que vous avez créé le système de fichiers :

- DomainName

- OrganizationalUnitDistinguishedName
- FileSystemAdministratorsGroup

Vous pouvez toutefois créer un nouveau système de fichiers à partir d'une sauvegarde et modifier ces propriétés dans la configuration d'intégration de Microsoft Active Directory pour le nouveau système de fichiers. Pour plus d'informations, consultez Procédure 2 : Création d'un système de fichiers à partir d'une sauvegarde.

> **Note**
>
> Amazon FSx ne prend pas en charge Active Directory Connector et Simple Active Directory.

Votre serveur de fichiers FSx for Windows peut être mal configuré si une modification de votre configuration Active Directory perturbe la connexion à votre système de fichiers. Pour rétablir l'état Disponible de votre système de fichiers, sélectionnez le bouton Tentative de restauration dans la console Amazon FSx ou utilisez la `StartMisconfiguredStateRecovery` commande dans l'API ou la console Amazon FSx. Pour plus d'informations, consultez Le système de fichiers est mal configuré.

Rubriques

- Utilisation d'Amazon FSx avec AWS Directory Service for Microsoft Active Directory
- Utilisation d'Amazon FSx avec votre Microsoft Active Directory autogéré

Utilisation d'Amazon FSx avec AWS Directory Service for Microsoft Active Directory

AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) fournit de véritables annuaires Active Directory entièrement gérés et hautement disponibles dans le cloud. Vous pouvez utiliser ces annuaires Active Directory dans le déploiement de votre charge de travail.

Si votre entreprise gère des identités et des appareils, nous vous recommandons d'y intégrer votre système de fichiers Amazon FSx. AWS Managed Microsoft AD AWS Managed Microsoft AD Ce faisant, vous obtenez une solution clé en main utilisant Amazon AWS Managed Microsoft AD FSx avec. AWS gère le déploiement, l'exploitation, la haute disponibilité, la fiabilité, la sécurité

et l'intégration transparente des deux services, vous permettant ainsi de vous concentrer sur l'exploitation efficace de votre propre charge de travail.

Pour utiliser Amazon FSx dans votre AWS Managed Microsoft AD configuration, vous pouvez utiliser la console Amazon FSx. Lorsque vous créez un nouveau système de fichiers FSx for Windows File Server dans la console, AWS choisissez Managed Active Directory dans la section Authentification Windows. Vous choisissez également le répertoire spécifique que vous souhaitez utiliser. Pour plus d'informations, consultez Créez votre système de fichiers.

Votre organisation peut gérer les identités et les appareils sur un domaine Active Directory autogéré (sur site ou dans le cloud). Dans ce cas, vous pouvez associer votre système de fichiers Amazon FSx directement à votre domaine Active Directory autogéré existant. Pour plus d'informations, consultez Utilisation d'Amazon FSx avec votre Microsoft Active Directory autogéré.

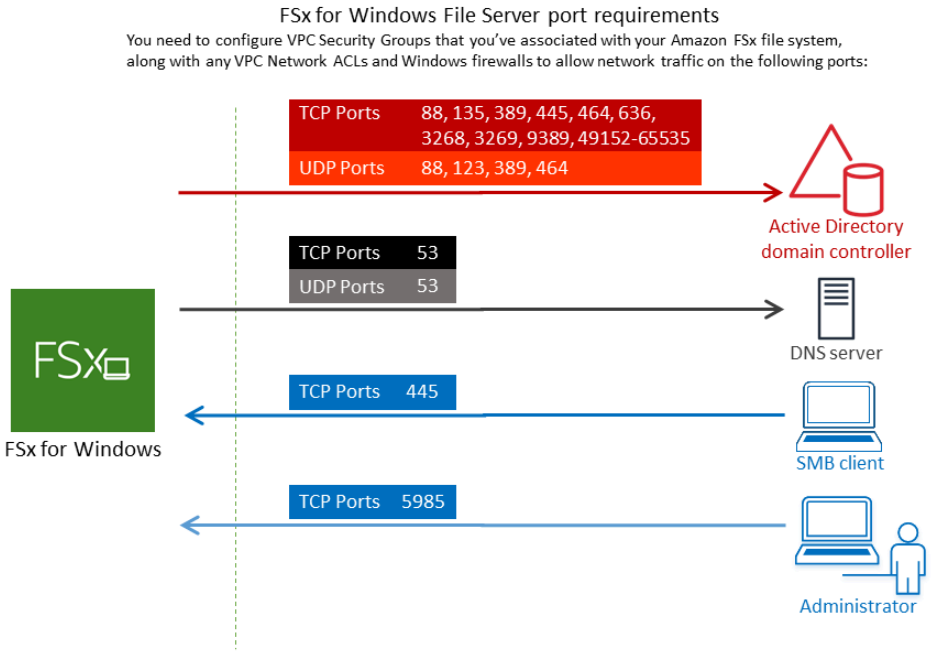
En outre, vous pouvez également configurer votre système pour bénéficier d'un modèle d'isolation des forêts de ressources. Dans ce modèle, vous isolez vos ressources, y compris vos systèmes de fichiers Amazon FSx, dans une forêt Active Directory distincte de celle où se trouvent vos utilisateurs.

> **Important**
>
> Pour les systèmes de fichiers mono-AZ 2 et tous les systèmes de fichiers multi-AZ, le nom de domaine Active Directory ne peut pas dépasser 47 caractères.

Conditions préalables à la mise en réseau

Avant de créer un système de fichiers FSx for Windows File Server joint à votre domaine AWS Microsoft Managed Active Directory, assurez-vous d'avoir créé et configuré les configurations réseau suivantes :

- Pour les groupes de sécurité VPC, le groupe de sécurité par défaut pour votre Amazon VPC par défaut est déjà ajouté à votre système de fichiers dans la console. Assurez-vous que le groupe de sécurité et les ACL du réseau VPC du ou des sous-réseaux sur lesquels vous créez votre système de fichiers FSx autorisent le trafic sur les ports et dans les directions indiquées dans le schéma suivant.



Le tableau suivant identifie le rôle de chaque port.

Protocole	Ports	Rôle
TCP/UDP	53	Systè de nom de domai (DNS)
TCP/UDP	88	Authe icatior Kerbe

Protocole	Ports	Rôle
TCP/UDP	464	Chang t/ définit ion de mot de passe
TCP/UDP	389	Protoc LDAP (Lightv ght Direct Acces Protoc
UDP	123	Protoc NTP (Netw Time Protoc
TCP	135	Distrib ed Comp Enviro nt / End Point Mappe (DCE EPMA

Protocole	Ports	Rôle
TCP	445	Partag de fichier SMB avec les servic d'annu e
TCP	636	Protoc LDAP (Light ght Direct Acces Protoc via TLS/ SSL (LDAP
TCP	3268	Catalo mondi Micros
TCP	3269	Micros Globa Catalo via SSL

Protocole	Ports	Rôle
TCP	5985	WinRI 2.0 (gestio à distan de Micros Windo
TCP	9389	Servic Web Micros AD DS, Powe l
TCP	49152 - 65535	Ports éphén pour RPC

Important

L'autorisation du trafic sortant sur le port TCP 9389 est requise pour les déploiements de systèmes de fichiers mono-AZ 2 et multi-AZ.

Note

Si vous utilisez des ACL de réseau VPC, vous devez également autoriser le trafic sortant sur les ports dynamiques (49152-65535) depuis votre système de fichiers FSx.

- Si vous connectez votre système de fichiers Amazon FSx à un répertoire AWS Microsoft Active Directory géré dans un autre VPC ou un autre compte, assurez-vous de la connectivité entre ce VPC et le VPC Amazon dans lequel vous souhaitez créer le système de fichiers. Pour plus d'informations, consultez Utilisation d'Amazon FSx avec AWS Managed Microsoft AD un autre VPC ou un autre compte.

  > **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, les ACL du réseau VPC nécessitent que les ports soient ouverts dans les deux sens.

Utilisez l'outil de validation réseau Amazon FSx pour valider la connectivité à vos contrôleurs de domaine Active Directory.

Utilisation d'un modèle d'isolation des forêts de ressources

Vous associez votre système de fichiers à une AWS Managed Microsoft AD installation. Vous établissez ensuite une relation d'approbation forestière unidirectionnelle entre un AWS Managed Microsoft AD domaine que vous créez et votre domaine Active Directory autogéré existant. Pour l'authentification Windows dans Amazon FSx, vous n'avez besoin que d'une approbation de forêt directionnelle unidirectionnelle, dans laquelle la forêt AWS gérée approuve la forêt de domaines d'entreprise.

Le domaine de votre entreprise joue le rôle de domaine approuvé, et le domaine AWS Directory Service géré joue le rôle de domaine de confiance. Les demandes d'authentification validées circulent entre les domaines dans une seule direction, ce qui permet aux comptes du domaine de votre entreprise de s'authentifier auprès des ressources partagées dans le domaine géré. Dans ce cas, Amazon FSx interagit uniquement avec le domaine géré. Le domaine géré transmet ensuite les demandes d'authentification à votre domaine d'entreprise.

Testez votre configuration Active Directory

Avant de créer votre système de fichiers Amazon FSx, nous vous recommandons de valider la connectivité à vos contrôleurs de domaine Active Directory à l'aide de l'outil de validation réseau Amazon FSx. Pour plus d'informations, consultez Validation de la connectivité à vos contrôleurs de domaine Active Directory.

Les ressources connexes suivantes peuvent vous aider lors de votre utilisation AWS Directory Service for Microsoft Active Directory de FSx for Windows File Server :

- Qu'est-ce que AWS le Directory Service dans le guide AWS Directory Service d'administration
- Créez votre annuaire Active Directory AWS géré dans le guide AWS Directory Service d'administration
- Quand créer une relation de confiance dans le guide AWS Directory Service d'administration
- Procédure 1 : Conditions préalables à la prise en main

Utilisation d'Amazon FSx avec AWS Managed Microsoft AD un autre VPC ou un autre compte

Vous pouvez associer votre système de fichiers FSx for Windows File Server à AWS Managed Microsoft AD un répertoire situé dans un autre VPC au sein du même compte en utilisant le peering VPC. Vous pouvez également associer votre système de fichiers à un AWS Managed Microsoft AD répertoire situé dans un autre AWS compte en utilisant le partage de répertoires.

> **Note**
>
> Vous ne pouvez sélectionner qu'un AWS Managed Microsoft AD élément Région AWS identique à celui de votre système de fichiers. Si vous souhaitez utiliser une configuration d'appairage VPC entre régions, vous devez utiliser un Microsoft Active Directory autogéré. Pour plus d’informations, consultez Utilisation d'Amazon FSx avec votre Microsoft Active Directory autogéré.

Le flux de travail pour joindre votre système de AWS Managed Microsoft AD fichiers à un autre VPC implique les étapes suivantes :

1. Configurez votre environnement réseau.
2. Partagez votre répertoire.
3. Joignez votre système de fichiers au répertoire partagé.

Pour plus d'informations, consultez la section Partager votre répertoire dans le Guide AWS Directory Service d'administration.

Pour configurer votre environnement réseau, vous pouvez utiliser AWS Transit Gateway Amazon VPC et créer une connexion d'appairage VPC. En outre, assurez-vous que le trafic réseau est autorisé entre les deux VPC.

Une passerelle de transit est un hub de transit de réseau que vous pouvez utiliser pour relier votre VPC et vos réseaux sur site. Pour plus d'informations sur l'utilisation des passerelles de transit de VPC, consultez Démarrez avec les passerelles de transit dans le Guide des passerelles de transit Amazon VPC.

Une connexion d’appairage de VPC est une connexion de mise en réseau entre deux VPC. Cette connexion vous permet d'acheminer le trafic entre eux à l'aide d'adresses privées du protocole Internet version 4 (IPv4) ou du protocole Internet version 6 (IPv6). Vous pouvez utiliser le peering VPC pour connecter des VPC au sein d'une même AWS région ou entre des régions. AWS Pour plus d’informations sur l’appairage VPC, consultez Qu’est-ce que l’appairage VPC ? dans le Guide d’appairage Amazon VPC.

Il existe une autre condition préalable lorsque vous associez votre système de fichiers à un AWS Managed Microsoft AD répertoire d'un compte différent de celui de votre système de fichiers. Vous devez également partager votre Microsoft Active Directory avec l'autre compte. Pour ce faire, vous pouvez utiliser la fonctionnalité de partage d'annuaires de AWS Managed Microsoft Active Directory. Pour en savoir plus, consultez la section Partager votre répertoire dans le Guide AWS Directory Service d'administration.

Validation de la connectivité à vos contrôleurs de domaine Active Directory

Avant de créer un système de fichiers FSx for Windows File Server joint à votre Active Directory, utilisez l'outil de validation Amazon FSx Active Directory pour valider la connectivité à votre domaine Active Directory. Vous pouvez utiliser ce test, que vous utilisiez FSx for Windows File Server AWS avec Microsoft Active Directory géré ou avec une configuration Active Directory autogérée. Le test de connectivité réseau du contrôleur de domaine (Test-FSxadControllerConnection) n'exécute pas la suite complète de contrôles de connectivité réseau sur tous les contrôleurs de domaine du domaine. Utilisez plutôt ce test pour exécuter la validation de la connectivité réseau sur un ensemble spécifique de contrôleurs de domaine.

Pour valider la connectivité à vos contrôleurs de domaine Active Directory

1. Lancez une instance Windows Amazon EC2 dans le même sous-réseau et avec les mêmes groupes de sécurité Amazon VPC que ceux que vous utiliserez pour votre système de fichiers

FSx for Windows File Server. Pour les types de déploiement multi-AZ, utilisez le sous-réseau du serveur de fichiers actif préféré.

2. Joignez votre instance Windows EC2 à votre Active Directory. Pour plus d'informations, voir Joindre manuellement une instance Windows dans le Guide AWS Directory Service d'administration.
3. Connectez-vous à votre instance EC2. Pour plus d'informations, consultez la section Connexion à votre instance Windows dans le guide de l'utilisateur Amazon EC2.
4. Ouvrez une PowerShell fenêtre Windows (en utilisant Exécuter en tant qu'administrateur) sur l'instance EC2.

   Pour vérifier si le module Active Directory requis pour Windows PowerShell est installé, utilisez la commande de test suivante.

   ```
   PS C:\> Import-Module ActiveDirectory
   ```

   Si le message ci-dessus renvoie une erreur, installez-le à l'aide de la commande suivante.

   ```
   PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
   ```
5. Téléchargez l'outil de validation réseau à l'aide de la commande suivante.

   ```
   PS C:\> Invoke-WebRequest "https://docs.aws.amazon.com/fsx/latest/WindowsGuide/
   samples/AmazonFSxADValidation.zip" -OutFile "AmazonFSxADValidation.zip"
   ```
6. Développez le fichier zip à l'aide de la commande suivante.

   ```
   PS C:\> Expand-Archive -Path "AmazonFSxADValidation.zip"
   ```
7. Ajoutez le module AmazonFSXADValidation à la session en cours.

   ```
   PS C:\> Import-Module .\AmazonFSxADValidation
   ```
8. Définissez la valeur de l'adresse IP du contrôleur de domaine Active Directory et exécutez le test de connectivité à l'aide des commandes suivantes :

   ```
   $ADControllerIp = '10.0.75.243'
   ```

```
$Result = Test-FSxADControllerConnection -ADControllerIp $ADControllerIp
```

9. L'exemple suivant montre comment récupérer le résultat du test, avec les résultats d'un test de connectivité réussi.

```
PS C:\AmazonFSxADValidation> $Result

Name                           Value
----                           -----
TcpDetails                     {@{Port=88; Result=Listening; Description=Kerberos
 authentication}, @{Port=135; Resul...
Server                         10.0.75.243
UdpDetails                     {@{Port=88; Result=Timed Out; Description=Kerberos
 authentication}, @{Port=123; Resul...
Success                        True


PS C:\AmazonFSxADValidation> $Result.TcpDetails

Port Result    Description
---- ------    -----------
  88 Listening Kerberos authentication
 135 Listening DCE / EPMAP (End Point Mapper)
 389 Listening Lightweight Directory Access Protocol (LDAP)
 445 Listening Directory Services SMB file sharing
 464 Listening Kerberos Change/Set password
 636 Listening Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
3268 Listening Microsoft Global Catalog
3269 Listening Microsoft Global Catalog over SSL
9389 Listening Microsoft AD DS Web Services, PowerShell
```

L'exemple suivant montre l'exécution du test et l'obtention d'un résultat d'échec.

```
PS C:\AmazonFSxADValidation> $Result = Test-FSxADControllerConnection -
ADControllerIp $ADControllerIp
WARNING: TCP 9389 failed to connect. Required for Microsoft AD DS Web Services,
 PowerShell.
Verify security group and firewall settings on both client and directory
 controller.
WARNING: 1 ports failed to connect to 10.0.75.243. Check pre-requisites in
https://docs.aws.amazon.com/fsx/latest/WindowsGuide/self-managed-AD.html#self-
manage-prereqs
```

```
PS C:\AmazonFSxADValidation> $Result

Name                           Value
----                           -----
TcpDetails                     {@{Port=88; Result=Listening; Description=Kerberos
 authentication}, @{Port=135; Resul...
Server                         10.0.75.243
UdpDetails                     {@{Port=88; Result=Timed Out; Description=Kerberos
 authentication}, @{Port=123; Resul...
Success                        False
FailedTcpPorts                 {9389}


PS C:\AmazonFSxADValidation> $Result.FailedTcpPorts
9389
```

```
Windows socket error code mapping

https://msdn.microsoft.com/en-us/library/ms740668.aspx
```

Utilisation d'Amazon FSx avec votre Microsoft Active Directory autogéré

Si votre entreprise gère les identités et les appareils sur un Active Directory autogéré sur site ou dans le cloud, vous pouvez associer votre système de fichiers Amazon FSx directement à votre domaine Active Directory autogéré existant. Pour utiliser Amazon FSx avec AWS Managed Microsoft AD, vous pouvez utiliser la console Amazon FSx. Lorsque vous créez un nouveau système de fichiers FSx for Windows File Server dans la console, choisissez Microsoft Active Directory autogéré sous Authentification Windows. Fournissez les informations suivantes pour votre Active Directory autogéré :

- Un nom de domaine complet pour votre annuaire autogéré

> **Note**
>
> Le nom de domaine ne doit pas être au format SLD (Single Label Domain). Amazon FSx ne prend actuellement pas en charge les domaines SLD.

> **Note**
>
> Pour les systèmes de fichiers mono-AZ 2 et multi-AZ, le nom de domaine Active Directory ne peut pas dépasser 47 caractères.

- Adresses IP du serveur DNS pour votre domaine

  Les adresses IP du serveur DNS, les adresses IP du contrôleur de domaine Active Directory et le réseau client doivent répondre aux exigences suivantes :

Pour les systèmes de fichiers créés avant le 17 décembre 2020	Pour les systèmes de fichiers créés après le 17 décembre 2020
Les adresses IP doivent se trouver dans une plage d'adresses IP privées RFC 1918 : • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	Les adresses IP peuvent être comprises dans n'importe quelle plage, sauf : • Adresses IP en conflit avec les adresses IP détenues par Amazon Web Services dans cette AWS région. Pour obtenir la liste des adresses IP AWS détenues par région, consultez les plages d'adresses AWS IP. • Adresses IP dans la plage de blocs CIDR suivante : 198.19.0.0/16

> **Note**
>
> Vos contrôleurs de domaine Active Directory doivent être accessibles en écriture.

- Nom d'utilisateur et mot de passe d'un compte de service sur votre domaine Active Directory, à utiliser par Amazon FSx pour joindre le système de fichiers à votre domaine Active Directory

- (Facultatif) L'unité organisationnelle (UO) de votre domaine à laquelle vous souhaitez associer votre système de fichiers
- (Facultatif) Le groupe de domaines auquel vous souhaitez déléguer 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, gérer les listes de contrôle d'accès (ACL) sur le dossier racine du système de fichiers, 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.

> **Note**
>
> Le nom de groupe de domaines que vous fournissez doit être unique dans votre Active Directory. FSx for Windows File Server ne créera pas le groupe de domaines dans les cas suivants :
>
> - Si un groupe existe déjà avec le nom que vous spécifiez
> - Si vous ne spécifiez pas de nom et qu'un groupe nommé « Administrateurs de domaine » existe déjà dans votre Active Directory.

Pour plus d'informations, consultez Joindre un système de fichiers Amazon FSx à un domaine Microsoft Active Directory autogéré.

> **Important**
>
> Amazon FSx enregistre les enregistrements DNS pour un système de fichiers uniquement si vous utilisez Microsoft DNS comme service DNS par défaut. Si vous utilisez un DNS tiers, vous devrez configurer manuellement les entrées DNS pour vos systèmes de fichiers Amazon FSx après les avoir créées.

Lorsque vous associez votre système de fichiers directement à votre Active Directory autogéré, votre serveur de fichiers FSx for Windows réside dans la même forêt Active Directory (le principal conteneur logique d'une configuration Active Directory contenant des domaines, des utilisateurs et des ordinateurs) et dans le même domaine Active Directory que vos utilisateurs et ressources existantes (y compris les serveurs de fichiers existants).

> **Note**
>
> Vous pouvez isoler vos ressources, y compris vos systèmes de fichiers Amazon FSx, dans une forêt Active Directory distincte de celle où résident vos utilisateurs. Pour ce faire, associez votre système de fichiers à un Active Directory AWS géré et établissez une relation d'approbation forestière unidirectionnelle entre un Active Directory AWS géré que vous créez et votre Active Directory autogéré existant.

Rubriques

Conditions préalables à l'utilisation d'un Microsoft Active Directory autogéré

Avant de créer un système de fichiers Amazon FSx joint à votre domaine Microsoft Active Directory autogéré, passez en revue les conditions préalables suivantes.

Rubriques

Configurations sur site

Assurez-vous que vous disposez d'un répertoire Microsoft Active Directory sur site ou autogéré auquel vous pouvez joindre le système de fichiers Amazon FSx. Votre Active Directory local doit avoir la configuration suivante :

- Le niveau fonctionnel de votre contrôleur de domaine Active Directory est Windows Server 2008 R2 ou supérieur.
- Les adresses IP du serveur DNS et les adresses IP du contrôleur de domaine Active Directory sont les suivantes, en fonction de la date de création de votre système de fichiers :

Pour les systèmes de fichiers créés avant le 17 décembre 2020	Pour les systèmes de fichiers créés après le 17 décembre 2020
Les adresses IP doivent se trouver dans une plage d'adresses IP privées RFC 1918 : • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	Les adresses IP peuvent être comprises dans n'importe quelle plage, sauf : • Adresses IP en conflit avec les adresses IP détenues par Amazon Web Services dans cette AWS région. Pour obtenir la liste des adresses IP AWS détenues par région, consultez les plages d'adresses AWS IP. • Adresses IP dans la plage de blocs CIDR suivante : 198.19.0.0/16

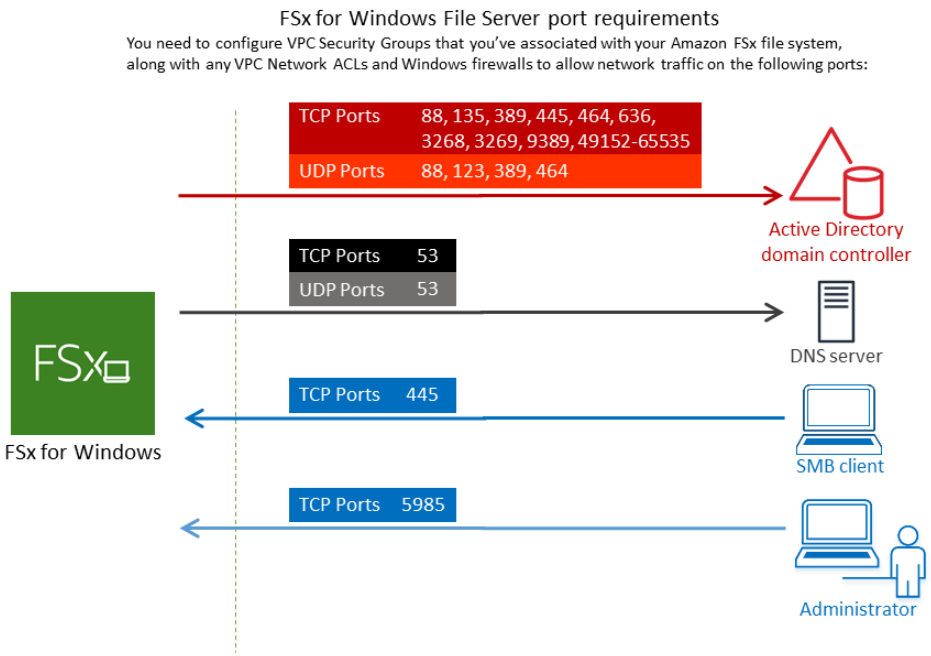
  Si vous devez accéder à un système de fichiers FSx for Windows File Server créé avant le 17 décembre 2020 à l'aide d'une plage d'adresses IP non privée, vous pouvez créer un nouveau système de fichiers en restaurant une sauvegarde du système de fichiers. Pour plus d'informations, consultez Utilisation des sauvegardes.
- Nom de domaine qui n'est pas au format Single Label Domain (SLD). Amazon FSx ne prend pas en charge les domaines SLD.
- Pour les systèmes de fichiers mono-AZ 2 et tous les systèmes de fichiers multi-AZ, le nom de domaine Active Directory ne peut pas dépasser 47 caractères.
- Si vous avez défini des sites Active Directory, les sous-réseaux du VPC associé à votre système de fichiers Amazon FSx doivent être définis dans un site Active Directory, et aucun conflit ne doit exister entre les sous-réseaux de votre VPC et ceux de vos autres sites.
- Vous devrez peut-être ajouter des règles à votre pare-feu pour autoriser le trafic ICMP entre vos contrôleurs de domaine Active Directory et Amazon FSx.

Configurations réseau

Cette section décrit les configurations réseau requises pour joindre un système de fichiers à votre Active Directory autogéré.

Nous vous recommandons d'utiliser l'outil de validation Amazon FSx Active Directory pour tester vos paramètres réseau avant de tenter de joindre votre système de fichiers à votre Active Directory autogéré.

- La connectivité doit être configurée entre le VPC Amazon sur lequel vous souhaitez créer le système de fichiers et votre Active Directory autogéré. Vous pouvez configurer cette connectivité à l'aide AWS Direct Connect du peering VPC ou. AWS Virtual Private NetworkAWS Transit Gateway
- Pour les groupes de sécurité VPC, le groupe de sécurité par défaut de votre Amazon VPC par défaut doit être ajouté à votre système de fichiers dans la console. Assurez-vous que le groupe de sécurité et les ACL du réseau VPC pour les sous-réseaux sur lesquels vous créez votre système de fichiers FSx autorisent le trafic sur les ports et dans les directions indiquées dans le schéma suivant.



Le tableau suivant identifie le rôle de chaque port.

Protocole	Ports	Rôle
TCP/UDP	53	Système de nom de domaine (DNS)
TCP/UDP	88	Authentification Kerberos
TCP/UDP	464	Modifier/définir le mot de passe
TCP/UDP	389	Protocole LDAP (Lightweight Directory Access Protocol)
UDP	123	Protocole NTP (Network Time Protocol)
TCP	135	Environnement informatique distribué/mappeur de points finaux (DCE/EPMAP)
TCP	445	Partage de fichiers SMB avec les services d'annuaire
TCP	636	Protocole LDAP (Lightweight Directory Access Protocol) via TLS/SSL (LDAPS)
TCP	3268	Catalogue mondial Microsoft
TCP	3269	Microsoft Global Catalog via SSL
TCP	5985	WinRM 2.0 (gestion à distance de Microsoft Windows)
TCP	9389	Services Web Microsoft Active Directory DS, PowerShell
TCP	49152 - 65535	Ports éphémères pour RPC

Assurez-vous que ces règles de trafic sont également reflétées sur les pare-feux qui s'appliquent à chacun des contrôleurs de domaine Active Directory, des serveurs DNS, des clients FSx et des administrateurs FSx.

Important

L'autorisation du trafic sortant sur le port TCP 9389 est requise pour les déploiements de systèmes de fichiers mono-AZ 2 et multi-AZ.

Note

Si vous utilisez des ACL de réseau VPC, vous devez également autoriser le trafic sortant sur les ports dynamiques (49152-65535) depuis votre système de fichiers FSx.

Important

Alors que les groupes de sécurité Amazon VPC nécessitent que les ports soient ouverts uniquement dans le sens où le trafic réseau est initié, la plupart des pare-feux Windows et des ACL de réseau VPC nécessitent que les ports soient ouverts dans les deux sens.

Autorisations relatives aux comptes de service

Assurez-vous que vous disposez d'un compte de service dans votre Microsoft Active Directory autogéré avec des autorisations déléguées pour associer des ordinateurs au domaine. Un compte de service est un compte utilisateur de votre Microsoft Active Directory autogéré auquel certaines tâches ont été déléguées.

Le compte de service doit, au minimum, se voir déléguer les autorisations suivantes dans l'unité d'organisation pour laquelle vous rejoignez le système de fichiers :

- Possibilité de réinitialiser les mots de passe
- Possibilité d'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 (déléguée) de créer et de supprimer des objets informatiques
- Aptitude validée à lire et à écrire les restrictions du compte
- Possibilité de modifier les autorisations

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 Microsoft 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 plus d'informations sur la création d'un compte de service doté des autorisations appropriées, consultez Délégation de privilèges à votre compte de service Amazon FSx .

Amazon FSx nécessite un compte de service valide pendant toute la durée de vie de votre système de fichiers Amazon FSx. Amazon FSx doit être en mesure de gérer entièrement le système de fichiers et d'effectuer des tâches qui nécessitent de dissocier puis de rejoindre votre domaine Active Directory à l'aide du compte de service. Ces tâches incluent le remplacement d'un serveur de fichiers défaillant ou l'application de correctifs au logiciel Windows Server. Il est impératif que vous mainteniez à jour votre configuration Active Directory, y compris les informations d'identification du compte de service, avec Amazon FSx. Pour plus d'informations, consultez Maintien à jour de votre configuration Active Directory.

Amazon FSx nécessite une connectivité à tous les contrôleurs de domaine de votre environnement Active Directory. Si vous avez plusieurs contrôleurs de domaine, assurez-vous qu'ils répondent tous aux exigences ci-dessus et assurez-vous que toute modification apportée à votre compte de service est répercutée sur tous les contrôleurs de domaine.

Vous pouvez valider votre configuration Active Directory, notamment tester la connectivité de plusieurs contrôleurs de domaine, à l'aide de l'outil de validation Active Directory d'Amazon FSx. Pour limiter le nombre de contrôleurs de domaine nécessitant une connectivité, vous pouvez également établir une relation de confiance entre vos contrôleurs de domaine sur site et AWS Managed Microsoft AD. Pour plus d'informations, consultez Utilisation d'un modèle d'isolation des forêts de ressources.

> **Important**
>
> Ne déplacez pas les objets informatiques créés par Amazon FSx dans l'unité d'organisation après la création de votre système de fichiers. Cela entraînera une mauvaise configuration de votre système de fichiers.

Meilleures pratiques pour joindre les systèmes de fichiers FSx for Windows File Server à un domaine Microsoft Active Directory autogéré

Nous recommandons ces bonnes pratiques lorsque vous associez les systèmes de fichiers Amazon FSx for Windows File Server à votre Microsoft Active Directory autogéré.

Délégation de privilèges à votre compte de service Amazon FSx

Assurez-vous de configurer le compte de service que vous fournissez à Amazon FSx avec les privilèges minimaux requis. En outre, séparez l'unité organisationnelle (UO) des autres préoccupations liées au contrôleur de domaine.

Pour associer les systèmes de fichiers Amazon FSx à votre domaine, assurez-vous que le compte de service dispose de privilèges délégués. Les membres du groupe des administrateurs de domaine disposent de privilèges suffisants pour effectuer cette tâche. Toutefois, il est recommandé d'utiliser un compte de service ne disposant que des privilèges minimaux nécessaires pour ce faire. Les procédures suivantes montrent comment déléguer uniquement les privilèges nécessaires pour joindre les systèmes de fichiers Amazon FSx à votre domaine.

Vous pouvez utiliser le contrôle délégué ou les fonctionnalités avancées du composant logiciel enfichable Active Directory User and Computers MMC pour attribuer ces autorisations.

Exécutez l'une de ces procédures sur une machine connectée à votre Active Directory et sur laquelle le Active Directory User and Computers MMC composant logiciel enfichable est installé.

Pour attribuer des autorisations à un compte de service ou à un groupe à l'aide du contrôle délégué

1. Connectez-vous à votre système en tant qu'administrateur de domaine pour votre domaine 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 le nom de votre compte ou groupe de service Amazon FSx, puis choisissez Next.
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. Pour Autorisations, choisissez ce qui suit :
    - Réinitialisation du mot
    - Restrictions relatives aux comptes en lecture et en écriture
    - Écriture validée sur le nom d'hôte DNS
    - Écriture validée sur le nom principal du service
11. Cliquez sur Suivant, puis sur Terminer.
12. Fermez le composant logiciel enfichable MMC Active Directory User and Computers.

Pour attribuer des autorisations à l'aide des fonctionnalités avancées

1. Connectez-vous à votre système en tant qu'administrateur de domaine pour votre domaine Active Directory.
2. Ouvrez le composant logiciel enfichable MMC Active Directory User and Computers.
3. Sélectionnez Afficher dans la barre de menu et assurez-vous que les fonctionnalités avancées sont activées (une coche apparaît à côté si la fonctionnalité est activée).
4. Dans le volet des tâches, développez le nœud de domaine.
5. Localisez et ouvrez (cliquez avec le bouton droit) le menu contextuel de l'unité d'organisation que vous souhaitez modifier, puis choisissez Propriétés.
6. Dans le volet Propriétés de l'unité d'organisation, sélectionnez l'onglet Sécurité.
7. Dans l'onglet Sécurité, sélectionnez Avancé. Sélectionnez ensuite Ajouter.
8. Sur la page de saisie des autorisations, choisissez Select a principal et entrez le nom de votre compte ou groupe de service Amazon FSx. Pour S'applique à :, choisissez Descendant Computer objects. Assurez-vous que les éléments suivants sont sélectionnés :
    - Modifier les autorisations
    - Création d'objets informatiques
    - Supprimer des objets informatiques
9. Sélectionnez Appliquer, puis OK.
10. Fermez le composant logiciel enfichable MMC Active Directory User and Computers.

> **Important**
>
> Ne déplacez pas les objets informatiques créés par Amazon FSx dans l'unité d'organisation après la création de votre système de fichiers. Cela entraînera une mauvaise configuration de votre système de fichiers. Si vous mettez à jour votre système de fichiers avec un nouveau compte de service, assurez-vous que le nouveau compte de service dispose d'autorisations de contrôle total pour les objets informatiques existants associés au système de fichiers.

Maintien à jour de votre configuration Active Directory

Pour garantir la disponibilité continue et ininterrompue de votre système de fichiers Amazon FSx, vous devez mettre à jour la configuration Active Directory du système de fichiers chaque fois que vous apportez des modifications à votre configuration Active Directory autogérée.

Par exemple, si votre Active Directory utilise une politique de réinitialisation du mot de passe basée sur le temps, assurez-vous de mettre à jour le mot de passe du compte de service avec Amazon FSx dès que le mot de passe est réinitialisé. De même, si les adresses IP du serveur DNS changent pour votre domaine Active Directory, mettez à jour les adresses IP du serveur DNS avec Amazon FSx dès que le changement se produit. Pour plus d'informations, consultez Mise à jour de la configuration autogérée d'Active Directory.

Lorsque vous mettez à jour la configuration autogérée d'Active Directory pour votre système de fichiers Amazon FSx, l'état de votre système de fichiers passe de Disponible à Mise à jour pendant que la mise à jour est appliquée. Vérifiez que l'état revient à Disponible une fois la mise à jour appliquée. Notez que la mise à jour peut prendre plusieurs minutes. Pour plus d'informations, consultez Surveillance des mises à jour d'Active Directory autogérées.

En cas de problème avec la mise à jour de la configuration autogérée d'Active Directory, l'état du système de fichiers passe à Mauvais configuration. Cet état affiche un message d'erreur et une action corrective recommandée à côté de la description du système de fichiers dans la console, l'API et la CLI. Après avoir pris les mesures correctives recommandées, vérifiez que l'état de votre système de fichiers passe finalement à Disponible.

Pour en savoir plus sur la résolution d'éventuelles erreurs de configuration autogérées d'Active Directory, consultez. Le système de fichiers est mal configuré

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 privilèges au minimum nécessaire. Pour ce faire, utilisez les règles des groupes de sécurité. Pour en savoir plus, veuillez consulter la section Groupes de sécurité Amazon VPC.

Création de règles de groupe de sécurité sortant pour l'interface réseau de votre système de fichiers

Pour plus de sécurité, envisagez de configurer un groupe de sécurité avec des règles de trafic sortant. Ces règles doivent autoriser le trafic sortant uniquement vers vos contrôleurs de domaines Microsoft Active Directory autogérés ou au sein du sous-réseau ou du groupe de sécurité. Appliquez ce groupe de sécurité au VPC associé à l'interface Elastic Network Interface de votre système de fichiers Amazon FSx. Pour en savoir plus, consultez Contrôle d'accès au système de fichiers avec Amazon VPC.

Validation de votre configuration Active Directory

Avant de créer un système de fichiers FSx for Windows File Server joint à votre Active Directory, nous vous recommandons de valider votre configuration Active Directory à l'aide de l'outil de validation Amazon FSx Active Directory. Notez qu'une connexion Internet sortante est requise pour valider correctement la configuration d'Active Directory.

Pour valider votre configuration Active Directory

1. Lancez une instance Windows Amazon EC2 dans le même sous-réseau et avec les mêmes groupes de sécurité Amazon VPC que ceux que vous utilisez pour votre système de fichiers FSx for Windows File Server. Assurez-vous que votre instance EC2 dispose des autorisations `AmazonEC2ReadOnlyAccess` IAM requises. Vous pouvez valider les autorisations de rôle d'instance EC2 à l'aide du simulateur de politique IAM. Pour plus d'informations, consultez la section Tester les politiques IAM avec le simulateur de politiques IAM dans le guide de l'utilisateur IAM.
2. Joignez votre instance Windows EC2 à votre Active Directory. Pour plus d'informations, voir Joindre manuellement une instance Windows dans le Guide AWS Directory Service d'administration.
3. Connectez-vous à votre instance EC2. Pour plus d'informations, consultez la section Connexion à votre instance Windows dans le guide de l'utilisateur Amazon EC2.

4. Ouvrez une PowerShell fenêtre Windows (en utilisant Exécuter en tant qu'administrateur) sur l'instance EC2.

   Pour vérifier si le module Active Directory requis pour Windows PowerShell est installé, utilisez la commande de test suivante.

   ```
   PS C:\> Import-Module ActiveDirectory
   ```

   Si le message ci-dessus renvoie une erreur, installez-le à l'aide de la commande suivante.

   ```
   PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
   ```

5. Téléchargez l'outil de validation réseau à l'aide de la commande suivante.

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

6. Développez le fichier zip à l'aide de la commande suivante.

   ```
   PS C:\> Expand-Archive -Path "AmazonFSxADValidation.zip"
   ```

7. Ajoutez le `AmazonFSxADValidation` module à la session en cours.

   ```
   PS C:\> Import-Module .\AmazonFSxADValidation
   ```

8. Définissez les paramètres requis en remplaçant dans la commande suivante votre :

   - Nom de domaine Active Directory (*`DOMAINNAME.COM`*)
   - Préparez l'`$Credential`objet pour le mot de passe du compte de service à l'aide de l'une des options suivantes.
     - Pour générer l'objet d'identification de manière interactive, utilisez la commande suivante.

       ```
       $Credential = Get-Credential
       ```

     - Pour générer l'objet d'identification à l'aide d'une AWS Secrets Manager ressource, utilisez la commande suivante.

```
$Secret = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
 $AdminSecret).SecretString
$Credential = (New-Object PSCredential($Secret.UserName,(ConvertTo-SecureString
 $Secret.Password -AsPlainText -Force)))
```

- *Adresses IP du serveur DNS (IP_ADDRESS_1, IP_ADDRESS_2)*
- *ID (s) de sous-réseau pour les sous-réseaux sur lesquels vous prévoyez de créer votre système de fichiers Amazon FSx (SUBNET_1, SUBNET_2, par exemple).* subnet-04431191671ac0d19

```
PS C:\>
$FSxADValidationArgs = @{
    # DNS root of ActiveDirectory domain
    DomainDNSRoot = 'DOMAINNAME.COM'

    # IP v4 addresses of DNS servers
    DnsIpAddresses = @('IP_ADDRESS_1', 'IP_ADDRESS_2')

    # Subnet IDs for Amazon FSx file server(s)
    SubnetIds = @('SUBNET_1', 'SUBNET_2')

    Credential = $Credential
}
```

9. (Facultatif) Définissez l'unité organisationnelle, le groupe des administrateurs délégués et activez la validation des autorisations du compte de service en suivant les instructions du `README.md` fichier inclus avant d'exécuter l'outil de validation. DomainControllersMaxCount

> **Note**
>
> Le `Domain Admins` groupe porte un nom différent si le système d'exploitation n'est pas en anglais. Par exemple, le groupe est nommé `Administrateurs du domaine` dans la version française du système d'exploitation. Si vous ne spécifiez aucune valeur, le nom de `Domain Admins` groupe par défaut est utilisé et la création du système de fichiers échoue.

10. Exécutez l'outil de validation à l'aide de cette commande.

```
PS C:\> $Result = Test-FSxADConfiguration @FSxADValidationArgs
```

11. Voici un exemple de résultat de test réussi.

```
Test 1 - Validate EC2 Subnets ...
...
Test 17 - Validate 'Delete Computer Objects' permission ...

Test computer object amznfsxtestd53f deleted!
...
SUCCESS - All tests passed! Please proceed to creating an Amazon FSx file system.
 For your convenience, SelfManagedActiveDirectoryConfiguration of result can be
 used directly in CreateFileSystemWindowsConfiguration for New-FSXFileSystem
PS C:\AmazonFSxADValidation> $Result.Failures.Count
0
PS C:\AmazonFSxADValidation> $Result.Warnings.Count
0
```

Voici un exemple de résultat de test comportant des erreurs.

```
Test 1 - Validate EC2 Subnets ...
...
Test 7 - Validate that provided EC2 Subnets belong to a single AD Site ...

Name          DistinguishedName
     Site
----          -----------------
     ----
10.0.0.0/19   CN=10.0.0.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local   CN=SiteB,CN=Sites,CN=Configu...
10.0.128.0/19 CN=10.0.128.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local CN=Default-First-Site-Name,C...
10.0.64.0/19  CN=10.0.64.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local  CN=SiteB,CN=Sites,CN=Configu...



Best match for EC2 subnet subnet-092f4caca69e360e7 is AD site CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=te
st-ad,DC=local
Best match for EC2 subnet subnet-04431191671ac0d19 is AD site
 CN=SiteB,CN=Sites,CN=Configuration,DC=test-ad,DC=local
```

```
WARNING: EC2 subnets subnet-092f4caca69e360e7 subnet-04431191671ac0d19 matched to
 different AD sites! Make sure they
are in a single AD site.
...
9 of 16 tests skipped.
FAILURE - Tests failed. Please see error details below:

Name                           Value
----                           -----
SubnetsInSeparateAdSites       {subnet-04431191671ac0d19, subnet-092f4caca69e360e7}



Please address all errors and warnings above prior to re-running validation to
 confirm fix.
PS C:\AmazonFSxADValidation> $Result.Failures.Count
1
PS C:\AmazonFSxADValidation> $Result.Failures

Name                           Value
----                           -----
SubnetsInSeparateAdSites       {subnet-04431191671ac0d19, subnet-092f4caca69e360e7}


PS C:\AmazonFSxADValidation> $Result.Warnings.Count
0
```

Si vous recevez des avertissements ou des erreurs lorsque vous exécutez l'outil de validation, reportez-vous au guide de résolution des problèmes inclus dans le package de l'outil de validation (`TROUBLESHOOTING.md`) et[Résolution des problèmes liés à Amazon FSx](#).

Joindre un système de fichiers Amazon FSx à un domaine Microsoft Active Directory autogéré

Lorsque vous créez un nouveau système de fichiers FSx for Windows File Server, vous pouvez configurer l'intégration de Microsoft Active Directory afin qu'il soit joint à votre domaine Microsoft Active Directory autogéré. Pour ce faire, fournissez les informations suivantes pour votre Microsoft Active Directory :

- Le nom de domaine complet de votre annuaire Microsoft Active Directory local.

> **Note**
>
> Amazon FSx ne prend actuellement pas en charge les domaines SLD (Single Label Domain).

- Les adresses IP des serveurs DNS de votre domaine.
- Informations d'identification pour un compte de service dans votre domaine Microsoft Active Directory local. Amazon FSx utilise ces informations d'identification pour rejoindre votre Active Directory autogéré.

Le cas échéant, vous pouvez également spécifier les options suivantes :

- Unité organisationnelle (UO) spécifique au sein du domaine que vous souhaitez associer à votre système de fichiers Amazon FSx.
- Le nom du groupe de domaines dont les membres sont dotés de privilèges administratifs pour le système de fichiers Amazon FSx.

> **Note**
>
> Le nom de groupe de domaines que vous fournissez doit être unique dans votre Active Directory. FSx for Windows File Server ne créera pas le groupe de domaines dans les cas suivants :
>
> - Si un groupe existe déjà avec le nom que vous spécifiez
> - Si vous ne spécifiez pas de nom et qu'un groupe nommé « Administrateurs de domaine » existe déjà dans votre Active Directory.

Après avoir spécifié ces informations, Amazon FSx joint votre nouveau système de fichiers à votre domaine Active Directory autogéré à l'aide du compte de service que vous avez fourni.

> **Important**
>
> Amazon FSx enregistre les enregistrements DNS pour un système de fichiers uniquement si le domaine Active Directory auquel vous le joignez utilise le DNS Microsoft comme DNS par défaut. Si vous utilisez un DNS tiers, vous devrez configurer manuellement les entrées DNS pour vos systèmes de fichiers Amazon FSx après avoir créé votre système de fichiers.

Pour plus d'informations sur le choix des adresses IP correctes à utiliser pour le système de fichiers, consultezObtention des adresses IP de système de fichiers correctes à utiliser pour le DNS.

Avant de commencer

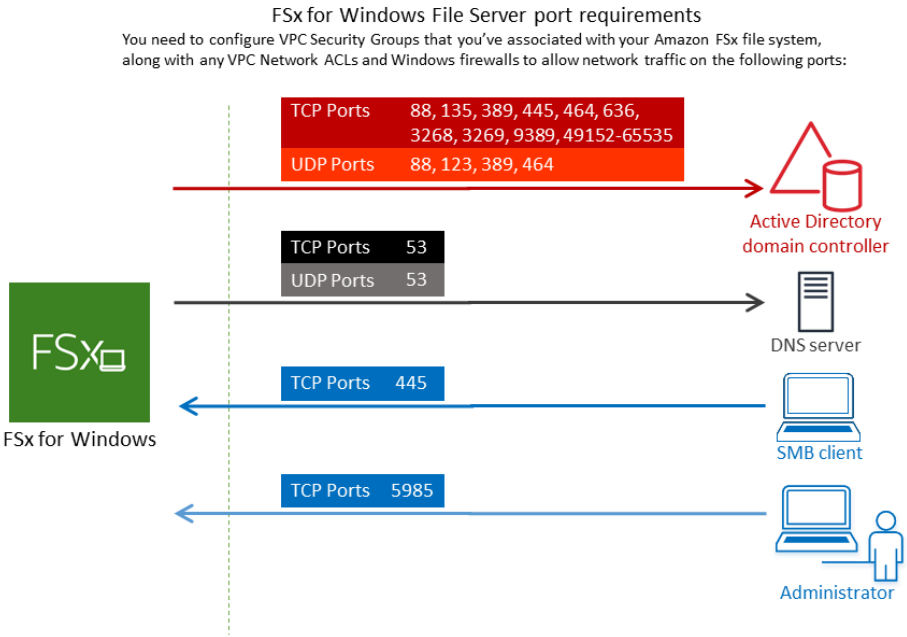
Assurez-vous d'avoir rempli les Conditions préalables à l'utilisation d'un Microsoft Active Directory autogéré informations détaillées dansUtilisation d'Amazon FSx avec votre Microsoft Active Directory autogéré.

Pour créer un système de fichiers FSx for Windows File Server joint à un Active Directory autogéré (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans Sur le tableau de bord, choisissez Create file system (Créer un système de fichiers) pour ouvrir l'assistant de création de système de fichiers.
3. Choisissez FSx for Windows File Server, puis Next. La page Create file system (Créer un système de fichiers) s'affiche.
4. Donnez un nom à votre système de fichiers. Vous pouvez utiliser un maximum de 256 lettres Unicode, espaces blancs et chiffres, plus les caractères spéciaux + - =. _ :/
5. Pour Capacité de stockage, entrez la capacité de stockage de votre système de fichiers, en GiB. Si vous utilisez un stockage SSD, entrez un nombre entier compris entre 32 et 65 536. Si vous utilisez un espace de stockage sur disque dur, entrez un nombre entier compris entre 2 000 et 65 536. Vous pouvez augmenter la capacité de stockage selon vos besoins à tout moment après avoir créé le système de fichiers. Pour plus d'informations, consultez Gestion de la capacité de stockage.
6. Conservez la valeur par défaut de Throughput capacity (Capacité de débit). La capacité de débit est la vitesse soutenue à laquelle le serveur de fichiers hébergeant votre système de fichiers peut traiter les données. Le paramètre de capacité de débit recommandée est basé sur la quantité de capacité de stockage que vous choisissez. Si vous avez besoin d'une capacité de débit supérieure à la capacité de débit recommandée, choisissez Spécifier la capacité de débit, puis choisissez une valeur. Pour plus d'informations, consultez Performances de FSx for Windows File Server.

   Vous pouvez modifier la capacité de débit selon vos besoins à tout moment après avoir créé le système de fichiers. Pour plus d'informations, consultez Gestion de la capacité de débit.

7. Choisissez le VPC que vous souhaitez associer à votre système de fichiers. Dans le cadre de cet exercice de démarrage, choisissez le même VPC que pour votre AWS Directory Service répertoire et votre instance Amazon EC2.
8. Choisissez n'importe quelle valeur pour les zones de disponibilité et le sous-réseau.
9. Pour les groupes de sécurité VPC, le groupe de sécurité par défaut pour votre Amazon VPC par défaut est déjà ajouté à votre système de fichiers dans la console. Assurez-vous que le groupe de sécurité et les ACL du réseau VPC du ou des sous-réseaux sur lesquels vous créez votre système de fichiers FSx autorisent le trafic sur les ports et dans les directions indiquées dans le schéma suivant.



Le tableau suivant identifie le rôle de chaque port.

Protocole	Ports	Rôle
TCP/UDP	53	Systè de nom de

Protocole	Ports	Rôle
		domai (DNS)
TCP/UDP	88	Authe icatior Kerbe
TCP/UDP	464	Chang t/ définit ion de mot de passe
TCP/UDP	389	Protoc LDAP (Light ght Direct Acces Protoc
UDP	123	Protoc NTP (Netw Time Protoc

Protocole	Ports	Rôle
TCP	135	Distrib ed Comp Enviro nt / End Point Mapp (DCE EPMA
TCP	445	Partag de fichier SMB avec les servic d'annu e
TCP	636	Protoc LDAP (Light ght Direct Acces Protoc via TLS/ SSL (LDAP

Protocole	Ports	Rôle
TCP	3268	Catalo mondi Micros
TCP	3269	Micros Globa Catalo via SSL
TCP	5985	WinRI 2.0 (gestio à distan de Micros Windo
TCP	9389	Servic Web Micros Active Direct DS, Powe l
TCP	49152 - 65535	Ports éphém pour RPC

> **Important**
>
> L'autorisation du trafic sortant sur le port TCP 9389 est requise pour les déploiements de systèmes de fichiers mono-AZ 2 et multi-AZ.

> **Note**
>
> Si vous utilisez des ACL de réseau VPC, vous devez également autoriser le trafic sortant sur les ports dynamiques (49152-65535) depuis votre système de fichiers FSx.

- Règles de trafic sortant pour autoriser tout le trafic vers les adresses IP associées aux serveurs DNS et aux contrôleurs de domaine pour votre domaine Microsoft Active Directory autogéré. Pour plus d'informations, consultez la documentation Microsoft sur la configuration de votre pare-feu pour les communications Active Directory.
- Assurez-vous que ces règles de trafic sont également reflétées sur les pare-feux qui s'appliquent à chacun des contrôleurs de domaine Active Directory, des serveurs DNS, des clients FSx et des administrateurs FSx.

> **Note**
>
> Si vous avez défini des sites Active Directory, vous devez vous assurer que le ou les sous-réseaux du VPC associé à votre système de fichiers Amazon FSx sont définis dans un site Active Directory et qu'aucun conflit n'existe entre le ou les sous-réseaux de votre VPC et ceux de vos autres sites. Vous pouvez afficher et modifier ces paramètres à l'aide du composant logiciel enfichable MMC Active Directory Sites and Services.

> **Important**
>
> Alors que les groupes de sécurité Amazon VPC nécessitent que les ports soient ouverts uniquement dans le sens où le trafic réseau est initié, la plupart des pare-feux Windows et des ACL de réseau VPC nécessitent que les ports soient ouverts dans les deux sens.

10. Pour l'authentification Windows, choisissez Microsoft Active Directory autogéré.
11. Entrez une valeur pour le nom de domaine complet pour l'annuaire Microsoft Active Directory autogéré.

> **Note**
>
> Le nom de domaine ne doit pas être au format SLD (Single Label Domain). Amazon FSx ne prend actuellement pas en charge les domaines SLD.

> **Important**
>
> Pour les systèmes de fichiers mono-AZ 2 et tous les systèmes de fichiers multi-AZ, le nom de domaine Active Directory ne peut pas dépasser 47 caractères.

12. Entrez une valeur pour l'unité organisationnelle pour le répertoire Microsoft Active Directory autogéré.

> **Note**
>
> Assurez-vous que le compte de service que vous avez fourni possède des autorisations déléguées à l'unité d'organisation que vous spécifiez ici ou à l'unité d'organisation par défaut si vous n'en spécifiez aucune.

13. Entrez au moins une valeur, mais pas plus de deux, pour les adresses IP des serveurs DNS pour l'annuaire Microsoft Active Directory autogéré.
14. Entrez une valeur de chaîne pour le nom d'utilisateur du compte de service sur votre domaine Active Directory autogéré, par exemple`ServiceAcct`. Amazon FSx utilise ce nom d'utilisateur pour rejoindre votre domaine Microsoft Active Directory.

> **Important**
>
> N'incluez PAS de préfixe de domaine (`corp.com\ServiceAcct`) ou de suffixe de domaine (`ServiceAcct@corp.com`) lors de la saisie du nom d'utilisateur du compte de service.
> N'utilisez PAS le nom distinctif (DN) lors de la saisie du nom d'utilisateur du compte de service (`CN=ServiceAcct,OU=example,DC=corp,DC=com`).

15. Entrez une valeur pour le mot de passe du compte de service de votre domaine Active Directory autogéré. Amazon FSx utilise ce mot de passe pour se connecter à votre domaine Microsoft Active Directory.
16. Entrez à nouveau le mot de passe pour le confirmer dans Confirmer le mot de passe.
17. Pour le groupe d'administrateurs de systèmes de fichiers délégués, spécifiez le `Domain Admins` groupe ou un groupe d'administrateurs de système de fichiers délégués personnalisé (si vous en avez créé un). Le groupe que vous spécifiez doit disposer de l'autorité déléguée pour effectuer des tâches administratives sur votre système de fichiers. Si vous ne fournissez aucune valeur, Amazon FSx utilise le groupe intégré`Domain Admins`. Notez qu'Amazon FSx ne prend pas en charge la présence d'un `Delegated file system administrators group` (`Domain Admins`groupe ou groupe personnalisé que vous spécifiez) situé dans le conteneur intégré.

> **Important**
>
> Si vous ne fournissez pas de groupe d'administrateurs de systèmes de fichiers délégués, Amazon FSx tente par défaut d'utiliser le `Domain Admins` groupe intégré dans votre domaine Active Directory. Si le nom de ce groupe intégré a été modifié ou si vous utilisez un autre groupe pour l'administration du domaine, vous devez fournir ce nom pour le groupe ici.

> **Important**
>
> N'incluez PAS de préfixe de domaine (corp.com \ FSxAdmins) ou de suffixe de domaine (F SxAdmins @corp .com) lorsque vous fournissez le paramètre de nom de groupe. N'UTILISEZ PAS le nom distinctif (DN) pour le groupe. Un exemple de nom distinctif est CN=FSxAdmins, OU=Example, DC=Corp, DC=com.

Pour créer un système de fichiers FSx for Windows File Server joint à un Active Directory autogéré ()AWS CLI

L'exemple suivant crée un système de fichiers FSx for Windows File Server avec `SelfManagedActiveDirectoryConfiguration` un dans `us-east-2` la zone de disponibilité.

```
aws fsx --region us-east-2 \
```

```
create-file-system \
--file-system-type WINDOWS \
--storage-capacity 300 \
--security-group-ids security-group-id \
--subnet-ids subnet-id\
--windows-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAdmini
 \
UserName="FSxService",Password="password", \
   DnsIps=["10.0.1.18"]}',ThroughputCapacity=8
```

> **Important**
>
> Ne déplacez pas les objets informatiques créés par Amazon FSx dans l'unité d'organisation après la création de votre système de fichiers. Cela entraînera une mauvaise configuration de votre système de fichiers.

Obtention des adresses IP de système de fichiers correctes à utiliser pour le DNS

Amazon FSx enregistre les enregistrements DNS pour un système de fichiers uniquement si vous utilisez Microsoft DNS comme service DNS par défaut. Si vous utilisez un DNS tiers, vous devrez configurer manuellement les entrées DNS pour vos systèmes de fichiers Amazon FSx. Cette section décrit comment obtenir les adresses IP de système de fichiers correctes à utiliser si vous devez ajouter manuellement le système de fichiers à votre DNS. Notez qu'une fois qu'un système de fichiers est créé, ses adresses IP ne changent pas tant que le système de fichiers n'est pas supprimé.

Comment obtenir les adresses IP des systèmes de fichiers à utiliser pour les entrées DNS A

1. Dans le https://console.aws.amazon.com/fsx/, choisissez le système de fichiers dont vous souhaitez obtenir l'adresse IP pour afficher la page de détails du système de fichiers.
2. Dans l'onglet Réseau et sécurité, effectuez l'une des opérations suivantes :

   - Pour les systèmes de fichiers mono-AZ 1 :
     - Dans le panneau Subnet, choisissez l'interface Elastic Network affichée sous Network interface pour ouvrir la page Network Interfaces dans la console Amazon EC2.

    - L'adresse IP du système de fichiers mono-AZ 1 à utiliser est indiquée dans la colonne IP IPv4 privée principale.
- Pour les systèmes de fichiers mono-AZ 2 ou multi-AZ :
    - Dans le panneau Sous-réseau préféré, choisissez l'interface réseau élastique affichée sous Interface réseau pour ouvrir la page Network Interfaces dans la console Amazon EC2.
    - L'adresse IP du sous-réseau préféré à utiliser est indiquée dans la colonne IP IPv4 privée secondaire.
    - Dans le panneau du sous-réseau Amazon FSx Standby, choisissez l'interface réseau élastique affichée sous Interface réseau pour ouvrir la page Network Interfaces dans la console Amazon EC2.
    - L'adresse IP du sous-réseau de secours à utiliser est indiquée dans la colonne IP IPv4 privée secondaire.

> **Note**
>
> Si vous devez configurer des entrées DNS pour votre Windows Remote PowerShell Endpoint pour les systèmes de fichiers mono-AZ 2 ou multi-AZ, vous devez utiliser l'adresse IPv4 privée principale pour l'interface elastic network de votre sous-réseau préféré. Pour plus d'informations, consultez Utilisation de l'interface de ligne de commande Amazon FSx pour PowerShell.

Mise à jour de la configuration autogérée d'Active Directory

Vous pouvez utiliser l' AWS Management Console API Amazon FSx ou AWS CLI pour mettre à jour le nom d'utilisateur et le mot de passe du compte de service ainsi que les adresses IP du serveur DNS de la configuration Active Directory autogérée d'un système de fichiers. Vous pouvez suivre la progression d'une mise à jour de configuration Active Directory autogérée à tout moment à l'aide de la AWS Management Console CLI et de l'API. Pour plus d'informations, consultez Surveillance des mises à jour d'Active Directory autogérées.

Pour mettre à jour la configuration autogérée d'Active Directory (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Accédez à Systèmes de fichiers, puis choisissez le système de fichiers Windows pour lequel vous souhaitez mettre à jour la configuration autogérée d'Active Directory.

3. Dans l'onglet Réseau et sécurité, choisissez ensuite Mettre à jour pour les adresses IP du serveur DNS ou pour le nom d'utilisateur du compte de service, selon les propriétés Active Directory que vous mettez à jour.
4. Entrez les nouvelles adresses IP du serveur DNS ou les nouvelles informations d'identification du compte de service dans la boîte de dialogue qui apparaît.
5. Choisissez Mettre à jour pour lancer la mise à jour de la configuration d'Active Directory.

   Vous pouvez suivre la progression de la mise à jour à l'aide du AWS Management Console ou du AWS CLI.

Pour mettre à jour la configuration autogérée d'Active Directory (CLI)

- Pour mettre à jour la configuration Active Directory autogérée d'un système de fichiers FSx for Windows File Server, utilisez AWS CLI la commande update-file-system. Définissez les paramètres suivants :
  - `--file-system-id`à l'ID du système de fichiers que vous mettez à jour.
  - `UserName`le nouveau nom d'utilisateur du compte de service Active Directory autogéré.
  - `Password`le nouveau mot de passe du compte de service Active Directory autogéré.
  - `DnsIps`les adresses IP des serveurs DNS Active Directory autogérés.

```
aws fsx update-file-system \
  --file-system-id fs-0123456789abcdef0 \
  --windows-configuration
 'SelfManagedActiveDirectoryConfiguration={UserName=username,Password=password,\
    DnsIps=[192.0.2.0,192.0.2.24]}'
```

  Si l'action de mise à jour aboutit, le service renvoie une réponse HTTP 200. L'`AdminstrativeActions`objet de la réponse décrit la demande et son statut.

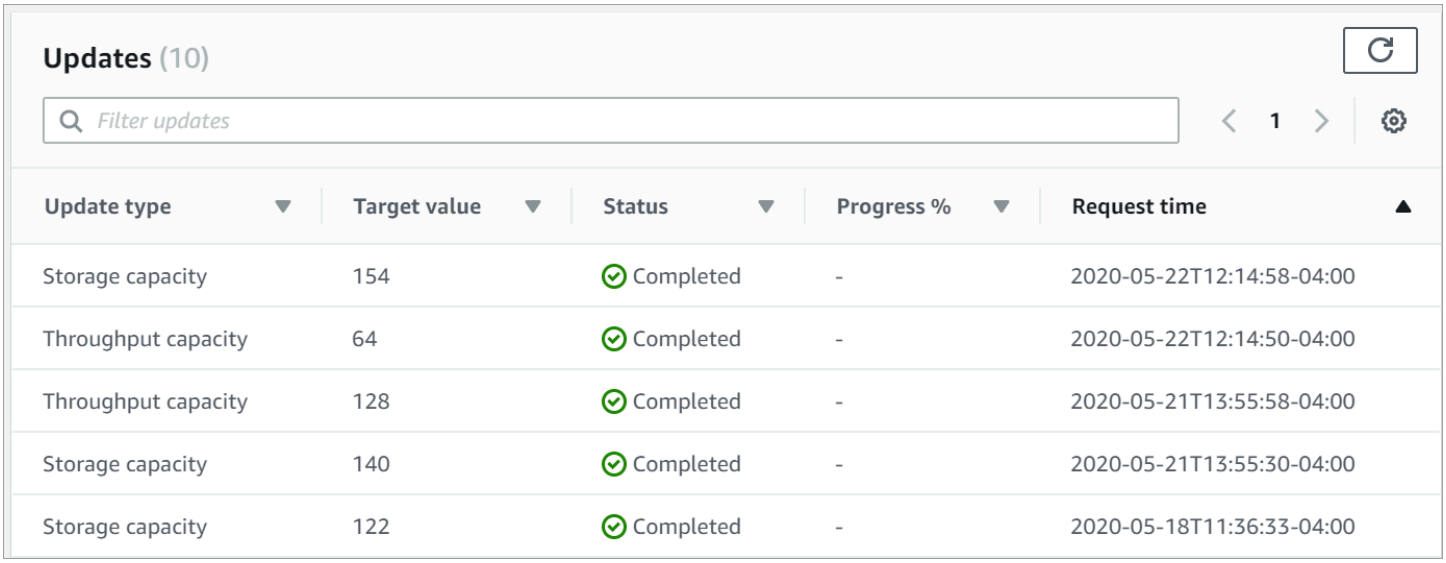
Surveillance des mises à jour d'Active Directory autogérées

Lorsque vous mettez à jour la configuration Active Directory autogérée de votre système de fichiers, l'état du système de fichiers passe de Disponible à Mise à jour pendant que la mise à jour est appliquée. Une fois la mise à jour terminée, l'état redevient Disponible. Notez que la mise à jour peut prendre plusieurs minutes.

Vous pouvez suivre la progression d'une mise à jour de configuration Active Directory autogérée à l' AWS Management Console aide de l'API ou du AWS CLI, décrit dans les sections suivantes.

Surveillance des mises à jour dans la console

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



Update type	Target value	Status	Progress %	Request time
Storage capacity	154	Completed	-	2020-05-22T12:14:58-04:00
Throughput capacity	64	Completed	-	2020-05-22T12:14:50-04:00
Throughput capacity	128	Completed	-	2020-05-21T13:55:58-04:00
Storage capacity	140	Completed	-	2020-05-21T13:55:30-04:00
Storage capacity	122	Completed	-	2020-05-18T11:36:33-04:00

Pour les mises à jour d'Active Directory autogérées, vous pouvez consulter les informations suivantes.

Type de mise à jour

Les types pris en charge sont les suivants :

- Adresse IP du serveur DNS
- Informations d'identification du compte de service

Valeur cible

La valeur souhaitée pour mettre à jour la propriété du système de fichiers. Pour les mises à jour des informations d'identification des comptes de service, seul le nom d'utilisateur est affiché, les mots de passe des comptes de service ne sont jamais inclus dans ce champ.

Statut

État actuel de la mise à jour. Pour les mises à jour Active Directory autogérées, les valeurs possibles sont les suivantes :

- En attente : Amazon FSx a reçu la demande de mise à jour, mais n'a pas commencé à la traiter.

- En cours — Amazon FSx traite la demande de mise à jour.
- Terminé — La mise à jour du système de fichiers s'est terminée avec succès.
- Échec — La mise à jour du système de fichiers a échoué. Choisissez le point d'interrogation (?) pour voir les détails de l'échec.

% de progression

Affiche la progression de la mise à jour du système de fichiers 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.

Surveillance des mises à jour à l'aide de l'API AWS CLI and

Vous pouvez consulter et surveiller les demandes de mise à jour du système de fichiers en cours à l'aide de la AWS CLI commande describe-file-systems et de l'action de l'DescribeFileAPI Systems. Le `AdministrativeActions` tableau répertorie les 10 actions de mise à jour les plus récentes pour chaque type d'action administrative.

L'exemple suivant montre un extrait de la réponse d'une commande describe-file-systems CLI montrant deux mises à jour autogérées du système de fichiers Active Directory.

```
{
    "OwnerId": "111122223333",
    .
    .
    .
    "StorageCapacity": 1000,
    "AdministrativeActions": [
        {
            "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
            "RequestTime": 1581694766.757,
            "Status": "PENDING",
            "TargetFileSystemValues": {
                "WindowsConfiguration": {
                    "SelfManagedActiveDirectoryConfiguration": {
                        "UserName": "serviceUser",
                    }
                }
```

```
                }
            },
            {
                "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                "RequestTime": 1619032957.759,
                "Status": "FAILED",
                "TargetFileSystemValues": {
                    "WindowsConfiguration": {
                        "SelfManagedActiveDirectoryConfiguration": {
                        "DnsIps": [
                                "10.0.138.161"
                            ]
                        }
                    }
                },
                "FailureDetails": {
                    "Message": "Failure details message."
                }
            }
        ],
    .
    .
    .
```

Utilisation des partages de fichiers Microsoft Windows

Un partage de fichiers Microsoft Windows est un dossier spécifique de votre système de fichiers. Il inclut les sous-dossiers de ce dossier, que vous rendez accessibles à vos instances de calcul à l'aide du protocole SMB (Server Message Block). Votre système de fichiers est fourni avec un partage de fichiers Windows par défaut, nommé`share`. Vous pouvez créer et gérer autant d'autres partages de fichiers Windows que vous le souhaitez à l'aide de l'outil d'interface utilisateur graphique (GUI) Windows nommé Dossiers partagés.

Accès aux partages de fichiers

Pour accéder à vos partages de fichiers, vous utilisez la fonctionnalité Windows Map Network Drive pour associer une lettre de lecteur de votre instance de calcul à votre partage de fichiers Amazon FSx. Le processus de mappage d'un partage de fichiers vers un lecteur de votre instance de calcul est connu sous le nom de montage d'un partage de fichiers sous Linux. Ce processus varie en fonction du type d'instance de calcul et du système d'exploitation. Une fois votre partage de fichiers mappé, vos applications et vos utilisateurs peuvent accéder aux fichiers et aux dossiers de votre partage de fichiers comme s'il s'agissait de fichiers et de dossiers locaux.

Les procédures suivantes permettent de mapper un partage de fichiers sur les différentes instances de calcul prises en charge.

Rubriques

- Mappage d'un partage de fichiers sur une instance Windows Amazon EC2
- Montage d'un partage de fichiers sur une instance Mac Amazon EC2
- Montage d'un partage de fichiers sur une instance Linux Amazon EC2
- Montage automatique de partages de fichiers sur une instance Amazon Linux EC2 non jointe à votre Active Directory

Mappage d'un partage de fichiers sur une instance Windows Amazon EC2

Vous pouvez mapper un partage de fichiers sur une instance Windows EC2 à l'aide de l'explorateur de fichiers Windows ou de l'invite de commande.

Pour mapper un partage de fichiers sur une instance Windows Amazon EC2 (console)

1. Lancez l'instance Windows EC2 et connectez-la au Microsoft Active Directory auquel vous avez joint votre système de fichiers Amazon FSx. Pour ce faire, choisissez l'une des procédures suivantes dans le guide AWS Directory Service d'administration :

   - Joindre facilement une instance Windows EC2
   - Joindre manuellement une instance Windows

2. Connectez-vous à votre instance EC2 Windows. Pour plus d'informations, consultez la section Connexion à votre instance Windows dans le guide de l'utilisateur Amazon EC2.
3. Une fois connecté, ouvrez l'Explorateur de fichiers.
4. Dans le volet de navigation, ouvrez le menu contextuel (clic droit) de Network, puis sélectionnez Map Network Drive.
5. Pour Drive, choisissez une lettre de lecteur.
6. Pour Dossier, entrez le nom DNS du système de fichiers ou un alias DNS associé au système de fichiers, ainsi que le nom du partage.

   > **Important**
   >
   > L'utilisation d'une adresse IP au lieu du nom DNS peut entraîner une indisponibilité lors du processus de basculement du système de fichiers multi-AZ. En outre, les noms DNS ou les alias DNS associés sont nécessaires pour l'authentification basée sur Kerberos dans les systèmes de fichiers multi-AZ et mono-AZ.

   Vous pouvez trouver le nom DNS du système de fichiers et tous les alias DNS associés sur la console Amazon FSx en choisissant Windows File Server, Network & security. Vous pouvez également les trouver dans la réponse de l'opération du CreateFilesystème ou de l'API du DescribeFilesystème. Pour plus d'informations sur l'utilisation des alias DNS, consultezGestion des alias DNS.

   - Pour un système de fichiers mono-AZ joint à un Microsoft Active Directory AWS géré, le nom DNS est le suivant.

     ```
     fs-0123456789abcdef0.ad-domain.com
     ```

- Pour un système de fichiers mono-AZ joint à un Active Directory autogéré, et pour tout système de fichiers multi-AZ, le nom DNS est le suivant.

```
amznfsxaa11bb22.ad-domain.com
```

Par exemple, pour utiliser le nom DNS d'un système de fichiers mono-AZ, entrez ce qui suit dans le champ Dossier.

```
\\fs-0123456789abcdef0.ad-domain.com\share
```

Pour utiliser le nom DNS d'un système de fichiers multi-AZ, entrez ce qui suit dans le champ Dossier.

```
\\famznfsxaa11bb22.ad-domain.com\share
```

Pour utiliser un alias DNS associé au système de fichiers, entrez ce qui suit dans le champ Dossier.

```
\\fqdn-dns-alias\share
```

7. Choisissez une option pour Reconnecter lors de la connexion, qui indique si le partage de fichiers doit se reconnecter lors de la connexion, puis choisissez Terminer.

Pour mapper un partage de fichiers sur une instance Windows Amazon EC2 (invite de commande)

1. Lancez l'instance Windows EC2 et connectez-la au Microsoft Active Directory auquel vous avez joint votre système de fichiers Amazon FSx. Pour ce faire, choisissez l'une des procédures suivantes dans le guide AWS Directory Service d'administration :
   - Joindre facilement une instance Windows EC2
   - Joindre manuellement une instance Windows
2. Connectez-vous à votre instance Windows EC2 en tant qu'utilisateur dans votre AWS Managed Microsoft AD annuaire. Pour plus d'informations, consultez la section Connexion à votre instance Windows dans le guide de l'utilisateur Amazon EC2.
3. Une fois connecté, ouvrez une fenêtre d'invite de commande.

4. Montez le partage de fichiers en utilisant la lettre de lecteur de votre choix, le nom DNS du système de fichiers et le nom du partage. Vous pouvez trouver le nom DNS à l'aide de la console Amazon FSx en choisissant Windows File Server, Network & security. Vous pouvez également les trouver dans la réponse de l'opération `CreateFileSystem` ou `DescribeFileSystems` API.

   - Pour un système de fichiers mono-AZ joint à un Microsoft Active Directory AWS géré, le nom DNS est le suivant.

     ```
     fs-0123456789abcdef0.ad-domain.com
     ```

   - Pour un système de fichiers mono-AZ joint à un Active Directory autogéré, et pour tout système de fichiers multi-AZ, le nom DNS est le suivant.

     ```
     amznfsxaa11bb22.ad-domain.com
     ```

   Voici un exemple de commande pour monter le partage de fichiers.

   ```
   $ net use H: \\amzfsxaa11bb22.ad-domain.com\share /persistent:yes
   ```

   Au lieu de la `net use` commande, vous pouvez également utiliser n'importe quelle PowerShell commande prise en charge pour monter un partage de fichiers.

Montage d'un partage de fichiers sur une instance Mac Amazon EC2

Vous pouvez monter un partage de fichiers sur une instance Mac Amazon EC2 jointe ou non jointe à votre Active Directory. Si l'instance n'est pas jointe à votre Active Directory, veillez à mettre à jour les options DHCP définies pour l'Amazon Virtual Private Cloud (Amazon VPC) dans lequel réside l'instance afin d'inclure les serveurs de noms DNS de votre domaine Active Directory. Relancez ensuite l'instance.

Pour monter un partage de fichiers sur une instance Mac Amazon EC2 (GUI)

1. Lancez l'instance Mac EC2. Pour ce faire, choisissez l'une des procédures suivantes dans le guide de l'utilisateur Amazon EC2 :

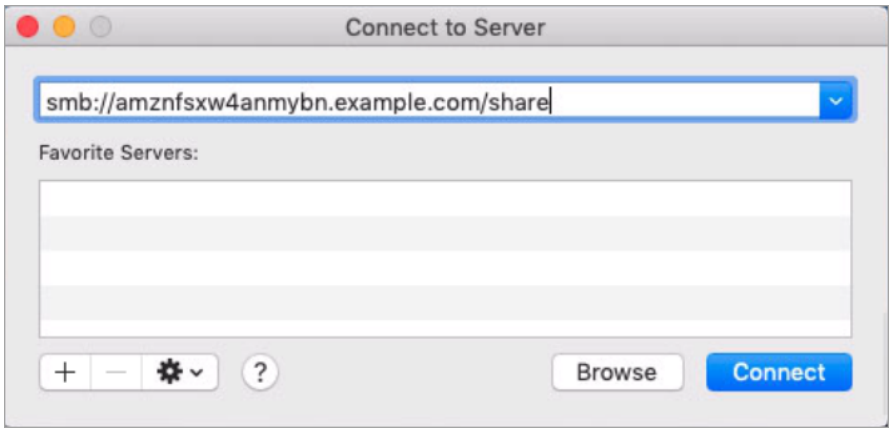
- Lancer une instance Mac à l'aide de la console
- Lancez une instance Mac à l'aide du AWS CLI

2. Connectez-vous à votre instance Mac EC2 à l'aide de Virtual Network Computing (VNC). Pour plus d'informations, consultez Connect to your instance using VNC dans le guide de l'utilisateur Amazon EC2.
3. Sur votre instance Mac EC2, connectez-vous à votre partage de fichiers Amazon FSx, comme suit :

   a. Ouvrez le Finder, choisissez Go, puis Connect to Server.

   b. Dans la boîte de dialogue Connect to Server, entrez le nom DNS du système de fichiers ou un alias DNS associé au système de fichiers, ainsi que le nom du partage. Choisissez ensuite Connect (Connecter).

      Vous pouvez trouver le nom DNS du système de fichiers et tous les alias DNS associés sur la console Amazon FSx en choisissant Windows File Server, Network & security. Vous pouvez également les trouver dans la réponse de l'opération du CreateFilesystème ou de l'API du DescribeFilesystème. Pour plus d'informations sur l'utilisation des alias DNS, consultezGestion des alias DNS.

   c. Sur l'écran suivant, choisissez Connect pour continuer.

   d. Entrez vos informations d'identification Microsoft Active Directory (AD) pour le compte de service Amazon FSx, comme indiqué dans l'exemple suivant. Choisissez ensuite Connect (Connecter).

e. Si la connexion est établie, vous pouvez voir le partage Amazon FSx sous Emplacements dans la fenêtre du Finder.

Pour monter un partage de fichiers sur une instance Mac Amazon EC2 (ligne de commande)

1. Lancez l'instance Mac EC2. Pour ce faire, choisissez l'une des procédures suivantes dans le guide de l'utilisateur Amazon EC2 :
   - Lancer une instance Mac à l'aide de la console
   - Lancez une instance Mac à l'aide du AWS CLI
2. Connectez-vous à votre instance Mac EC2 à l'aide de Virtual Network Computing (VNC). Pour plus d'informations, consultez Connect to your instance using VNC dans le guide de l'utilisateur Amazon EC2.
3. Montez le partage de fichiers à l'aide de la commande suivante.

   ```
   mount_smbfs //file_system_dns_name/file_share mount_point
   ```

   Vous pouvez trouver le nom DNS sur la console Amazon FSx en choisissant Windows File Server, Network & security. Vous pouvez également les trouver dans la réponse de l'opération `CreateFileSystem` ou `DescribeFileSystems` API.

   - Pour un système de fichiers mono-AZ joint à un Microsoft Active Directory AWS géré, le nom DNS est le suivant.

     ```
     fs-0123456789abcdef0.ad-domain.com
     ```

- Pour un système de fichiers mono-AZ joint à un Active Directory autogéré, et pour tout système de fichiers multi-AZ, le nom DNS est le suivant.

```
amznfsxaa11bb22.ad-domain.com
```

La commande mount utilisée dans cette procédure effectue les opérations suivantes aux points indiqués :

- *//file_system_dns_name/file_share*— Spécifie le nom DNS et le partage du système de fichiers à monter.
- *mount_point* — Le répertoire de l'instance EC2 sur lequel vous montez le système de fichiers.

Montage d'un partage de fichiers sur une instance Linux Amazon EC2

Vous pouvez monter un partage de fichiers FSx for Windows File Server sur une instance Linux Amazon EC2 jointe ou non jointe à votre Active Directory.

> **Note**
>
> - Les commandes suivantes spécifient des paramètres tels que le protocole SMB, la mise en cache et la taille de la mémoire tampon de lecture et d'écriture à titre d'exemple uniquement. Les choix de paramètres pour la `cifs` commande Linux, ainsi que la version du noyau Linux utilisée, peuvent avoir un impact sur le débit et la latence des opérations réseau entre le client et le système de fichiers Amazon FSx. Pour plus d'informations, consultez `cifs` la documentation de l'environnement Linux que vous utilisez.
> - Les clients Linux ne prennent pas en charge le basculement automatique basé sur le DNS. Pour plus d'informations, consultez Expérience de basculement sur les clients Linux.

Pour monter un partage de fichiers sur une instance Linux Amazon EC2 jointe à votre Active Directory

1. Si aucune instance Linux EC2 en cours d'exécution n'est associée à votre Microsoft Active Directory, voir Joindre manuellement une instance Linux dans le Guide d'AWS Directory Service administration pour obtenir des instructions à cet effet.
2. Connectez-vous à votre instance Linux EC2. Pour plus d'informations, consultez Connect to your Linux instance dans le guide de l'utilisateur Amazon EC2.
3. Pour installer le package `cifs-utils`, exécutez la commande suivante : Ce package est utilisé pour monter des systèmes de fichiers réseau tels qu'Amazon FSx sous Linux.

   ```
   $ sudo yum install cifs-utils
   ```

4. Créez le répertoire des points de montage**`/mnt/fsx`**. C'est ici que vous allez monter le système de fichiers Amazon FSx.

   ```
   $ sudo mkdir -p /mnt/fsx
   ```

5. Authentifiez-vous auprès de Kerberos à l'aide de la commande suivante.

   ```
   $ kinit
   ```

6. Montez le partage de fichiers à l'aide de la commande suivante.

   ```
   $ sudo mount -t cifs //file_system_dns_name/file_share mount_point --verbose -o
    vers=SMB_version,sec=krb5,cruid=ad_user,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=no
   file-server-Ip
   ```

   Vous pouvez trouver le nom DNS sur la console Amazon FSx en choisissant Windows File Server, Network & security. Vous pouvez également les trouver dans la réponse `CreateFileSystem` ou dans l'opération de `DescribeFileSystems` l'API.

   - Pour un système de fichiers mono-AZ joint à un Microsoft Active Directory AWS géré, le nom DNS est le suivant.

     ```
     fs-0123456789abcdef0.ad-domain.com
     ```

   - Pour un système de fichiers mono-AZ joint à un Active Directory autogéré, et pour tout système de fichiers multi-AZ, le nom DNS est le suivant.

```
amznfsxaa11bb22.ad-domain.com
```

Remplacez *CIFSMaxBufSize* par la plus grande valeur autorisée par votre noyau. Exécutez la commande suivante pour obtenir cette valeur.

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

La sortie indique que la taille maximale de la mémoire tampon est de 130048.

7. Vérifiez que le système de fichiers est monté en exécutant la commande suivante, qui renvoie uniquement les systèmes de fichiers du type CIFS (Common Internet File System).

```
$ mount -l -t cifs
//fs-0123456789abcdef0/share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=krb5,cache=cache_mode,username=user1@CORP.NETWORK.COM,ui
```

La commande mount utilisée dans cette procédure effectue les opérations suivantes aux points indiqués :

- *//file_system_dns_name/file_share*— Spécifie le nom DNS et le partage du système de fichiers à monter.
- *mount_point* — Le répertoire de l'instance EC2 sur lequel vous montez le système de fichiers.
- `-t cifs vers=`*SMB_version*— Spécifie le type de système de fichiers CIFS et la version du protocole SMB. Amazon FSx for Windows File Server prend en charge les versions SMB 2.0 à 3.1.1.
- `sec=krb5`— Spécifie d'utiliser la version 5 de Kerberos pour l'authentification.
- `cache=`*cache_mode*— Définit le mode de cache. Cette option pour le cache CIFS peut avoir un impact sur les performances, et vous devez tester les paramètres qui fonctionnent le mieux (et consulter la documentation Linux) pour votre noyau et votre charge de travail. Les options `strict` 1 et `none` 2 sont recommandées, car elles `loose` peuvent entraîner des incohérences dans les données en raison de la sémantique plus souple du protocole.
- `cruid=`*ad_user*— Définit l'UID du propriétaire du cache d'informations d'identification pour l'administrateur de l'annuaire AD.

- */mnt/fsx*— Spécifie le point de montage pour le partage de fichiers Amazon FSx sur votre instance EC2.
- `rsize=`*CIFSMaxBufSize*`,wsize=`*CIFSMaxBufSize*— Spécifie la taille maximale de la mémoire tampon de lecture et d'écriture autorisée par le protocole CIFS. Remplacez *CIFSMaxBufSize* par la plus grande valeur autorisée par votre noyau. Déterminez le `CIFSMaxBufSize` en exécutant la commande suivante.

  ```
  $ modinfo cifs | grep CIFSMaxBufSize
  parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
   16384 Range: 8192 to 130048 (uint)
  ```

  La sortie indique que la taille maximale de la mémoire tampon est de 130048.
- `ip=`*preferred-file-server-Ip*— Définit l'adresse IP de destination sur celle du serveur de fichiers préféré du système de fichiers.

  Vous pouvez récupérer l'adresse IP du serveur de fichiers préféré du système de fichiers comme suit :
  - À l'aide de la console Amazon FSx, sur l'onglet Réseau et sécurité de la page de détails du système de fichiers.
  - En réponse à la commande `describe-file-systems` CLI ou à la commande équivalente de l'API DescribeFileSystems.

Pour monter un partage de fichiers sur une instance Linux Amazon EC2 non connectée à votre Active Directory

La procédure suivante monte un partage de fichiers Amazon FSx sur une instance Linux Amazon EC2 qui n'est pas jointe à votre Active Directory (AD). Pour une instance Linux EC2 qui n'est pas jointe à votre AD, vous pouvez uniquement monter un partage de fichiers FSx for Windows File Server à l'aide de son adresse IP privée. Vous pouvez obtenir l'adresse IP privée du système de fichiers à l'aide de la console Amazon FSx, dans l'onglet Réseau et sécurité, dans Adresse IP du serveur de fichiers préféré.

Cet exemple utilise l'authentification NTLM. Pour ce faire, vous montez le système de fichiers en tant qu'utilisateur membre du domaine Microsoft Active Directory auquel le système de fichiers FSx for Windows File Server est joint. Les informations d'identification du compte utilisateur sont fournies dans un fichier texte que vous créez sur votre instance EC2. `creds.txt` Ce fichier contient le nom d'utilisateur, le mot de passe et le domaine de l'utilisateur.

```
$ cat creds.txt
username=user1
password=Password123
domain=EXAMPLE.COM
```

Pour lancer et configurer l'instance Amazon Linux EC2

1. Lancez une instance Amazon Linux EC2 à l'aide de la console Amazon EC2. Pour plus d'informations, consultez Lancer une instance dans le guide de l'utilisateur Amazon EC2.
2. Connectez-vous à votre instance Amazon Linux EC2. Pour plus d'informations, consultez Connect to your Linux instance dans le guide de l'utilisateur Amazon EC2.
3. Pour installer le package `cifs-utils`, exécutez la commande suivante : Ce package est utilisé pour monter des systèmes de fichiers réseau tels qu'Amazon FSx sous Linux.

   ```
   $ sudo yum install cifs-utils
   ```
4. Créez le point de montage **`/mnt/fsxx`** où vous prévoyez de monter le système de fichiers Amazon FSx.

   ```
   $ sudo mkdir -p /mnt/fsx
   ```
5. Créez le fichier `creds.txt` d'informations d'identification dans le `/home/ec2-user` répertoire, en utilisant le format indiqué précédemment.
6. Définissez les autorisations du `creds.txt` fichier afin que vous seul (le propriétaire) puissiez lire et écrire dans le fichier en exécutant la commande suivante.

   ```
   $ chmod 700 creds.txt
   ```

Pour monter le système de fichiers.

1. Vous montez un partage de fichiers non joint à votre Active Directory à l'aide de son adresse IP privée. Vous pouvez obtenir l'adresse IP privée du système de fichiers à l'aide de la console Amazon FSx, dans l'onglet Réseau et sécurité, dans l'adresse IP du serveur de fichiers préféré.
2. Montez le système de fichiers à l'aide de la commande suivante :

```
$ sudo mount -t cifs //file-system-IP-address/file_share /mnt/fsx
 --verbose -o vers=SMB_version,sec=ntlmsspi,cred=/home/ec2-user/
creds.txt,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=none
```

Remplacez *CIFSMaxBufSize* par la plus grande valeur autorisée par votre noyau. Exécutez la commande suivante pour obtenir cette valeur.

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

La sortie indique que la taille maximale de la mémoire tampon est de 130048.

3. Vérifiez que le système de fichiers est monté en exécutant la commande suivante, qui renvoie uniquement les systèmes de fichiers CIFS.

```
$ mount -l -t cifs
//file-system-IP-address/file_share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=ntlmsspi,cache=cache_mode,username=user1,domain=CORP.EXA
```

La commande mount utilisée dans cette procédure effectue les opérations suivantes aux points indiqués :

- *//file-system-IP-address/file_share*— Spécifie l'adresse IP et le partage du système de fichiers que vous montez.
- `-t cifs vers=`*SMB_version*— Spécifie le type de système de fichiers CIFS et la version du protocole SMB. Amazon FSx for Windows File Server prend en charge les versions SMB 2.0 à 3.1.1.
- `sec=ntlmsspi`— Spécifie l'utilisation de l'interface NTLMSSPI (NT LAN Manager Security Support Provider Interface) pour l'authentification.
- `cache=`*cache_mode*— Définit le mode de cache. Cette option pour le cache CIFS peut avoir un impact sur les performances, et vous devez tester les paramètres qui fonctionnent le mieux (et consulter la documentation Linux) pour votre noyau et votre charge de travail. Les options `strict` 1 et `none` 2 sont recommandées, car elles `loose` peuvent entraîner des incohérences dans les données en raison de la sémantique plus souple du protocole.

- `cred=/home/ec2-user/creds.txt`— Spécifie où obtenir les informations d'identification de l'utilisateur.
- *`/mnt/fsx`*— Spécifie le point de montage pour le partage de fichiers Amazon FSx sur votre instance EC2.
- `rsize=`*`CIFSMaxBufSize`*`,wsize=`*`CIFSMaxBufSize`*— Spécifie la taille maximale de la mémoire tampon de lecture et d'écriture autorisée par le protocole CIFS. Remplacez *`CIFSMaxBufSize`* par la plus grande valeur autorisée par votre noyau. Déterminez le `CIFSMaxBufSize` en exécutant la commande suivante.

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

Montage automatique de partages de fichiers sur une instance Amazon Linux EC2 non jointe à votre Active Directory

Vous pouvez monter automatiquement votre partage de fichiers FSx for Windows File Server chaque fois que l'instance Linux Amazon EC2 sur laquelle il est monté redémarre. Pour ce faire, ajoutez une entrée au `/etc/fstab` fichier sur l'instance EC2. Le fichier `/etc/fstab` contient des informations sur les systèmes de fichiers. La commandemount -a, qui s'exécute au démarrage de l'instance, monte les systèmes de fichiers répertoriés dans le `/etc/fstab` fichier.

Pour une instance Linux Amazon EC2 qui n'est pas jointe à votre Active Directory, vous pouvez uniquement monter un partage de fichiers FSx for Windows File Server à l'aide de son adresse IP privée. Vous pouvez obtenir l'adresse IP privée du système de fichiers à l'aide de la console Amazon FSx, dans l'onglet Réseau et sécurité, dans Adresse IP du serveur de fichiers préféré.

La procédure suivante utilise l'authentification Microsoft NTLM. Vous montez le système de fichiers en tant qu'utilisateur membre du domaine Microsoft Active Directory auquel le système de fichiers FSx for Windows File Server est joint. Les informations d'identification du compte utilisateur sont fournies dans le fichier text`creds.txt`. Ce fichier contient le nom d'utilisateur, le mot de passe et le domaine de l'utilisateur.

```
$ cat creds.txt
username=user1
```

```
password=Password123
domain=EXAMPLE.COM
```

Pour monter automatiquement un partage de fichiers sur une instance Amazon Linux EC2 non jointe à votre Active Directory

Pour lancer et configurer l'instance Amazon Linux EC2

1. Lancez une instance Amazon Linux EC2 à l'aide de la console Amazon EC2. Pour plus d'informations, consultez Lancer une instance dans le guide de l'utilisateur Amazon EC2.
2. Connectez-vous à votre instance. Pour plus d'informations, consultez Connect to your Linux instance dans le guide de l'utilisateur Amazon EC2.
3. Pour installer le package `cifs-utils`, exécutez la commande suivante : Ce package est utilisé pour monter des systèmes de fichiers réseau tels qu'Amazon FSx sous Linux.

   ```
   $ sudo yum install cifs-utils
   ```
4. Créez le répertoire `/mnt/fsx`. C'est ici que vous allez monter le système de fichiers Amazon FSx.

   ```
   $ sudo mkdir /mnt/fsx
   ```
5. Créez le fichier `creds.txt` d'informations d'identification dans le `/home/ec2-user` répertoire.
6. Définissez les autorisations du fichier afin que vous seul (le propriétaire) puissiez lire le fichier en exécutant la commande suivante.

   ```
   $ sudo chmod 700 creds.txt
   ```

Pour monter automatiquement le système de fichiers

1. Vous montez automatiquement un partage de fichiers non joint à votre Active Directory en utilisant son adresse IP privée. Vous pouvez obtenir l'adresse IP privée du système de fichiers à l'aide de la console Amazon FSx, dans l'onglet Réseau et sécurité, dans Adresse IP du serveur de fichiers préféré.
2. Pour monter automatiquement le partage de fichiers à l'aide de son adresse IP privée, ajoutez la ligne suivante au `/etc/fstab` fichier.

```
//file-system-IP-address/file_share /mnt/fsx cifs
 vers=SMB_version,sec=ntlmsspi,cred=/home/ec2-user/
creds.txt,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=none
```

Remplacez *CIFSMaxBufSize* par la plus grande valeur autorisée par votre noyau. Exécutez la commande suivante pour obtenir cette valeur.

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

La sortie indique que la taille maximale de la mémoire tampon est de 130048.

3. Testez l'`fstab`entrée en utilisant la `mount` commande avec l'option « fake » en conjonction avec les options « all » et « verbose ».

```
$ sudo mount -fav
home/ec2-user/fsx      : successfully mounted
```

4. Pour monter le partage de fichiers, redémarrez l'instance Amazon EC2.
5. Lorsque l'instance est de nouveau disponible, vérifiez que le système de fichiers est monté en exécutant la commande suivante.

```
$ sudo mount -l -t cifs
//file-system-IP-address/file_share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=ntlmsspi,cache=cache_code,username=user1,domain=CORP.EXA
```

La ligne ajoutée au `/etc/fstab` fichier dans cette procédure effectue les opérations suivantes aux points indiqués :

- *//file-system-IP-address/file_share*— Spécifie l'adresse IP et le partage du système de fichiers Amazon FSx que vous montez.
- `/mnt/fsx`— Spécifie le point de montage du système de fichiers Amazon FSx sur votre instance EC2.
- `cifs vers=`*SMB_version*— Spécifie le type de système de fichiers CIFS et la version du protocole SMB. Amazon FSx for Windows File Server prend en charge les versions SMB 2.0 à 3.1.1.

- `sec=ntlmsspi`— Spécifie l'utilisation de l'interface du fournisseur de support de sécurité de NT LAN Manager pour faciliter l'authentification par défi et réponse NTLM.
- `cache=`*`cache_mode`*— Définit le mode de cache. Cette option pour le cache CIFS peut avoir un impact sur les performances, et vous devez tester les paramètres qui fonctionnent le mieux (et consulter la documentation Linux) pour votre noyau et votre charge de travail. Les options `strict` 1 et `none` 2 sont recommandées, car elles `loose` peuvent entraîner des incohérences dans les données en raison de la sémantique plus souple du protocole.
- `cred=/home/ec2-user/creds.txt`— Spécifie où obtenir les informations d'identification de l'utilisateur.
- `_netdev`— Indique au système d'exploitation que le système de fichiers réside sur un appareil nécessitant un accès au réseau. L'utilisation de cette option empêche l'instance de monter le système de fichiers tant que le service réseau n'est pas activé sur le client.
- `0`— Indique que le système de fichiers doit être sauvegardé pardump, s'il s'agit d'une valeur différente de zéro. Pour Amazon FSx, cette valeur doit être. `0`
- `0`— Spécifie l'ordre dans lequel `fsck` les systèmes de fichiers sont vérifiés au démarrage. Pour les systèmes de fichiers Amazon FSx, cette valeur doit indiquer qu'ils ne `0` doivent pas `fsck` être exécutés au démarrage.

Migration du stockage de fichiers existant vers Amazon FSx

FSx for Windows File Server possède les fonctionnalités, les performances et la compatibilité nécessaires pour vous aider à transférer et à transférer facilement des applications d'entreprise vers le cloud Amazon Web Services. Le processus de migration vers FSx for Windows File Server implique les étapes suivantes :

1. Migrez vos fichiers vers FSx for Windows File Server. Pour plus d'informations, consultez Migration du stockage de fichiers existant vers FSx for Windows File Server.
2. Migrez votre configuration de partage de fichiers vers FSx for Windows File Server. Pour plus d'informations, consultez Migration des configurations de partage de fichiers vers Amazon FSx.
3. Associez votre nom DNS existant en tant qu'alias DNS pour votre système de fichiers Amazon FSx. Pour plus d'informations, consultez Associer un alias DNS à Amazon FSx.
4. Passez à FSx for Windows File Server. Pour plus d'informations, consultez Passage à Amazon FSx.

Vous trouverez les détails de chaque étape du processus dans les sections suivantes.

Rubriques

Migration du stockage de fichiers existant vers FSx for Windows File Server

Pour migrer vos fichiers existants vers les systèmes de fichiers FSx for Windows File Server, nous vous recommandons d' AWS DataSync utiliser un service de transfert de données en ligne conçu pour simplifier, automatiser et accélérer la copie de grandes quantités de données vers et AWS depuis les services de stockage. DataSync copie des données sur Internet ou AWS Direct Connect. En tant que service entièrement géré, il DataSync n'est plus nécessaire de modifier des applications, de développer des scripts ou de gérer l'infrastructure. Pour plus d'informations, consultez Migration de fichiers existants vers FSx for Windows File Server à l'aide de AWS DataSync.

Comme solution alternative, vous pouvez utiliser Robust File Copy, ou Robocopy, qui est un répertoire de ligne de commande et un ensemble de commandes de réplication de fichiers pour Microsoft Windows. Pour des procédures détaillées sur l'utilisation de Robocopy pour migrer le stockage de fichiers vers FSx for Windows File Server, consultez. Migration de fichiers existants vers FSx for Windows File Server à l'aide de Robocopy

Bonnes pratiques pour la migration du stockage de fichiers existant vers FSx for Windows File Server

Pour migrer de grandes quantités de données vers FSx for Windows File Server le plus rapidement possible, utilisez les systèmes de fichiers Amazon FSx configurés avec un stockage sur disque SSD (Solid State Drive). Une fois la migration terminée, vous pouvez déplacer les données vers les systèmes de fichiers Amazon FSx en utilisant le stockage sur disque dur (HDD) si c'est la meilleure solution pour votre application.

Pour déplacer des données d'un système de fichiers Amazon FSx utilisant un stockage SDD vers un stockage sur disque dur, vous pouvez suivre les étapes suivantes. (Notez que les systèmes de fichiers HDD ont une capacité de stockage minimale de 2 To et que vous ne pouvez pas modifier la capacité de stockage lors d'une restauration à partir d'une sauvegarde.)

1. Effectuez une sauvegarde de votre système de fichiers SSD. Pour plus d’informations, consultez Création de sauvegardes initiées par l'utilisateur.
2. Restaurez la sauvegarde sur un système de fichiers à l'aide du stockage sur disque dur. Pour plus d’informations, consultez Restauration des sauvegardes.

Migration de fichiers existants vers FSx for Windows File Server à l'aide de AWS DataSync

Nous vous recommandons AWS DataSync de l'utiliser pour transférer des données entre les systèmes de fichiers FSx for Windows File Server. 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 sur site et d'autres 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.

DataSync prend en charge la copie des listes de contrôle d'accès (ACL) NTFS et prend également en charge la copie des informations de contrôle d'audit des fichiers, également appelées listes de

contrôle d'accès au système NTFS (SACL), qui sont utilisées par les administrateurs pour contrôler la journalisation des audits des tentatives d'accès aux fichiers par les utilisateurs.

Vous pouvez l'utiliser DataSync pour transférer des fichiers entre deux systèmes de fichiers FSx for Windows File Server, ainsi que pour déplacer des données vers un système de fichiers appartenant à un Région AWS autre compte AWS OR. Vous pouvez l'utiliser DataSync avec les systèmes de fichiers FSx for Windows File Server 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 AWS DataSync, un emplacement pour FSx for Windows File Server est un point de terminaison pour un serveur de fichiers FSx for Windows. Vous pouvez transférer des fichiers entre un emplacement pour FSx for Windows File Server et un emplacement pour d'autres systèmes de fichiers. Pour plus d'informations, consultez la section Utilisation des emplacements dans le guide de AWS DataSync l'utilisateur.

DataSync accède à votre serveur de fichiers FSx for Windows à l'aide du protocole SMB (Server Message Block). Il s'authentifie avec le nom d'utilisateur et le mot de passe que vous configurez dans la AWS DataSync console ou AWS CLI.

Prérequis

Pour migrer des données vers votre configuration de serveur de fichiers Amazon FSx for Windows, vous avez besoin d'un serveur et d'un réseau répondant DataSync aux exigences. Pour en savoir plus, consultez la section Exigences DataSync du guide de AWS DataSync l'utilisateur.

Si vous effectuez une migration de données volumineuse ou une migration impliquant de nombreux petits fichiers, nous vous recommandons d'utiliser un système de fichiers Amazon FSx avec un type de stockage SSD. Cela est dû au fait que DataSync les tâches impliquent des analyses des métadonnées des fichiers, ce qui peut épuiser les limites d'IOPS du disque dur, ce qui entraîne des migrations de longue durée et un impact sur les performances du système de fichiers. Pour plus d'informations, consultez Bonnes pratiques pour la migration du stockage de fichiers existant vers FSx for Windows File Server.

Si votre ensemble de données se compose principalement de petits fichiers, que le nombre de fichiers se chiffre en millions ou si vous disposez d'une bande passante réseau supérieure à celle que vous consommez pour une seule DataSync tâche, vous pouvez également accélérer vos transferts de données grâce à une architecture évolutive. Pour plus d'informations, voir : Comment accélérer vos transferts de données grâce AWS DataSync à des architectures évolutives.

Vous pouvez surveiller l'utilisation des E/S de disque de votre système de fichiers à l'aide des indicateurs de performance FSx.

Étapes de base pour la migration de fichiers à l'aide de DataSync

Pour transférer des fichiers d'un emplacement source vers un emplacement de destination à l'aide de DataSync, suivez les étapes de base suivantes :

- Téléchargez et déployez un agent dans votre environnement et activez-le.
- Créez et configurez un emplacement source et de destination.
- Créez et configurez une tâche.
- Exécutez la tâche pour transférer les fichiers depuis la source vers la destination.

Pour savoir comment transférer des fichiers d'un système de fichiers sur site existant vers votre serveur de fichiers FSx for Windows, consultez les sections Transfert de données entre un stockage autogéré AWS et, Création d'un emplacement pour SMB, et Création d'un emplacement pour Amazon FSx for Windows File Server dans le guide de l'utilisateur.AWS DataSync

Pour savoir comment transférer des fichiers d'un système de fichiers existant dans le cloud vers votre serveur de fichiers FSx for Windows, consultez la section Déployer votre agent en tant qu'instance Amazon EC2 dans le guide de l'utilisateur.AWS DataSync

Migration entre deux systèmes de fichiers Amazon FSx

Vous pouvez l'utiliser DataSync pour migrer des données entre deux systèmes de fichiers Amazon FSx. Cela peut être utile si vous devez déplacer votre charge de travail d'un système de fichiers existant vers un nouveau système de fichiers avec une configuration différente, par exemple d'une configuration mono-AZ à une configuration multi-AZ. Vous pouvez également l'utiliser DataSync pour répartir votre charge de travail entre deux systèmes de fichiers.

Voici un exemple d'aperçu du processus de migration :

1. Créez DataSync des emplacements pour les systèmes de fichiers source et de destination. Notez que la source et la destination doivent appartenir au même domaine Active Directory (AD) ou avoir une relation d'approbation AD entre leurs domaines.
2. Créez et configurez une DataSync tâche pour transférer les données de la source vers la destination. Vous pouvez exécuter la tâche en tant qu'instance unique ou la configurer pour qu'elle s'exécute automatiquement selon un calendrier que vous configurez.

3. Une fois la tâche terminée avec succès, les données de votre système de fichiers de destination sont une copie exacte de votre source. Notez que vous devrez suspendre temporairement toute activité d'écriture ou toute mise à jour de fichiers sur votre système de fichiers source pour terminer la tâche. Vous pouvez ensuite accéder à votre système de fichiers de destination et supprimer le système de fichiers source.

Avant de procéder à la migration depuis votre système de fichiers de production, vous pouvez tester le processus de migration sur un système de fichiers restauré à partir d'une sauvegarde récente. Cela vous permet d'estimer la durée du processus de transfert de données et de résoudre les DataSync erreurs à l'avance.

Pour réduire le temps de transition, vous pouvez exécuter des DataSync tâches à l'avance, en déplaçant la majorité de vos données de votre système de fichiers source vers votre système de fichiers de destination. Après avoir arrêté le trafic vers votre système de fichiers source, vous pouvez exécuter un dernier transfert de tâches pour synchroniser les données récemment mises à jour depuis l'arrêt du trafic, puis passer à votre système de fichiers de destination.

Vous pouvez configurer DataSync les tâches pour qu'elles s'exécutent uniquement dans certains répertoires, ou pour inclure ou exclure certains chemins. Cela peut être utile si vous exécutez plusieurs tâches en parallèle ou si vous souhaitez migrer un sous-ensemble de vos données.

Vous pouvez créer un alias DNS sur votre système de fichiers de destination identique au nom DNS de votre système de fichiers source. Cela permet à vos utilisateurs finaux et à vos applications de continuer à accéder aux données des fichiers en utilisant le nom DNS de votre système de fichiers source. Pour plus d'informations sur la configuration d'un alias DNS, voir :Procédure pas à pas 5 : Utilisation d'alias DNS pour accéder à votre système de fichiers.

Lorsque vous effectuez ce type de migration, nous vous recommandons ce qui suit :

- Planifiez votre migration pour éviter les sauvegardes du système de fichiers, votre fenêtre de maintenance hebdomadaire et les `Data Deduplication` tâches. Plus précisément, nous vous recommandons de désactiver la `Data Deduplication GarbageCollection` tâche si elle coïncide avec votre migration planifiée.
- Utilisez un type de stockage SSD pour vos systèmes de fichiers source et de destination. Vous pouvez passer d'un type de stockage sur disque dur à un type de stockage SSD en effectuant une restauration à partir d'une sauvegarde. Pour plus d'informations, voir :Migration du stockage de fichiers existant vers FSx for Windows File Server.

- Configurez vos systèmes de fichiers source et de destination avec une capacité de débit suffisante pour le volume de données que vous devez transférer. Au cours des processus de DataSync tâches, surveillez l'utilisation des performances des systèmes de fichiers source et de destination. Pour plus d'informations, consultez Surveillance des métriques avec Amazon CloudWatch.
- Configurez le DataSync suivi pour vous aider à comprendre l'avancement des tâches en cours. Vous pouvez également envoyer DataSync des journaux au groupe Amazon CloudWatch Logs pour vous aider à déboguer vos tâches en cas d'erreur.

Migration de fichiers existants vers FSx for Windows File Server à l'aide de Robocopy

Basé sur Microsoft Windows Server, Amazon FSx for Windows File Server vous permet de migrer entièrement vos ensembles de données existants vers vos systèmes de fichiers Amazon FSx. Vous pouvez migrer les données de chaque fichier. Vous pouvez également migrer toutes les métadonnées pertinentes des fichiers, notamment les attributs, les horodatages, les listes de contrôle d'accès (ACL), les informations sur le propriétaire et les informations d'audit. Grâce à cette prise en charge totale de la migration, Amazon FSx permet de déplacer vos charges de travail et applications Windows basées sur ces ensembles de données de fichiers vers le cloud Amazon Web Services.

Utilisez les rubriques suivantes pour vous guider dans le processus de copie de données de fichiers existants. Lorsque vous effectuez cette copie, vous conservez toutes les métadonnées des fichiers provenant de vos centres de données locaux ou de vos serveurs de fichiers autogérés sur Amazon EC2.

Prérequis

Avant de commencer, assurez-vous d'effectuer les opérations suivantes :

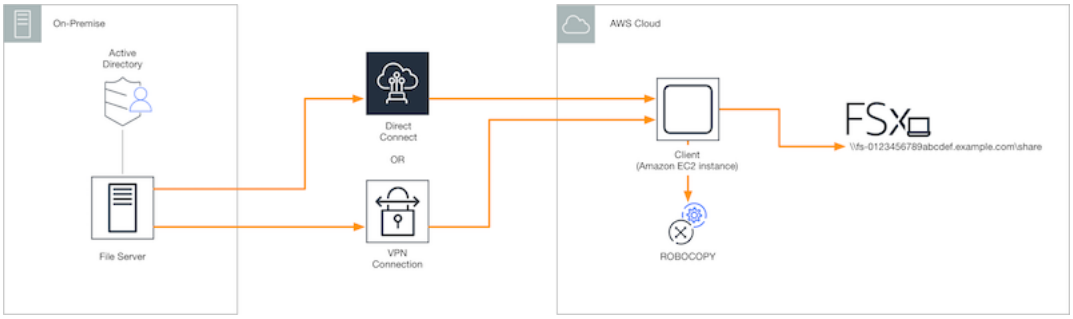
- Établissez une connectivité réseau (à l'aide AWS Direct Connect d'un VPN) entre votre Active Directory local et le VPC sur lequel vous souhaitez créer le système de fichiers Amazon FSx.
- Créez un compte de service sur votre Active Directory avec des autorisations déléguées pour associer des ordinateurs au domaine. Pour plus d'informations, voir Déléguer des privilèges à votre compte de service dans le Guide d'AWS Directory Service administration.
- Créez un système de fichiers Amazon FSx, joint à votre répertoire Microsoft AD autogéré (sur site).
- Notez l'emplacement (par exemple`\\Source\Share`) du partage de fichiers (sur site ou dans AWS) qui contient les fichiers existants que vous souhaitez transférer vers Amazon FSx.

- Notez l'emplacement (par exemple`\\Target\Share`) du partage de fichiers sur votre système de fichiers Amazon FSx vers lequel vous souhaitez transférer vos fichiers existants.

Le tableau suivant récapitule les exigences d'accessibilité des systèmes de fichiers source et de destination pour trois modèles d'accès utilisateur de migration.

Modèle d'accès utilisateur de migration	Exigences relatives à l'accessibilité du système de fichiers source	Exigences d'accessibilité du serveur de fichiers FSx de destination
Modèle d'autorisations de lecture/écriture directes	L'utilisateur doit au moins disposer d'autorisations de lecture (ACL NTFS) sur les fichiers et dossiers en cours de migration.	L'utilisateur doit au moins disposer d'autorisations d'écriture (ACL NTFS) sur les fichiers et dossiers à migrer.
Modèle de privilèges de sauvegarde/restauration pour annuler les autorisations d'accès	L'utilisateur doit être membre du groupe Backup Operators d'Active Directory local et utiliser l'indicateur /b avec. RoboCopy	L'utilisateur doit être membre du groupe d'administrateurs du système de fichiers Amazon FSx* et utiliser l'indicateur /b avec. RoboCopy
Modèle de privilèges d'administrateur de domaine (complet) pour annuler les autorisations d'accès	L'utilisateur doit être membre du groupe d'administrateurs de domaine d'Active Directory sur site.	L'utilisateur doit être membre du groupe d'administrateurs du système de fichiers Amazon FSx* et utiliser l'indicateur /b avec RoboCopy

> **Note**
>
> * Pour les systèmes de fichiers associés à un Microsoft AD AWS géré, le groupe d'administrateurs du système de fichiers Amazon FSx est Delegated AWS FSx Administrators. Dans votre Microsoft AD autogéré, le groupe d'administrateurs du système de fichiers Amazon FSx est le groupe des administrateurs de domaine ou le groupe personnalisé que vous avez spécifié pour l'administration lors de la création de votre système de fichiers.



Comment migrer des fichiers existants vers Amazon FSx à l'aide de Robocopy

Vous pouvez migrer des fichiers existants vers Amazon FSx en suivant la procédure suivante.

Pour migrer des fichiers existants vers Amazon FSx

1. Lancez une instance Amazon EC2 Windows Server 2016 dans le même Amazon VPC que celui de votre système de fichiers Amazon FSx.
2. Connectez-vous à votre instance EC2 Amazon. Pour plus d'informations, consultez Connexion à votre instance Windows à l'aide de RDP dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.
3. Ouvrez l'invite de commande et mappez le partage de fichiers source sur votre serveur de fichiers existant (sur site ou AWS interne) à une lettre de lecteur (par exemple, *Y*:) comme suit. Dans ce cadre, vous fournissez les informations d'identification d'un membre du groupe d'administrateurs de domaine Active Directory local.

   ```
   C:\>net use Y: \\fileserver1.mydata.com\localdata /user:mydata.com\Administrator
   Enter the password for 'fileserver1.mydata.com': _

   Drive Y: is now connected to \\fileserver1.mydata.com\localdata.

   The command completed successfully.
   ```

4. Mappez le partage de fichiers cible sur votre système de fichiers Amazon FSx à une autre lettre de lecteur (par exemple, *Z*) sur votre instance Amazon EC2 comme suit. Dans ce cadre, vous fournissez les informations d'identification d'un compte utilisateur membre du groupe d'administrateurs de domaine de votre Active Directory local et du groupe d'administrateurs de votre système de fichiers Amazon FSx. Pour les systèmes de fichiers joints à un Microsoft AD AWS géré, ce groupe est **`AWS Delegated FSx Administrators`**. Dans votre Microsoft AD autogéré, il s'agit du groupe **`Domain Admins`** ou du groupe personnalisé que vous avez spécifié pour l'administration lors de la création de votre système de fichiers.

Pour plus d'informations, consultez le tableau des exigences d'accessibilité des systèmes de fichiers source et de destination dans lePrérequis.

```
C:\>net use Z: \\amznfsxabcdef1.mydata.com\share /user:mydata.com\Administrator
Enter the password for 'amznfsxabcdef1.mydata.com': _

Drive Z: is now connected to \\amznfsxabcdef1.mydata.com\share.

The command completed successfully.
```

5. Choisissez Exécuter en tant qu'administrateur dans le menu contextuel. Ouvrez Command Prompt ou Windows PowerShell en tant qu'administrateur, puis exécutez la commande Robocopy suivante pour copier les fichiers du partage source vers le partage cible.

   La ROBOCOPY commande est un utilitaire de transfert de fichiers flexible doté de plusieurs options pour contrôler le processus de transfert de données. Grâce à ce processus de ROBOCOPY commande, tous les fichiers et répertoires du partage source sont copiés vers le partage cible Amazon FSx. La copie préserve les ACL NTFS des fichiers et des dossiers, les attributs, les horodatages, les informations sur le propriétaire et les informations d'audit.

   ```
   robocopy Y:\ Z:\ /copy:DATSOU /secfix /e /b /MT:8
   ```

   L'exemple de commande précédent utilise les éléments et options suivants :

   - Y — Fait référence au partage source situé dans la forêt Active Directory locale mydata.com.
   - Z — Fait référence au partage cible \ \ amznfsxabcdef1.mydata.com \ share sur Amazon FSx.
   - /copy — Spécifie les propriétés de fichier suivantes à copier :
     - D — données
     - A — attributs
     - T — horodatages
     - S — ACL NTFS
     - O — informations sur le propriétaire
     - U — informations d'audit.
   - /secfix — Corrige la sécurité des fichiers sur tous les fichiers, même ceux qui ont été ignorés.
   - /e — Copie les sous-répertoires, y compris les sous-répertoires vides.

- /b — Utilise le privilège de sauvegarde et de restauration de Windows pour copier des fichiers même si leurs ACL NTFS refusent les autorisations à l'utilisateur actuel.
- /MT:8 — Spécifie le nombre de threads à utiliser pour effectuer des copies multithread.

> **Note**
>
> Si vous copiez des fichiers volumineux via une connexion lente ou peu fiable, vous pouvez activer le mode redémarrable en utilisant l'/zboption robocopy à la place de l'/boption. En mode redémarrable, si le transfert d'un fichier volumineux est interrompu, une opération Robocopy ultérieure peut reprendre au milieu du transfert au lieu d'avoir à recopier le fichier entier depuis le début. L'activation du mode redémarrable peut réduire la vitesse de transfert des données.

Migration des configurations de partage de fichiers vers Amazon FSx

Vous pouvez migrer une configuration de partage de fichiers existante vers Amazon FSx en suivant la procédure suivante. Dans cette procédure, le serveur de fichiers source est le serveur de fichiers dont vous souhaitez migrer la configuration de partage de fichiers vers Amazon FSx.

> **Note**
>
> Migrez d'abord vos fichiers vers Amazon FSx avant de migrer votre configuration de partage de fichiers. Pour plus d’informations, consultez Migration du stockage de fichiers existant vers FSx for Windows File Server.

Pour migrer des partages de fichiers existants vers FSx for Windows File Server

1. Sur le serveur de fichiers source, choisissez Exécuter en tant qu'administrateur dans le menu contextuel. Ouvrez Windows PowerShell en tant qu'administrateur.
2. Exportez les partages de fichiers du serveur de fichiers source vers un fichier nommé `SmbShares.xml` en exécutant les commandes suivantes dans le PowerShell. Dans cet exemple, remplacez F : par la lettre du lecteur de votre serveur de fichiers à partir duquel vous exportez les partages de fichiers.

```
$shareFolder = Get-SmbShare -Special $false | ? { $_.Path -like “F:\*” }
$shareFolder | Export-Clixml -Path F:\SmbShares.xml
```

3. Modifiez le `SmbShares.xml` fichier en remplaçant toutes les références à F : (votre lettre de lecteur) par D:\share car les systèmes de fichiers Amazon FSx résident sur D:\share.
4. Importez la configuration de partage de fichiers existante dans FSx for Windows File Server. Sur un client ayant accès à votre système de fichiers Amazon FSx de destination et au serveur de fichiers source, copiez la configuration de partage de fichiers enregistrée. Importez-le ensuite dans une variable à l'aide de la commande suivante.

   ```
   $shares = Import-Clixml -Path F:\SmbShares.xml
   ```

5. Préparez l'objet d'identification requis pour créer les partages de fichiers sur votre serveur de fichiers FSx for Windows File Server à l'aide de l'une des options suivantes.

   Pour générer l'objet d'identification de manière interactive, utilisez la commande suivante.

   ```
   $credential = Get-Credential
   ```

   Pour générer l'objet d'identification à l'aide d'une AWS Secrets Manager ressource, utilisez la commande suivante.

   ```
   $credential = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
    $AdminSecret).SecretString
   $FSxAdminUserCredential = (New-Object PSCredential($credential.UserName,(ConvertTo-
   SecureString $credential.Password -AsPlainText -Force)))
   ```

6. Migrez la configuration du partage de fichiers vers votre serveur de fichiers Amazon FSx à l'aide du script suivant.

   ```
   $FSxAcceptedParameters = ("ContinuouslyAvailable", "Description",
    "ConcurrentUserLimit", "CATimeout", "FolderEnumerationMode", "CachingMode",
    "FullAccess", "ChangeAccess", "ReadAccess", "NoAccess", "SecurityDescriptor",
    "Path", "Name", "EncryptData")
   ForEach ($item in $shares) {
       $param = @{};
       Foreach ($property in $item.psObject.properties) {
           if ($property.Name -In $FSxAcceptedParameters) {
               $param[$property.Name] = $property.Value
   ```

```
        }
    }
    Invoke-Command -ConfigurationName FSxRemoteAdmin -ComputerName
 amznfsxxxxxxxxx.corp.com -ErrorVariable errmsg -ScriptBlock { New-FSxSmbShare -
Credential $Using:credential @Using:param }
}
```

Migration de la configuration DNS pour utiliser Amazon FSx

FSx for Windows File Server fournit un nom de système de noms de domaine (DNS) par défaut pour chaque système de fichiers que vous pouvez utiliser pour accéder aux données de votre système de fichiers. Vous pouvez également accéder à vos systèmes de fichiers en utilisant le nom DNS de votre choix en configurant le nom DNS alternatif en tant qu'alias DNS pour votre système de fichiers Amazon FSx.

Avec les alias DNS, vous pouvez continuer à utiliser vos noms DNS existants pour accéder aux données stockées sur Amazon FSx lors de la migration du stockage du système de fichiers sur site vers Amazon FSx. Cela permet d'éliminer le besoin de mettre à jour les outils ou les applications qui utilisent vos noms DNS lors de la migration vers Amazon FSx. Vous pouvez associer des alias DNS aux systèmes de fichiers FSx for Windows File Server existants, lorsque vous créez de nouveaux systèmes de fichiers ou lorsque vous créez un nouveau système de fichiers à partir d'une sauvegarde. Vous pouvez associer jusqu'à 50 alias DNS à un système de fichiers à la fois. Pour plus d’informations, consultez Gestion des alias DNS.

Un nom d'alias DNS doit répondre aux exigences suivantes :

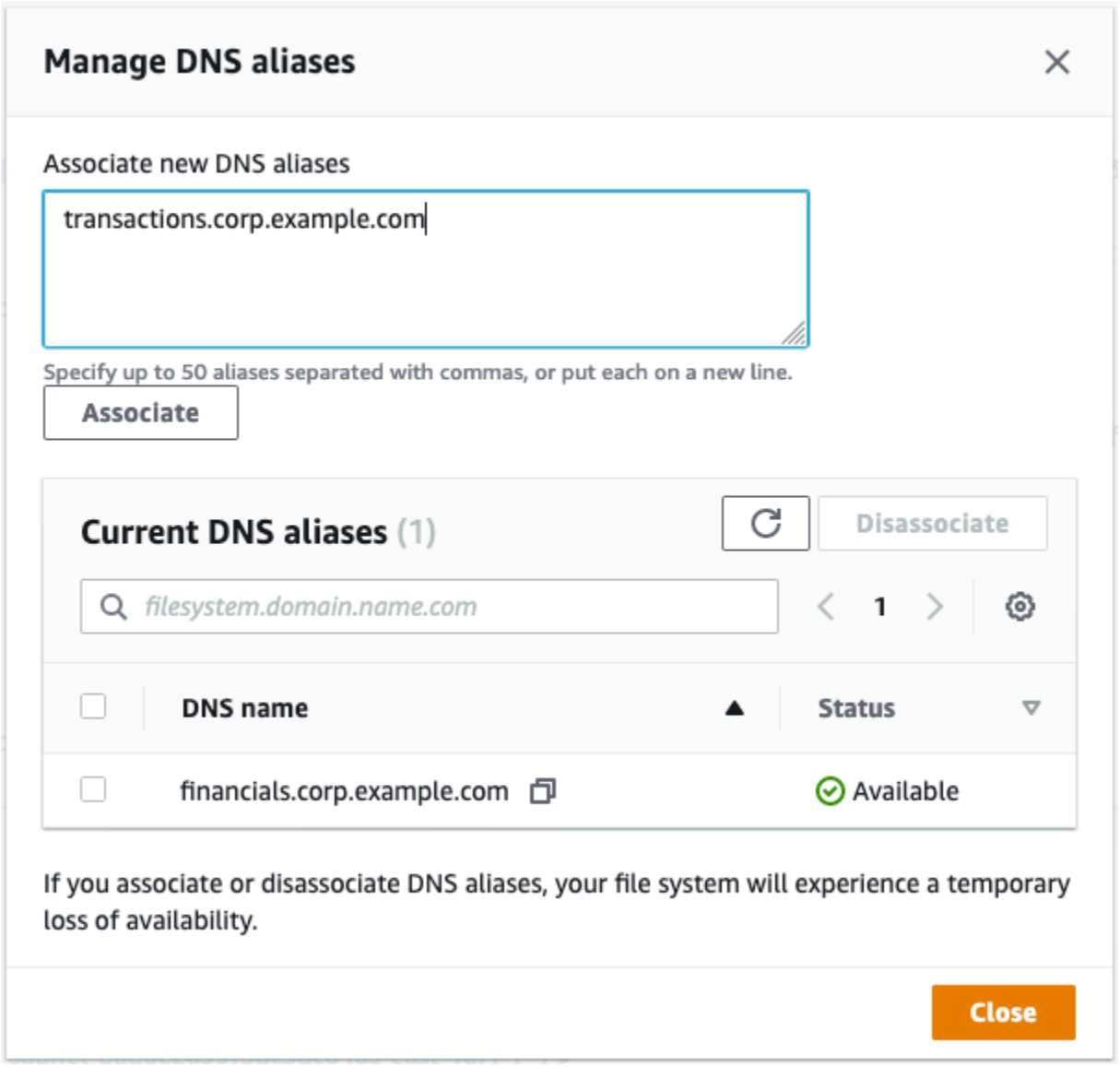
- Doit être formaté en tant que nom de domaine complet (FQDN), par exemple,. `accounting.example.com`
- Peut contenir des caractères alphanumériques et le trait d'union (-).
- Il ne peut pas commencer ni se terminer par un trait d'union.
- Il peut commencer par un caractère numérique.

Pour les noms d'alias DNS, Amazon FSx stocke les caractères alphabétiques sous forme de lettres minuscules (a-z), quelle que soit la manière dont vous les spécifiez : lettres majuscules, lettres minuscules ou lettres correspondantes sous forme de codes d'échappement.

Les procédures suivantes décrivent comment associer des alias DNS à vos systèmes de fichiers FSx for Windows File Server existants à l'aide de la console, de la CLI et de l'API Amazon FSx. Pour plus d'informations sur l'association d'alias DNS lors de la création de nouveaux systèmes de fichiers, y compris de nouveaux systèmes de fichiers issus d'une sauvegarde, consultezAssocier des alias DNS à des systèmes de fichiers.

Pour associer des alias DNS à un système de fichiers existant (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Accédez à Systèmes de fichiers, puis choisissez le système de fichiers Windows auquel vous souhaitez associer vos alias DNS.
3. Dans l'onglet Réseau et sécurité, choisissez Gérer les alias DNS pour ouvrir la boîte de dialogue Gérer les alias DNS.



4. Dans le champ Associer de nouveaux alias, entrez les alias DNS que vous souhaitez associer.
5. Choisissez Associer pour ajouter les alias au système de fichiers.

   Vous pouvez surveiller le statut des alias que vous venez d'associer dans la liste des alias actuels. Lorsque le statut indique Disponible, l'alias est associé au système de fichiers (un processus qui peut prendre jusqu'à 2,5 minutes).

Pour associer des alias DNS à un système de fichiers existant (CLI)

- Utilisez la commande `associate-file-system-aliases` CLI ou l'opération AssociateFileSystemAliasesAPI pour associer des alias DNS à un système de fichiers existant.

La requête CLI suivante associe deux alias au système de fichiers spécifié.

```
aws fsx associate-file-system-aliases \
    --file-system-id fs-0123456789abcdef0 \
    --aliases financials.corp.example.com transfers.corp.example.com
```

La réponse indique l'état des alias qu'Amazon FSx associe au système de fichiers.

```
{
      "Aliases": [
          {
              "Name": "financials.corp.example.com",
              "Lifecycle": CREATING
          },
          {
              "Name": "transfers.corp.example.com",
              "Lifecycle": CREATING
          }
      ]
  }
```

Pour surveiller l'état des alias que vous associez, utilisez la commande `describe-file-system-aliases` CLI (DescribeFileSystemAliasesopération d'API équivalente). Lorsqu'`Lifecycle`un alias a la valeur AVAILABLE, vous pouvez l'utiliser pour accéder au système de fichiers (un processus qui peut prendre jusqu'à 2,5 minutes).

Passage à Amazon FSx

Pour accéder à votre système de fichiers FSx for Windows File Server, vous devez effectuer les étapes suivantes :

- Préparez-vous à la découpe.
  - Déconnectez temporairement les clients SMB du système de fichiers d'origine.
  - Effectuez une synchronisation finale de la configuration des fichiers et du partage de fichiers.
- Configurez les noms principaux de service (SPN) pour votre système de fichiers Amazon FSx.

- Mettez à jour les enregistrements DNS CNAME pour qu'ils pointent vers votre système de fichiers Amazon FSx.

Les procédures permettant d'effectuer chacune de ces étapes sont décrites dans les sections suivantes.

Rubriques

Préparation du passage à Amazon FSx

Pour préparer le transfert vers votre système de fichiers Amazon FSx, vous devez effectuer les opérations suivantes :

- Déconnectez tous les clients qui écrivent dans le système de fichiers d'origine.
- Effectuez une synchronisation finale des fichiers à l'aide AWS DataSync de Robocopy. Pour plus d'informations, consultez Migration du stockage de fichiers existant vers FSx for Windows File Server.
- Effectuez une synchronisation finale de la configuration du partage de fichiers. Pour plus d'informations, consultez Migration des configurations de partage de fichiers vers Amazon FSx.

Configurer les SPN pour l'authentification Kerberos

Nous vous recommandons d'utiliser l'authentification et le chiffrement basés sur Kerberos lors du transit avec Amazon FSx. Kerberos fournit l'authentification la plus sécurisée pour les clients qui accèdent à votre système de fichiers. Pour activer l'authentification Kerberos pour les clients accédant à Amazon FSx à l'aide d'un alias DNS, vous devez ajouter des noms principaux de service (SPN) correspondant à l'alias DNS sur l'objet informatique Active Directory de votre système de fichiers Amazon FSx.

Deux SPN sont requis pour l'authentification Kerberos.

```
HOST/alias
HOST/alias.domain
```

Par exemple, si l'alias est le cas`finance.domain.com`, les deux SPN requis sont les suivants.

```
HOST/finance
HOST/finance.domain.com
```

Un SPN ne peut être associé qu'à un seul objet informatique Active Directory à la fois. S'il existe des SPN existants pour le nom DNS configuré pour l'objet informatique Active Directory de votre système de fichiers d'origine, vous devez les supprimer avant de créer des SPN pour votre système de fichiers Amazon FSx.

Les procédures suivantes décrivent comment rechercher les SPN existants, les supprimer et créer de nouveaux SPN pour l'objet informatique Active Directory de votre système de fichiers Amazon FSx.

Pour installer le module PowerShell Active Directory requis

1. Connectez-vous à une instance Windows jointe à l'Active Directory auquel votre système de fichiers Amazon FSx est joint.
2. Ouvrez PowerShell en tant qu'administrateur.
3. Installez le module PowerShell Active Directory à l'aide de la commande suivante.

   ```
   Install-WindowsFeature RSAT-AD-PowerShell
   ```

Pour rechercher et supprimer des alias DNS SPN existants sur l'objet informatique Active Directory du système de fichiers d'origine

1. Trouvez tous les SPN existants à l'aide des commandes suivantes. *`alias_fqdn`*Remplacez-le par l'alias DNS que vous avez associé au système de fichiers dansMigration de la configuration DNS pour utiliser Amazon FSx.

   ```
   ## Find SPNs for original file system's AD computer object
   $ALIAS = "alias_fqdn"
   SetSPN /Q ("HOST/" + $ALIAS)
   SetSPN /Q ("HOST/" + $ALIAS.Split(".")[0])
   ```
2. Supprimez les SPN HOST existants renvoyés à l'étape précédente à l'aide de l'exemple de script suivant.

   - *`alias_fqdn`*Remplacez-le par l'alias DNS complet que vous avez associé au système de fichiers dansMigration de la configuration DNS pour utiliser Amazon FSx.

- *file_system_DNS_name*Remplacez-le par le nom DNS du système de fichiers d'origine.

```
## Delete SPNs for original file system's AD computer object
$Alias = "alias_fqdn"
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})

SetSPN /D ("HOST/" + ${Alias}) ${FSxAdComputer}.Name
SetSPN /D ("HOST/" + ${Alias}.Split(".")[0]) ${FSxAdComputer}.Name
```

3. Répétez ces étapes pour chaque alias DNS que vous avez associé au système de fichiersMigration de la configuration DNS pour utiliser Amazon FSx.

Pour définir des SPN sur l'objet informatique Active Directory de votre système de fichiers Amazon FSx

1. Définissez de nouveaux SPN pour votre système de fichiers Amazon FSx en exécutant les commandes suivantes.

   - *file_system_DNS_name*Remplacez-le par le nom DNS attribué par Amazon FSx au système de fichiers.

     Pour trouver le nom DNS de votre système de fichiers sur la console Amazon FSx, sélectionnez Systèmes de fichiers, puis choisissez votre système de fichiers. Choisissez le volet Réseau et sécurité de la page de détails du système de fichiers. Vous pouvez également obtenir le nom DNS en réponse à l'opération de l'API DescribeFileSystems.

   - *alias_fqdn*Remplacez-le par l'alias DNS complet que vous avez associé au système de fichiers dansMigration de la configuration DNS pour utiliser Amazon FSx.

```
## Set SPNs for FSx file system AD computer object
$FSxDnsName = "file_system_DNS_name"
$Alias = "alias_fqdn"
$FileSystemHost = (Resolve-DnsName $FSxDnsName | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity $FileSystemHost)
```

```
Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-
AdditionalDnsHostname"="$Alias"}
SetSpn /S ("HOST/" + $Alias.Split('.')[0]) $FSxAdComputer.Name
SetSpn /S ("HOST/" + $Alias) $FSxAdComputer.Name
```

> **Note**
>
> La définition d'un SPN pour votre système de fichiers Amazon FSx échouera si un SPN pour l'alias DNS existe dans l'AD pour l'objet informatique du système de fichiers d'origine. Pour plus d'informations sur la recherche et la suppression de SPN existants, consultezPour rechercher et supprimer des alias DNS SPN existants sur l'objet informatique Active Directory du système de fichiers d'origine.

2. Vérifiez que les nouveaux SPN sont configurés pour l'alias DNS à l'aide de l'exemple de script suivant. Assurez-vous que la réponse inclut deux SPN HOST, `HOST/`*`alias`* et`HOST/`*`alias_fqdn`*.

   *`file_system_DNS_name`*Remplacez-le par le nom DNS attribué par Amazon FSx à votre système de fichiers. Pour trouver le nom DNS de votre système de fichiers sur la console Amazon FSx, choisissez Systèmes de fichiers, choisissez votre système de fichiers, puis choisissez le volet Réseau et sécurité sur la page de détails du système de fichiers.

   Vous pouvez également obtenir le nom DNS en réponse à l'opération de l'API DescribeFileSystems.

   ```
   ## Verify SPNs on FSx file system AD computer object
   $FileSystemDnsName = "file_system_dns_name"
   $FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
   [0].Name.Split(".")[0]
   $FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})
   SetSpn /L ${FSxAdComputer}.Name
   ```

3. Répétez les étapes précédentes pour chaque alias DNS que vous avez associé au système de fichiers dansMigration de la configuration DNS pour utiliser Amazon FSx.

> **Note**
>
> Vous pouvez appliquer l'authentification et le chiffrement Kerberos en transit avec les clients qui se connectent à votre système de fichiers à l'aide d'alias DNS en définissant les objets de stratégie de groupe (GPO) suivants dans votre Active Directory :
>
> - Restreindre le protocole NTLM : trafic NTLM sortant vers des serveurs distants
> - Restreindre NTLM : ajouter des exceptions de serveur distant pour l'authentification NTLM
>
> Pour plus d'informations, consultez la section Procédure pas Application de l'authentification Kerberos à l'aide de GPO à pas 5 : Utilisation d'alias DNS pour accéder à votre système de fichiers.

Mettre à jour les enregistrements DNS CNAME pour le système de fichiers Amazon FSx

Après avoir correctement configuré les SPN pour votre système de fichiers, vous pouvez passer à Amazon FSx en remplaçant chaque enregistrement DNS résolu dans le système de fichiers d'origine par un enregistrement DNS correspondant au nom DNS par défaut du système de fichiers Amazon FSx.

Pour installer les applets de commande requis PowerShell

1. Connectez-vous à une instance Windows jointe à l'Active Directory à laquelle votre système de fichiers Amazon FSx est joint en tant qu'utilisateur membre d'un groupe disposant d'autorisations d'administration DNS (administrateurs de systèmes de noms de domaine AWS délégués dans AWS Microsoft Active Directory géré, administrateurs de domaine ou autre groupe auquel vous avez délégué des autorisations d'administration DNS dans votre Active Directory autogéré)

   Pour plus d'informations, consultez la section Connexion à votre instance Windows dans le guide de l'utilisateur Amazon EC2.
2. Ouvrez PowerShell en tant qu'administrateur.
3. Le module de serveur PowerShell DNS est nécessaire pour exécuter les instructions de cette procédure. Installez-le à l'aide de la commande suivante.

```
Install-WindowsFeature RSAT-DNS-Server
```

Pour mettre à jour un enregistrement DNS CNAME existant

1. Le script suivant met à jour tous les enregistrements DNS CNAME existants *alias_fqdn* pour l'objet informatique de votre système de fichiers Amazon FSx. Si aucun n'est trouvé, il crée un nouvel enregistrement DNS CNAME pour l'alias DNS *alias_fqdn* qui correspond au nom DNS par défaut de votre système de fichiers Amazon FSx.

   Pour exécuter le script :

   - *alias_fqdn*Remplacez-le par l'alias DNS que vous avez associé au système de fichiers.
   - Remplacez *file_system_DNS_name* par le nom DNS par défaut qu'Amazon FSx a attribué au système de fichiers.

   ```
   $Alias="alias_fqdn"
   $FSxDnsName="file_system_dns_name"
   $AliasHost=$Alias.Split('.')[0]
   $ZoneName=((Get-WmiObject Win32_ComputerSystem).Domain)
   $DnsServerComputerName = (Resolve-DnsName $ZoneName -Type NS | Where Type -eq 'A' |
    Select -ExpandProperty Name)[0]

   Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName
    $DnsServerComputerName -HostNameAlias $FSxDnsName -ZoneName $ZoneName
   ```

2. Répétez l'étape précédente pour chaque alias DNS que vous avez associé au système de fichiersMigration de la configuration DNS pour utiliser Amazon FSx.

Utilisation de FSx for Windows File Server avec Microsoft SQL Server

Microsoft SQL Server à haute disponibilité (HA) est généralement déployé sur plusieurs nœuds de base de données au sein d'un cluster Windows Server Failover (WSFC), chaque nœud ayant accès à un stockage de fichiers partagé. Vous pouvez utiliser FSx for Windows File Server comme stockage partagé pour les déploiements Microsoft SQL Server à haute disponibilité (HA) de deux manières : en tant que stockage pour les fichiers de données actifs et en tant que témoin de partage de fichiers SMB.

> **Note**
>
> Actuellement, Amazon FSx ne prend pas en charge la fonctionnalité IFI (initialisation instantanée des fichiers) de Microsoft SQL Server.

Le stockage sur SSD est recommandé pour SQL Server. Le stockage SSD est conçu pour les charges de travail les plus performantes et les plus sensibles à la latence, y compris les bases de données.

Pour plus d'informations sur l'utilisation d'Amazon FSx afin de réduire la complexité et les coûts de vos déploiements de haute disponibilité de SQL Server, consultez les articles suivants sur le blogAWS Storage :

- Simplifiez vos déploiements de haute disponibilité de Microsoft SQL Server à l'aide d'Amazon FSx for Windows File Server
- Optimisation des coûts de vos déploiements SQL Server à haute disponibilité surAWS
- Simplifiez les déploiements de SQL Server Always On avecAWS Launch Wizard et Amazon FSx

Utilisation d'Amazon FSx pour les fichiers de données Active SQL Server

Microsoft SQL Server peut être déployé avec un partage de fichiers SMB comme option de stockage pour les fichiers de données actifs. Amazon FSx est optimisé pour fournir un stockage partagé pour les bases de données SQL Server en prenant en charge les partages de fichiers disponibles en

permanence (CA). Ces partages de fichiers sont conçus pour des applications telles que SQL Server qui nécessitent un accès ininterrompu aux données de fichiers partagées. Bien que vous puissiez créer des partages CA sur des systèmes de fichiers mono-AZ 2, vous devez utiliser des partages CA sur des systèmes de fichiers multi-AZ pour tous les déploiements SQL Server, qu'ils soient en haute disponibilité ou non.

Créez un partage disponible en permanence

Vous pouvez créer des partages CA à l'aide de l'interface de ligne de commande Amazon FSx pour la gestion à distance sur PowerShell. Pour spécifier que le partage est un partage disponible en permanence, utilisez le`New-FSxSmbShare` avec l'`-ContinuouslyAvailable`option définie sur`$True`. Pour de plus amples informations sur la création d'un nouveau partage de CA, veuillez consulterCréation d'un partage disponible en continu (CA).

Configurer les paramètres de délai d'expiration SMB

Comme décrit dans la sectionProcessus de basculement pour FSx for Windows File Server, le basculement et le retour arrière pour Multi-AZ peuvent entraîner des pauses d'E/S qui se terminent généralement en moins de 30 secondes. Votre application SQL Server peut avoir une sensibilité différente aux paramètres de délai d'expiration en fonction de la manière dont elle est configurée.

Vous pouvez régler le délai d'expiration de la session de configuration du client SMB pour vous assurer que votre application résiste aux basculements de systèmes de fichiers Multi-AZ. Vous pouvez tester le comportement de votre application lors des basculements en mettant à jour la capacité de débit de votre système de fichiers, ce qui déclenche un basculement et un retour arrière automatiques.

Utilisation d'Amazon FSx en tant que témoin de partage de fichiers SMB

Les déploiements de clusters Windows Server Failover déploient généralement un témoin de partage de fichiers SMB afin de maintenir le quorum des ressources du cluster. Les partages de fichiers témoins ne nécessitent qu'une faible quantité de stockage pour les informations de quorum. Les systèmes de fichiers Amazon FSx peuvent être utilisés comme témoins de partage de fichiers SMB pour les déploiements de clusters Windows Server Failover.

Utilisation de FSx for Windows File Server avec Amazon Kendra

Amazon Kendra est un service de recherche très précis et intelligent. Les systèmes de fichiers FSx for Windows File Server peuvent être utilisés comme sources de données pour Amazon Kendra, ce qui vous permet d'indexer et de rechercher intelligemment les informations contenues dans les documents stockés sur votre système de fichiers.

- Pour plus d'informations sur Amazon Kendra, consultezQu'est-ce qu'Amazon Kendradans leGuide du développeur Amazon Kendra.
- Pour plus d'informations sur l'ajout de votre système de fichiers en tant que source de données Amazon Kendra, consultezPremiers pas avec une source de données Amazon FSx (console)dans leGuide du développeur Amazon Kendra.
- Pour obtenir des informations de présentation sur Amazon Kendra, consultez leSite Web Amazon Kendra.
- Pour savoir comment effectuer des recherches dans votre système de fichiers à l'aide d'Amazon Kendra, voirRecherchez en toute sécurité des données non structurées sur des systèmes de fichiers Windows avec Amazon Kendra Connector for Amazon FSx for Windows File Serversur leAWSBlog de Machine Learning.

Performances d'un système

Lorsque vous ajoutez un système de fichiers FSx for Windows File Server en tant que source de données, Amazon Kendra analyse les fichiers et les dossiers du système de fichiers à une fréquence de synchronisation normale pour créer et maintenir son index de recherche. (Vous pouvez sélectionner la fréquence de synchronisation lorsque vous établissez l'intégration.) Cette activité d'accès aux fichiers d'Amazon Kendra consomme des ressources du système de fichiers, semblables à celles de vos propres charges de travail accédant au système de fichiers.

Assurez-vous que votre système de fichiers est configuré avec suffisamment de ressources afin que les performances de votre charge de travail ne soient pas affectées. Plus précisément, si vous envisagez d'indexer un grand nombre de fichiers, nous vous recommandons d'utiliser un système de fichiers avec un type de stockage SSD, qui offre un débit maximal et des niveaux d'IOPS plus élevés pour les demandes qui doivent accéder aux volumes de stockage.

Pour plus d'informations sur le modèle de performance Amazon FSx, consultezPerformances de FSx for Windows File Server.

Protection de vos données à l'aide de sauvegardes, de copies instantanées et de réplications planifiées

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

- Les sauvegardes natives d'Amazon FSx répondent à vos besoins en matière de conservation des sauvegardes et de conformité au sein d'Amazon FSx.
- AWS Backup les sauvegardes de vos systèmes de fichiers Amazon FSx font partie d'une solution de sauvegarde centralisée et automatisée pour tous les AWS services dans le cloud et sur site.
- Les copies instantanées de Windows permettent à vos utilisateurs d'annuler facilement les modifications apportées aux fichiers et de comparer les versions de fichiers en restaurant les versions précédentes.
- AWS DataSync la réplication planifiée de votre système de fichiers Amazon FSx vers un second système de fichiers assure la protection et la restauration des données.

Rubriques

Utilisation des sauvegardes

Avec Amazon FSx, les sauvegardes sont file-system-consistent extrêmement durables et incrémentielles. Chaque sauvegarde contient toutes les informations nécessaires à la création d'un nouveau système de fichiers, ce qui permet de restaurer efficacement un point-in-time instantané du système de fichiers. Pour garantir la cohérence du système de fichiers, Amazon FSx utilise le Volume Shadow Copy Service (VSS) sous Microsoft Windows. Pour garantir une durabilité élevée, Amazon FSx stocke les sauvegardes dans Amazon Simple Storage Service (Amazon S3).

Les sauvegardes Amazon FSx sont incrémentielles, qu'elles soient générées à l'aide de la sauvegarde quotidienne automatique ou de la fonction de sauvegarde initiée par l'utilisateur.

Cela signifie que seules les données du système de fichiers qui ont changé après votre dernière sauvegarde sont enregistrées. Cela permet de réduire le temps nécessaire à la création de la sauvegarde et de réduire les coûts de stockage en évitant de dupliquer les données.

À un moment donné du processus de sauvegarde, les E/S de stockage peuvent être brièvement interrompues, généralement pendant quelques secondes. Étant donné que le service VSS doit vider toutes les écritures mises en cache sur le disque avant de reprendre les E/S, la durée de la pause peut être plus longue si votre charge de travail comporte un grand nombre d'opérations d'écriture par seconde (). `DataWriteOperations` La plupart des utilisateurs finaux et des applications ressentiront cette suspension des E/S sous la forme d'une brève pause d'E/S. La sensibilité de vos applications aux paramètres de délai d'expiration peut varier en fonction de leur configuration.

La création de sauvegardes régulières pour votre système de fichiers est une bonne pratique qui complète la réplication qu'Amazon FSx for Windows File Server effectue pour votre système de fichiers. Les sauvegardes Amazon FSx vous aident à répondre à vos besoins en matière de conservation des sauvegardes et de conformité. Il est facile d'utiliser les sauvegardes Amazon FSx, qu'il s'agisse de créer des sauvegardes, de copier une sauvegarde, de restaurer un système de fichiers à partir d'une sauvegarde ou de supprimer une sauvegarde. Notez que pour visualiser l'utilisation d'une sauvegarde de système de fichiers unique, vous devez activer les balises pour cette sauvegarde spécifique et activer les rapports de facturation basés sur les balises.

Rubriques

Utilisation de sauvegardes quotidiennes automatiques

Par défaut, Amazon FSx effectue une sauvegarde quotidienne automatique de votre système de fichiers. Ces sauvegardes quotidiennes automatiques ont lieu pendant la fenêtre de sauvegarde quotidienne établie lors de la création du système de fichiers. Lorsque vous choisissez votre fenêtre de sauvegarde quotidienne, nous vous recommandons de choisir un moment de la journée qui vous

convient. Cette durée se situe idéalement en dehors des heures de fonctionnement normales pour les applications qui utilisent le système de fichiers.

Les sauvegardes quotidiennes automatiques sont conservées pendant une certaine période, connue sous le nom de période de conservation. Lorsque vous créez un système de fichiers dans la console Amazon FSx, la période de conservation quotidienne automatique des sauvegardes par défaut est de 30 jours. La période de rétention par défaut est différente dans l'API et la CLI Amazon FSx. Vous pouvez définir une période de conservation comprise entre 0 et 90 jours. La définition de la période de rétention sur 0 (zéro) jour désactive les sauvegardes quotidiennes automatiques. Les sauvegardes quotidiennes automatiques sont supprimées lorsque le système de fichiers est supprimé.

> **Note**
>
> Si vous définissez la période de conservation sur 0 jour, votre système de fichiers n'est jamais automatiquement sauvegardé. Nous vous recommandons vivement d'utiliser des sauvegardes quotidiennes automatiques pour les systèmes de fichiers associés à un niveau quelconque de fonctionnalités critiques.

Vous pouvez utiliser le AWS CLI ou l'un des AWS SDK pour modifier la fenêtre de sauvegarde et la période de conservation des sauvegardes pour vos systèmes de fichiers. Utilisez l'opération `UpdateFileSystem`API ou la commande `update-file-system`CLI. Pour plus d'informations, consultez Procédure 3 : Mettre à jour un système de fichiers existant.

Utilisation de sauvegardes initiées par l'utilisateur

Avec Amazon FSx, vous pouvez effectuer des sauvegardes manuelles de vos systèmes de fichiers à tout moment. Vous pouvez le faire à l'aide de la console Amazon FSx, de l'API ou du AWS Command Line Interface ()AWS CLI. Vos sauvegardes des systèmes de fichiers Amazon FSx initiées par l'utilisateur n'expirent jamais et sont disponibles aussi longtemps que vous souhaitez les conserver. Les sauvegardes initiées par l'utilisateur sont conservées même après la suppression du système de fichiers sauvegardé. Vous pouvez supprimer des sauvegardes initiées par l'utilisateur uniquement à l'aide de la console, de l'API ou de la CLI Amazon FSx. Ils ne sont jamais automatiquement supprimés par Amazon FSx. Pour plus d'informations, consultez Suppression de sauvegardes.

Si une sauvegarde est lancée alors que le système de fichiers est en cours de modification (par exemple lors d'une mise à jour de la capacité de débit ou lors de la maintenance du système de fichiers), la demande de sauvegarde est mise en file d'attente et reprendra une fois l'activité terminée.

Création de sauvegardes initiées par l'utilisateur

La procédure suivante explique comment créer une sauvegarde initiée par l'utilisateur dans la console Amazon FSx pour un système de fichiers existant.

Pour créer une sauvegarde du système de fichiers initiée par l'utilisateur

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le tableau de bord de la console, choisissez le nom du système de fichiers que vous souhaitez sauvegarder.
3. Dans Actions, sélectionnez Créer une sauvegarde.
4. 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. + - = _ :/
5. Choisissez Créer une sauvegarde.

Vous venez de créer la sauvegarde de votre système de fichiers. Vous pouvez trouver un tableau de toutes vos sauvegardes dans la console Amazon FSx en choisissant Sauvegardes dans la barre de navigation de gauche. Vous pouvez rechercher le nom que vous avez donné à votre sauvegarde, et le tableau filtre pour n'afficher que les résultats correspondants.

Lorsque vous créez une sauvegarde initiée par l'utilisateur comme décrit dans cette procédure, elle possède le type `USER_INITIATED` et le `CREATING` statut jusqu'à ce qu'elle soit entièrement disponible.

Utilisation AWS Backup avec Amazon FSx

AWS Backup est un moyen simple et économique de protéger vos données en sauvegardant vos systèmes de fichiers Amazon FSx. AWS Backup est un service de sauvegarde unifié conçu pour simplifier la création, la copie, la restauration et la suppression des sauvegardes, tout en fournissant des rapports et des audits améliorés. AWS Backup facilite le développement d'une stratégie de sauvegarde centralisée à des fins de conformité légale, réglementaire et professionnelle. AWS Backup simplifie également la protection AWS de vos volumes de stockage, de vos bases de données et de vos systèmes de fichiers en fournissant un emplacement central où vous pouvez effectuer les opérations suivantes :

- Configurez et auditez les AWS ressources que vous souhaitez sauvegarder.

- Automatiser la planification des sauvegardes.
- Définir des stratégies de conservation.
- Copiez les sauvegardes entre AWS les régions et les AWS comptes.
- 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 effectuées depuis la AWS Backup console présentent le même niveau de cohérence et de performance du système de fichiers, ainsi que les mêmes options de restauration que les sauvegardes effectuées via la console Amazon FSx. Les sauvegardes effectuées depuis AWS Backup sont incrémentielles par rapport à toutes les autres sauvegardes Amazon FSx que vous effectuez, qu'elles soient initiées par l'utilisateur ou automatiques.

Si vous gérez AWS Backup ces sauvegardes, vous bénéficiez de fonctionnalités supplémentaires, telles que des options de rétention illimitées et la possibilité de créer des sauvegardes planifiées toutes les heures. En outre, AWS Backup conserve vos sauvegardes immuables même après la suppression du système de fichiers source. Cela permet d'éviter les suppressions accidentelles ou malveillantes.

Les sauvegardes effectuées 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. Vous pouvez consulter et restaurer les sauvegardes effectuées AWS Backup dans la console, la CLI et l'API Amazon FSx. Toutefois, vous ne pouvez pas supprimer les sauvegardes effectuées AWS Backup dans la console, la CLI ou l'API Amazon FSx. Pour plus d'informations sur la façon de AWS Backup sauvegarder vos systèmes de fichiers Amazon FSx, consultez la section Travailler avec les systèmes de fichiers Amazon FSx dans le manuel du développeur.AWS Backup

Copie de sauvegardes

Vous pouvez utiliser Amazon FSx pour copier manuellement les sauvegardes d'un même AWS compte vers une autre AWS région (copies entre régions) ou au sein de la même AWS région (copies internes). Vous ne pouvez effectuer des copies entre régions qu'au sein d' AWS une même partition. Vous pouvez créer des copies de sauvegarde initiées par l'utilisateur à l'aide de la console Amazon FSx ou de AWS CLI l'API. Lorsque vous créez une copie de sauvegarde initiée par l'utilisateur, elle est de type`USER_INITIATED`.

Vous pouvez également l'utiliser AWS Backup pour copier des sauvegardes d'une AWS région à l'autre et d'un AWS compte à l'autre. AWS Backup est un service de gestion des sauvegardes

entièrement géré qui fournit une interface centrale pour les plans de sauvegarde basés sur des règles. Grâce à sa gestion entre comptes, vous pouvez automatiquement utiliser des politiques de sauvegarde pour appliquer des plans de sauvegarde à tous les comptes de votre organisation.

Les copies de sauvegarde interrégionales sont particulièrement utiles pour la reprise après sinistre entre régions. Vous effectuez des sauvegardes et vous les copiez dans une autre AWS région afin qu'en cas de sinistre dans la AWS région principale, vous puissiez effectuer une restauration à partir d'une sauvegarde et rétablir rapidement la disponibilité dans l'autre AWS région. Vous pouvez également utiliser des copies de sauvegarde pour cloner votre jeu de données de fichiers dans une autre AWS région ou au sein de la même AWS région. Vous pouvez effectuer des copies de sauvegarde au sein du même AWS compte (entre régions ou dans une région) à l'aide de la console Amazon FSx ou de l'API AWS CLI Amazon FSx. Vous pouvez également l'utiliser AWS Backuppour effectuer des copies de sauvegarde, à la demande ou selon des règles.

Les copies de sauvegarde entre comptes sont utiles pour répondre à vos exigences de conformité réglementaire en matière de copie de sauvegardes sur un compte isolé. Ils fournissent également une couche supplémentaire de protection des données pour empêcher la suppression accidentelle ou malveillante des sauvegardes, la perte d'informations d'identification ou la compromission des AWS KMS clés. Les sauvegardes entre comptes prennent en charge le fan-in (copie des sauvegardes de plusieurs comptes principaux vers un compte de copie de sauvegarde isolé) et le fan-out (copie des sauvegardes d'un compte principal vers plusieurs comptes de copie de sauvegarde isolés).

Vous pouvez créer des copies de sauvegarde entre comptes en les utilisant AWS Backup avec le AWS Organizations support. Les limites des comptes pour les copies entre comptes sont définies par des AWS Organizations politiques. Pour plus d'informations sur l'utilisation AWS Backup pour créer des copies de sauvegarde entre comptes, consultez la section Création de copies de sauvegarde Comptes AWS dans le Guide du AWS Backup développeur.

Limites relatives à la copie de sauvegarde

Les restrictions suivantes s'appliquent lorsque vous copiez des sauvegardes :

- Les copies de sauvegarde entre régions ne sont prises en charge qu'entre deux AWS régions commerciales, entre les régions Chine (Pékin) et Chine (Ningxia), et entre les régions AWS GovCloud (USA Est) et AWS GovCloud (USA Ouest), mais pas entre ces ensembles de régions.
- Les copies de sauvegarde entre régions ne sont pas prises en charge dans les régions optionnelles.
- Vous pouvez créer des copies de sauvegarde régionales dans n'importe quelle AWS région.

- Le statut de la sauvegarde source doit être défini sur « `AVAILABLE` Pour que vous puissiez la copier ».
- Vous ne pouvez pas supprimer une sauvegarde source si elle est copiée. Un court délai peut s'écouler entre le moment où la sauvegarde de destination devient disponible et le moment où vous êtes autorisé à supprimer la sauvegarde source. Vous devez garder ce délai à l'esprit si vous essayez à nouveau de supprimer une sauvegarde source.
- Vous pouvez avoir jusqu'à cinq demandes de copie de sauvegarde en cours vers une seule AWS région de destination par compte.

Autorisations pour les copies de sauvegarde interrégionales

Vous utilisez une déclaration de politique IAM pour accorder l'autorisation d'effectuer une opération de copie de sauvegarde. Pour communiquer avec la AWS région source afin de demander une copie de sauvegarde interrégionale, le demandeur (rôle IAM ou utilisateur IAM) doit avoir accès à la sauvegarde source et à la région source. AWS

Vous utilisez cette politique pour accorder des autorisations à l'`CopyBackup`action relative à l'opération de copie de sauvegarde. Vous spécifiez l'action dans le `Action` champ de la stratégie et vous spécifiez la valeur de la ressource dans le `Resource` champ de la stratégie, comme dans l'exemple suivant.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "fsx:CopyBackup",
            "Resource": "arn:aws:fsx:*:111111111111:backup/*"
        }
    ]
}
```

Pour plus d'informations sur les politiques IAM, consultez la section Politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.

Copies complètes et incrémentielles

Lorsque vous copiez une sauvegarde vers une AWS région ou un AWS compte de destination différent de celui de la sauvegarde source, la première copie est une copie de sauvegarde complète,

même si vous utilisez la même clé KMS pour chiffrer les copies source et de destination de la sauvegarde.

Après la première copie de sauvegarde, toutes les copies de sauvegarde suivantes vers la même région de destination au sein du même AWS compte sont incrémentielles, à condition que vous n'ayez pas supprimé toutes les sauvegardes précédemment copiées dans cette région et que vous utilisiez la même clé. AWS KMS Si l'une ou l'autre des conditions n'est pas remplie, l'opération de copie aboutit à une copie de sauvegarde complète (et non incrémentielle).

Pour copier une sauvegarde au sein du même compte (entre régions ou dans une région) à l'aide de la console

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation, choisissez Sauvegardes.
3. Dans le tableau Sauvegardes, choisissez la sauvegarde que vous souhaitez copier, puis choisissez Copier la sauvegarde.
4. Dans la section Settings (Paramètres), procédez comme suit :
   - Dans la liste Région de destination, choisissez une AWS région de destination dans laquelle copier la sauvegarde. La destination peut se trouver dans une autre AWS région (copie interrégionale) ou dans la même AWS région (copie régionale).
   - (Facultatif) Sélectionnez Copier les balises pour copier les balises de la sauvegarde source vers la sauvegarde de destination. Si vous sélectionnez Copier les balises et que vous ajoutez également des balises à l'étape 6, toutes les balises sont fusionnées.
5. Pour le chiffrement, choisissez la clé de AWS KMS chiffrement pour chiffrer la sauvegarde copiée.
6. Pour les balises (facultatif), entrez une clé et une valeur pour ajouter des balises à votre sauvegarde copiée. Si vous ajoutez des balises ici et que vous avez également sélectionné Copier les balises à l'étape 4, toutes les balises sont fusionnées.
7. Choisissez Copier la sauvegarde.

Votre sauvegarde est copiée dans le même AWS compte dans la AWS région sélectionnée.

Pour copier une sauvegarde dans le même compte (entre régions ou dans une région) à l'aide de la CLI

- Utilisez la commande `copy-backup` CLI ou l'opération CopyBackupAPI pour copier une sauvegarde dans le même AWS compte, que ce soit dans une AWS région ou au sein d'une AWS région.

  La commande suivante copie une sauvegarde dont l'ID est « `backup-0abc123456789cba7` from the `us-east-1` Region ».

  ```
  aws fsx copy-backup \
    --source-backup-id backup-0abc123456789cba7 \
    --source-region us-east-1
  ```

  La réponse indique la description de la sauvegarde copiée.

  Vous pouvez consulter vos sauvegardes sur la console Amazon FSx ou par programmation à l'aide de la commande `describe-backups` CLI ou de l'opération API. DescribeBackups

Restauration des sauvegardes

Vous pouvez utiliser une sauvegarde disponible pour créer un nouveau système de fichiers, en restaurant efficacement un point-in-time instantané d'un autre système de fichiers. Vous pouvez restaurer une sauvegarde à l'aide de la AWS CLI console ou de l'un des AWS SDK. La restauration d'une sauvegarde sur un nouveau système de fichiers prend le même temps que la création d'un nouveau système de fichiers. Les données restaurées à partir de la sauvegarde sont chargées latéralement dans le système de fichiers, période pendant laquelle vous constaterez une latence légèrement plus élevée.

Pour que les utilisateurs puissent continuer à accéder au système de fichiers restauré, assurez-vous que le domaine Active Directory associé au système de fichiers restauré est le même que celui du système de fichiers d'origine ou qu'il est approuvé par le domaine AD du système de fichiers d'origine. Pour plus d'informations sur Active Directory, consultezUtilisation de Microsoft Active Directory dans FSx for Windows File Server.

La procédure suivante explique comment restaurer une sauvegarde à l'aide de la console pour créer un nouveau système de fichiers.

> **Note**
>
> Vous ne pouvez restaurer votre sauvegarde que sur un système de fichiers ayant le même type de déploiement et la même capacité de stockage que le système d'origine. Vous pouvez augmenter la capacité de stockage de votre système de fichiers restauré une fois qu'il sera disponible. Pour plus d'informations, consultez Gestion de la capacité de stockage.

Pour restaurer un système de fichiers à partir d'une sauvegarde

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le tableau de bord de la console, choisissez Sauvegardes dans la barre de navigation de gauche.
3. Choisissez la sauvegarde que vous souhaitez restaurer dans le tableau des sauvegardes, puis choisissez Restaurer la sauvegarde.

   Cela ouvre l'assistant de création du système de fichiers. Cet assistant est identique à l'assistant de création de système de fichiers standard, sauf que le type de déploiement et la capacité de stockage sont déjà définis et ne peuvent pas être modifiés. Toutefois, vous pouvez modifier la capacité de débit, le VPC associé et d'autres paramètres, ainsi que le type de stockage. Le type de stockage est défini sur SSD par défaut, mais vous pouvez le remplacer par HDD dans les conditions suivantes :

   - Le type de déploiement du système de fichiers est Multi-AZ ou Single-AZ 2.
   - La capacité de stockage est d'au moins 2 000 GiB.
4. Complétez l'assistant comme vous le faites lorsque vous créez un nouveau système de fichiers.
5. Choisissez Review and create.
6. Passez en revue les paramètres que vous avez choisis pour votre système de fichiers Amazon FSx, puis choisissez Create file system.

Vous avez effectué une restauration à partir d'une sauvegarde et un nouveau système de fichiers est en cours de création. Lorsque son statut passe à`AVAILABLE`, vous pouvez utiliser le système de fichiers normalement.

Suppression de sauvegardes

La suppression d'une sauvegarde est une action permanente irrécupérable. Toutes les données d'une sauvegarde supprimée sont également supprimées. Ne supprimez pas une sauvegarde si vous n'êtes pas certain de ne pas en avoir besoin à nouveau à l'avenir. Vous ne pouvez pas supprimer les sauvegardes effectuées par AWS Backup des personnes de type AWS Backup dans la console, la CLI ou l'API Amazon FSx.

Pour supprimer une sauvegarde

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le tableau de bord de la console, choisissez Sauvegardes dans la barre de navigation de gauche.
3. Choisissez la sauvegarde que vous souhaitez supprimer dans le tableau des sauvegardes, puis choisissez Supprimer la sauvegarde.
4. Dans la boîte de dialogue Supprimer les sauvegardes qui s'ouvre, vérifiez que l'ID de la sauvegarde identifie 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.

Taille des sauvegardes

La taille des sauvegardes est déterminée en fonction du stockage utilisé dans le système de fichiers, plutôt que de la capacité de stockage totale allouée. La taille de vos sauvegardes dépend de la capacité de stockage utilisée ainsi que de la quantité de perte de données sur votre système de fichiers. En fonction de la manière dont vos données sont réparties sur les volumes de stockage du système de fichiers et de la fréquence à laquelle elles changent, votre utilisation totale des sauvegardes peut être supérieure ou inférieure à votre capacité de stockage utilisée. Lorsque vous supprimez une sauvegarde, seules les données propres à cette sauvegarde sont supprimées. Avec Amazon FSx, les économies d'efficacité du stockage réalisées grâce à la déduplication et à la compression s'appliquent non seulement à votre stockage SSD/HDD principal, mais également aux sauvegardes.

Afin de fournir des file-system-consistent sauvegardes durables et incrémentielles, Amazon FSx sauvegarde les données au niveau des blocs. Les données des volumes de stockage du système de fichiers peuvent être stockées sur plusieurs blocs en fonction du modèle dans lequel elles ont été écrites ou remplacées. Par conséquent, la taille totale de l'utilisation des sauvegardes peut ne pas correspondre à la taille exacte des fichiers et des répertoires du système de fichiers.

L'utilisation et le coût globaux de vos sauvegardes se trouvent dans le AWS Billing tableau de bord ou AWS Cost Management Console. Pour calculer la taille et le coût des sauvegardes de systèmes de fichiers individuelles, vous pouvez baliser les sauvegardes individuelles et activer les rapports de facturation basés sur des balises.

Protection de vos données à l'aide de clichés instantanés

Un cliché instantané de Microsoft Windows est un instantané d'un système de fichiers Windows à un moment donné. Lorsque les copies instantanées sont activées, les utilisateurs peuvent rapidement récupérer les fichiers supprimés ou modifiés stockés sur le réseau et comparer les versions de fichiers. Les administrateurs de stockage peuvent facilement planifier la prise périodique de clichés instantanés à l'aide des PowerShell commandes Windows.

Les copies instantanées sont stockées avec les données de votre système de fichiers et n'utilisent la capacité de stockage du système de fichiers que pour les parties modifiées des fichiers. Toutes les copies instantanées stockées dans votre système de fichiers sont incluses dans les sauvegardes du système de fichiers.

> **Note**
>
> Les clichés instantanés ne sont pas activés par défaut sur FSx for Windows File Server. Pour protéger les données de votre système de fichiers à l'aide de clichés instantanés, vous devez activer les clichés instantanés et configurer un calendrier de clichés instantanés sur votre système de fichiers. Pour plus d'informations, consultez Configuration des clichés instantanés pour utiliser le stockage et la planification par défaut.

> **Warning**
>
> Les copies instantanées ne remplacent pas les sauvegardes. Si vous activez les clichés instantanés, assurez-vous de continuer à effectuer des sauvegardes régulières.

Rubriques

Bonnes pratiques en matière d'utilisation de clichés instantanés

Vous pouvez activer les clichés instantanés pour votre système de fichiers afin de permettre aux utilisateurs finaux de visualiser et de restaurer des fichiers ou des dossiers individuels à partir d'un instantané antérieur dans l'Explorateur de fichiers Windows. Amazon FSx utilise la fonctionnalité de copie instantanée fournie par Microsoft Windows Server. Utilisez les meilleures pratiques suivantes pour les clichés instantanés :

- Assurez-vous que votre système de fichiers dispose de ressources de performance suffisantes : Microsoft Windows utilise, de par sa conception, une copy-on-write méthode pour enregistrer les modifications depuis le point de copie instantanée le plus récent, et cette copy-on-write activité peut entraîner jusqu'à trois opérations d'E/S pour chaque opération d'écriture de fichier.
- Utilisez le stockage SSD et augmentez la capacité de débit : Windows ayant besoin de performances d'E/S élevées pour conserver des copies instantanées, nous vous recommandons d'utiliser le stockage SSD et d'augmenter la capacité de débit jusqu'à une valeur trois fois supérieure à la charge de travail prévue. Cela permet de garantir que votre système de fichiers dispose de suffisamment de ressources pour éviter des problèmes tels que la suppression indésirable de clichés instantanés.

- Conservez uniquement le nombre de clichés instantanés dont vous avez besoin : si vous disposez d'un grand nombre de clichés instantanés (par exemple, plus de 64 clichés instantanés les plus récents) ou de clichés instantanés occupant une grande quantité de stockage (échelle en To) sur un même système de fichiers, les processus tels que le basculement et le retour arrière peuvent prendre un certain temps. Cela est dû à la nécessité pour FSx pour Windows d'exécuter des contrôles de cohérence sur le stockage des clichés instantanés. La latence des opérations d'E/S peut également être plus élevée en raison de la nécessité pour FSx pour Windows d' copy-on-write effectuer des activités tout en conservant les clichés instantanés. Pour minimiser l'impact sur la disponibilité et les performances des clichés instantanés, supprimez manuellement les clichés instantanés non utilisés ou configurez des scripts pour supprimer automatiquement les anciens clichés instantanés de votre système de fichiers.

> **Note**
>
> Lors d'événements de basculement pour les systèmes de fichiers multi-AZ, FSx pour Windows exécute un contrôle de cohérence qui nécessite de scanner le stockage des clichés instantanés de votre système de fichiers avant que le nouveau serveur de fichiers actif ne soit mis en ligne. La durée du contrôle de cohérence est liée au nombre de clichés instantanés présents sur votre système de fichiers ainsi qu'à l'espace de stockage consommé. Pour éviter les événements de basculement et de retour en arrière différés, nous vous recommandons de conserver moins de 64 clichés instantanés sur votre système de fichiers et de suivre les étapes ci-dessous pour surveiller et supprimer régulièrement vos clichés instantanés les plus anciens.

Configuration des clichés instantanés

Vous activez et planifiez des clichés instantanés périodiques sur votre système de fichiers à l'aide des PowerShell commandes Windows définies par Amazon FSx. Voici les trois principaux paramètres de configuration des clichés instantanés sur votre système de fichiers FSx for Windows File Server :

- Définition de la quantité maximale d'espace de stockage que les clichés instantanés peuvent consommer sur votre système de fichiers
- (Facultatif) Définissez le nombre maximum de clichés instantanés pouvant être stockés sur votre système de fichiers. La valeur par défaut est 20.

- (Facultatif) Définition d'un calendrier qui définit les heures et intervalles auxquels prendre des clichés instantanés, par exemple une fois par jour, une semaine ou un mois

Vous pouvez stocker un maximum de 500 clichés instantanés par système de fichiers à tout moment ; nous vous recommandons toutefois de conserver moins de 64 clichés instantanés à tout moment pour garantir la disponibilité et les performances. Lorsque vous atteignez cette limite, le cliché instantané suivant remplace le cliché instantané le plus ancien. De même, lorsque la quantité maximale de stockage du cliché instantané est atteinte, un ou plusieurs des clichés instantanés les plus anciens sont supprimés afin de libérer de l'espace de stockage pour le cliché instantané suivant.

Pour plus d'informations sur la façon d'activer et de planifier rapidement des clichés instantanés périodiques à l'aide des paramètres par défaut d'Amazon FSx, consultez. Configuration des clichés instantanés pour utiliser le stockage et la planification par défaut

Considérations relatives à l'allocation de stockage de clichés instantanés

Un cliché instantané est une copie au niveau du bloc des modifications apportées au fichier depuis le dernier cliché instantané. Le fichier entier n'est pas copié, seules les modifications sont copiées. Par conséquent, les versions précédentes des fichiers n'occupent généralement pas autant d'espace de stockage que le fichier actuel. La quantité d'espace volumique utilisée pour les modifications peut varier en fonction de votre charge de travail. Lorsqu'un fichier est modifié, l'espace de stockage utilisé par les clichés instantanés dépend de votre charge de travail. Lorsque vous déterminez l'espace de stockage à allouer aux clichés instantanés, vous devez tenir compte des habitudes d'utilisation du système de fichiers de votre charge de travail.

Lorsque vous activez les clichés instantanés, vous pouvez spécifier la quantité maximale d'espace de stockage que les clichés instantanés peuvent consommer sur le système de fichiers. La limite par défaut est de 10 % de votre système de fichiers. Nous vous recommandons d'augmenter la limite si vos utilisateurs ajoutent ou modifient fréquemment des fichiers. Si la limite est trop faible, les clichés instantanés les plus anciens peuvent être supprimés plus souvent que prévu par les utilisateurs.

Vous pouvez définir le stockage des clichés instantanés comme étant illimité ()`Set-FsxShadowStorage -Maxsize "UNBOUNDED"`. Cependant, une configuration illimitée peut entraîner la consommation d'un grand nombre de clichés instantanés sur l'espace de stockage de votre système de fichiers. Cela peut entraîner une capacité de stockage insuffisante pour vos charges de travail. Si vous définissez un espace de stockage illimité, veillez à augmenter votre capacité de stockage au fur et à mesure que les limites de copies instantanées sont atteintes. Pour plus d'informations sur la configuration de votre espace de stockage de clichés instantanés à une

taille spécifique ou illimitée, consultez. Définition de la quantité maximale de stockage de clichés instantanés

Après avoir activé les clichés instantanés, vous pouvez contrôler la quantité d'espace de stockage consommée par les clichés instantanés. Pour plus d'informations, consultez Afficher votre espace de stockage de clichés instantanés.

Considérations relatives à la définition du nombre maximum de clichés instantanés

Lorsque vous activez les clichés instantanés, vous pouvez spécifier le nombre maximum de clichés instantanés stockés dans le système de fichiers. La limite par défaut est de 20, et pour minimiser l'impact sur la disponibilité et les performances des clichés instantanés, Microsoft recommande de configurer le nombre maximum de clichés instantanés à moins de 64. Windows ayant besoin de performances d'E/S élevées pour conserver des copies instantanées, nous vous recommandons d'utiliser le stockage SSD et d'augmenter la capacité de débit jusqu'à une valeur trois fois supérieure à celle de votre charge de travail prévue. Cela permet de garantir que votre système de fichiers dispose de suffisamment de ressources pour éviter des problèmes tels que la suppression indésirable de clichés instantanés.

Vous pouvez définir le nombre maximum de clichés instantanés à 500. Toutefois, si vous disposez d'un grand nombre de clichés instantanés ou de clichés instantanés occupant une grande quantité de stockage (échelle en To) sur un seul système de fichiers, les processus tels que le basculement et le retour en arrière peuvent prendre plus de temps que prévu. Cela est dû au fait que Windows doit exécuter des contrôles de cohérence sur le stockage des clichés instantanés. La latence des opérations d'E/S peut également être plus élevée car Windows doit effectuer des copy-on-write activités tout en conservant les clichés instantanés.

Recommandations relatives aux systèmes de fichiers pour les clichés instantanés

Vous trouverez ci-dessous les recommandations relatives au système de fichiers concernant l'utilisation de clichés instantanés.

- Assurez-vous de fournir une capacité de performance suffisante pour répondre aux besoins de votre charge de travail sur votre système de fichiers. Amazon FSx fournit la fonctionnalité Shadow Copies fournie par Microsoft Windows Server. De par sa conception, Microsoft Windows utilise une copy-on-write méthode pour enregistrer les modifications depuis le point de copie instantanée le plus récent, et cette copy-on-write activité peut entraîner jusqu'à trois opérations d'E/S pour chaque opération d'écriture de fichier. Si Windows n'est pas en mesure de suivre le rythme des opérations d'E/S entrantes par seconde, il peut entraîner la suppression de tous les clichés instantanés, car

il ne peut plus conserver les clichés instantanés via copy-on-write. Il est donc important que vous disposiez d'une capacité de performance d'E/S suffisante pour répondre aux besoins de votre système de fichiers en termes de charge de travail (à la fois la dimension de capacité de débit qui détermine les performances d'E/S du serveur de fichiers et le type et la capacité de stockage qui déterminent les performances d'E/S de stockage).

- Nous vous recommandons généralement d'utiliser des systèmes de fichiers configurés avec un stockage SSD plutôt qu'un stockage sur disque dur lorsque vous activez les clichés instantanés, étant donné que Windows consomme des performances d'E/S supérieures pour conserver les clichés instantanés et que le stockage sur disque dur offre une capacité de performance inférieure pour les opérations d'E/S.
- Votre système de fichiers doit disposer d'au moins 320 Mo d'espace libre, en plus de la quantité maximale de stockage de clichés instantanés configurée (`MaxSpace`). Par exemple, si vous avez alloué 5 Go `MaxSpace` aux clichés instantanés, votre système de fichiers doit toujours disposer d'au moins 320 Mo d'espace libre en plus des 5 Go`MaxSpace`.

> **Warning**
>
> Lorsque vous configurez votre calendrier de clichés instantanés, assurez-vous de ne pas planifier de clichés instantanés lors de la migration des données ou lorsque des tâches de déduplication des données sont planifiées pour être exécutées. Vous devez planifier des clichés instantanés lorsque vous vous attendez à ce que votre système de fichiers soit inactif. Pour plus d'informations sur la configuration d'un calendrier personnalisé de clichés instantanés, consultezCréation d'un calendrier personnalisé pour les clichés instantanés.

Configuration des clichés instantanés pour utiliser le stockage et la planification par défaut

Vous pouvez configurer rapidement des clichés instantanés sur votre système de fichiers en utilisant le paramètre et le calendrier de stockage des clichés instantanés par défaut. Le paramètre de stockage des clichés instantanés par défaut permet aux clichés instantanés de consommer au maximum 10 % de la capacité de stockage de votre système de fichiers. Si vous augmentez la capacité de stockage de votre système de fichiers, la quantité de stockage actuellement allouée aux clichés instantanés n'est pas augmentée de la même manière.

Le calendrier par défaut prend automatiquement des clichés instantanés tous les lundis, mardis, mercredis, jeudis et vendredis, à 7 h 00 et 12 h 00 UTC.

Pour configurer le niveau par défaut de stockage des clichés instantanés

1. Connectez-vous à une instance de calcul Windows dotée d'une connectivité réseau avec votre système de fichiers.
2. Connectez-vous à l'instance de calcul Windows en tant que membre du groupe d'administrateurs du système de fichiers. Dans AWS Managed Microsoft AD, ce groupe est celui des AWS administrateurs FSx délégués. Dans votre Microsoft AD autogéré, il s'agit des administrateurs de domaine ou du groupe personnalisé que vous avez spécifié pour l'administration lors de la création de votre système de fichiers. Pour plus d'informations, consultez la section Connexion à votre instance Windows dans le guide de l'utilisateur Amazon EC2.
3. Définissez la quantité de stockage parallèle par défaut à l'aide de la commande suivante. *FSxFileSystem-Remote-PowerShell-Endpoint*Remplacez-le par le PowerShell point de terminaison Windows Remote du système de fichiers que vous souhaitez administrer. Vous pouvez trouver le point de PowerShell terminaison Windows Remote dans la console Amazon FSx, dans la section Réseau et sécurité de l'écran des détails du système de fichiers ou dans la réponse à l'opération de l'`DescribeFileSystem`API.

   ```
   PS C:\Users\delegateadmin> Invoke-Command -ComputerName FSxFileSystem-Remote-
   PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {Set-
   FsxShadowStorage -Default}
   ```

   La réponse se présente comme suit.

   ```
   FSx Shadow Storage Configuration

   AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
   -------------- ---------    -------- -------------------
                0         0 10737418240                  20
   ```

Pour définir le calendrier de cliché instantané par défaut

1. Connectez-vous à une instance de calcul Windows dotée d'une connectivité réseau avec votre système de fichiers.

2. Connectez-vous à l'instance de calcul Windows en tant que membre du groupe d'administrateurs du système de fichiers. Dans AWS Managed Microsoft AD, ce groupe est celui des AWS administrateurs FSx délégués. Dans votre Microsoft AD autogéré, il s'agit des administrateurs de domaine ou du groupe personnalisé que vous avez spécifié pour l'administration lors de la création de votre système de fichiers. Pour plus d'informations, consultez la section Connexion à votre instance Windows dans le guide de l'utilisateur Amazon EC2.
3. Définissez le calendrier de cliché instantané par défaut à l'aide de la commande suivante.

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName FSxFileSystem-Remote-
PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {Set-
FsxShadowCopySchedule -Default}
```

La réponse affiche le calendrier par défaut qui est désormais défini.

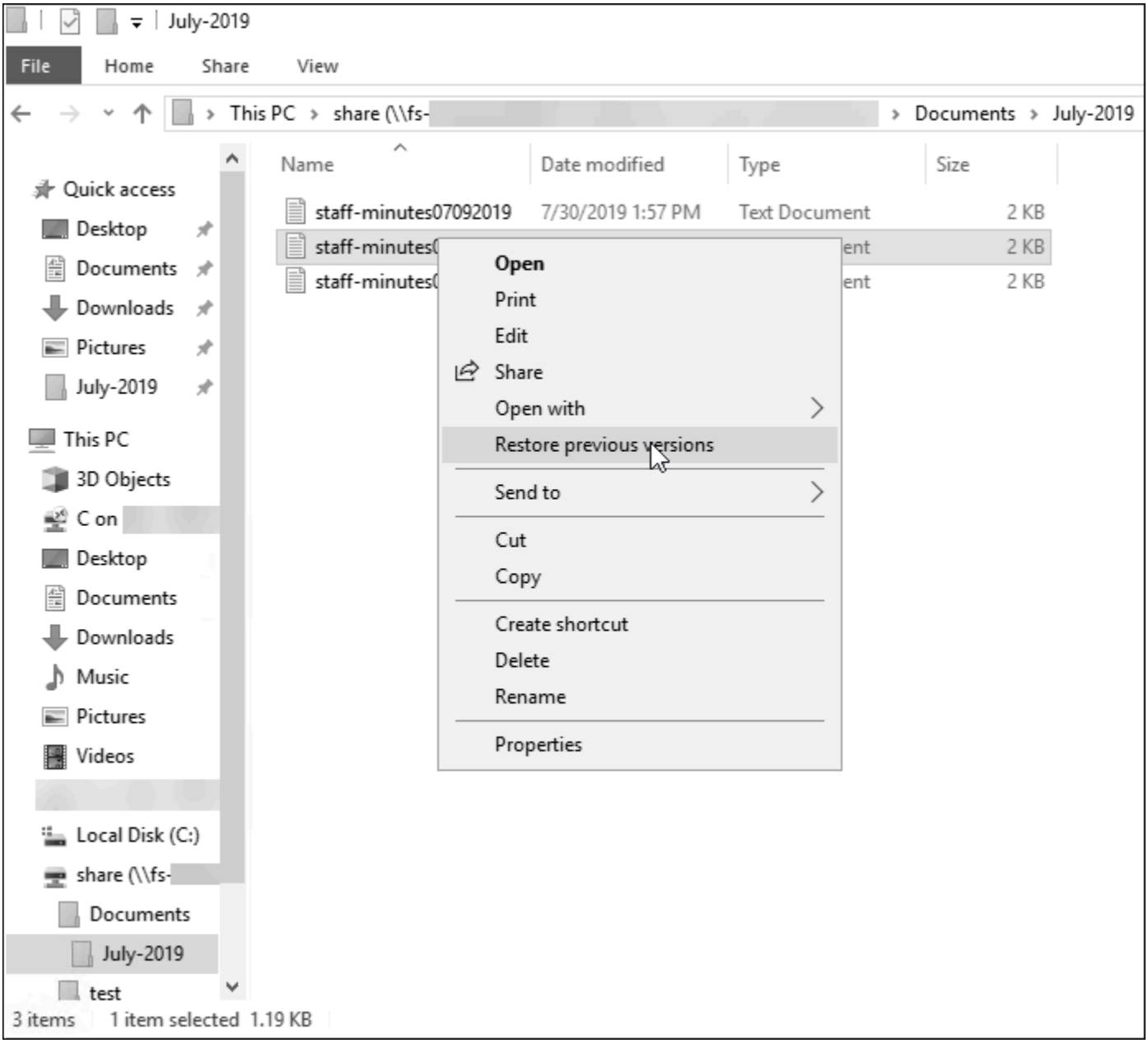
```
FSx Shadow Copy Schedule

Start Time                Days of week                            WeeksInterval
----------                ------------                            -------------
2019-07-16T07:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
2019-07-16T12:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
```

Pour en savoir plus sur les options supplémentaires et la création d'un calendrier de cliché instantané personnalisé, voirCréation d'un calendrier personnalisé pour les clichés instantanés.

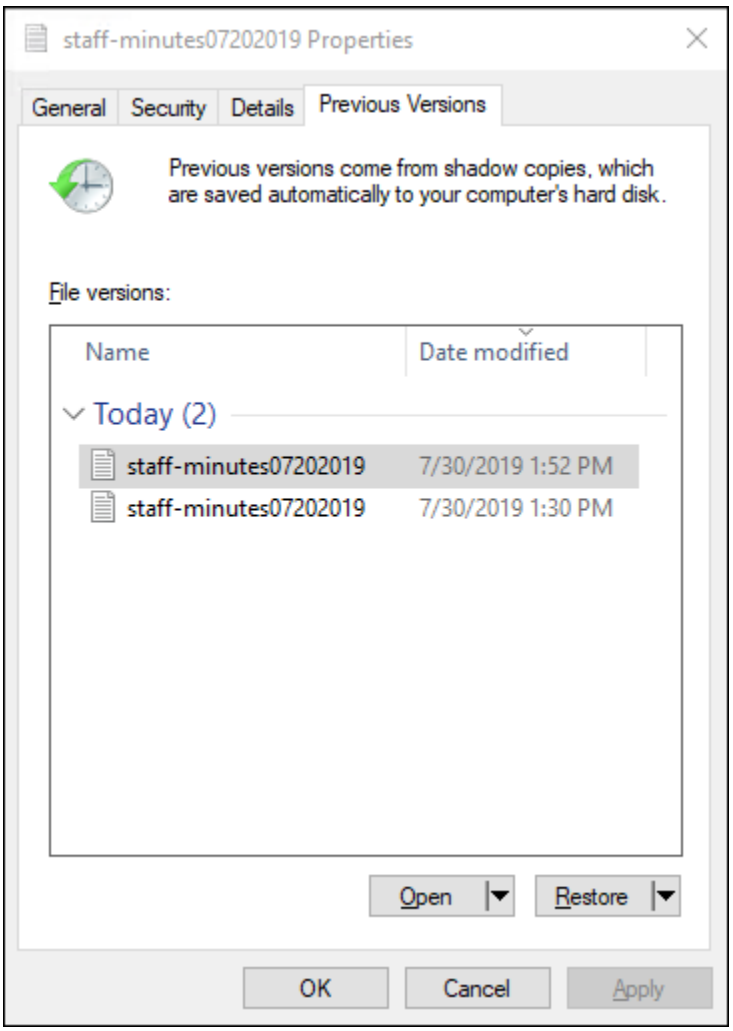
Restauration de fichiers et de dossiers individuels

Après avoir configuré des copies instantanées sur votre système de fichiers Amazon FSx, vos utilisateurs peuvent rapidement restaurer les versions précédentes de fichiers ou de dossiers individuels et récupérer les fichiers supprimés.

Les utilisateurs restaurent les fichiers aux versions précédentes à l'aide de l'interface familière de l'explorateur de fichiers Windows. Pour restaurer un fichier, vous choisissez le fichier à restaurer, puis choisissez Restaurer les versions précédentes dans le menu contextuel (clic droit).



Les utilisateurs peuvent ensuite consulter et restaurer une version précédente à partir de la liste des versions précédentes.



Définition de la quantité maximale de stockage de clichés instantanés

Vous définissez la quantité maximale de stockage que les clichés instantanés peuvent consommer sur un système de fichiers à l'aide de la PowerShell commande `Set-FsxShadowStorage` personnalisée. Vous pouvez définir la taille maximale que les clichés instantanés peuvent atteindre en utilisant les paramètres `-Maxsize` ou les `-Default` paramètres. L'utilisation `Default` définit le maximum à 10 % de la capacité de stockage du système de fichiers. Vous ne pouvez pas spécifier les `-Default` paramètres `-Maxsize` et dans la même commande.

À l'aide de`-Maxsize`, vous pouvez définir le stockage des clichés instantanés comme suit :

- En octets : `Set-FsxShadowStorage -Maxsize 2500000000`
- En kilo-octets, mégaoctets, gigaoctets ou autres unités : ou `Set-FsxShadowStorage -Maxsize (2500MB)` `Set-FsxShadowStorage -Maxsize (2.5GB)`
- En pourcentage du stockage global : `Set-FsxShadowStorage -Maxsize "20%"`

- Comme illimité : `Set-FsxShadowStorage -Maxsize "UNBOUNDED"`

`-Default`À utiliser pour configurer le stockage parallèle de manière à utiliser jusqu'à 10 % du système de fichiers :`Set-FsxShadowStorage -Default`. Pour en savoir plus sur l'utilisation de l'option par défaut, consultezConfiguration des clichés instantanés pour utiliser le stockage et la planification par défaut.

Pour définir la quantité de stockage de clichés instantanés sur un système de fichiers FSx for Windows File Server

1. Connectez-vous à une instance de calcul dotée d'une connectivité réseau avec votre système de fichiers en tant qu'utilisateur membre du groupe d'administrateurs du système de fichiers. Dans AWS Managed Microsoft AD, ce groupe est celui des AWS administrateurs FSx délégués. Dans votre Microsoft AD autogéré, il s'agit des administrateurs de domaine ou du groupe personnalisé que vous avez spécifié pour l'administration lors de la création de votre système de fichiers. Pour plus d'informations, consultez la section Connexion à votre instance Windows dans le guide de l'utilisateur Amazon EC2.
2. Ouvrez une PowerShell fenêtre Windows sur l'instance de calcul.
3. Utilisez la commande suivante pour ouvrir une PowerShell session à distance sur votre système de fichiers Amazon FSx. *`FSxFileSystem-Remote-PowerShell-Endpoint`*Remplacez-le par le PowerShell point de terminaison Windows Remote du système de fichiers que vous souhaitez administrer. Vous pouvez trouver le point de PowerShell terminaison Windows Remote dans la console Amazon FSx, dans la section Réseau et sécurité de l'écran des détails du système de fichiers ou dans la réponse à l'opération de l'`DescribeFileSystem`API.

   ```
   PS C:\Users\delegateadmin> enter-pssession -computername FSxFileSystem-Remote-
   PowerShell-Endpoint -configurationname fsxremoteadmin
   ```

4. Vérifiez que le stockage des clichés instantanés n'est pas déjà configuré sur le système de fichiers à l'aide de la commande suivante.

   ```
   [fs-1234567890abcef12]: PS>Get-FsxShadowStorage
   No Fsx Shadow Storage Configured
   ```

5. Réglez la quantité de stockage des ombres à 10 % du volume et le nombre maximum de zones d'ombres à 20 à l'aide de `-Default` cette option.

   ```
   [fs-1234567890abcef12]: PS>Set-FsxShadowStorage -Default
   ```

```
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- ------------------
             0         0 32530536858                 20
```

Vous pouvez limiter le nombre maximum de clichés instantanés autorisés sur votre système de fichiers en utilisant la `Set-FSxShadowStorage` commande associée au `-MaxShadowCopyNumber` paramètre et en spécifiant une valeur comprise entre 1 et 500. Par défaut, le nombre maximum de clichés instantanés est défini sur 20, comme le recommande Microsoft pour les charges de travail actives.

Afficher votre espace de stockage de clichés instantanés

Vous pouvez consulter la quantité de stockage actuellement consommée par les clichés instantanés sur votre système de fichiers à l'aide de la `Get-FsxShadowStorage` commande lors d'une PowerShell session à distance sur votre système de fichiers. Pour obtenir des instructions sur le lancement d'une PowerShell session à distance sur votre système de fichiers, consultezUtilisation de l'interface de ligne de commande Amazon FSx pour PowerShell.

```
[fs-1234567890abcef12]: PS>PS>Get-fsxshadowstorage
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- ------------------
             0         0 10737418240                 20
```

La sortie montre la configuration du stockage parallèle, comme suit :

- `AllocatedSpace`— La quantité de stockage sur le système de fichiers en octets actuellement allouée aux clichés instantanés. Au départ, cette valeur est 0.
- `UsedSpace`— La quantité de stockage, en octets, actuellement utilisée par les clichés instantanés. Au départ, cette valeur est 0.
- `MaxSpace`— La quantité maximale de stockage, en octets, que le stockage parallèle peut atteindre. Il s'agit de la valeur que vous définissez pour le stockage des clichés instantanés à l'aide de la `Set-FsxShadowStorage` commande.
- `MaxShadowCopyNumber`— Le nombre maximum de copies instantanées que le système de fichiers peut avoir, de 1 à 500.

Lorsque la `UsedSpace` quantité atteint la quantité maximale de stockage de clichés instantanés configurée (`MaxSpace`) ou que le nombre de clichés instantanés atteint le nombre maximal de clichés instantanés configuré (`MaxShadowCopyNumber`), le cliché instantané suivant que vous prenez remplace le cliché instantané le plus ancien. Si vous ne voulez pas perdre vos clichés instantanés les plus anciens, surveillez votre espace de stockage pour vous assurer que vous disposez d'un espace de stockage suffisant pour les nouveaux clichés instantanés. Si vous avez besoin de plus d'espace, vous pouvez supprimer des clichés instantanés existants ou augmenter la capacité maximale de stockage des clichés instantanés.

> **Note**
>
> Lorsque des clichés instantanés sont créés automatiquement ou manuellement, ils utilisent la quantité de stockage de clichés instantanés que vous avez configurée comme limite de stockage. La taille des clichés instantanés augmente au fil du temps et utilisent l'espace de stockage disponible indiqué par la CloudWatch `FreeStorageCapacity` métrique jusqu'à la quantité maximale de stockage de clichés instantanés configurée (`MaxSpace`).

Suppression du stockage des clichés instantanés, de la planification et de tous les clichés instantanés

Vous pouvez supprimer votre configuration de cliché instantané, y compris tous les clichés instantanés existants, ainsi que le calendrier des clichés instantanés. Dans le même temps, vous pouvez libérer le stockage des clichés instantanés sur le système de fichiers.

Pour ce faire, entrez la `Remove-FsxShadowStorage` commande dans une PowerShell session à distance sur votre système de fichiers. Pour obtenir des instructions sur le lancement d'une PowerShell session à distance sur votre système de fichiers, consultezUtilisation de l'interface de ligne de commande Amazon FSx pour PowerShell.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowStorage

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FsxShadowStorage" on target "Removing all Shadow
 Copies, Shadow Copy Schedule, and Shadow Storage".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y": Y
FSx Shadow Storage Configuration
```

```
Removing Shadow Copy Schedule
Removing Shadow Copies
All shadow copies removed.
Removing Shadow Storage
Shadow Storage removed successfully.
```

Création d'un calendrier personnalisé pour les clichés instantanés

Les planifications de clichés instantanés utilisent des déclencheurs de tâches planifiées dans Microsoft Windows pour spécifier à quel moment les clichés instantanés sont automatiquement réalisés. Un calendrier de copie instantanée peut avoir plusieurs déclencheurs, ce qui vous offre une grande flexibilité de planification. Il ne peut exister qu'un seul calendrier de clichés instantanés à la fois. Avant de créer un calendrier de cliché instantané, vous devez d'abord définir la quantité de stockage du cliché instantané.

Lorsque vous exécutez la `Set-FsxShadowCopySchedule` commande sur un système de fichiers, vous remplacez tout programme de cliché instantané existant. Si votre ordinateur client se trouve dans le fuseau horaire UTC, vous pouvez également spécifier le fuseau horaire d'un déclencheur à l'aide des fuseaux horaires Windows et de l'`-TimezoneId`option. Pour obtenir la liste des fuseaux horaires Windows, consultez la documentation du fuseau horaire par défaut de Microsoft ou exécutez ce qui suit à l'invite de commande Windows : `tzutil /l` Pour en savoir plus sur les déclencheurs de tâches Windows, consultez la section Déclencheurs de tâches dans la documentation du Microsoft Windows Developer Center.

Vous pouvez également utiliser `-Default` cette option pour configurer rapidement un calendrier de cliché instantané par défaut. Pour en savoir plus, veuillez consulter la section Configuration des clichés instantanés pour utiliser le stockage et la planification par défaut.

Pour créer un calendrier personnalisé de clichés instantanés

1. Créez un ensemble de déclencheurs de tâches planifiées Windows pour définir à quel moment les clichés instantanés sont pris dans le cadre du calendrier des clichés instantanés. Utilisez la `new-scheduledTaskTrigger` commande PowerShell sur votre machine locale pour définir plusieurs déclencheurs.

   L'exemple suivant crée un calendrier de clichés instantanés personnalisé qui prend des clichés instantanés du lundi au vendredi, à 6 h 00 et à 18 h 00 UTC. Par défaut, les heures sont exprimées en UTC, sauf si vous spécifiez un fuseau horaire dans les déclencheurs de tâches planifiées Windows que vous créez.

```
PS C:\Users\delegateadmin> $trigger1 = new-scheduledTaskTrigger -weekly -DaysOfWeek
 Monday,Tuesday,Wednesday,Thursday,Friday -at 06:00
PS C:\Users\delegateadmin> $trigger2 = new-scheduledTaskTrigger -weekly -DaysOfWeek
 Monday,Tuesday,Wednesday,Thursday,Friday -at 18:00
```

2. `invoke-command`À utiliser pour exécuter la `scriptblock` commande. Cela permet d'écrire un script qui définit le calendrier des clichés instantanés avec la `new-scheduledTaskTrigger` valeur que vous venez de créer. *`FSxFileSystem-Remote-PowerShell-Endpoint`*Remplacez-le par le PowerShell point de terminaison Windows Remote du système de fichiers que vous souhaitez administrer. Vous pouvez trouver le point de PowerShell terminaison Windows Remote dans la console Amazon FSx, dans la section Réseau et sécurité de l'écran des détails du système de fichiers ou dans la réponse à l'opération de l'`DescribeFileSystem`API.

```
PS C:\Users\delegateadmin> invoke-command -ComputerName FSxFileSystem-Remote-
PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {
```

3. Entrez la ligne suivante à l'>>invite pour définir votre calendrier de cliché instantané à l'aide de la `set-fsxshadowcopyschedule` commande.

```
>> set-fsxshadowcopyschedule -scheduledtasktriggers $Using:trigger1,$Using:trigger2
 -Confirm:$false }
```

La réponse affiche le calendrier des clichés instantanés que vous avez configuré sur le système de fichiers.

```
FSx Shadow Copy Schedule


Start Time:    : 2019-07-16T06:00:00+00:00
Days of Week   : Monday,Tuesday,Wednesday,Thursday,Friday
WeeksInterval  : 1
PSComputerName : fs-0123456789abcdef1
RunspaceId     : 12345678-90ab-cdef-1234-567890abcde1

Start Time:    : 2019-07-16T18:00:00+00:00
Days of Week   : Monday,Tuesday,Wednesday,Thursday,Friday
WeeksInterval  : 1
PSComputerName : fs-0123456789abcdef1
```

```
RunspaceId     : 12345678-90ab-cdef-1234-567890abcdef
```

Afficher le calendrier de vos clichés instantanés

Pour consulter le calendrier des clichés instantanés existant sur votre système de fichiers, entrez la commande suivante lors d'une PowerShell session à distance sur votre système de fichiers. Pour obtenir des instructions sur le lancement d'une PowerShell session à distance sur votre système de fichiers, consultezUtilisation de l'interface de ligne de commande Amazon FSx pour PowerShell.

```
[fs-0123456789abcdef1]PS> Get-FsxShadowCopySchedule
FSx Shadow Copy Schedule

Start Time                Days of week                              WeeksInterval
----------                ------------                              -------------
2019-07-16T07:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
2019-07-16T12:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
```

Supprimer un calendrier de cliché instantané

Pour supprimer le programme de clichés instantanés existant sur votre système de fichiers, entrez la commande suivante lors d'une PowerShell session à distance sur votre système de fichiers. Pour obtenir des instructions sur le lancement d'une PowerShell session à distance sur votre système de fichiers, consultezUtilisation de l'interface de ligne de commande Amazon FSx pour PowerShell.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopySchedule

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FsxShadowCopySchedule" on target "Removing FSx Shadow
 Copy Schedule".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y"): Y
[fs-0123456789abcdef1]PS>
```

Création d'un cliché instantané

Pour créer manuellement un cliché instantané, entrez la commande suivante dans une PowerShell session à distance sur votre système de fichiers. Pour obtenir des instructions sur le lancement d'une PowerShell session à distance sur votre système de fichiers, consultezUtilisation de l'interface de ligne de commande Amazon FSx pour PowerShell.

```
[fs-0123456789abcdef1]PS>New-FsxShadowCopy

Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} taken successfully
```

Afficher des clichés instantanés existants

Pour afficher l'ensemble des clichés instantanés existants sur votre système de fichiers, entrez la commande suivante lors d'une PowerShell session à distance sur votre système de fichiers. Pour obtenir des instructions sur le lancement d'une PowerShell session à distance sur votre système de fichiers, consultezUtilisation de l'interface de ligne de commande Amazon FSx pour PowerShell.

```
[fs-0123456789abcdef1]PS>Get-FsxShadowCopies
FSx Shadow Copies: 2 total

Shadow Copy ID                          Creation Time
--------------                          -----------------
{ABCDEF12-3456-7890-ABCD-EF1234567890} 6/17/2019 7:11:09 AM
{FEDCBA21-6543-0987-0987-EF3214567892} 6/19/2019 11:24:19 AM
```

Supprimer des clichés instantanés

Vous pouvez supprimer un ou plusieurs clichés instantanés existants sur votre système de fichiers à l'aide de la `Remove-FsxShadowCopies` commande lors d'une PowerShell session à distance sur votre système de fichiers. Pour obtenir des instructions sur le lancement d'une PowerShell session à distance sur votre système de fichiers, consultezUtilisation de l'interface de ligne de commande Amazon FSx pour PowerShell.

Spécifiez les clichés instantanés à supprimer à l'aide de l'une des options obligatoires suivantes :

- `-Oldest`supprime le cliché instantané le plus ancien
- `-All`supprime tous les clichés instantanés existants
- `-ShadowCopyId`supprime un cliché instantané spécifique par identifiant.

Vous ne pouvez utiliser qu'une seule option avec la commande. Une erreur se produit si vous ne spécifiez pas le cliché instantané à supprimer, si vous spécifiez plusieurs identifiants de cliché instantané ou si vous spécifiez un identifiant de cliché instantané non valide.

Pour supprimer le cliché instantané le plus ancien de votre système de fichiers, entrez la commande suivante lors d'une PowerShell session à distance sur votre système de fichiers.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopies -Oldest
Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FSxShadowCopies" on target "Removing oldest shadow
 copy".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y": Y
Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} deleted
```

Pour supprimer un cliché instantané spécifique de votre système de fichiers, entrez la commande suivante lors d'une PowerShell session à distance sur votre système de fichiers.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopies -ShadowCopyId "{ABCDEF12-3456-7890-
ABCD-EF1234567890}"
Are you sure you want to perform this action?
Performing the operation "Remove-FSxShadowCopies" on target "Removing shadow copy
 {ABCDEF12-3456-7890-ABCD-EF1234567890}".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y":>Y
Shadow Copy \\AMZNFSXABCDE123\root\cimv2:Wind32_ShadowCopy.ID{ABCDEF12-3456-7890-ABCD-
EF1234567890}".ID deleted.
```

Pour supprimer un certain nombre des clichés instantanés les plus anciens de votre système de fichiers, mettez à jour vos `-MaxShadowCopyNumber` paramètres en fonction du nombre de clichés instantanés que vous souhaitez conserver. Toutefois, cette modification ne prendra effet qu'après la prise du cliché instantané suivant, lorsque le système supprimera automatiquement les clichés instantanés excédentaires. Utilisez la commande suivante lors d'une PowerShell session à distance sur votre système de fichiers.

```
[fs-1234567890abcef12]: PS>Get-fsxshadowstorage
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace MaxSpace    MaxShadowCopyNumber
-------------- --------- ----------- -------------------
     556679168  21659648 10737418240                  50

[fs-1234567890abcef12]: PS>Set-FsxShadowStorage  -MaxShadowCopyNumber 5
Validation
You have 50 shadow copies. Older versions of shadow copies will be deleted, keeping 5
 latest shadow copies on your file system.
Do you want to continue?
[Y] Yes  [N] No  [?] Help (default is "N"): y
FSx Shadow Storage Configuration
```

```
AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- -------------------
     556679168  21659648 10737418240                   5
```

Réplication planifiée avec AWS DataSync

Vous pouvez l'utiliser AWS DataSync pour planifier la réplication périodique de votre système de fichiers FSx for Windows File Server vers un second système de fichiers. Cette fonctionnalité est disponible pour les déploiements régionaux et interrégionaux. Pour en savoir plus, consultez Migration de fichiers existants vers FSx for Windows File Server à l'aide de AWS DataSync ce guide et le transfert de données entre les services AWS de stockage dans le guide de AWS DataSync l'utilisateur.

Administration des systèmes de fichiers

Ce chapitre décrit comment accéder à la CLI Amazon FSx pour la gestion à distance et comment effectuer les tâches d'administration du système de fichiers disponibles. PowerShell Vous pouvez également utiliser l'interface utilisateur graphique (GUI) native de Microsoft Windows pour effectuer certaines tâches administratives.

Rubriques

Utilisation de l'interface de ligne de commande Amazon FSx pour PowerShell

L'interface de ligne de commande Amazon FSx pour la gestion à distance PowerShell permet l'administration du système de fichiers pour les utilisateurs du groupe des administrateurs du système de fichiers. Pour démarrer une PowerShell session à distance sur votre système de fichiers FSx for Windows File Server, vous devez d'abord remplir les conditions préalables suivantes :

- Être en mesure de vous connecter à une instance de calcul Windows dotée d'une connectivité réseau avec votre système de fichiers FSx for Windows File Server.

- Être connecté à l'instance de calcul Windows en tant que membre du groupe d'administrateurs du système de fichiers. Si vous utilisez AWS Managed Microsoft AD, il s'agit du groupe AWS Delegated FSx Administrators. Si vous utilisez un Microsoft Active Directory autogéré, il s'agit du groupe d'administrateurs de domaine ou du groupe personnalisé que vous avez spécifié pour l'administration lors de la création de votre système de fichiers. Pour plus d'informations, consultez Meilleures pratiques d'autogestion d'Active Directory.
- Les règles entrantes du groupe de sécurité VPC de votre système de fichiers autorisent le trafic sur le port 5985.

L'interface de ligne de commande Amazon FSx pour la gestion à distance PowerShell utilise les fonctionnalités de sécurité suivantes :

- Les informations d'identification de l'utilisateur sont authentifiées à l'aide de l'authentification Kerberos.
- Les communications de session de gestion entre le client connecté et le système de fichiers sont chiffrées à l'aide de Kerberos.

Deux options s'offrent à vous pour exécuter des commandes CLI de gestion à distance sur votre système de fichiers Amazon FSx :

- Vous pouvez établir une PowerShell session distante de longue durée et exécuter les commandes au sein de la session.
- Vous pouvez utiliser le `Invoke-Command` pour exécuter une seule commande ou un seul bloc de commandes sans établir une longue PowerShell session à distance.

Si vous souhaitez définir et transmettre des variables en tant que paramètres à la commande de gestion à distance, vous devez utiliser`Invoke-Command`.

> **Note**
>
> Pour les systèmes de fichiers multi-AZ, vous ne pouvez utiliser la CLI Amazon FSx pour la gestion à distance que lorsque le système de fichiers utilise son serveur de fichiers préféré. Pour plus d'informations, consultez Disponibilité et durabilité : systèmes de fichiers mono-AZ et multi-AZ.

Vous devez utiliser le point de PowerShell terminaison Windows Remote du système de fichiers lorsque vous utilisez la télécommande PowerShell. À l'aide de AWS Management Console, vous pouvez trouver le point de terminaison dans l'onglet Réseau et sécurité, sur la page des détails du système de fichiers. À l'aide de la AWS CLI `describe-file-systems` commande, la `RemoteAdministrationEndpoint` propriété est renvoyée dans la réponse. Le point de terminaison d'administration à distance utilise le format`amznfsxctlyaa1k.`*`ActiveDirectory-DNS-name`*, par exemple,`amznfsxctlyaa1k.corp.example.com`.

Vous pouvez utiliser l'`Get-Command`applet de commande pour obtenir des informations sur les applets de commande, les fonctions et les alias disponibles dans. PowerShell Pour plus d'informations, consultez la documentation Microsoft Get-Command.

Vous pouvez également exécuter la CLI Amazon FSx pour la gestion à distance sur des PowerShell commandes de votre système de fichiers à l'aide de l'`Invoke-Command`applet de commande, en utilisant la syntaxe suivante.

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName
 amznfsxctlyaa1k.corp.example.com -ConfigurationName FSxRemoteAdmin -scriptblock { fsx-
command}
```

Pour savoir comment démarrer une PowerShell session à distance de longue durée sur votre système de fichiers FSx for Windows File Server, voir Démarrage d'une session à distance Amazon FSx PowerShell

Démarrage d'une session à distance Amazon FSx PowerShell

Cette rubrique fournit des instructions pour démarrer une PowerShell session à distance de longue durée sur votre serveur de fichiers FSx for Windows File Server.

Pour démarrer une PowerShell session à distance sur votre système de fichiers

1. Connectez-vous à une instance de calcul dotée d'une connectivité réseau avec votre système de fichiers en tant qu'utilisateur membre du groupe d'administrateurs FSx délégué que vous avez choisi lors de la création du système de fichiers.
2. Ouvrez une PowerShell fenêtre Windows sur l'instance de calcul.
3. Dans le PowerShell, entrez la commande suivante pour ouvrir une session à distance de longue durée sur votre système de fichiers Amazon FSx. *`Remote-PowerShell-Endpoint`*Remplacez-le par le PowerShell point de terminaison Windows Remote du système

de fichiers que vous souhaitez administrer. À utiliser `FsxRemoteAdmin` comme nom de configuration de session.

```
PS C:\Users\delegateadmin> enter-pssession -ComputerName Remote-PowerShell-Endpoint
 -ConfigurationName FsxRemoteAdmin
[fs-0123456789abcdef0]: PS>
```

Si votre instance ne fait pas partie du domaine Amazon FSx Active Directory, vous êtes invité à saisir les informations d'identification de l'utilisateur dans une fenêtre contextuelle. Entrez les informations d'identification de l'utilisateur membre du groupe d'administrateurs FSx. Si votre instance est jointe au domaine, aucune information d'identification ne vous sera demandée.

Gestion des alias DNS

FSx for Windows File Server fournit un nom de système de noms de domaine (DNS) par défaut pour chaque système de fichiers que vous pouvez utiliser pour accéder aux données de votre système de fichiers. Vous pouvez également accéder à vos systèmes de fichiers à l'aide d'un alias DNS de votre choix. Avec les alias DNS, vous pouvez continuer à utiliser les noms DNS existants pour accéder aux données stockées sur Amazon FSx lors de la migration du stockage du système de fichiers sur site vers Amazon FSx, sans avoir à mettre à jour d'outils ou d'applications. Pour plus d'informations, consultez Migration du stockage de fichiers existant vers Amazon FSx.

> **Note**
>
> Support pour les alias DNS est disponible sur les systèmes de fichiers FSx for Windows File Server créés après 12 h 00 ET le 9 novembre 2020. Pour utiliser des alias DNS sur un système de fichiers créé avant 12 h 00 ET le 9 novembre 2020, procédez comme suit :
>
> 1. Effectuez une sauvegarde du système de fichiers existant. Pour plus d'informations, consultez Utilisation de sauvegardes initiées par l'utilisateur.
> 2. Restaurez la sauvegarde sur un nouveau système de fichiers. Pour plus d'informations, consultez Restauration des sauvegardes.
>
> Une fois le nouveau système de fichiers disponible, vous pourrez utiliser des alias DNS pour y accéder, en utilisant les informations fournies dans cette section.

> **Note**
>
> Les informations présentées ici supposent que vous travaillez entièrement dans Active Directory et que vous n'utilisez pas de fournisseurs DNS externes. Les fournisseurs DNS tiers peuvent provoquer un comportement inattendu.
> Amazon FSx enregistre les enregistrements DNS pour un système de fichiers uniquement si le domaine AD auquel vous le joignez utilise le DNS Microsoft comme DNS par défaut.
> Si vous utilisez un DNS tiers, vous devrez configurer manuellement les entrées DNS pour vos systèmes de fichiers Amazon FSx après avoir créé votre système de fichiers. Pour plus d'informations sur le choix des adresses IP correctes à utiliser pour le système de fichiers, consultezObtention des adresses IP de système de fichiers correctes à utiliser pour le DNS.

Vous pouvez associer des alias DNS aux systèmes de fichiers FSx for Windows File Server existants, lorsque vous créez de nouveaux systèmes de fichiers ou lorsque vous créez un nouveau système de fichiers à partir d'une sauvegarde. Vous pouvez associer jusqu'à 50 alias DNS à un système de fichiers à la fois.

Outre l'association d'alias DNS à votre système de fichiers, pour que les clients puissent se connecter au système de fichiers à l'aide des alias DNS, vous devez également effectuer les opérations suivantes :

- Configurez les noms principaux de service (SPN) pour l'authentification et le chiffrement Kerberos.
- Configurez un enregistrement DNS CNAME pour l'alias DNS qui correspond au nom DNS par défaut de votre système de fichiers Amazon FSx.

Pour plus d’informations, consultez Procédure pas à pas 5 : Utilisation d'alias DNS pour accéder à votre système de fichiers.

Un nom d'alias DNS pour votre système de fichiers FSx for Windows File Server doit répondre aux exigences suivantes :

- Doit être formaté en tant que nom de domaine complet (FQDN).
- Peut contenir des caractères alphanumériques et des tirets (-).
- Il ne peut pas commencer ni se terminer par un trait d'union.
- Il peut commencer par un caractère numérique.

Pour les noms d'alias DNS, Amazon FSx stocke les caractères alphabétiques sous forme de lettres minuscules (a-z), quelle que soit la manière dont vous les spécifiez : lettres majuscules, lettres minuscules ou lettres correspondantes sous forme de codes d'échappement.

Si vous essayez d'associer un alias déjà associé au système de fichiers, cela n'a aucun effet. Si vous essayez de dissocier un alias d'un système de fichiers qui n'est pas associé au système de fichiers, Amazon FSx répond avec une erreur de demande incorrecte.

> **Note**
>
> Lorsqu'Amazon FSx ajoute ou supprime des alias sur un système de fichiers, les clients connectés sont temporairement déconnectés et se reconnectent automatiquement au système de fichiers. Tous les fichiers ouverts par des clients mappant un partage non disponible en continu (non CA) au moment de la déconnexion doivent être rouverts par le client.

Rubriques

État de l'alias DNS

Les alias DNS peuvent avoir l'une des valeurs d'état suivantes :

- Disponible — L'alias DNS est associé à un système de fichiers Amazon FSx.
- Création : Amazon FSx crée l'alias DNS et l'associe au système de fichiers.
- Suppression : Amazon FSx dissocie l'alias DNS du système de fichiers et le supprime.
- Impossible de créer : Amazon FSx n'a pas pu associer l'alias DNS au système de fichiers.
- Impossible de supprimer : Amazon FSx n'a pas pu dissocier l'alias DNS du système de fichiers.

Utilisation d'alias DNS avec authentification Kerberos

Nous vous recommandons d'utiliser l'authentification et le chiffrement basés sur Kerberos lors du transit avec Amazon FSx. Kerberos fournit l'authentification la plus sécurisée pour les clients accédant à votre système de fichiers. Pour activer l'authentification Kerberos pour les clients qui accèdent à votre système de fichiers Amazon FSx à l'aide d'un alias DNS, vous devez configurer les noms principaux de service (SPN) qui correspondent à l'alias DNS sur l'objet informatique Active Directory de votre système de fichiers.

Si vous avez configuré des SPN pour l'alias DNS que vous avez attribué à un autre système de fichiers sur un objet informatique de votre Active Directory, vous devez d'abord supprimer ces SPN avant d'ajouter des SPN à l'objet informatique de votre système de fichiers. Pour plus d'informations, consultez Procédure pas à pas 5 : Utilisation d'alias DNS pour accéder à votre système de fichiers.

Affichage des alias DNS pour les systèmes de fichiers et les sauvegardes

Vous pouvez voir les alias DNS actuellement associés aux systèmes de fichiers et aux sauvegardes à l'aide de la console Amazon FSx, de la AWS CLI et de l'API. Cette rubrique fournit des instructions sur la façon d'afficher les alias DNS de vos systèmes de fichiers et de vos sauvegardes.

Pour afficher les alias DNS associés aux systèmes de fichiers

- Utilisation de la console : choisissez un système de fichiers pour afficher la page détaillée des systèmes de fichiers. Choisissez l'onglet Réseau et sécurité pour afficher les alias DNS.
- Utilisation de la CLI ou de l'API : utilisez la commande `describe-file-system-aliases` CLI ou l'opération DescribeFileSystemAliasesAPI.

Pour afficher les alias DNS associés aux sauvegardes

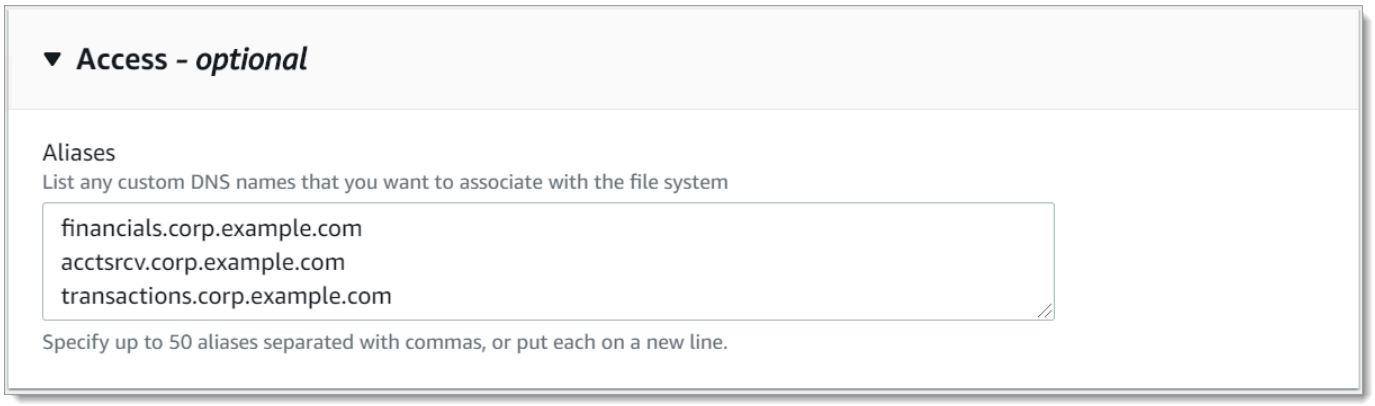
- Utilisation de la console : dans le volet de navigation, choisissez Backups, puis choisissez la sauvegarde que vous souhaitez consulter. Dans le volet Résumé, consultez le champ Alias DNS.
- Utilisation de la CLI ou de l'API : utilisez la commande `describe-backups` CLI ou l'opération DescribeBackupsAPI.

Associer des alias DNS à des systèmes de fichiers

Cette rubrique explique comment associer des alias DNS lors de la création d'un nouveau système de fichiers FSx for Windows File Server à partir de zéro, ou lors de la création d'un système de fichiers à partir d'une sauvegarde, à l'aide de l' AWS Management Console API AWS CLI, et.

Pour associer des alias DNS lors de la création d'un nouveau système de fichiers (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Suivez la procédure de création d'un nouveau système de fichiers décrite Créez votre système de fichiers dans la section Mise en route.
3. Dans la section Accès - facultatif de l'assistant de création de système de fichiers, entrez les alias DNS que vous souhaitez associer à votre système de fichiers.



4. Lorsque le système de fichiers est disponible, vous pouvez y accéder à l'aide de l'alias DNS en configurant les noms principaux des services (SPN) et en mettant à jour ou en créant un enregistrement DNS CNAME pour l'alias. Pour plus d'informations, consultez Procédure pas à pas 5 : Utilisation d'alias DNS pour accéder à votre système de fichiers.

Pour associer des alias DNS lors de la création d'un nouveau système de fichiers (CLI) Amazon FSx

1. Lorsque vous créez un nouveau système de fichiers, utilisez la propriété Alias avec l'opération d'CreateFileSystemAPI pour associer des alias DNS au nouveau système de fichiers.

```
aws fsx create-file-system \
  --file-system-type WINDOWS \
  --storage-capacity 2000 \
  --storage-type SSD \
  --subnet-ids subnet-123456 \
```

```
  --windows-configuration Aliases=[financials.corp.example.com,accts-
rcv.corp.example.com]
```

2. Lorsque le système de fichiers est disponible, vous pouvez y accéder à l'aide de l'alias DNS en configurant les noms principaux des services (SPN) et en mettant à jour ou en créant un enregistrement DNS CNAME pour l'alias. Pour plus d'informations, consultez Procédure pas à pas 5 : Utilisation d'alias DNS pour accéder à votre système de fichiers.

Pour ajouter ou supprimer des alias DNS lors de la restauration d'une sauvegarde (CLI)

1. Lorsque vous créez un nouveau système de fichiers à partir d'une sauvegarde d'un système de fichiers existant, vous pouvez utiliser la propriété Aliases avec l'opération d'CreateFileSystemFromBackupAPI comme suit :

   - Tous les alias associés à la sauvegarde sont associés au nouveau système de fichiers par défaut.
   - Pour créer un système de fichiers sans conserver les alias de la sauvegarde, utilisez la `Aliases` propriété avec un ensemble vide.

     Pour associer des alias DNS supplémentaires, utilisez la `Aliases` propriété et incluez à la fois les alias d'origine associés à la sauvegarde et les nouveaux alias que vous souhaitez associer.

   La commande CLI suivante associe deux alias au système de fichiers qu'Amazon FSx est en train de créer à partir d'une sauvegarde.

   ```
   aws fsx create-file-system-from-backup \
     --backup-id backup-0123456789abcdef0
     --storage-capacity 2000 \
     --storage-type HDD \
     --subnet-ids subnet-123456 \
     --windows-configuration Aliases=[transactions.corp.example.com,accts-
   rcv.corp.example.com]
   ```

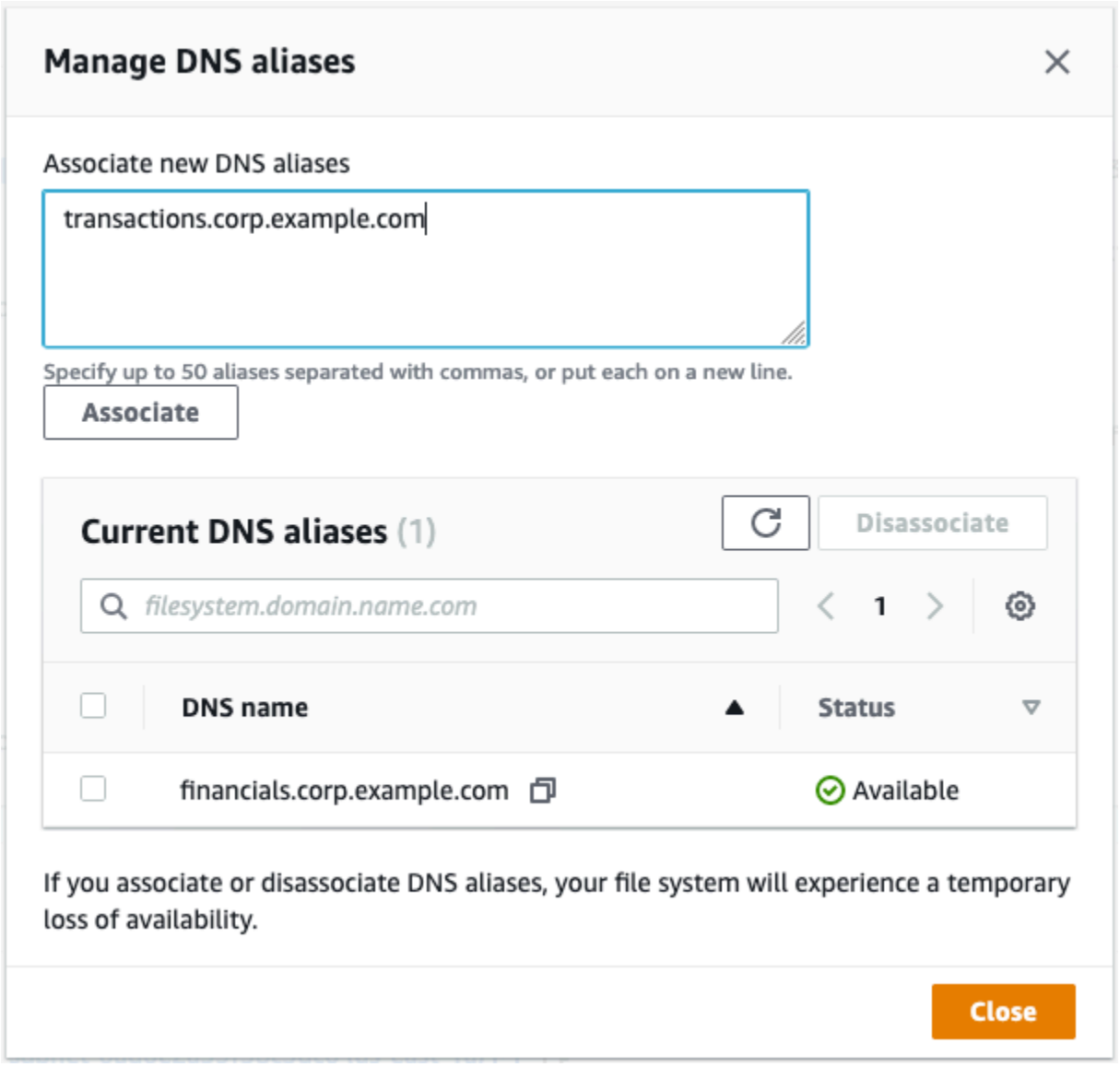
2. Lorsque le système de fichiers est disponible, vous pouvez y accéder à l'aide de l'alias DNS en configurant les noms principaux des services (SPN) et en mettant à jour ou en créant un enregistrement DNS CNAME pour l'alias. Pour plus d'informations, consultez Procédure pas à pas 5 : Utilisation d'alias DNS pour accéder à votre système de fichiers.

Gestion des alias DNS sur les systèmes de fichiers existants

Cette rubrique décrit comment utiliser le AWS Management Console et AWS CLI pour ajouter et supprimer des alias sur les systèmes de fichiers existants.

Pour gérer les alias DNS des systèmes de fichiers (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Accédez à Systèmes de fichiers, puis choisissez le système de fichiers Windows pour lequel vous souhaitez gérer les alias DNS.
3. Dans l'onglet Réseau et sécurité, choisissez Gérer les alias DNS pour afficher la boîte de dialogue Gérer les alias DNS.



- Pour associer des alias DNS : dans le champ Associer de nouveaux alias, entrez les alias DNS que vous souhaitez associer. Choisissez Associer.
- Pour dissocier les alias DNS : dans la liste des alias actuels, choisissez les alias dont vous souhaitez vous dissocier. Choisissez Dissocier.

Vous pouvez contrôler l'état des alias que vous avez gérés dans la liste des alias actuels. Actualisez la liste pour mettre à jour le statut. Il faut jusqu'à 2,5 minutes pour qu'un alias soit associé ou dissocié d'un système de fichiers.

4. Lorsque l'alias est disponible, vous pouvez accéder à votre système de fichiers à l'aide de l'alias DNS en configurant les noms principaux de service (SPN) et en mettant à jour ou en créant un enregistrement DNS CNAME pour l'alias. Pour plus d'informations, consultez Procédure pas à pas 5 : Utilisation d'alias DNS pour accéder à votre système de fichiers.

Pour associer des alias DNS à des systèmes de fichiers existants (CLI)

1. Utilisez la commande `associate-file-system-aliases` CLI ou l'opération AssociateFileSystemAliasesAPI pour associer des alias DNS à un système de fichiers existant.

   La requête CLI suivante associe deux alias au système de fichiers spécifié.

```
aws fsx associate-file-system-aliases \
  --file-system-id fs-0123456789abcdef0 \
  --aliases financials.corp.example.com transfers.corp.example.com
```

   La réponse indique l'état des alias qu'Amazon FSx associe au système de fichiers.

```
{
    "Aliases": [
        {
            "Name": "financials.corp.example.com",
            "Lifecycle": CREATING
        },
        {
            "Name": "transfers.corp.example.com",
            "Lifecycle": CREATING
        }
    ]
```

```
}
```

2. Utilisez la commande `describe-file-system-aliases` CLI (DescribeFileSystemAliasesopération d'API équivalente) pour surveiller l'état des alias que vous associez.
3. Lorsque la valeur de AVAILABLE `Lifecycle` est disponible (un processus qui prend jusqu'à 2,5 minutes), vous pouvez accéder à votre système de fichiers à l'aide de l'alias DNS en configurant les noms principaux des services (SPN) et en mettant à jour ou en créant un enregistrement DNS CNAME pour l'alias. Pour plus d'informations, consultez Procédure pas à pas 5 : Utilisation d'alias DNS pour accéder à votre système de fichiers.

Pour dissocier les alias DNS des systèmes de fichiers (CLI)

- Utilisez la commande `disassociate-file-system-aliases` CLI ou l'opération DisassociateFileSystemAliasesAPI pour dissocier les alias DNS d'un système de fichiers existant.

  La commande suivante dissocie un alias d'un système de fichiers.

  ```
  aws fsx disassociate-file-system-aliases \
    --file-system-id fs-0123456789abcdef0 \
    --aliases financials.corp.example.com
  ```

  La réponse indique l'état des alias qu'Amazon FSx dissocie du système de fichiers.

  ```
  {
      "Aliases": [
          {
              "Name": "financials.corp.example.com",
              "Lifecycle": DELETING
          }
      ]
  }
  ```

  Utilisez la commande `describe-file-system-aliases` CLI (DescribeFileSystemAliasesopération d'API équivalente) pour surveiller l'état des alias. La suppression de l'alias prend jusqu'à 2,5 minutes.

Gestion des partages de fichiers sur les systèmes de fichiers FSx for Windows File Server

Cette rubrique décrit comment gérer les partages de fichiers en effectuant les tâches suivantes.

- Création d'un nouveau partage de fichiers
- Modifier un partage de fichiers existant
- Supprimer un partage de fichiers existant

Vous pouvez utiliser l'interface graphique des dossiers partagés native pour Windows et la CLI Amazon FSx pour la gestion à distance PowerShell afin de gérer les partages de fichiers sur votre système de fichiers FSx for Windows File Server. Vous pouvez rencontrer des retards lors de l'utilisation de l'interface graphique des dossiers partagés (fsmgmt.msc) lors de la première ouverture du menu contextuel pour les partages situés sur un autre système de fichiers. Pour éviter ces retards, utilisez-le PowerShell pour gérer les partages de fichiers situés sur plusieurs systèmes de fichiers.

Notez que des règles et des limitations sont requises pour tous les systèmes de fichiers pris en charge par Windows en ce qui concerne les noms de fichiers et de répertoires. ». Pour vous assurer que vous pouvez créer et accéder à vos données avec succès, vous devez nommer vos fichiers et répertoires conformément à ces directives Windows. Pour plus d'informations, consultez la section Conventions de dénomination.

> ⚠ Warning
>
> Amazon FSx exige que l'utilisateur du SYSTÈME dispose des autorisations ACL NTFS de contrôle total sur chaque dossier dans lequel vous créez un partage de fichiers SMB. Ne modifiez pas les autorisations ACL NTFS de cet utilisateur sur vos dossiers, car cela pourrait rendre vos partages de fichiers inaccessibles.

Gestion des partages de fichiers à l'aide de l'interface graphique des dossiers partagés

Pour gérer les partages de fichiers sur votre système de fichiers Amazon FSx, vous pouvez utiliser l'interface graphique des dossiers partagés. L'interface graphique des dossiers partagés fournit un

emplacement central pour gérer tous les dossiers partagés sur un serveur Windows. Les procédures suivantes décrivent comment gérer vos partages de fichiers.

Pour connecter des dossiers partagés à votre système de fichiers FSx for Windows File Server

1. Lancez votre instance Amazon EC2 et connectez-la au Microsoft Active Directory auquel votre système de fichiers Amazon FSx est joint. Pour ce faire, choisissez l'une des procédures suivantes dans le guide AWS Directory Service d'administration :

   - Joindre facilement une instance Windows EC2
   - Joindre manuellement une instance Windows

2. Connectez-vous à votre instance en tant qu'utilisateur membre du groupe des administrateurs du système de fichiers. Dans AWS Managed Microsoft Active Directory, ce groupe est appelé AWS Administrateurs FSx délégués. Dans votre Microsoft Active Directory autogéré, ce groupe est appelé Administrateurs de domaine ou le nom personnalisé du groupe d'administrateurs que vous avez indiqué lors de sa création. Pour plus d'informations, consultez Connect to your Windows instance dans le guide de l'utilisateur Amazon Elastic Compute Cloud pour les instances Windows.
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 du système de noms de domaine (DNS) de votre système de fichiers Amazon FSx, par exemple. **`amznfsxabcd0123.corp.example.com`**

   Pour trouver le nom DNS de votre système de fichiers sur la console Amazon FSx, choisissez Systèmes de fichiers, choisissez votre système de fichiers, puis consultez la section Réseau et sécurité de la page de détails du système de fichiers. Vous pouvez également obtenir le nom DNS dans la réponse à l'opération de l'API DescribeFileSystems.
6. Choisissez OK. Une entrée pour votre système de fichiers Amazon FSx apparaît ensuite dans la liste de l'outil Dossiers partagés.

Maintenant que Shared Folders est connecté à votre système de fichiers Amazon FSx, vous pouvez gérer les partages de fichiers Windows sur le système de fichiers. Le partage par défaut est appelé`\share`. Vous pouvez le faire à l'aide des actions suivantes :

- Créer un nouveau partage de fichiers : dans l'outil Dossiers partagés, choisissez Shares dans le volet de gauche pour voir les partages actifs de votre système de fichiers Amazon FSx. 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 : cliquez sur « Parcourir » lorsque vous spécifiez le chemin du dossier local et cliquez sur « Créer un nouveau dossier » pour créer le dossier local.
  - À l'aide de la ligne de commande :

    ```
    New-Item -Type Directory -Path \\amznfsxabcd0123.corp.example.com\D$\share
    \MyNewShare
    ```

- 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**
>
> Pour les systèmes de fichiers mono-AZ 2 et multi-AZ, il est possible de supprimer des partages de fichiers ou de modifier des partages de fichiers (y compris la mise à jour des autorisations, des limites d'utilisateur et d'autres propriétés) à l'aide de l'outil graphique Shared Folders uniquement si vous vous connectez à fsmgmt.msc en utilisant le nom DNS du système de fichiers Amazon FSx. L'outil graphique des dossiers partagés ne prend pas en charge ces actions si vous vous connectez à l'aide de l'adresse IP ou du nom d'alias DNS du système de fichiers.

> **Note**
>
> Si vous utilisez l'outil graphique des dossiers partagés fsmgmt.msc pour accéder à des partages situés sur plusieurs systèmes de fichiers FSx, vous risquez de rencontrer des retards lorsque vous ouvrez pour la première fois le menu contextuel de partage de fichiers

pour un partage situé sur un autre système de fichiers. Pour éviter ces retards, vous pouvez gérer les partages de fichiers PowerShell en suivant les instructions ci-dessous.

Gestion des partages de fichiers avec PowerShell

Vous pouvez gérer les partages de fichiers à l'aide de commandes de gestion à distance personnalisées pour. PowerShell Les commandes suivantes peuvent vous aider à automatiser plus facilement ces tâches :

- Migration des partages de fichiers sur des serveurs de fichiers existants vers Amazon FSx
- Synchronisation des partages de fichiers entre AWS les régions pour la reprise après sinistre
- Gestion programmatique des partages de fichiers pour les flux de travail permanents, tels que le provisionnement du partage de fichiers en équipe

Pour savoir comment utiliser l'interface de ligne de commande Amazon FSx pour la gestion à distance PowerShell, consultez. Utilisation de l'interface de ligne de commande Amazon FSx pour PowerShell

Le tableau suivant répertorie les PowerShell commandes de gestion à distance de la CLI Amazon FSx que vous pouvez utiliser pour gérer les partages de fichiers sur les systèmes de fichiers FSx for Windows File Server.

Commande de gestion de partage	Description
New-FSxSmbShare	Crée un nouveau partage de fichiers.
Remove-FSxSmbShare	Supprime un partage de fichiers.
Get-FSxSmbShare	Récupère les partages de fichiers existants.
Set-FSxSmbShare	Définit les propriétés d'un partage.
Get-FSxSmbShareAccess	Récupère la liste de contrôle d'accès (ACL) d'un partage.
Grant-FSxSmbShareAccess	Ajoute une entrée de contrôle d'accès (ACE) pour un administr ateur au descripteur de sécurité d'un partage.

Commande de gestion de partage	Description
Revoke-FSxSmbShareAccess	Supprime tous les ACE autorisés pour un administrateur du descripteur de sécurité d'un partage.
Block-FSxSmbShareAccess	Ajoute un ACE de refus pour un administrateur au descripteur de sécurité d'un partage.
Unblock-FSxSmbShareAccess	Supprime tous les ACE de refus d'un administrateur du descripteur de sécurité d'un partage.

L'aide en ligne de chaque commande fournit une référence de toutes les options de commande. Pour accéder à cette aide, exécutez la commande avec un`-?`, par exemple`New-FSxSmbShare -?`.

Transmission des informations d'identification à New-F Share SxSmb

Vous pouvez transmettre des informations d'identification à New-F SxSmbShare afin de pouvoir l'exécuter en boucle pour créer des centaines ou des milliers de partages sans avoir à saisir à nouveau les informations d'identification à chaque fois.

Préparez l'objet d'identification requis pour créer les partages de fichiers sur votre serveur de fichiers FSx for Windows File Server à l'aide de l'une des options suivantes.

- Pour générer l'objet d'identification de manière interactive, utilisez la commande suivante.

```
$credential = Get-Credential
```

- Pour générer l'objet d'identification à l'aide d'une AWS Secrets Manager ressource, utilisez la commande suivante.

```
$credential = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
 $AdminSecret).SecretString
$FSxAdminUserCredential = (New-Object PSCredential($credential.UserName,(ConvertTo-
SecureString $credential.Password -AsPlainText -Force)))
```

Création d'un partage disponible en continu (CA)

Vous pouvez créer des partages disponibles en continu (CA) à l'aide de la CLI Amazon FSx pour la gestion à distance sur. PowerShell Les partages CA créés sur un système de fichiers multi-AZ FSx for Windows File Server sont extrêmement durables et hautement disponibles. Un système de fichiers Amazon FSx Single-AZ est construit sur un cluster à nœud unique. Par conséquent, les partages CA créés sur un système de fichiers mono-AZ sont très durables, mais ne sont pas hautement disponibles. Utilisez la `New-FSxSmbShare` commande avec l'`-ContinuouslyAvailable`option définie sur `$True` pour spécifier que le partage est un partage disponible en permanence. Voici un exemple de commande permettant de créer un partage CA.

```
New-FSxSmbShare -Name "New CA Share" -Path "D:\share\new-share" -Description "CA share"
 -ContinuouslyAvailable $True
```

Vous pouvez modifier l'`-ContinuouslyAvailable`option sur un partage de fichiers existant à l'aide de la `Set-FSxSmbShare` commande.

Déterminer si un partage de fichiers existant est disponible en permanence

Utilisez la commande suivante pour afficher la valeur de la propriété Continuellement disponible pour un partage de fichiers existant.

```
Invoke-Command -ComputerName powershell_endpoint -ConfigurationName FSxRemoteAdmin -
scriptblock { get-fsxsmbshare -name share_name }
```

Si CA est activé, la sortie inclura la ligne suivante :

```
[...]
ContinuouslyAvailable : True
[...]
```

Si CA n'est pas activé, la sortie inclura la ligne suivante :

```
[...]
ContinuouslyAvailable : False
[...]
```

Pour activer la disponibilité continue sur un partage de fichiers existant, utilisez la commande suivante :

```
Invoke-Command -ComputerName powershell_endpoint -ConfigurationName FSxRemoteAdmin -
scriptblock { set-fsxsmbshare -name share_name -ContinuouslyAvailable $True}
```

Audit de l'accès aux fichiers

Amazon FSx for Windows File Server prend en charge l'audit de l'accès des utilisateurs finaux aux fichiers, aux dossiers et aux partages de fichiers. Vous pouvez choisir d'envoyer les journaux des événements d'audit d'un système de fichiers à d'autres AWS services proposant un ensemble complet de fonctionnalités. Il s'agit notamment de permettre l'interrogation, le traitement, le stockage et l'archivage des journaux, l'émission de notifications et le déclenchement d'actions pour améliorer encore vos objectifs de sécurité et de conformité.

Pour plus d'informations sur l'utilisation de l'audit d'accès aux fichiers pour obtenir des informations sur les modèles d'accès et implémenter des notifications de sécurité pour l'activité des utilisateurs finaux, consultez les sections Informations sur les modèles d'accès au stockage de fichiers et Implémentation de notifications de sécurité pour l'activité des utilisateurs finaux.

L'audit d'accès aux fichiers vous permet d'enregistrer les accès des utilisateurs finaux à des fichiers, dossiers et partages de fichiers individuels en fonction des contrôles d'audit que vous avez définis. Les contrôles d'audit sont également appelés listes de contrôle d'accès au système NTFS (SACL). Si vous avez déjà configuré des contrôles d'audit sur vos données de fichiers existantes, vous pouvez tirer parti de l'audit d'accès aux fichiers en créant un nouveau système de fichiers Amazon FSx for Windows File Server et en migrant vos données.

Amazon FSx prend en charge les événements d'audit Windows suivants pour les accès aux fichiers, aux dossiers et aux partages de fichiers :

- Pour les accès aux fichiers, il prend en charge : Tout, Traverser le dossier/Exécuter le fichier, Lister le dossier/Lire les données, Lire les attributs, créer des fichiers/Écrire des données, créer des dossiers/Ajouter des données, Écrire des attributs, supprimer des sous-dossiers et des fichiers, supprimer, lire les autorisations, modifier les autorisations et prendre possession.
- Pour les accès au partage de fichiers, il prend en charge : Se connecter à un partage de fichiers.

Pour les accès aux fichiers, aux dossiers et aux partages de fichiers, Amazon FSx prend en charge la journalisation des tentatives réussies (par exemple, lorsqu'un utilisateur disposant des autorisations suffisantes accède à un fichier ou à un partage de fichiers), des tentatives infructueuses, ou les deux.

Vous pouvez configurer si vous souhaitez un audit d'accès uniquement sur les fichiers et les dossiers, uniquement sur les partages de fichiers, ou les deux. Vous pouvez également configurer les types d'accès qui doivent être enregistrés (tentatives réussies uniquement, tentatives infructueuses uniquement, ou les deux). Vous pouvez également désactiver l'audit d'accès aux fichiers à tout moment.

> **Note**
>
> L'audit d'accès aux fichiers enregistre les données d'accès des utilisateurs finaux uniquement à partir du moment où il est activé. En d'autres termes, l'audit de l'accès aux fichiers ne génère pas de journaux des événements d'audit des activités d'accès aux fichiers, aux dossiers et aux partages de fichiers de l'utilisateur final survenues avant l'activation de l'audit d'accès aux fichiers.

Le taux maximum d'événements d'audit d'accès pris en charge est de 5 000 événements par seconde. Les événements d'audit d'accès ne sont pas générés pour chaque opération de lecture et d'écriture de fichier, mais une fois par opération de métadonnées de fichier, par exemple lorsqu'un utilisateur crée, ouvre ou supprime un fichier.

Rubriques

Auditer les destinations des journaux d'événements

Lorsque vous activez l'audit d'accès aux fichiers, vous devez configurer un AWS service auquel Amazon FSx envoie les journaux des événements d'audit. Vous pouvez envoyer des journaux d'événements d'audit à un flux de CloudWatch journaux Amazon Logs d'un groupe de CloudWatch journaux Logs ou à un flux de diffusion Amazon Data Firehose. Vous choisissez la destination des journaux d'événements d'audit soit lorsque vous créez votre système de fichiers Amazon FSx for Windows File Server, soit à tout moment par la suite en mettant à jour un système de fichiers existant. Pour plus d’informations, consultez Gestion de l'audit des accès aux fichiers.

Voici quelques recommandations qui peuvent vous aider à choisir la destination des journaux des événements d'audit :

- Choisissez CloudWatch Logs si vous souhaitez stocker, consulter et rechercher des journaux d'événements d'audit dans la CloudWatch console Amazon, exécuter des requêtes sur les journaux à l'aide CloudWatch de Logs Insights et déclencher des CloudWatch alarmes ou des fonctions Lambda.
- Choisissez Firehose si vous souhaitez diffuser en continu des événements vers le stockage d'Amazon S3, vers une base de données d'Amazon Redshift, vers OpenSearch Amazon Service ou vers des solutions partenaires (telles que Splunk ou Datadog) AWS pour une analyse plus approfondie.

Par défaut, Amazon FSx crée et utilise un groupe de CloudWatch journaux par défaut dans votre compte comme destination du journal des événements d'audit. Si vous souhaitez utiliser un groupe de journaux de CloudWatch journaux personnalisé ou utiliser Firehose comme destination du journal des événements d'audit, voici les exigences relatives aux noms et aux emplacements de la destination du journal des événements d'audit :

- Le nom du groupe de CloudWatch journaux Logs doit commencer par le `/aws/fsx/` préfixe. Si vous ne disposez pas d'un groupe de CloudWatch journaux Logs existant lorsque vous créez ou mettez à jour un système de fichiers sur la console, Amazon FSx peut créer et utiliser un flux de journaux par défaut dans le groupe de CloudWatch `/aws/fsx/windows` journaux Logs. Si vous ne souhaitez pas utiliser le groupe de journaux par défaut, l'interface utilisateur de configuration vous permet de créer un groupe de CloudWatch journaux de journaux lorsque vous créez ou mettez à jour votre système de fichiers sur la console.
- Le nom du flux de diffusion Firehose doit commencer par le `aws-fsx-` préfixe. Si vous ne disposez pas d'un flux de diffusion Firehose existant, vous pouvez en créer un lorsque vous créez ou mettez à jour votre système de fichiers sur la console.
- Le flux de diffusion Firehose doit être configuré pour être utilisé `Direct PUT` comme source. Vous ne pouvez pas utiliser un flux de données Kinesis existant comme source de données pour votre flux de diffusion.
- La destination (groupe de CloudWatch journaux Logs ou flux de diffusion Firehose) doit se trouver sur la même AWS partition et sur Compte AWS celle de votre système de fichiers Amazon FSx. Région AWS

Vous pouvez modifier la destination du journal des événements d'audit à tout moment (par exemple, de CloudWatch Logs à Firehose). Dans ce cas, les nouveaux journaux des événements d'audit sont envoyés uniquement à la nouvelle destination.

Meilleur effort de livraison du journal des événements d'audit

Généralement, les enregistrements du journal des événements d'audit sont livrés à destination en quelques minutes, mais cela peut parfois prendre plus de temps. Dans de très rares cas, les enregistrements du journal des événements d'audit peuvent être manqués. Si votre cas d'utilisation nécessite une sémantique particulière (par exemple, pour s'assurer qu'aucun événement d'audit n'est manqué), nous vous recommandons de prendre en compte les événements manqués lors de la conception de vos flux de travail. Vous pouvez vérifier les événements manqués en analysant la structure des fichiers et des dossiers de votre système de fichiers.

Migration de vos contrôles d'audit

Si des contrôles d'audit (SACL) sont déjà configurés sur vos données de fichiers existantes, vous pouvez créer un système de fichiers Amazon FSx et migrer vos données vers votre nouveau système de fichiers. Nous vous recommandons AWS DataSync de l'utiliser pour transférer les données et les SACL associées vers votre système de fichiers Amazon FSx. Comme solution alternative, vous pouvez utiliser Robocopy (Robust File Copy). Pour plus d'informations, consultez Migration du stockage de fichiers existant vers Amazon FSx.

Affichage des journaux d'événements

Vous pouvez consulter les journaux des événements d'audit une fois qu'Amazon FSx a commencé à les émettre. L'emplacement et le mode d'affichage des journaux dépendent de la destination du journal des événements d'audit :

- Vous pouvez consulter CloudWatch les journaux en accédant à la CloudWatch console et en choisissant le groupe de journaux et le flux de journaux auxquels vos journaux d'événements d'audit sont envoyés. Pour plus d'informations, consultez Afficher les données de journal envoyées à CloudWatch Logs dans le guide de l'utilisateur Amazon CloudWatch Logs.

  Vous pouvez utiliser CloudWatch Logs Insights pour rechercher et analyser les données de vos journaux de manière interactive. Pour plus d'informations, consultez Analyser les données des CloudWatch journaux avec Logs Insights dans le guide de l'utilisateur Amazon CloudWatch Logs.

Vous pouvez également exporter les journaux des événements d'audit vers Amazon S3. Pour plus d'informations, consultez Exportation de données de journal vers Amazon S3, également dans le guide de l'utilisateur d'Amazon CloudWatch Logs.

- Vous ne pouvez pas consulter les journaux des événements d'audit sur Firehose. Cependant, vous pouvez configurer Firehose pour transférer les journaux vers une destination à partir de laquelle vous pouvez les lire. Les destinations incluent Amazon S3, Amazon Redshift, Amazon OpenSearch Service et des solutions partenaires telles que Splunk et Datadog. Pour plus d'informations, consultez Choisir une destination dans le guide du développeur Amazon Data Firehose.

Champs d'événements d'audit

Cette section décrit les informations contenues dans les journaux des événements d'audit et fournit des exemples d'événements d'audit.

Vous trouverez ci-dessous une description des principaux champs d'un événement d'audit Windows.

- EventID fait référence à l'ID d'événement du journal des événements Windows défini par Microsoft. Consultez la documentation Microsoft pour plus d'informations sur les événements du système de fichiers et les événements de partage de fichiers.
- SubjectUserNamefait référence à l'utilisateur effectuant l'accès.
- ObjectNamefait référence au fichier, au dossier ou au partage de fichiers cible auquel vous avez accédé.
- ShareNameest disponible pour les événements générés pour l'accès au partage de fichiers. Par exemple, `EventID 5140` est généré lors de l'accès à un objet de partage réseau.
- IpAddressfait référence au client qui a initié l'événement pour les événements de partage de fichiers.
- Les mots clés, lorsqu'ils sont disponibles, indiquent si l'accès au fichier a réussi ou échoué. Pour les accès réussis, la valeur est`0x8020000000000000`. Pour les accès échoués, la valeur est`0x8010000000000000`.
- TimeCreated SystemTimefait référence à l'heure à laquelle l'événement a été généré dans le système et affiché au <YYYY-MM-DDThh:mm:ss.s>format Z.
- L'ordinateur fait référence au nom DNS du système de fichiers Windows Remote PowerShell Endpoint et peut être utilisé pour identifier le système de fichiers.
- AccessMask, lorsqu'il est disponible, fait référence au type d'accès au fichier effectué (par exemple ReadData, WriteData).

- AccessListfait référence à l'accès demandé ou accordé à un objet. Pour plus de détails, consultez le tableau ci-dessous et la documentation Microsoft (comme dans Event 4556).

Type d'accès	Masque d'accès	Valeur
Lire le répertoire de données ou de listes	0x1	%4416
Écrire des données ou ajouter un fichier	0x2	%417
Ajouter des données ou ajouter un sous-répertoire	0x4	%418
Lire les attributs étendus	0x8	%4419
Écrire des attributs étendus	0x10	%4420
Exécuter/Traverser	0x20	%4421
Supprimer l'enfant	0x40	%442
Lire les attributs	0x80	%4423
Écrire des attributs	0 x 100	%424
Suppression	0 x 10000	%1537
Lire ACL	0 x 20000	%1538
Écrire ACL	0x40000	%1539
Écrivez le propriétaire	0 x 80000	% 1540
Synchroniser	0 x 100000	%1541
ACL de sécurité d'accès	0x1000000	%1542

Voici quelques événements clés accompagnés d'exemples. Notez que le XML est formaté dans un souci de lisibilité.

L'ID d'événement 4660 est enregistré lorsqu'un objet est supprimé.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4660</EventID><Version>0</Version><Level>0</Level>
<Task>12800</Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-05-18T04:51:56.916563800Z'/>
<EventRecordID>315452</EventRecordID><Correlation/>
<Execution ProcessID='4' ThreadID='5636'/><Channel>Security</Channel>
<Computer>amznfsxgyzohmw8.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x50932f71</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='HandleId'>0x12e0</Data><Data Name='ProcessId'>0x4</Data><Data
 Name='ProcessName'></Data>
<Data Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data></EventData></
Event>
```

L'ID d'événement 4659 est enregistré lors d'une demande de suppression de fichier.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4659</EventID><Version>0</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-0603T19:18:09.951551200Z'/>
<EventRecordID>308888</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='5540'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device\HarddiskVolume8\shar
\event.txt</Data>
```

```
<Data Name='HandleId'>0x0</Data><Data
 Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data>
<Data Name='AccessList'>%%1537
    %%4423
    </Data><Data Name='AccessMask'>0x10080</Data><Data Name='PrivilegeList'>-</Data>
<Data Name='ProcessId'>0x4</Data></EventData></Event>
```

L'ID d'événement 4663 est enregistré lorsqu'une opération spécifique a été effectuée sur l'objet. L'exemple suivant montre la lecture de données à partir d'un fichier, qui peuvent être interprétées à partir de celui-ci`AccessList %%4416`.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4663< /EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:10:13.887145400Z'/>
<EventRecordID>308831</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='6916'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData>< Data
 Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113< /Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\event.txt</Data>
<Data Name='HandleId'>0x101c</Data><Data Name='AccessList'>%%4416
    </Data>
<Data Name='AccessMask'>0x1</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data><Data Name='ResourceAttributes'>S:AI</Data>
</EventData></Event>
```

L'exemple suivant montre comment écrire/ajouter des données à partir d'un fichier, qui peuvent être interprétées à partir de celui-ci. `AccessList %%4417`

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4663</EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
```

```
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:12:16.813827100Z'/>
<EventRecordID>308838</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='5828'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\event.txt</Data>
<Data Name='HandleId'>0xa38</Data><Data Name='AccessList'>%%4417
    </Data><Data Name='AccessMask'>0x2</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data><Data Name='ResourceAttributes'>S:AI</Data></
EventData></Event>
```

L'ID d'événement 4656 indique qu'un accès spécifique a été demandé pour un objet. Dans l'exemple suivant, la demande Read a été lancée pour ObjectName « permtest » et a échoué, comme le montre la valeur Keywords de. `0x8010000000000000`

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4656</EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8010000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:22:55.113783500Z'/>
<EventRecordID>308919</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='4924'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\permtest</Data>
<Data Name='HandleId'>0x0</Data><Data
 Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data>
<Data Name='AccessList'>%%1541
    %%4416
    %%4423
```

```
    </Data><Data Name='AccessReason'>%%1541: %%1805
    %%4416: %%1805
    %%4423: %%1811 D:(A;OICI;0x1301bf;;;AU)
    </Data><Data Name='AccessMask'>0x100081</Data><Data Name='PrivilegeList'>-</Data>
<Data Name='RestrictedSidCount'>0</Data><Data Name='ProcessId'>0x4</Data><Data
 Name='ProcessName'></Data>
<Data Name='ResourceAttributes'>-</Data></EventData></Event>
```

L'ID d'événement 4670 est enregistré lorsque les autorisations associées à un objet sont modifiées. L'exemple suivant montre que l'utilisateur « admin » a modifié l'autorisation sur « permtest » pour ajouter des autorisations au SID ObjectName « S-1-5-21-658495921-4185342820-3824891517-1113 ». Reportez-vous à la documentation Microsoft pour plus d'informations sur l'interprétation des autorisations.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4670</EventID><Version>0</Version><Level>0</Level>
<Task>13570</Task><Opcode>0</Opcode><Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime='2021-06-03T19:39:47.537129500Z'/><EventRecordID>308992</
EventRecordID>
<Correlation/><Execution ProcessID='4' ThreadID='2776'/><Channel>Security</Channel>
<Computer>amznfsxgyzohmw8.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\permtest</Data>
<Data Name='HandleId'>0xcc8</Data>
<Data Name='OldSd'>D:PAI(A;OICI;FA;;;SY)
(A;OICI;FA;;;S-1-5-21-658495921-4185342820-3824891517-2622)</Data>
<Data Name='NewSd'>D:PARAI(A;OICI;FA;;;S-1-5-21-658495921-4185342820-3824891517-1113)
(A;OICI;FA;;;SY)(A;OICI;FA;;;
S-1-5-21-658495921-4185342820-3824891517-2622)</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data></EventData></Event>
```

L'ID d'événement 5140 est enregistré à chaque accès à un partage de fichiers.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
```

```
<EventID>5140</EventID><Version>1</Version><Level>0</Level><Task>12808</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:32:07.535208200Z'/>
<EventRecordID>308947</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='3120'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-2620</
Data>
<Data Name='SubjectUserName'>EC2AMAZ-1GP4HMN$</Data><Data
 Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2d4ca529</Data><Data Name='ObjectType'>File</Data><Data
 Name='IpAddress'>172.45.6.789</Data>
<Data Name='IpPort'>49730</Data><Data Name='ShareName'>\\AMZNFSXCYDKLDZZ\share</Data>
<Data Name='ShareLocalPath'>\??\D:\share</Data><Data Name='AccessMask'>0x1</Data><Data
 Name='AccessList'>%%4416
    </Data></EventData></Event>
```

L'ID d'événement 5145 est enregistré lorsque l'accès est refusé au niveau du partage de fichiers. L'exemple suivant montre que l'accès à ShareName « demoshare01 » a été refusé.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>5145</EventID><Version>0</Version><Level>0</Level>
<Task>12811</Task><Opcode>0</Opcode><Keywords>0x8010000000000000</Keywords>
<TimeCreated SystemTime='2021-05-19T22:30:40.485188700Z'/><EventRecordID>282939</
EventRecordID>
<Correlation/><Execution ProcessID='4' ThreadID='344'/><Channel>Security</Channel>
<Computer>amznfsxtmn9autz.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-
1113</Data><Data Name='SubjectUserName'>Admin</Data><Data
 Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x95b3fb7</Data><Data Name='ObjectType'>File</Data>
<Data Name='IpAddress'>172.31.7.112</Data><Data Name='IpPort'>59979</Data>
<Data Name='ShareName'>\\AMZNFSXDPNTE0DC\demoshare01</Data><Data Name='ShareLocalPath'>
\??\D:\demoshare01</Data>
<Data Name='RelativeTargetName'>Desktop.ini</Data><Data Name='AccessMask'>0x120089</
Data>
<Data Name='AccessList'>%%1538 %%1541 %%4416 %%4419 %%4423 </Data><Data
 Name='AccessReason'>%%1538:
```

```
%%1804 %%1541: %%1805 %%4416: %%1805 %%4419: %%1805 %%4423: %%1805 </Data></
EventData></Event>
```

Si vous utilisez CloudWatch Logs Insights pour rechercher les données de vos journaux, vous pouvez exécuter des requêtes sur les champs d'événements, comme le montrent les exemples suivants :

- Pour demander un ID d'événement spécifique, procédez comme suit :

```
fields @message
   | filter @message like /4660/
```

- Pour interroger tous les événements correspondant à un nom de fichier donné, procédez comme suit :

```
fields @message
   | filter @message like /event.txt/
```

Pour plus d'informations sur le langage de requête CloudWatch Logs Insights, consultez Analyzing Log Data with CloudWatch Logs Insights, dans le guide de l'utilisateur Amazon CloudWatch Logs.

Configuration des contrôles d'audit des fichiers et des dossiers

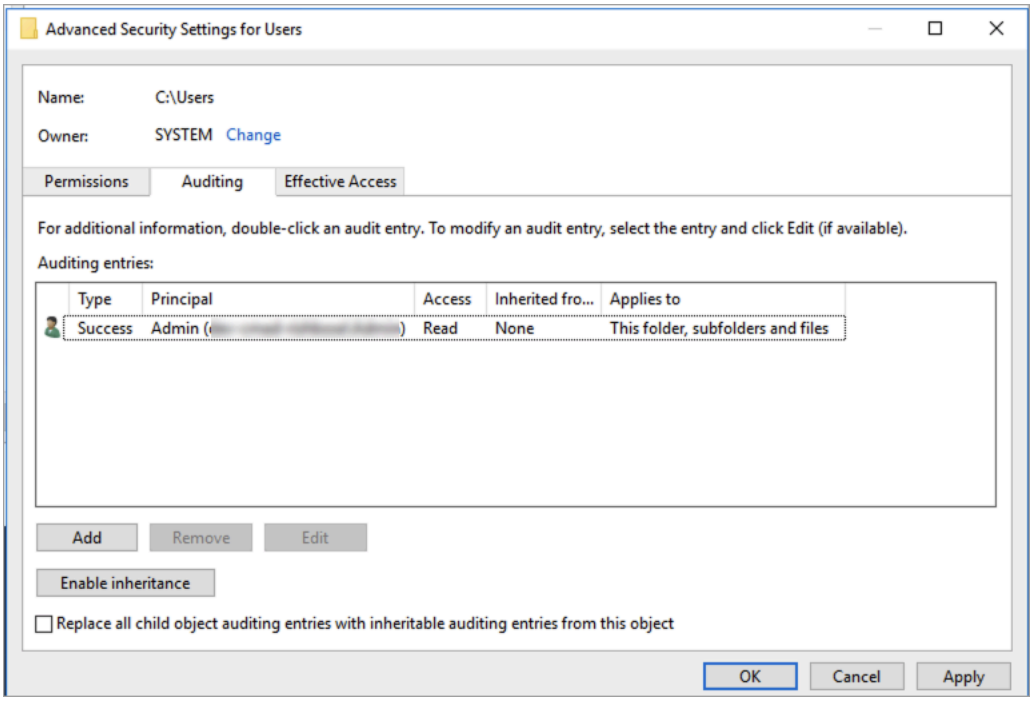
Vous devez définir des contrôles d'audit sur les fichiers et dossiers que vous souhaitez auditer pour les tentatives d'accès des utilisateurs. Les contrôles d'audit sont également appelés listes de contrôle d'accès au système NTFS (SACL).

Vous configurez les contrôles d'audit à l'aide de l'interface graphique native de Windows ou par programmation à l'aide de commandes Windows. PowerShell Si l'héritage est activé, vous devez généralement définir des contrôles d'audit uniquement sur les dossiers de niveau supérieur auxquels vous souhaitez enregistrer les accès.

Utilisation de l'interface graphique Windows pour définir l'accès à l'audit

Pour utiliser une interface graphique afin de définir des contrôles d'audit sur vos fichiers et dossiers, utilisez l'Explorateur de fichiers Windows. Sur un fichier ou un dossier donné, ouvrez l'Explorateur de fichiers Windows et sélectionnez l'onglet Propriétés > Sécurité > Avancé > Audit.

L'exemple de contrôle d'audit suivant permet d'auditer les événements réussis pour un dossier. Une entrée du journal des événements Windows est émise chaque fois que ce handle est ouvert pour être lu avec succès par l'utilisateur administrateur.



Le champ Type indique les actions que vous souhaitez auditer. Définissez ce champ sur Réussite pour auditer les tentatives réussies, Échec pour auditer les tentatives infructueuses ou Tout pour auditer à la fois les tentatives réussies et les tentatives infructueuses.

Pour plus d'informations sur les champs de saisie d'audit, voir Appliquer une politique d'audit de base à un fichier ou à un dossier dans la documentation Microsoft.

Utilisation de PowerShell commandes pour définir l'accès à l'audit

Vous pouvez utiliser la `Set-Acl` commande Microsoft Windows pour définir la SACL d'audit sur n'importe quel fichier ou dossier. Pour plus d'informations sur cette commande, consultez la documentation Microsoft Set-Acl.

Voici un exemple d'utilisation d'une série de PowerShell commandes et de variables pour définir l'accès à l'audit en cas de tentatives réussies. Vous pouvez adapter ces exemples de commandes aux besoins de votre système de fichiers.

```
$path = "C:\Users\TestUser\Desktop\DemoTest\"

$ACL = Get-Acl $path

$ACL | Format-List
```

```
$AuditUser = "TESTDOMAIN\TestUser"

$AuditRules = "FullControl"

$InheritType = "ContainerInherit,ObjectInherit"

$AuditType = "Success"

$AccessRule = New-Object System.Security.AccessControl.FileSystemAuditRule($AuditUser,
$AuditRules,$InheritType,"None",$AuditType)

$ACL.SetAuditRule($AccessRule)

$ACL | Set-Acl $path

Get-Acl $path -Audit | Format-List
```

Gestion de l'audit des accès aux fichiers

Vous pouvez activer l'audit d'accès aux fichiers lors de la création d'un nouveau système de fichiers Amazon FSx for Windows File Server. L'audit d'accès aux fichiers est désactivé par défaut lorsque vous créez un système de fichiers depuis la console Amazon FSx.

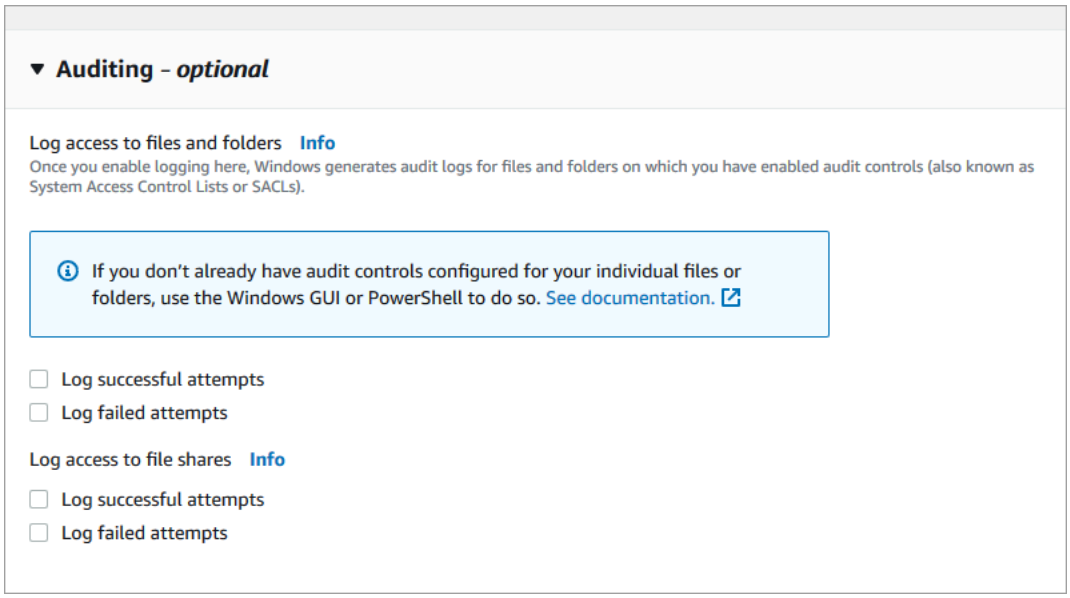
Sur les systèmes de fichiers existants sur lesquels l'audit d'accès aux fichiers est activé, vous pouvez modifier les paramètres d'audit d'accès aux fichiers, notamment les types de tentatives d'accès pour les accès aux fichiers et aux partages de fichiers, ainsi que la destination du journal des événements d'audit. Vous pouvez effectuer ces tâches à l'aide de la console Amazon FSx ou de l' AWS CLI API.

> **Note**
>
> L'audit d'accès aux fichiers n'est pris en charge que sur les systèmes de fichiers Amazon FSx for Windows File Server avec une capacité de débit de 32 Mo/s ou plus. Vous ne pouvez pas créer ou mettre à jour un système de fichiers avec une capacité de débit inférieure à 32 Mo/s si l'audit d'accès aux fichiers est activé. Vous pouvez modifier la capacité de débit à tout moment après avoir créé le système de fichiers. Pour plus d'informations, consultez Gestion de la capacité de débit.

Pour activer l'audit de l'accès aux fichiers lors de la création d'un système de fichiers (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.

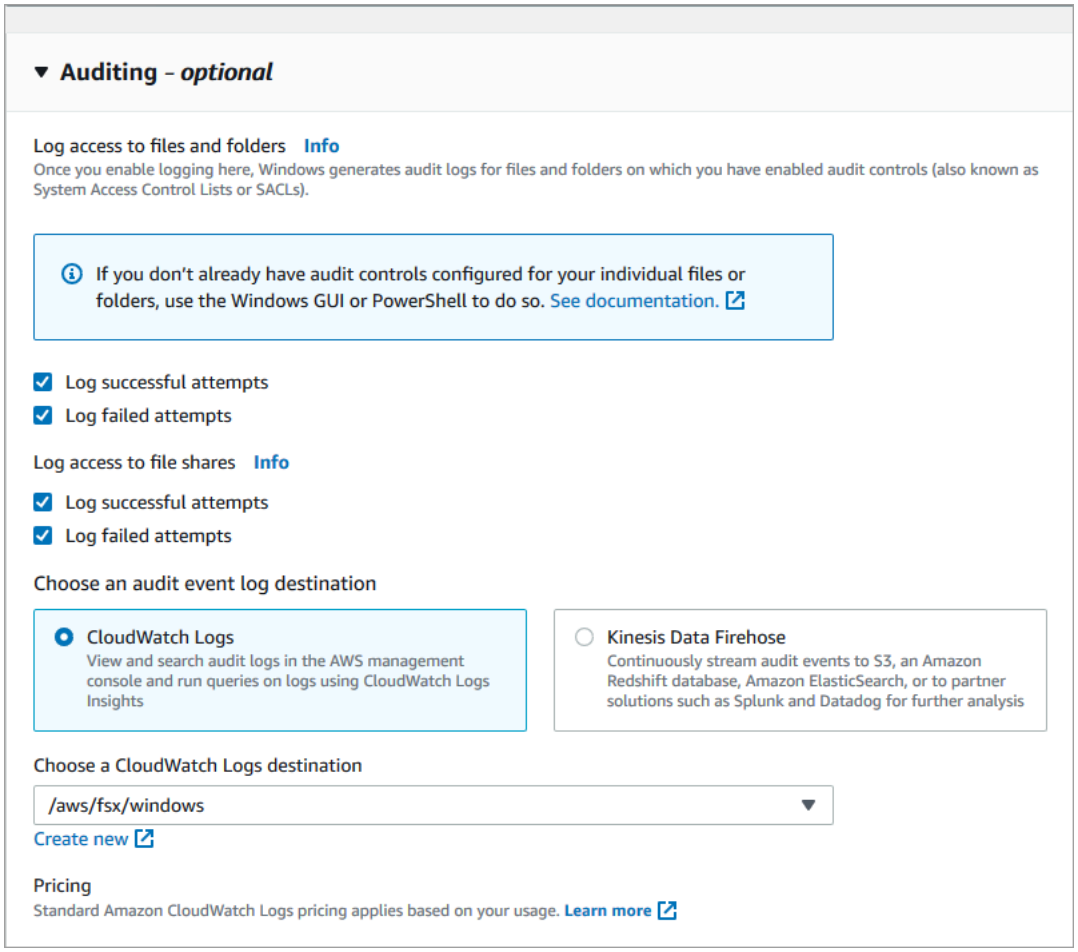
2. Suivez la procédure de création d'un nouveau système de fichiers décrite Créez votre système de fichiers dans la section Mise en route.
3. Ouvrez la section Audit - facultatif. L'audit d'accès aux fichiers est désactivé par défaut.



4. Pour activer et configurer l'audit d'accès aux fichiers, procédez comme suit.

   - Pour l'accès au journal des fichiers et des dossiers, sélectionnez l'enregistrement des tentatives réussies et/ou infructueuses. La journalisation est désactivée pour les fichiers et les dossiers si vous n'effectuez aucune sélection.
   - Pour l'accès au journal des partages de fichiers, sélectionnez l'enregistrement des tentatives réussies et/ou infructueuses. La journalisation est désactivée pour les partages de fichiers si vous n'effectuez aucune sélection.
   - Pour Choisir une destination du journal des événements d'audit, choisissez CloudWatch Logs ou Firehose. Choisissez ensuite un journal ou un flux de diffusion existant ou créez-en un nouveau. Pour les CloudWatch journaux, Amazon FSx peut créer et utiliser un flux de journal par défaut dans le groupe de CloudWatch `/aws/fsx/windows` journaux Logs.

   Vous trouverez ci-dessous un exemple de configuration d'audit d'accès aux fichiers qui vérifiera les tentatives d'accès réussies et infructueuses des utilisateurs finaux aux fichiers, aux dossiers et aux partages de fichiers. Les journaux des événements d'audit seront envoyés à la destination par défaut du groupe de CloudWatch `/aws/fsx/windows` journaux Logs.



5. Passez à la section suivante de l'assistant de création de système de fichiers.

Lorsque le système de fichiers est disponible, la fonctionnalité d'audit d'accès aux fichiers est activée.

Pour activer l'audit de l'accès aux fichiers lors de la création d'un système de fichiers (CLI)

1. Lorsque vous créez un nouveau système de fichiers, utilisez la `AuditLogConfiguration` propriété avec l'opération d'CreateFileSystemAPI pour activer l'audit de l'accès aux fichiers pour le nouveau système de fichiers.

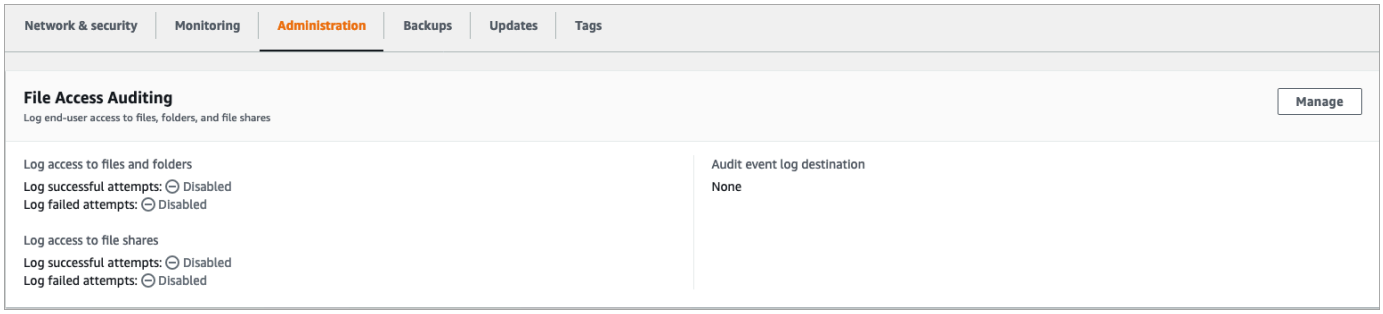
```
aws fsx create-file-system \
  --file-system-type WINDOWS \
  --storage-capacity 300 \
  --subnet-ids subnet-123456 \
  --windows-configuration
 AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
    FileShareAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
```

```
    AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-customer-log-group"}'
```

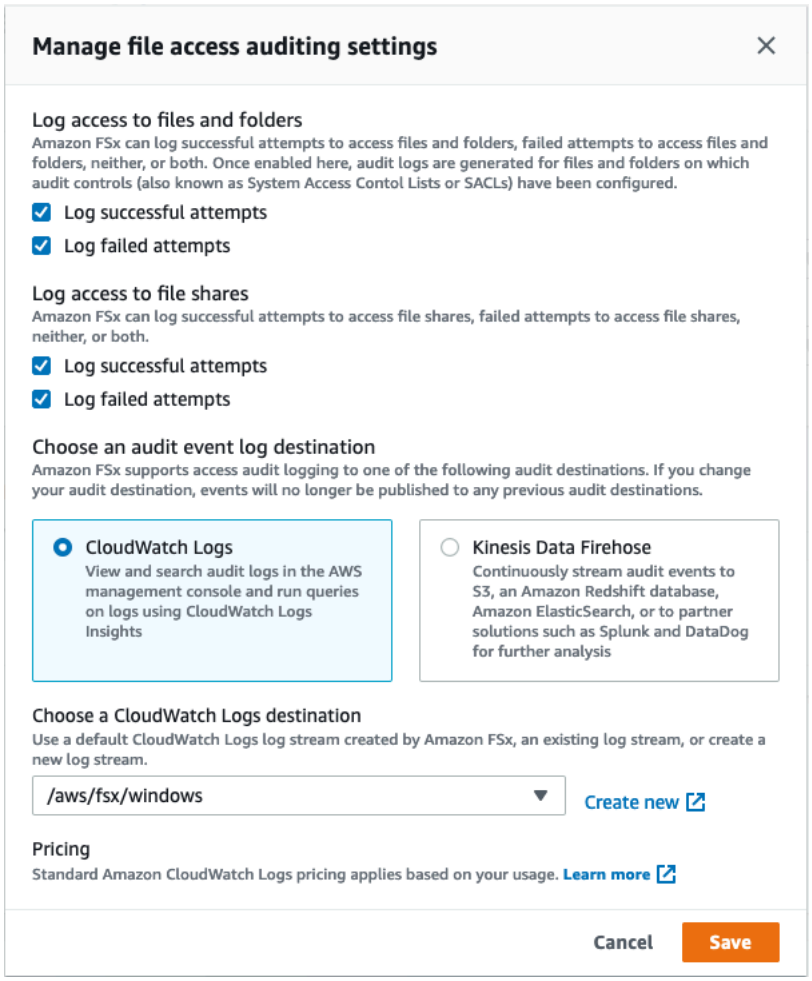
2. Lorsque le système de fichiers est disponible, la fonctionnalité d'audit d'accès aux fichiers est activée.

Pour modifier la configuration de l'audit d'accès aux fichiers (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Accédez à Systèmes de fichiers, puis choisissez le système de fichiers Windows pour lequel vous souhaitez gérer l'audit d'accès aux fichiers.
3. Choisissez l'onglet Administration.
4. Dans le panneau d'audit de l'accès aux fichiers, choisissez Gérer.



5. Dans la boîte de dialogue Gérer les paramètres d'audit d'accès aux fichiers, modifiez les paramètres souhaités.



- Pour l'accès au journal des fichiers et des dossiers, sélectionnez l'enregistrement des tentatives réussies et/ou infructueuses. La journalisation est désactivée pour les fichiers et les dossiers si vous n'effectuez aucune sélection.
- Pour l'accès au journal des partages de fichiers, sélectionnez l'enregistrement des tentatives réussies et/ou infructueuses. La journalisation est désactivée pour les partages de fichiers si vous n'effectuez aucune sélection.
- Pour Choisir une destination du journal des événements d'audit, choisissez CloudWatch Logs ou Firehose. Choisissez ensuite un journal ou un flux de diffusion existant ou créez-en un nouveau.

6. Choisissez Enregistrer.

Pour modifier la configuration de l'audit d'accès aux fichiers (CLI)

- Utilisez la commande update-file-systemCLI ou l'opération UpdateFileSystemAPI équivalente.

```
aws fsx update-file-system \
  --file-system-id fs-0123456789abcdef0 \
  --windows-configuration
 AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_ONLY", \
    FileShareAccessAuditLogLevel="FAILURE_ONLY", \
    AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-
customer-log-group"}'
```

Sessions utilisateur et fichiers ouverts

Vous pouvez surveiller les sessions utilisateur connectées et ouvrir des fichiers sur votre système de fichiers FSx for Windows File Server à l'aide de l'outil Dossiers partagés. L'outil Dossiers partagés fournit un emplacement central permettant de contrôler qui est connecté au système de fichiers, ainsi que les fichiers ouverts et par qui. Vous pouvez utiliser cet outil pour effectuer les opérations suivantes :

- Restaurez l'accès aux fichiers verrouillés.
- Déconnectez une session utilisateur, qui ferme tous les fichiers ouverts par cet utilisateur.

Vous pouvez utiliser l'outil graphique Shared Folders natif de Windows et la CLI Amazon FSx pour la gestion PowerShell à distance afin de gérer les sessions utilisateur et d'ouvrir des fichiers sur votre système de fichiers FSx for Windows File Server.

Utilisation de l'interface graphique pour gérer les utilisateurs et les sessions

Les procédures suivantes expliquent comment gérer les sessions utilisateur et ouvrir des fichiers sur votre système de fichiers Amazon FSx à l'aide de l'outil de dossiers partagés Microsoft Windows.

Pour lancer l'outil de dossiers partagés

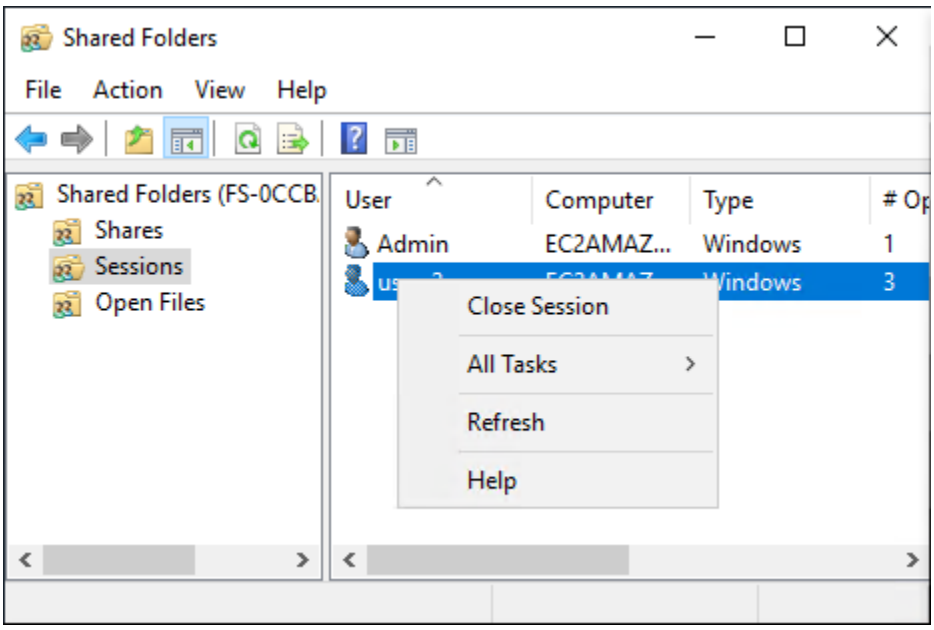
1. Lancez votre instance Amazon EC2 et connectez-la au Microsoft Active Directory auquel votre système de fichiers Amazon FSx est joint. Pour ce faire, choisissez l'une des procédures suivantes dans le guide AWS Directory Service d'administration :

- Joindre facilement une instance Windows EC2
- Joindre manuellement une instance Windows

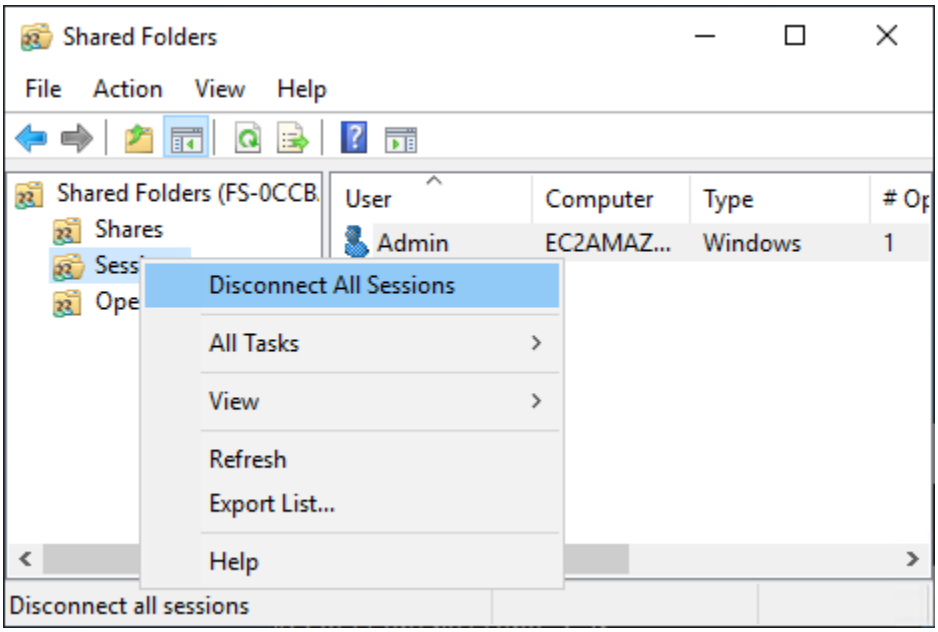
2. Connectez-vous à votre instance en tant qu'utilisateur membre du groupe des administrateurs du système de fichiers. Dans AWS Managed Microsoft Active Directory, ce groupe est appelé AWS Administrateurs FSx délégués. Dans votre Microsoft Active Directory autogéré, ce groupe est appelé Administrateurs de domaine ou le nom personnalisé du groupe d'administrateurs que vous avez indiqué lors de sa création. Pour plus d'informations, consultez la section Connexion à votre instance Windows dans le guide de l'utilisateur Amazon EC2.
3. Ouvrez le menu Démarrer et exécutez fsmgmt.msc à l'aide de. `Run As Administrator` 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 système de fichiers Amazon FSx, par exemple. `fs-`*`012345678901234567`*`.`*`ad-domain`*`.com`
6. Choisissez OK. Une entrée pour votre système de fichiers Amazon FSx apparaît ensuite dans la liste de l'outil Dossiers partagés.

Pour gérer les sessions utilisateur (GUI)

Dans l'outil Dossiers partagés, choisissez Sessions pour afficher toutes les sessions utilisateur connectées à votre système de fichiers FSx for Windows File Server. Si un utilisateur ou une application accède à un partage de fichiers sur votre système de fichiers Amazon FSx, ce composant logiciel enfichable affiche sa session. Vous pouvez déconnecter des sessions en ouvrant le menu contextuel (clic droit) d'une session et en choisissant Fermer la session.



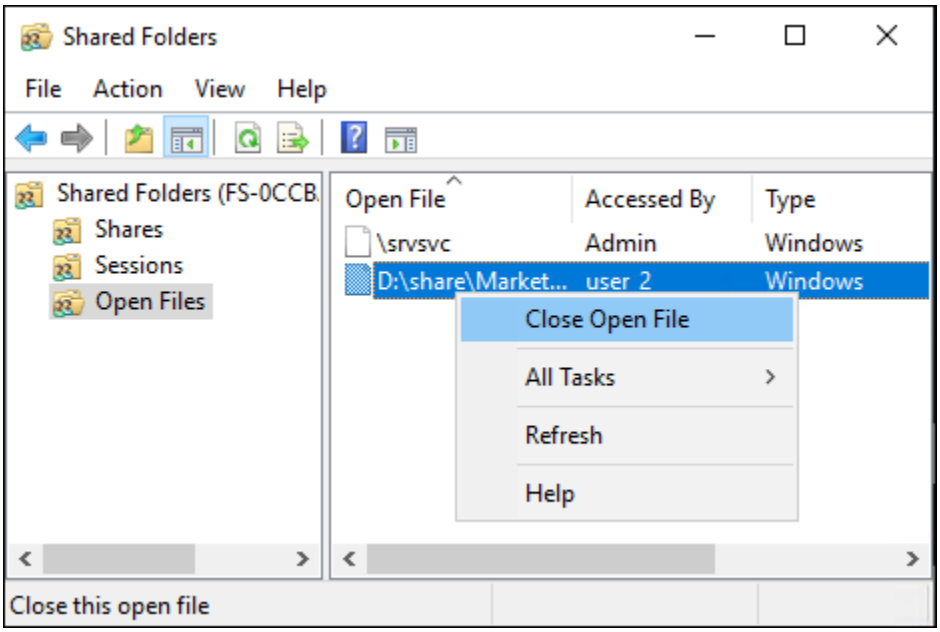
Pour déconnecter toutes les sessions ouvertes, ouvrez le menu contextuel (clic droit) des sessions, choisissez Déconnecter toutes les sessions et confirmez votre action.



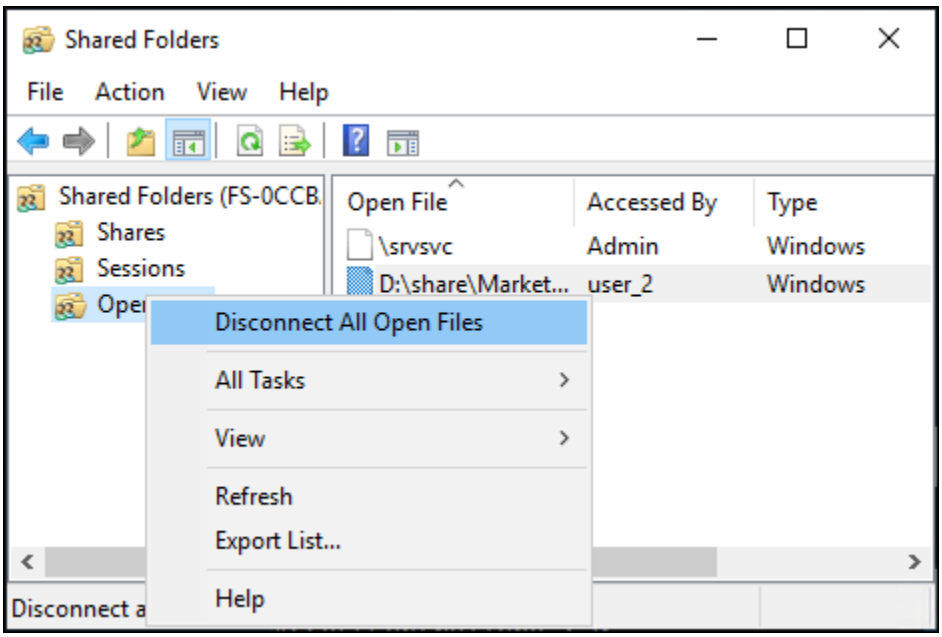
Pour gérer les fichiers ouverts (GUI)

Dans l'outil Dossiers partagés, choisissez Ouvrir des fichiers pour afficher tous les fichiers actuellement ouverts sur le système. La vue indique également quels utilisateurs ont ouvert les fichiers ou les dossiers. Ces informations peuvent être utiles pour déterminer pourquoi les autres utilisateurs ne peuvent pas ouvrir certains fichiers. Vous pouvez fermer n'importe quel fichier ouvert

par un utilisateur en ouvrant simplement le menu contextuel (clic droit) correspondant à l'entrée du fichier dans la liste et en choisissant Fermer le fichier ouvert.



Pour déconnecter tous les fichiers ouverts du système de fichiers, cliquez sur le menu contextuel (clic droit) pour Ouvrir les fichiers, choisissez Déconnecter tous les fichiers ouverts, puis confirmez votre action.



Utilisation PowerShell pour gérer les sessions utilisateur et ouvrir des fichiers

Vous pouvez gérer les sessions utilisateur actives et ouvrir des fichiers sur votre système de fichiers à l'aide de l'interface de ligne de commande Amazon FSx pour la gestion à distance sur. PowerShell Pour savoir comment utiliser cette CLI, consultezUtilisation de l'interface de ligne de commande Amazon FSx pour PowerShell.

Vous trouverez ci-dessous les commandes que vous pouvez utiliser pour la gestion des sessions utilisateur et des fichiers ouverts.

Command	Description
Get-FSxSmbSession	Récupère des informations sur les sessions SMB (Server Message Block) actuellement établies entre le système de fichiers et les clients associés.
Close-FSxSmbSession	Met fin à une session SMB.
Get-FSxSmbOpenFile	Récupère des informations sur les fichiers ouverts pour les clients connectés au système de fichiers.
Close-FSxSmbOpenFile	Ferme un fichier ouvert pour l'un des clients du serveur SMB.

L'aide en ligne de chaque commande fournit une référence de toutes les options de commande. Pour accéder à cette aide, exécutez la commande avec un-?, par exempleGet-FSxSmbSession -?.

Déduplication des données

FSx prend en charge l'utilisation de Microsoft Data Deduplication pour identifier et éliminer les données redondantes. Les grands ensembles de données contiennent souvent des données redondantes, ce qui augmente les coûts de stockage des données. Par exemple, avec les partages de fichiers utilisateur, plusieurs utilisateurs peuvent stocker de nombreuses copies ou versions d'un même fichier. Avec les partages de développement logiciel, de nombreux fichiers binaires restent inchangés d'une version à l'autre.

Vous pouvez réduire les coûts de stockage des données en activant la déduplication des données pour votre système de fichiers. La déduplication des données réduit ou élimine les données

redondantes en ne stockant qu'une seule fois les parties dupliquées du jeu de données. La compression des données est activée par défaut lorsque vous utilisez la déduplication des données, ce qui réduit encore la quantité de stockage de données en compressant les données après la déduplication. La déduplication des données s'exécute comme un processus d'arrière-plan qui analyse et optimise continuellement et automatiquement votre système de fichiers, et elle est transparente pour vos utilisateurs et clients connectés.

Les économies de stockage que vous pouvez réaliser grâce à la déduplication des données dépendent de la nature de votre ensemble de données, notamment du niveau de duplication existant entre les fichiers. En général, les économies réalisées sont de 50 à 60 % en moyenne pour les partages de fichiers à usage général. En ce qui concerne les actions, les économies vont de 30 à 50 % pour les documents utilisateur à 70 à 80 % pour les ensembles de données de développement logiciel. Vous pouvez mesurer les économies potentielles liées à la déduplication à l'aide de la `Measure-FSxDedupFileMetadata` commande décrite ci-dessous.

Vous pouvez également personnaliser la déduplication des données pour répondre à vos besoins de stockage spécifiques. Par exemple, vous pouvez configurer la déduplication pour qu'elle s'exécute uniquement sur certains types de fichiers, ou vous pouvez créer un calendrier de travail personnalisé. Les tâches de déduplication pouvant consommer les ressources du serveur de fichiers, nous vous recommandons de surveiller l'état de vos tâches de déduplication à l'aide de la `Get-FSxDedupStatus` commande décrite ci-dessous.

Pour plus d'informations sur la déduplication des données, consultez la documentation Microsoft Understanding Data Deduplication.

> **Note**
>
> Consultez nos meilleures pratiques pourBonnes pratiques lors de l'utilisation de la déduplication des données. Si vous rencontrez des problèmes pour exécuter correctement les tâches de déduplication des données, consultezRésolution des problèmes de déduplication des données.

> **Warning**
>
> Il n'est pas recommandé d'exécuter certaines commandes Robocopy avec déduplication des données, car ces commandes peuvent avoir un impact sur l'intégrité des données du Chunk

Store. Pour plus d'informations, consultez la documentation relative à l'interopérabilité avec Microsoft Data Deduplication.

Bonnes pratiques lors de l'utilisation de la déduplication des données

Voici quelques bonnes pratiques relatives à l'utilisation de la déduplication des données :

- Planifiez les tâches de déduplication des données pour qu'elles s'exécutent lorsque votre système de fichiers est inactif : la planification par défaut inclut une `GarbageCollection` tâche hebdomadaire à 2h45 UTC le samedi. Cette opération peut prendre plusieurs heures si votre système de fichiers enregistre une importante perte de données. Si cette période n'est pas idéale pour votre charge de travail, planifiez cette tâche pour qu'elle s'exécute à un moment où vous vous attendez à un faible trafic sur votre système de fichiers.
- Configurez une capacité de débit suffisante pour que la déduplication des données soit terminée : des capacités de débit supérieures fournissent des niveaux de mémoire plus élevés. Microsoft recommande de disposer de 1 Go de mémoire pour 1 To de données logiques pour exécuter la déduplication des données. Utilisez le tableau des performances d'Amazon FSx pour déterminer la mémoire associée à la capacité de débit de votre système de fichiers et vous assurer que les ressources de mémoire sont suffisantes pour la taille de vos données.
- Personnalisez les paramètres de déduplication des données pour répondre à vos besoins de stockage spécifiques et réduire les exigences en matière de performances : vous pouvez limiter l'optimisation pour qu'elle s'exécute sur des types de fichiers ou des dossiers spécifiques, ou définir une taille et un âge de fichier minimaux pour l'optimisation. Pour en savoir plus, veuillez consulter la section Déduplication des données.

Gestion de la déduplication des données

Vous pouvez gérer la déduplication des données sur votre système de fichiers à l'aide de l'interface de ligne de commande Amazon FSx pour la gestion à distance PowerShell sur. Pour savoir comment utiliser cette CLI, consultezUtilisation de l'interface de ligne de commande Amazon FSx pour PowerShell.

Vous trouverez ci-dessous les commandes que vous pouvez utiliser pour la déduplication des données.

Commande de déduplication des données	Description
Enable-FSxDedup	Permet la déduplication des données sur le partage de fichiers. La compression des données après déduplication est activée par défaut lorsque vous activez la déduplication des données.
Disable-FSxDedup	Désactive la déduplication des données sur le partage de fichiers.
Get-FSxDedupConfiguration	Récupère les informations de configuration de la déduplication, notamment la taille et l'âge minimaux des fichiers pour l'optimis ation, les paramètres de compression et les types de fichiers et dossiers exclus.
Set-FSxDedupConfiguration	Modifie les paramètres de configuration de la déduplication, notamment la taille et l'âge minimaux des fichiers pour l'optimis ation, les paramètres de compression et les types de fichiers et dossiers exclus.
Get-FSxDedupStatus	Récupère l'état de déduplication et inclut des propriétés en lecture seule qui décrivent les économies d'optimisation et l'état du système de fichiers, les délais et l'état d'achèvement des dernières tâches sur le système de fichiers.
Get-FSxDedupMetadata	Récupère les métadonnées d'optimisation de la déduplication.
Update-FSxDedupStatus	Calcule et extrait des informations actualisées sur les économies réalisées grâce à la déduplication des données.
Measure-FSxDedupFi leMetadata	Mesure et extrait l'espace de stockage potentiel que vous pouvez récupérer sur votre système de fichiers si vous supprimez un groupe de dossiers. Les fichiers contiennent souvent des fragments partagés entre d'autres dossiers, et le moteur de déduplication calcule quels fragments sont uniques et devraient être supprimés.

Commande de déduplication des données	Description
Get-FSxDedupSchedule	Récupère les programmes de déduplication actuellement définis.
New-FSxDedupSchedule	Crée et personnalise un calendrier de déduplication des données.
Set-FSxDedupSchedule	Modifie les paramètres de configuration pour les programmes de déduplication de données existants.
Remove-FSxDedupSchedule	Supprime un calendrier de déduplication.
Get-FSxDedupJob	Obtient le statut et les informations de toutes les tâches de déduplication en cours d'exécution ou en attente.
Stop-FSxDedupJob	Annulez une ou plusieurs tâches de déduplication de données spécifiées.

L'aide en ligne de chaque commande fournit une référence de toutes les options de commande. Pour accéder à cette aide, exécutez la commande avec-?, par exempleEnable-FSxDedup -?.

Activation de la déduplication des données

Vous activez la déduplication des données sur un partage de fichiers Amazon FSx for Windows File Server à l'aide de `Enable-FSxDedup` la commande suivante.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {Enable-FsxDedup }
```

Lorsque vous activez la déduplication des données, une planification et une configuration par défaut sont créées. Vous pouvez créer, modifier et supprimer des plannings et des configurations à l'aide des commandes ci-dessous.

Vous pouvez utiliser cette `Disable-FSxDedup` commande pour désactiver complètement la déduplication des données sur votre système de fichiers.

Création d'un calendrier de déduplication des données

Même si le calendrier par défaut fonctionne bien dans la plupart des cas, vous pouvez créer un nouveau calendrier de déduplication à l'aide de la `New-FsxDedupSchedule` commande illustrée ci-dessous. Les plannings de déduplication des données utilisent l'heure UTC.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
New-FSxDedupSchedule -Name "CustomOptimization" -Type Optimization -Days Mon,Wed,Sat -
Start 08:00 -DurationHours 7
}
```

Cette commande crée un calendrier nommé `CustomOptimization` qui s'exécute les jours du lundi, du mercredi et du samedi, en commençant le travail à 8 h 00 (UTC) chaque jour, avec une durée maximale de 7 heures, après quoi le travail s'arrête s'il est toujours en cours d'exécution.

Notez que la création de nouveaux plannings de tâches de déduplication personnalisés ne remplace ni ne supprime le planning par défaut existant. Avant de créer une tâche de déduplication personnalisée, vous souhaiterez peut-être désactiver la tâche par défaut si vous n'en avez pas besoin.

Vous pouvez désactiver le calendrier de déduplication par défaut à l'aide de la `Set-FsxDedupSchedule` commande illustrée ci-dessous.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com
 -ConfigurationName FSxRemoteAdmin -ScriptBlock {Set-FSxDedupSchedule -Name
 “BackgroundOptimization” -Enabled $false}
```

Vous pouvez supprimer un calendrier de déduplication à l'aide de la `Remove-FSxDedupSchedule -Name "ScheduleName"` commande. Notez que le calendrier de `BackgroundOptimization` déduplication par défaut ne peut être ni modifié ni supprimé et qu'il devra être désactivé à la place.

Modification d'un calendrier de déduplication des données

Vous pouvez modifier un calendrier de déduplication existant à l'aide de la `Set-FsxDedupSchedule` commande illustrée ci-dessous.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
```

```
Set-FSxDedupSchedule -Name "CustomOptimization" -Type Optimization -Days
 Mon,Tues,Wed,Sat -Start 09:00 -DurationHours 9
}
```

Cette commande modifie le `CustomOptimization` calendrier existant pour qu'il soit exécuté les jours du lundi au mercredi et le samedi, en commençant le travail à 9 h 00 (UTC) chaque jour, avec une durée maximale de 9 heures, après quoi le travail s'arrête s'il est toujours en cours d'exécution.

Pour modifier l'âge minimum du fichier avant d'optimiser le paramètre, utilisez la `Set-FSxDedupConfiguration` commande.

Afficher la quantité d'espace économisé

Pour afficher la quantité d'espace disque que vous économisez grâce à l'exécution de la déduplication des données, utilisez la `Get-FSxDedupStatus` commande suivante.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FsxRemoteAdmin -ScriptBlock {
Get-FSxDedupStatus } | select
 OptimizedFilesCount,OptimizedFilesSize,SavedSpace,OptimizedFilesSavingsRate

OptimizedFilesCount OptimizedFilesSize SavedSpace OptimizedFilesSavingsRate
------------------- ------------------ ---------- -------------------------
              12587           31163594   25944826                        83
```

> **Note**
>
> Les valeurs affichées dans la réponse de commande pour les paramètres suivants ne sont pas fiables et vous ne devez pas utiliser ces valeurs : Capacity FreeSpace, UsedSpace, UnoptimizedSize, et SavingsRate.

Résolution des problèmes de déduplication des données

Les problèmes de déduplication des données peuvent avoir plusieurs causes, comme décrit dans la section suivante.

Rubriques

- La déduplication des données ne fonctionne pas

- Les valeurs de déduplication sont définies de manière inattendue sur 0
- L'espace n'est pas libéré sur le système de fichiers après la suppression de fichiers

La déduplication des données ne fonctionne pas

À l'aide des instructions de notre documentation sur la déduplication des données, exécutez la `Get-FSxDedupStatus` commande pour afficher l'état d'achèvement des tâches de déduplication les plus récentes. Si une ou plusieurs tâches échouent, il est possible que vous ne constatiez aucune augmentation de la capacité de stockage disponible sur votre système de fichiers.

La raison la plus courante de l'échec des tâches de déduplication est le manque de mémoire.

- Microsoft recommande de disposer de manière optimale de 1 Go de mémoire pour 1 To de données logiques (ou d'un minimum de 300 Mo + 50 Mo pour 1 To de données logiques). Utilisez le tableau des performances d'Amazon FSx pour déterminer la mémoire associée à la capacité de débit de votre système de fichiers et vous assurer que les ressources de mémoire sont suffisantes pour la taille de vos données.
- Les tâches de déduplication sont configurées avec l'allocation de mémoire par défaut recommandée par Windows de 25 %, ce qui signifie que pour un système de fichiers doté de 32 Go de mémoire, 8 Go seront disponibles pour la déduplication. L'allocation de mémoire est configurable (à l'aide de la `Set-FSxDedupSchedule` commande avec paramètre`-Memory`), mais la consommation de mémoire supplémentaire peut avoir un impact sur les performances du système de fichiers.
- Vous pouvez modifier la configuration des tâches de déduplication afin de réduire davantage les besoins en mémoire. Par exemple, vous pouvez limiter l'optimisation pour qu'elle s'exécute sur des types de fichiers ou des dossiers spécifiques, ou définir une taille et un âge de fichier minimaux pour l'optimisation. Nous recommandons également de configurer les tâches de déduplication pour qu'elles s'exécutent pendant les périodes d'inactivité lorsque la charge de votre système de fichiers est minimale.

Des erreurs peuvent également s'afficher si les tâches de déduplication ne sont pas terminées suffisamment longtemps. Vous devrez peut-être modifier la durée maximale des tâches, comme décrit dansModification d'un calendrier de déduplication des données.

Si les tâches de déduplication échouent depuis longtemps et que des modifications ont été apportées aux données du système de fichiers au cours de cette période, les tâches de déduplication suivantes peuvent nécessiter davantage de ressources pour être exécutées correctement pour la première fois.

Les valeurs de déduplication sont définies de manière inattendue sur 0

Les valeurs pour `SavedSpace` et `OptimizedFilesSavingsRate` sont étonnamment égales à 0 pour un système de fichiers sur lequel vous avez configuré la déduplication des données.

Cela peut se produire pendant le processus d'optimisation du stockage lorsque vous augmentez la capacité de stockage du système de fichiers. Lorsque vous augmentez la capacité de stockage d'un système de fichiers, Amazon FSx annule les tâches de déduplication de données existantes pendant le processus d'optimisation du stockage, qui fait migrer les données des anciens disques vers les nouveaux disques plus grands. Amazon FSx reprend la déduplication des données sur le système de fichiers une fois la tâche d'optimisation du stockage terminée. Pour plus d'informations sur l'augmentation de la capacité de stockage et l'optimisation du stockage, consultezGestion de la capacité de stockage.

L'espace n'est pas libéré sur le système de fichiers après la suppression de fichiers

Le comportement attendu de la déduplication des données est le suivant : si les données supprimées ont permis d'économiser de l'espace, cet espace n'est pas réellement libéré sur votre système de fichiers tant que la tâche de collecte des déchets n'est pas exécutée.

Une pratique qui pourrait vous être utile consiste à planifier l'exécution de la tâche de collecte des déchets juste après avoir supprimé un grand nombre de fichiers. Une fois le travail de collecte des ordures terminé, vous pouvez rétablir les paramètres d'origine du calendrier de collecte des déchets. Cela vous permet de voir rapidement et immédiatement l'espace contenu dans vos suppressions.

Utilisez la procédure suivante pour configurer la tâche de collecte des déchets de manière à ce qu'elle s'exécute en 5 minutes.

1. Pour vérifier que la déduplication des données est activée, utilisez la `Get-FSxDedupStatus` commande. Pour plus d'informations sur la commande et le résultat attendu, consultezAfficher la quantité d'espace économisé.
2. Utilisez ce qui suit pour définir le calendrier d'exécution de la tâche de collecte des déchets dans 5 minutes.

```
$FiveMinutesFromNowUTC = ((get-date).AddMinutes(5)).ToUniversalTime()
$DayOfWeek = $FiveMinutesFromNowUTC.DayOfWeek
$Time = $FiveMinutesFromNowUTC.ToString("HH:mm")

Invoke-Command -ComputerName ${RPS_ENDPOINT} -ConfigurationName FSxRemoteAdmin -
ScriptBlock {
```

```
    Set-FSxDedupSchedule -Name "WeeklyGarbageCollection" -Days $Using:DayOfWeek -
Start $Using:Time -DurationHours 9
}
```

3. Une fois que le travail de collecte des ordures est terminé et que l'espace a été libéré, redéfinissez le calendrier à ses paramètres d'origine.

Quotas de stockage

Vous pouvez configurer des quotas de stockage utilisateur sur vos systèmes de fichiers afin de limiter la quantité de stockage de données que les utilisateurs peuvent consommer. Après avoir défini les quotas, vous pouvez suivre l'état des quotas pour surveiller l'utilisation et voir quand les utilisateurs dépassent leurs quotas.

Vous pouvez également appliquer des quotas en empêchant les utilisateurs qui atteignent leurs quotas d'écrire dans l'espace de stockage. Lorsque vous appliquez des quotas, un utilisateur qui dépasse son quota reçoit un message d'erreur « espace disque insuffisant ».

Vous pouvez définir les seuils suivants pour les paramètres de quota :

- Avertissement : utilisé pour savoir si un utilisateur ou un groupe approche de sa limite de quota, uniquement pour le suivi.
- Limite : limite de quota de stockage pour un utilisateur ou un groupe.

Vous pouvez configurer des quotas par défaut qui sont appliqués aux nouveaux utilisateurs qui accèdent à un système de fichiers et des quotas qui s'appliquent à des utilisateurs ou à des groupes spécifiques. Vous pouvez également consulter un rapport indiquant la quantité de stockage consommée par chaque utilisateur ou groupe et indiquant s'ils dépassent leurs quotas.

La consommation de stockage au niveau de l'utilisateur est suivie en fonction de la propriété des fichiers. La consommation de stockage est calculée en fonction de la taille logique des fichiers, et non de l'espace de stockage physique réel occupé par les fichiers. Les quotas de stockage des utilisateurs sont suivis au moment où les données sont écrites dans un fichier.

La mise à jour des quotas pour plusieurs utilisateurs nécessite soit d'exécuter la commande de mise à jour une fois pour chaque utilisateur, soit d'organiser les utilisateurs dans un groupe et de mettre à jour le quota pour ce groupe.

Gestion des quotas de stockage des utilisateurs

Vous pouvez gérer les quotas de stockage des utilisateurs sur votre système de fichiers à l'aide de l'interface de ligne de commande Amazon FSx pour la gestion à distance sur. PowerShell Pour savoir comment utiliser cette CLI, consultezUtilisation de l'interface de ligne de commande Amazon FSx pour PowerShell.

Vous trouverez ci-dessous les commandes que vous pouvez utiliser pour gérer les quotas de stockage des utilisateurs.

Commande de quotas de stockage utilisateur	Description
Enable-FSxUserQuotas	Commence à suivre ou à appliquer les quotas de stockage des utilisateurs, ou les deux.
Disable-FSxUserQuotas	Arrête le suivi et l'application des quotas de stockage des utilisateurs.
Get-FSxUserQuotaSettings	Récupère les paramètres actuels du quota de stockage utilisate ur pour le système de fichiers.
Get-FSxUserQuotaEntries	Récupère les entrées de quota de stockage utilisateur actuelles pour les utilisateurs individuels et les groupes du système de fichiers.
Set-FSxUserQuotas	Définissez le quota de stockage utilisateur pour un utilisateur ou un groupe individuel. Les valeurs de quota sont spécifiées en octets.

L'aide en ligne de chaque commande fournit une référence de toutes les options de commande. Pour accéder à cette aide, exécutez la commande avec-?, par exempleEnable-FSxUserQuotas -?.

Gestion du chiffrement en transit

Vous pouvez utiliser un ensemble de PowerShell commandes personnalisées pour contrôler le chiffrement de vos données en transit entre votre système de fichiers FSx for Windows File Server et les clients. Vous pouvez limiter l'accès au système de fichiers aux seuls clients prenant en charge

le chiffrement SMB afin que celui-ci data-in-transit soit toujours chiffré. Lorsque l'application du chiffrement est activée data-in-transit, les utilisateurs accédant au système de fichiers depuis des clients qui ne prennent pas en charge le chiffrement SMB 3.0 ne pourront pas accéder aux partages de fichiers pour lesquels le chiffrement est activé.

Vous pouvez également contrôler le chiffrement au niveau du data-in-transit partage de fichiers plutôt qu'au niveau du serveur de fichiers. Vous pouvez utiliser les contrôles de chiffrement au niveau du partage de fichiers pour associer des partages de fichiers chiffrés et non chiffrés sur le même système de fichiers si vous souhaitez appliquer le chiffrement en transit à certains partages de fichiers contenant des données sensibles et permettre à tous les utilisateurs d'accéder à d'autres partages de fichiers. Le chiffrement à l'échelle du serveur a priorité sur le chiffrement au niveau du partage. Si le chiffrement global est activé, vous ne pouvez pas désactiver le chiffrement de manière sélective pour certains partages.

Vous pouvez gérer le chiffrement des utilisateurs en transit sur votre système de fichiers à l'aide de l'interface de ligne de commande Amazon FSx pour la gestion à distance PowerShell sur. Pour savoir comment utiliser cette CLI, consultezUtilisation de l'interface de ligne de commande Amazon FSx pour PowerShell.

Vous trouverez ci-dessous les commandes que vous pouvez utiliser pour gérer le chiffrement des utilisateurs en transit sur votre système de fichiers.

Chiffrement dans Transit Command	Description
Get-FSxSmbServerConfiguration	Récupère la configuration du serveur SMB (Server Message Block).
Set-FSxSmbServerConfiguration	Cette commande propose deux options pour configurer le chiffrement en transit : • `-EncryptData $True\|$False` — Définissez ce paramètre sur pour `True` activer le chiffrement des données en transit. Définissez ce paramètre sur `False` pour désactiver le chiffrement des données en transit. • `-RejectUnencryptedAccess $True\|$False` — Définissez ce paramètre sur pour `True` interdire aux clients qui ne prennent pas en charge le chiffrement d'accéder au

Chiffrement dans Transit Command	Description
	système de fichiers. Définissez ce paramètre sur `False` pour autoriser les clients qui ne prennent pas en charge le chiffrement à accéder au système de fichiers.

L'aide en ligne de chaque commande fournit une référence de toutes les options de commande. Pour accéder à cette aide, exécutez la commande avec-?, par exempleGet-FSxSmbServerConfiguration -?.

Gestion de la configuration du stockage

La configuration de stockage de votre système de fichiers inclut la capacité de stockage, le type de stockage et les IOPS du SSD. Vous pouvez configurer ces ressources ainsi que la capacité de débit afin d'atteindre le niveau de performance souhaité pour votre charge de travail, pendant et après la création de votre système de fichiers. Pour plus d'informations, consultez les rubriques suivantes.

Rubriques

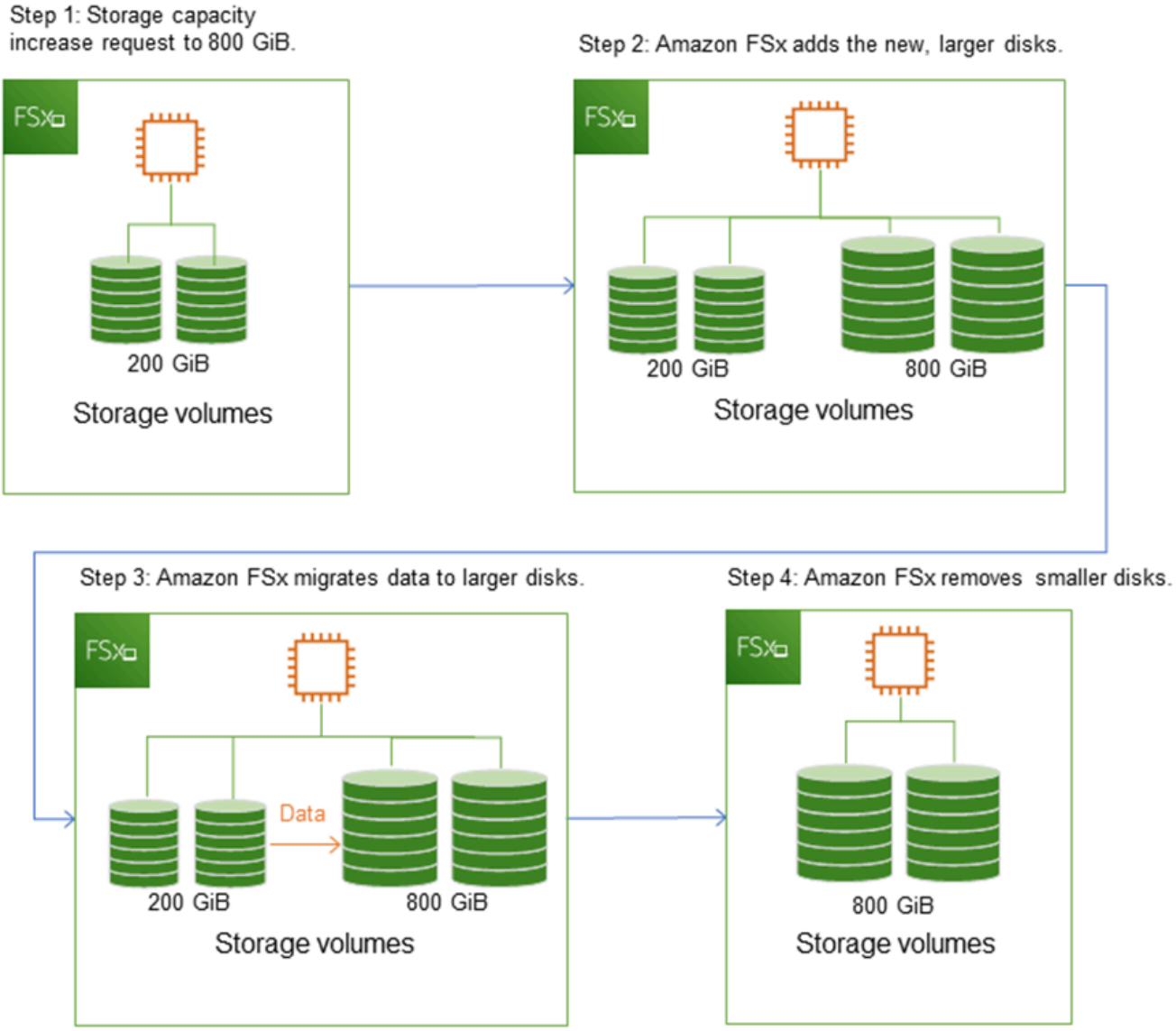
Gestion de la capacité de stockage

Vous pouvez augmenter la capacité de stockage configurée sur votre système de fichiers FSx for Windows File Server selon vos besoins. Vous pouvez le faire à l'aide de la console Amazon FSx, de l'API Amazon FSx ou du (). AWS Command Line Interface AWS CLI Vous pouvez uniquement augmenter la capacité de stockage d'un système de fichiers ; vous ne pouvez pas diminuer la capacité de stockage.

> **Note**
>
> Vous ne pouvez pas augmenter la capacité de stockage des systèmes de fichiers créés avant le 23 juin 2019 ou des systèmes de fichiers restaurés à partir d'une sauvegarde appartenant à un système de fichiers créé avant le 23 juin 2019.

Lorsque vous augmentez la capacité de stockage de votre système de fichiers Amazon FSx, Amazon FSx ajoute en arrière-plan un nouvel ensemble de disques plus volumineux à votre système de fichiers. Amazon FSx exécute ensuite un processus d'optimisation du stockage en arrière-plan afin de migrer de manière transparente les données des anciens disques vers les nouveaux disques. L'optimisation du stockage peut prendre de quelques heures à quelques jours, avec un impact notable minime sur les performances de la charge de travail. Au cours de cette optimisation, l'utilisation des sauvegardes est temporairement plus élevée, car les anciens et les nouveaux volumes de stockage sont inclus dans les sauvegardes au niveau du système de fichiers. Les deux ensembles de volumes de stockage sont inclus pour garantir qu'Amazon FSx puisse prendre et restaurer avec succès à partir de sauvegardes, même pendant les activités de dimensionnement du stockage. L'utilisation des sauvegardes revient à son niveau de référence précédent une fois que les anciens volumes de stockage ne sont plus inclus dans l'historique des sauvegardes. Lorsque la nouvelle capacité de stockage est disponible, seule la nouvelle capacité de stockage vous est facturée.

L'illustration suivante montre les quatre étapes principales du processus utilisé par Amazon FSx pour augmenter la capacité de stockage d'un système de fichiers.



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

Rubriques

- Points importants à connaître lors de l'augmentation de la capacité de stockage

- Quand augmenter la capacité de stockage
- Augmentation de la capacité de stockage et des performances du système de fichiers
- Comment augmenter la capacité de stockage
- Surveillance de l'augmentation de la capacité de stockage
- Augmenter dynamiquement la capacité de stockage d'un système de fichiers FSx for Windows File Server

Points importants à connaître lors de l'augmentation de la capacité de stockage

Voici quelques points importants à prendre en compte lors de l'augmentation de la capacité de stockage :

- Augmenter uniquement : vous pouvez uniquement augmenter la capacité de stockage d'un système de fichiers ; vous ne pouvez pas diminuer la capacité de stockage.
- Augmentation minimale : chaque augmentation de capacité de stockage doit être d'au moins 10 % de la capacité de stockage actuelle du système de fichiers, jusqu'à la valeur maximale autorisée de 65 536 GiB.
- Capacité de débit minimale : pour augmenter la capacité de stockage, un système de fichiers doit avoir une capacité de débit minimale de 16 Mo/s. Cela est dû au fait que l'étape d'optimisation du stockage est un processus gourmand en débit.
- Intervalle entre les augmentations : vous ne pouvez pas augmenter davantage la capacité de stockage d'un système de fichiers jusqu'à 6 heures après la dernière demande d'augmentation ou avant la fin du processus d'optimisation du stockage, selon le délai le plus long. L'optimisation du stockage peut prendre de quelques heures à quelques jours. Pour réduire le temps nécessaire à l'optimisation du stockage, nous vous recommandons d'augmenter la capacité de débit de votre système de fichiers avant d'augmenter la capacité de stockage (la capacité de débit peut être réduite une fois le dimensionnement du stockage terminé), et d'augmenter la capacité de stockage lorsque le trafic sur le système de fichiers est minimal.

> **Note**
>
> Certains événements du système de fichiers peuvent consommer les ressources de performance des E/S du disque. Par exemple :
> La phase d'optimisation de la mise à l'échelle de la capacité de stockage peut générer une augmentation du débit du disque et éventuellement provoquer des avertissements en

matière de performances. Pour plus d'informations, veuillez consulter Avertissements et recommandations en matière de performances.

Quand augmenter la capacité de stockage

Augmentez la capacité de stockage de votre système de fichiers lorsque la capacité de stockage disponible est insuffisante. Utilisez cette `FreeStorageCapacity` CloudWatch métrique pour contrôler la quantité de stockage gratuit disponible sur le système de fichiers. Vous pouvez créer une CloudWatch alarme Amazon sur cette métrique et être averti lorsqu'elle tombe en dessous d'un seuil spécifique. Pour plus d'informations, veuillez consulter Surveillance des métriques avec Amazon CloudWatch.

Nous vous recommandons de conserver à tout moment au moins 10 % de la capacité de stockage disponible sur votre système de fichiers. L'utilisation de l'ensemble de votre capacité de stockage peut avoir un impact négatif sur vos performances et entraîner des incohérences dans les données.

Vous pouvez augmenter automatiquement la capacité de stockage de votre système de fichiers lorsque la capacité de stockage disponible tombe en dessous d'un seuil défini que vous spécifiez. Utilisez le AWS AWS CloudFormation modèle personnalisé développé pour déployer tous les composants nécessaires à la mise en œuvre de la solution automatisée. Pour plus d'informations, veuillez consulter Augmenter la capacité de stockage de manière dynamique.

Augmentation de la capacité de stockage et des performances du système de fichiers

La plupart des charges de travail ont un impact minimal sur les performances tandis qu'Amazon FSx exécute le processus d'optimisation du stockage en arrière-plan une fois que la nouvelle capacité de stockage est disponible. Les applications à forte intensité d'écriture avec de grands ensembles de données actifs peuvent temporairement voir leurs performances d'écriture réduites de moitié. Dans ces cas, vous pouvez d'abord augmenter la capacité de débit de votre système de fichiers avant d'augmenter la capacité de stockage. Cela vous permet de continuer à fournir le même niveau de débit pour répondre aux besoins de performance de votre application. Pour plus d'informations, veuillez consulter Gestion de la capacité de débit.

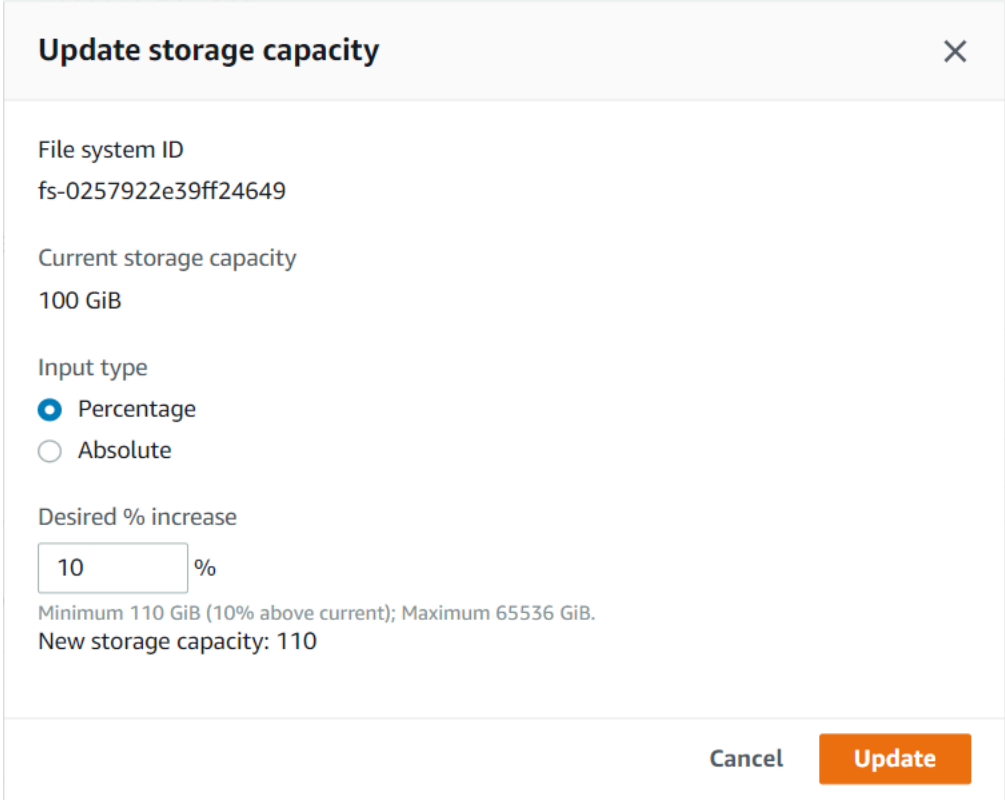
Comment augmenter la capacité de stockage

Vous pouvez augmenter la capacité de stockage d'un système de fichiers à l'aide de la console Amazon FSx, de l'AWS CLIAPI Amazon FSx ou de l'API Amazon FSx.

Pour augmenter la capacité de stockage d'un système de fichiers (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Accédez à Systèmes de fichiers et choisissez le système de fichiers Windows pour lequel vous souhaitez augmenter la capacité de stockage.
3. Pour Actions, choisissez Mettre à jour le stockage. Ou, dans le panneau Résumé, choisissez Mettre à jour à côté de la capacité de stockage du système de fichiers.

   La fenêtre Mettre à jour la capacité de stockage apparaît.



4. Pour Type d'entrée, choisissez Pourcentage pour saisir la nouvelle capacité de stockage sous forme de variation en pourcentage par rapport à la valeur actuelle, ou choisissez Absolu pour saisir la nouvelle valeur en GiB.
5. Entrez la capacité de stockage souhaitée.

   > **Note**
   >
   > La valeur de capacité souhaitée doit être supérieure d'au moins 10 % à la valeur actuelle, jusqu'à la valeur maximale de 65 536 GiB.

6. Choisissez Mettre à jour pour lancer la mise à jour de la capacité de stockage.

7. Vous pouvez suivre la progression de la mise à jour sur la page détaillée des systèmes de fichiers, dans l'onglet Mises à jour.

Pour augmenter la capacité de stockage d'un système de fichiers (CLI)

Pour augmenter la capacité de stockage d'un système de fichiers FSx for Windows File Server, utilisez AWS CLI la update-file-systemcommande. Définissez les paramètres suivants :

- `--file-system-id`à l'ID du système de fichiers que vous mettez à jour.
- `--storage-capacity`à une valeur supérieure d'au moins 10 % à la valeur actuelle.

Vous pouvez suivre la progression de la mise à jour à l'aide de la AWS CLI commande describe-file-systems. Recherchez le `administrative-actions` dans la sortie.

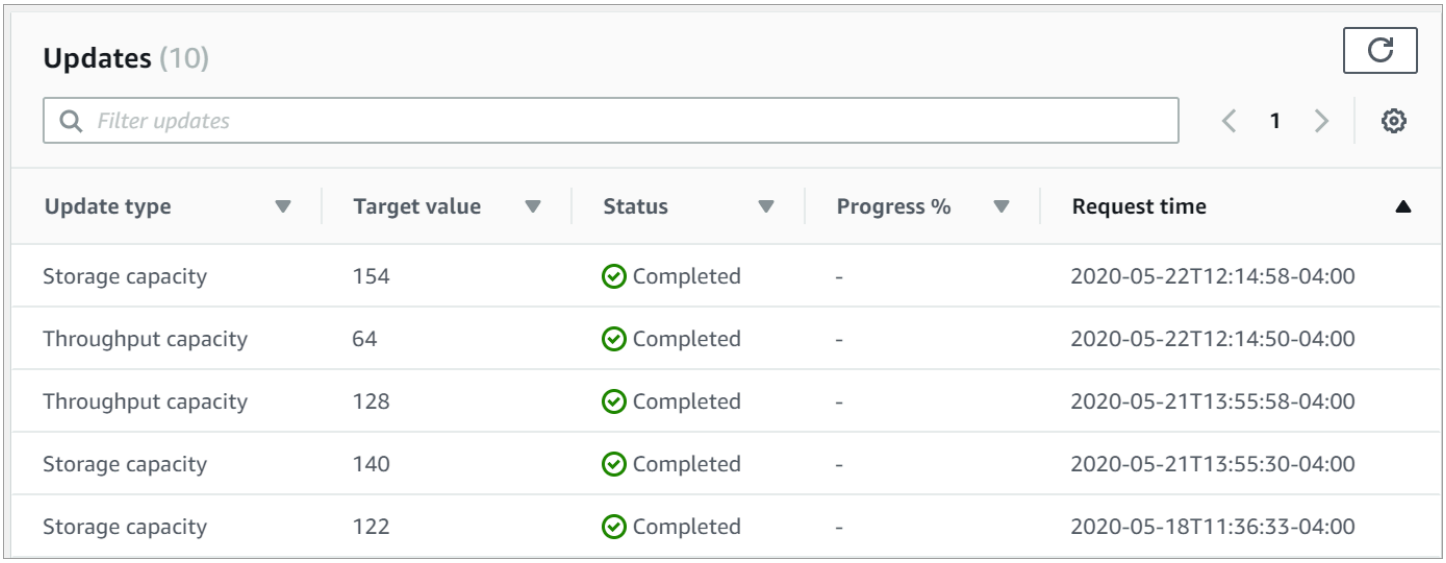
Pour plus d'informations, consultez AdministrativeAction.

Surveillance de l'augmentation de la capacité de stockage

Vous pouvez suivre la progression d'une augmentation de capacité de stockage à l'aide de la console Amazon FSx, de l'API ou du. AWS CLI

Surveillance des augmentations dans la console

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



Pour les mises à jour de la capacité de stockage, vous pouvez consulter les informations suivantes.

Type de mise à jour

Les valeurs possibles sont Capacité de stockage.

Valeur cible

La valeur souhaitée pour mettre à jour la capacité de stockage du système de fichiers.

État

État actuel de la mise à jour. Pour les mises à jour de la capacité de stockage, les valeurs possibles sont les suivantes :

- En attente : Amazon FSx a reçu la demande de mise à jour, mais n'a pas commencé à la traiter.
- En cours — Amazon FSx traite la demande de mise à jour.
- Optimisation mise à jour : Amazon FSx a augmenté la capacité de stockage du système de fichiers. Le processus d'optimisation du stockage déplace désormais les données du système de fichiers vers les nouveaux disques plus grands.
- Terminé — L'augmentation de la capacité de stockage s'est terminée avec succès.
- Échec — L'augmentation de la capacité de stockage a échoué. Choisissez le point d'interrogation (?) pour connaître les raisons de l'échec de la mise à jour du stockage.

% 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.

La surveillance des augmentations avec l'API AWS CLI and

Vous pouvez afficher et surveiller les demandes d'augmentation de la capacité de stockage du système de fichiers à l'aide de la describe-file-systemsAWS CLIcommande et de l'action de l'DescribeFileSystemsAPI. Le `AdministrativeActions` tableau répertorie les 10 actions de mise à jour les plus récentes pour chaque type d'action administrative. Lorsque vous augmentez la capacité de stockage d'un système de fichiers, deux `AdministrativeActions` sont générés : une action `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 a une capacité de stockage de 300 Go et une action administrative est en cours pour augmenter la capacité de stockage à 1 000 Go.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 300,
            "AdministrativeActions": [
                {
                     "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                     "RequestTime": 1581694764.757,
                     "Status": "PENDING",
                     "TargetFileSystemValues": {
                         "StorageCapacity": 1000
                     }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "PENDING",
                }
            ]
```

Amazon FSx traite `FILE_SYSTEM_UPDATE` d'abord l'action, en ajoutant les nouveaux disques de stockage plus volumineux au système de fichiers. Lorsque le nouveau stockage est disponible pour le système de fichiers, l'`FILE_SYSTEM_UPDATE`état passe à`UPDATED_OPTIMIZING`. La capacité de stockage indique la nouvelle valeur supérieure, et Amazon FSx commence à traiter l'action `STORAGE_OPTIMIZATION` administrative. Cela 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.

```
{
```

```
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 1000,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "RequestTime": 1581694764.757,
                    "Status": "UPDATED_OPTIMIZING",
                    "TargetFileSystemValues": {
                        "StorageCapacity": 1000
                }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "IN_PROGRESS",
                    "ProgressPercent": 50,
                }
            ]
```

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

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 300,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "FailureDetails": {
                        "Message": "string"
                    },
```

```
                "RequestTime": 1581694764.757,
                "Status": "FAILED",
                "TargetFileSystemValues":
                    "StorageCapacity": 1000
            }
        ]
```

Pour plus d'informations sur le dépannage des actions ayant échoué, consultezLes mises à jour de capacité de stockage ou de débit échouent.

Augmenter dynamiquement la capacité de stockage d'un système de fichiers FSx for Windows File Server

Vous pouvez utiliser la solution suivante pour augmenter dynamiquement la capacité de stockage d'un système de fichiers FSx for Windows File Server lorsque la capacité de stockage disponible tombe en dessous d'un seuil défini que vous spécifiez. Ce AWS CloudFormation modèle déploie automatiquement tous les composants nécessaires pour définir le seuil de capacité de stockage disponible, l' CloudWatchalarme Amazon basée sur ce seuil et la AWS Lambda fonction qui augmente la capacité de stockage du système de fichiers.

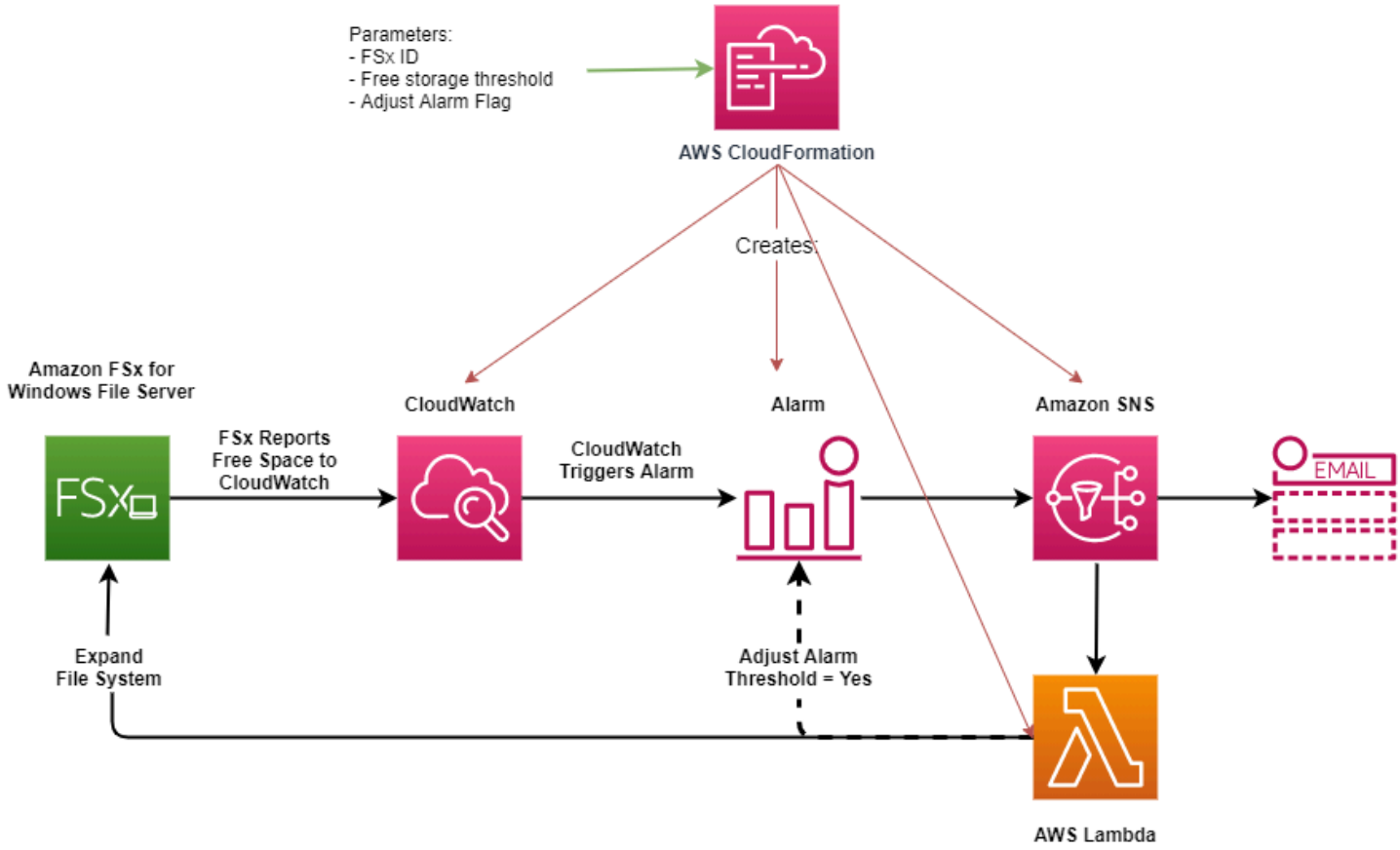
La solution déploie automatiquement tous les composants nécessaires et prend en compte les paramètres suivants :

- L'ID du système de fichiers
- Le seuil de capacité de stockage disponible (valeur numérique)
- Unité de mesure (pourcentage [par défaut] ou GiB)
- Pourcentage d'augmentation de la capacité de stockage (%)
- L'adresse e-mail pour l'abonnement SNS
- Régler le seuil d'alarme (Oui/Non)

Rubriques

Présentation de l'architecture

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



Le diagramme suivant illustre les étapes suivantes :

1. Le AWS CloudFormation modèle déploie une CloudWatch alarme, une AWS Lambda fonction, une file d'attente Amazon Simple Notification Service (Amazon SNS) et tous les rôles requis AWS Identity and Access Management (IAM). Le rôle IAM autorise la fonction Lambda à appeler les opérations de l'API Amazon FSx.
2. CloudWatch déclenche une alarme lorsque la capacité de stockage disponible du système de fichiers passe en dessous du seuil spécifié et envoie un message à la file d'attente Amazon SNS.
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. La fonction Lambda peut éventuellement ajuster le seuil de capacité de stockage disponible afin qu'il soit égal à un pourcentage spécifié de la nouvelle capacité de stockage du système de fichiers.
6. 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.

Modèle AWS CloudFormation

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 Windows File Server. Pour utiliser cette solution, téléchargez le SxSize AWS CloudFormation modèle IncreaseF.

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 initial de capacité de stockage libre à partir duquel déclencher une alarme et augmenter automatiquement la capacité de stockage du système de fichiers, spécifié en GiB ou en pourcentage (%) de la capacité de stockage actuelle du système de fichiers. Exprimé en pourcentage, le CloudFormation modèle est recalculé en GiB pour correspondre aux paramètres de l'alarme. CloudWatch

LowFreeDataStorageCapacityThresholdUnit

La valeur par défaut est %. Spécifie les unités pour le`LowFreeDataStorageCapacityThreshold`, soit en GiB, soit en pourcentage de la capacité de stockage actuelle.

AlarmModificationNotification

La valeur par défaut est Oui. Si elle est définie sur Oui, la valeur initiale `LowFreeDataStorageCapacityThreshold` est augmentée proportionnellement à la valeur des `PercentIncrease` seuils d'alarme suivants.

Par exemple, lorsqu'il `PercentIncrease` est défini sur 20 et AlarmModificationNotification défini sur Oui, le seuil d'espace libre disponible (`LowFreeDataStorageCapacityThreshold`) spécifié en GiB est augmenté de 20 % pour les événements d'augmentation de capacité de stockage ultérieurs.

EmailAddress

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

PercentIncrease

Aucune valeur par défaut. Spécifie le montant d'augmentation de la capacité de stockage, exprimé en pourcentage de la capacité de stockage actuelle.

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 Windows File Server. Le déploiement prend environ 5 minutes.

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

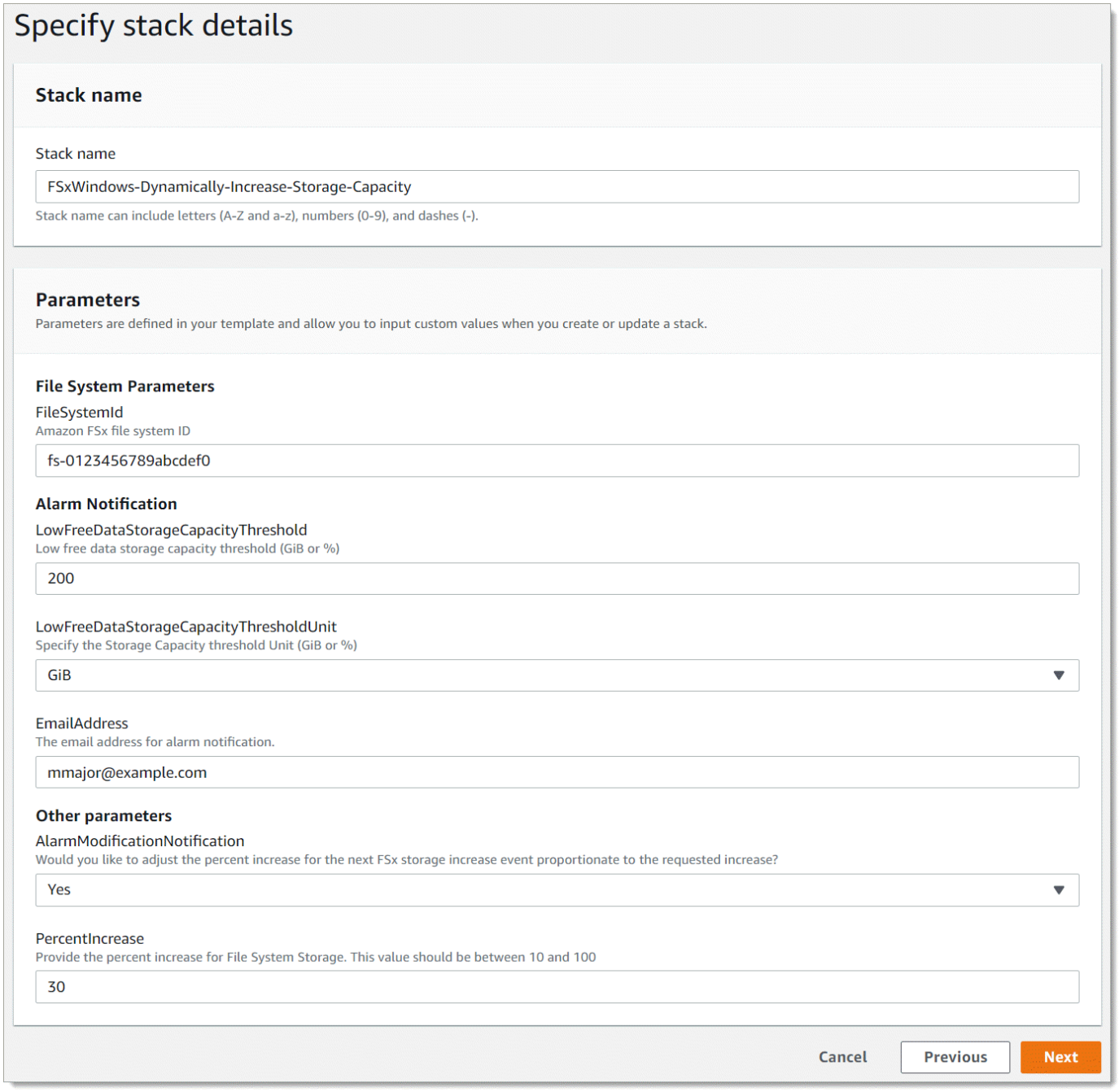
Avant de commencer, vous devez disposer de l'ID du système de fichiers Amazon FSx exécuté dans un Amazon Virtual Private Cloud (Amazon VPC) sur votre compte. AWS Pour plus d'informations sur la création de ressources Amazon FSx, consultez. Commencer à utiliser Amazon FSx for Windows File Server

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

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

2. Dans Spécifier les détails de la pile, entrez les valeurs de votre solution d'augmentation automatique de la capacité de stockage.



3. Entrez un nom de pile.
4. Pour les paramètres, passez en revue les paramètres du modèle et modifiez-les en fonction des besoins de votre système de fichiers. Sélectionnez ensuite Next (Suivant).
5. Entrez les paramètres d'options que vous souhaitez pour votre solution personnalisée, puis choisissez Next.
6. Pour Révision, vérifiez et confirmez les paramètres de la solution. Vous devez cocher la case indiquant que le modèle crée des ressources IAM.

7. Choisissez Create pour déployer la pile.

Vous pouvez voir l'état de la pile dans la console AWS CloudFormation dans la colonne Status (État). Vous devriez voir le statut CREATE_COMPLETE dans environ 5 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 CloudFormationutilisateur.

Gestion du type de stockage

FSx for Windows File Server propose des types de stockage sur disque SSD (Solid State Drive) et sur disque dur magnétique (HDD). Le stockage SSD est conçu pour les charges de travail les plus performantes et les plus sensibles à la latence, notamment les bases de données, les charges de travail de traitement multimédia et les applications d'analyse de données. Le stockage sur disque dur est conçu pour un large éventail de charges de travail, notamment les répertoires personnels, les partages de fichiers entre utilisateurs et départements et les systèmes de gestion de contenu.

Vous pouvez modifier le type de stockage de votre système de fichiers, du disque dur au SSD à l'aide de la console Amazon FSx ou de l'API Amazon FSx. Vous ne pouvez pas modifier le type de stockage de votre système de fichiers de SSD à HDD. N'oubliez pas que vous ne pouvez pas mettre à jour à nouveau la configuration de votre système de fichiers 6 heures après la dernière demande de mise à jour ou avant la fin du processus d'optimisation du stockage, selon le délai le plus long. L'optimisation du stockage peut prendre entre quelques heures et quelques jours. Pour réduire ce temps, nous vous recommandons de mettre à jour votre type de stockage lorsque le trafic sur votre système de fichiers est minimal.

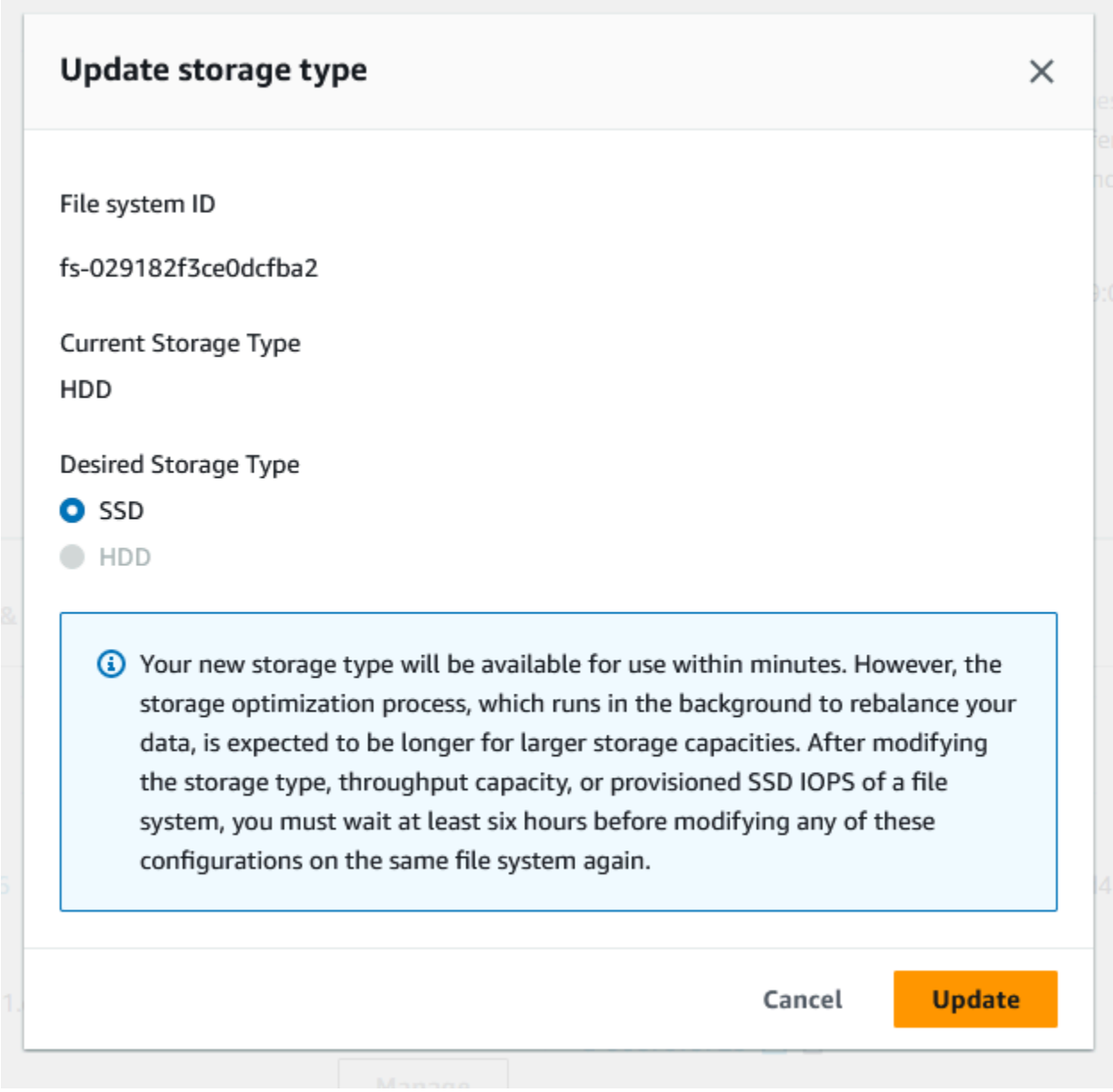
Vous pouvez également modifier le type de stockage de votre système de fichiers du disque dur au SSD en restaurant une sauvegarde disponible pour créer un nouveau système de fichiers et en sélectionnant un nouveau type de stockage. Pour plus d'informations, veuillez consulter Restauration des sauvegardes.

Comment mettre à jour le type de stockage

Vous pouvez mettre à jour le type de stockage d'un système de fichiers à l'aide de la console Amazon FSx, de l'AWS CLIAPI Amazon FSx ou de l'API Amazon FSx.

Pour mettre à jour le type de stockage d'un système de fichiers (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Accédez à Systèmes de fichiers et choisissez le système de fichiers Windows pour lequel vous souhaitez mettre à jour le type de stockage.
3. Sous Actions, sélectionnez Mettre à jour le type de stockage. Ou, dans le panneau Résumé, sélectionnez le bouton Mettre à jour à côté du disque dur. La fenêtre Mettre à jour le type de stockage apparaît.



4. Pour le type de stockage souhaité, choisissez SSD. Choisissez Mettre à jour pour lancer la mise à jour du type de stockage.

5. Vous pouvez suivre la progression de la mise à jour sur la page détaillée des systèmes de fichiers, dans l'onglet Mises à jour.

Pour mettre à jour le type de stockage d'un système de fichiers (CLI)

Pour mettre à jour le type de stockage d'un système de fichiers FSx for Windows File Server, utilisez AWS CLI la update-file-systemcommande. Définissez les paramètres suivants :

- `--file-system-id`à l'ID du système de fichiers que vous souhaitez mettre à jour.
- `--storage-type`sur SSD. Vous ne pouvez pas passer d'un type de stockage SSD à un type de stockage HDD.

Vous pouvez suivre la progression de la mise à jour à l'aide de la AWS CLI commande describe-file-systems. Recherchez le `administrative-actions` dans la sortie.

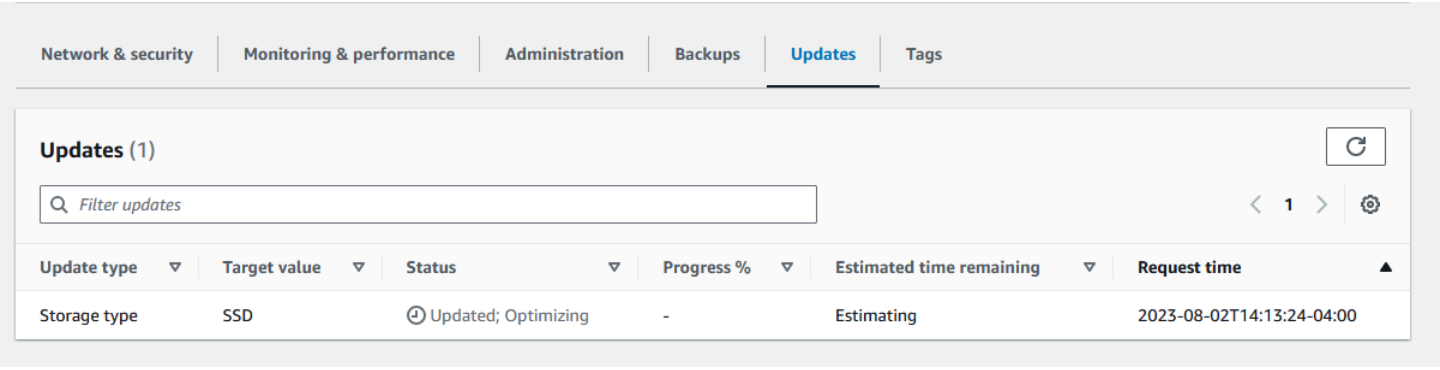
Pour plus d'informations, consultez AdministrativeAction.

Surveillance des mises à jour des types de stockage

Vous pouvez suivre la progression d'une mise à jour d'un type de stockage à l'aide de la console Amazon FSx, de l'API ou du. AWS CLI

Surveillance des mises à jour dans la console

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



Pour les mises à jour des types de stockage, vous pouvez consulter les informations suivantes.

Type de mise à jour

La valeur possible est le type de stockage.

Valeur cible

SSD

État

État actuel de la mise à jour. Pour les mises à jour des types de stockage, les valeurs possibles sont les suivantes :

- En attente : Amazon FSx a reçu la demande de mise à jour, mais n'a pas commencé à la traiter.
- En cours — Amazon FSx traite la demande de mise à jour.
- Optimisation mise à jour : les performances du stockage SSD sont disponibles pour les opérations d'écriture de votre charge de travail. Votre mise à jour entrera dans un état d'optimisation actualisé, qui dure généralement quelques heures, au cours duquel les opérations de lecture de votre charge de travail auront des niveaux de performance entre le disque dur et le SSD. Une fois votre action de mise à jour terminée, les performances de votre nouveau SSD sont disponibles en lecture et en écriture.
- Terminé : la mise à jour du type de stockage s'est terminée avec succès.
- Échec : la mise à jour du type de stockage a échoué. Choisissez le point d'interrogation (?) pour en savoir plus.

% de progression

Affiche la progression du processus d'optimisation du stockage en pourcentage d'achèvement.

Heure de la demande

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

Surveillance des mises à jour avec l'API AWS CLI and

Vous pouvez afficher et surveiller les demandes de mise à jour du type de stockage du système de fichiers à l'aide de la describe-file-systemsAWS CLIcommande et de l'action de l'DescribeFileSystemsAPI. Le `AdministrativeActions` tableau répertorie les 10 actions de mise à jour les plus récentes pour chaque type d'action administrative. Lorsque vous augmentez le nombre d'IOPS du SSD d'un système de fichiers, deux `AdministrativeActions` sont générés : un `FILE_SYSTEM_UPDATE` et une `STORAGE_TYPE_OPTIMIZATION` action.

Gestion des IOPS sur SSD

Pour les volumes de stockage SSD, vous pouvez sélectionner et dimensionner les IOPS indépendamment de la capacité de stockage. Le nombre maximal d'IOPS sur SSD que vous pouvez provisionner dépend de la capacité de stockage et de la capacité de débit que vous sélectionnez pour votre système de fichiers. Si vous essayez d'augmenter le nombre d'IOPS de votre SSD au-dessus de la limite prise en charge par votre capacité de débit, vous devrez peut-être augmenter votre capacité de débit pour prendre en charge le niveau d'IOPS SSD requis. Pour plus d'informations, consultez Performances de FSx for Windows File Server et Gestion de la capacité de débit.

Rubriques

Points importants à connaître lors de la mise à jour des IOPS d'un SSD

Voici quelques points importants à prendre en compte lors de la mise à jour des IOPS d'un SSD :

- Pour spécifier le nombre d'IOPS SSD provisionnés pour votre système de fichiers, vous devez choisir l'un des deux modes d'IOPS suivants :
  - Automatique : Amazon FSx adapte automatiquement les IOPS de votre SSD pour maintenir 3 IOPS par GiB de capacité de stockage, soit jusqu'à 400 000 IOPS par SSD par système de fichiers.
  - Provisionné par l'utilisateur : vous spécifiez le nombre d'IOPS SSD compris entre 96 et 400 000. Spécifiez un nombre compris entre 3 et 50 IOPS par GiB de capacité de stockage pour tous les sites où Régions AWS Amazon FSx est disponible, ou entre 3 et 500 IOPS par GiB de capacité de stockage dans l'est des États-Unis (Virginie du Nord), l'ouest des États-Unis (Oregon), l'est des États-Unis (Ohio), l'Europe (Irlande), l'Asie-Pacifique (Tokyo) et l'Asie-Pacifique (Singapour). Si le nombre d'IOPS du SSD n'est pas d'au moins 3 IOPS par GiB, la demande échoue. Pour des niveaux plus élevés d'IOPS sur SSD provisionnés, vous payez pour une moyenne d'IOPS supérieure à 3 IOPS par GiB et par système de fichiers.
- Mises à jour de la capacité de stockage : si vous augmentez votre capacité de stockage et que la nouvelle capacité nécessite un niveau d'IOPS SSD supérieur au niveau d'IOPS SSD fourni

par l'utilisateur, Amazon FSx fait automatiquement passer votre système de fichiers en mode automatique.

- Mises à jour de la capacité de débit : si vous augmentez votre capacité de débit et que le nombre maximal d'IOPS SSD pris en charge par votre nouvelle capacité de débit est supérieur au niveau d'IOPS SSD fourni par l'utilisateur, Amazon FSx fait automatiquement passer votre système de fichiers en mode automatique.
- Délai entre les augmentations : vous ne pouvez pas augmenter davantage le nombre d'IOPS sur le SSD, augmenter la capacité de débit ou mettre à jour le type de stockage sur un système de fichiers jusqu'à 6 heures après la dernière demande d'augmentation ou avant la fin du processus d'optimisation du stockage, selon le délai le plus long. L'optimisation du stockage peut prendre de quelques heures à quelques jours. Pour réduire le temps nécessaire à l'optimisation du stockage, nous recommandons de dimensionner les IOPS des SSD lorsque le trafic sur le système de fichiers est minimal.

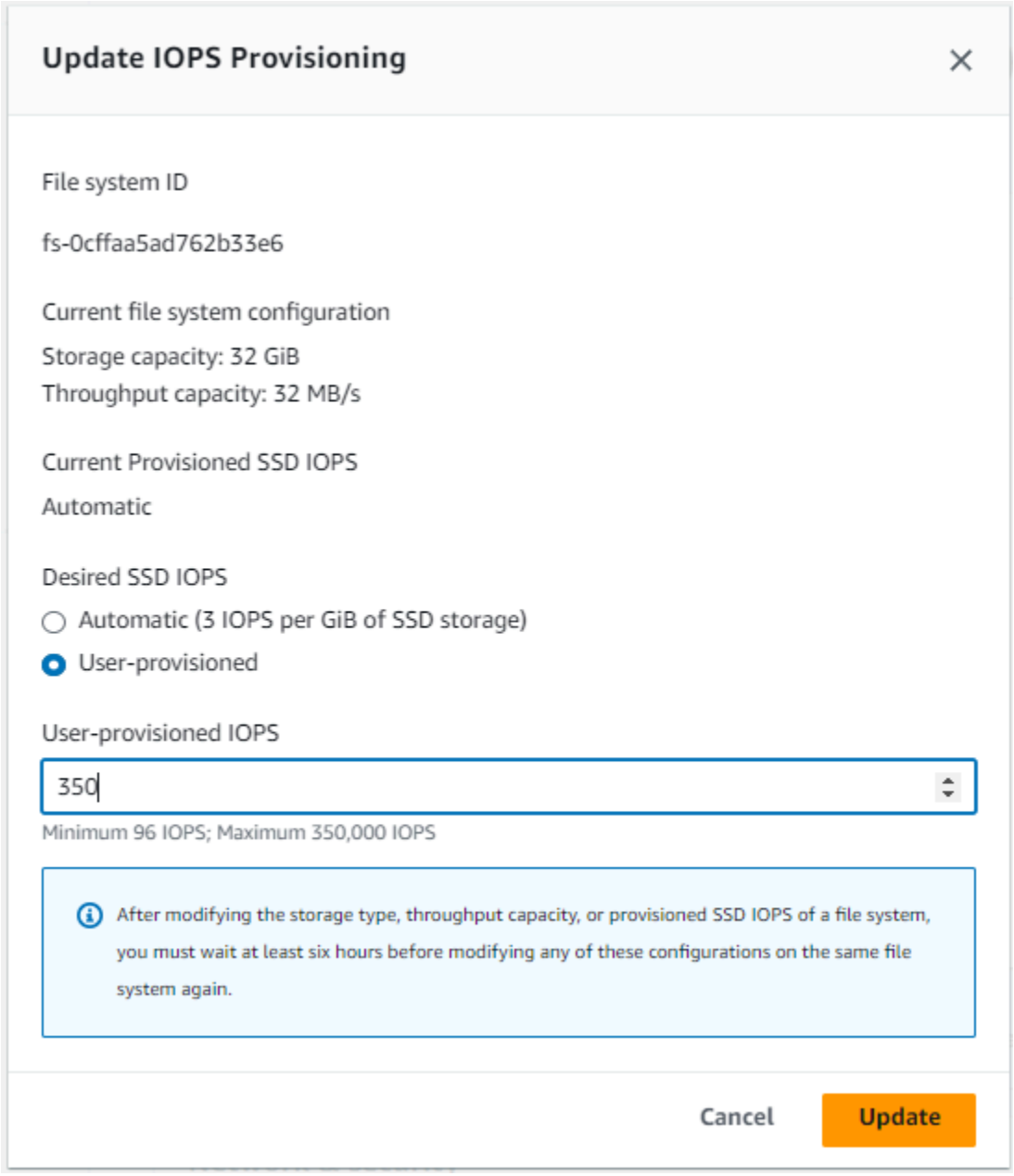
> **Note**
>
> Notez que les niveaux de capacité de débit supérieurs ou égaux à 4 608 Mbit/s ne sont pris en charge que dans les pays suivants Régions AWS : USA Est (Virginie du Nord), USA Ouest (Oregon), USA Est (Ohio), Europe (Irlande), Asie-Pacifique (Tokyo) et Asie-Pacifique (Singapour).

Comment mettre à jour les IOPS d'un SSD

Vous pouvez mettre à jour les IOPS SSD pour un système de fichiers à l'aide de la console Amazon FSx, de l'API Amazon FSx ou de AWS CLI l'API Amazon FSx.

Pour mettre à jour les IOPS du SSD pour un système de fichiers (console)

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Accédez à Systèmes de fichiers et choisissez le système de fichiers Windows pour lequel vous souhaitez mettre à jour les IOPS du SSD.
3. Sous Actions, sélectionnez Mettre à jour les IOPS du SSD. Ou, dans le panneau Résumé, sélectionnez le bouton Mettre à jour à côté de Provisioned SSD IOPS. La fenêtre Mettre à jour le provisionnement IOPS s'ouvre.



4. Pour Mode, choisissez Automatique ou Provisionné par l'utilisateur. Si vous choisissez Automatique, Amazon FSx fournit automatiquement 3 IOPS SSD par GiB de capacité de stockage pour votre système de fichiers. Si vous choisissez Provisionné par l'utilisateur, entrez un nombre entier compris entre 96 et 400 000.
5. Choisissez Mettre à jour pour lancer la mise à jour des IOPS du SSD provisionné.
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.

Pour mettre à jour les IOPS du SSD pour un système de fichiers (CLI)

Pour mettre à jour les IOPS SSD pour un système de fichiers FSx for Windows File Server, utilisez `--windows-configuration DiskIopsConfiguration` la propriété. Cette propriété comporte deux paramètres, à `Iops` savoir `Mode` :

- Si vous souhaitez spécifier le nombre d'IOPS sur SSD`Iops=`*`number_of_IOPS`*, utilisez un maximum de 400 000 dans les AWS régions prises en charge et. `Mode=USER_PROVISIONED`
- Si vous souhaitez qu'Amazon FSx augmente automatiquement les IOPS de votre SSD, utilisez `Mode=AUTOMATIC` et n'utilisez pas le paramètre. `Iops` Amazon FSx gère automatiquement 3 IOPS SSD par GiB de capacité de stockage sur votre système de fichiers, jusqu'à un maximum de 400 000 dans les régions prises en charge. AWS

Vous pouvez suivre la progression de la mise à jour à l'aide de la AWS CLI commande describe-file-systems. Recherchez le `administrative-actions` dans la sortie.

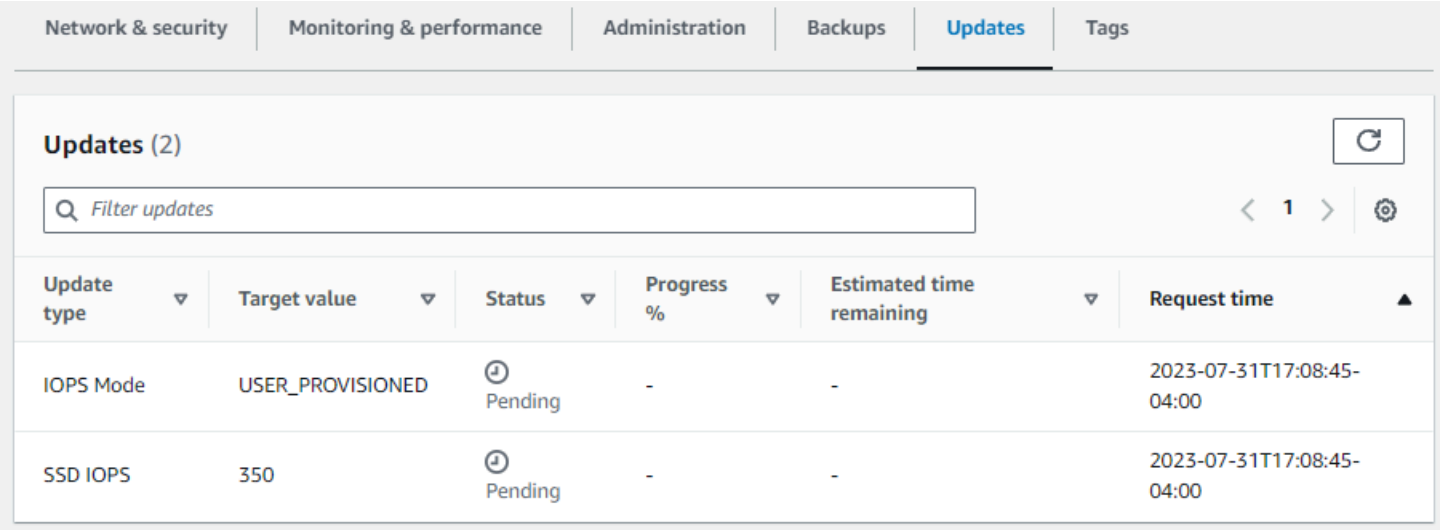
Pour plus d'informations, consultez AdministrativeAction.

Surveillance des mises à jour des IOPS SSD provisionnées

Vous pouvez suivre la progression d'une mise à jour des IOPS d'un SSD provisionné à l'aide de la console Amazon FSx, de l'API ou du. AWS CLI

Surveillance des mises à jour dans la console

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



Pour les mises à jour des IOPS des SSD provisionnés, vous pouvez consulter les informations suivantes.

Type de mise à jour

Les valeurs possibles sont le mode IOPS et le SSD IOPS.

Valeur cible

La valeur souhaitée pour mettre à jour le mode IOPS du système de fichiers et le mode IOPS du SSD vers.

Statut

État actuel de la mise à jour. Pour les mises à jour des IOPS sur SSD, les valeurs possibles sont les suivantes :

- En attente : Amazon FSx a reçu la demande de mise à jour, mais n'a pas commencé à la traiter.
- En cours — Amazon FSx traite la demande de mise à jour.
- Optimisation mise à jour : le nouveau niveau d'IOPS est disponible pour les opérations d'écriture de votre charge de travail. Votre mise à jour passe à un état d'optimisation mis à jour, qui dure généralement quelques heures, pendant lequel les opérations de lecture de votre charge de travail ont des performances IOPS comprises entre le niveau précédent et le nouveau niveau. Une fois votre action de mise à jour terminée, votre nouveau niveau d'IOPS est disponible en lecture et en écriture.
- Terminé — La mise à jour des IOPS du SSD s'est terminée avec succès.
- Échec — La mise à jour des IOPS du SSD a échoué. Choisissez le point d'interrogation (?) pour connaître les raisons de l'échec de la mise à jour du stockage.

% 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.

Surveillance des mises à jour avec l'API AWS CLI and

Vous pouvez afficher et surveiller les demandes de mise à jour des IOPS des SSD du système de fichiers à l'aide de la describe-file-systemsAWS CLIcommande et de l'action de l'DescribeFileSystemsAPI. Le `AdministrativeActions` tableau répertorie les 10 actions de mise à jour les plus récentes pour chaque type d'action administrative. Lorsque vous augmentez le nombre d'IOPS du SSD d'un système de fichiers, deux `AdministrativeActions` sont générés : un `FILE_SYSTEM_UPDATE` et une `IOPS_OPTIMIZATION` action.

Gestion de la capacité de débit

Chaque système de fichiers FSx pour Windows File Server possède une capacité de débit qui est configurée lorsque vous créez le système de fichiers. Vous pouvez modifier la capacité de débit de votre système de fichiers à tout moment, selon vos besoins. La capacité de débit est l'un des facteurs qui détermine la vitesse à laquelle le serveur de fichiers hébergeant le système de fichiers peut traiter les données de fichiers. Des niveaux de capacité de débit plus élevés s'accompagnent également de niveaux plus élevés d'opérations d'E/S par seconde (IOPS) et d'une augmentation de la mémoire pour la mise en cache des données sur le serveur de fichiers. Pour plus d'informations, veuillez consulter Performances de FSx for Windows File Server.

Lorsque vous modifiez la capacité de débit de votre système de fichiers, Amazon FSx désactive le serveur de fichiers du système de fichiers en arrière-plan. Pour les systèmes de fichiers multi-AZ, cela entraîne un basculement et un retour arrière automatiques tandis qu'Amazon FSx remplace les serveurs de fichiers préférés et secondaires. Pour les systèmes mono-AZ, votre système de fichiers ne sera pas disponible pendant quelques minutes pendant le dimensionnement de la capacité de débit. La nouvelle capacité de débit vous est facturée dès qu'elle est disponible pour votre système de fichiers.

> **Note**
>
> Lors d'une opération de maintenance sur le back-end, les modifications du système (telles que la modification de votre capacité de débit) peuvent être retardées. La maintenance peut entraîner la mise en file d'attente de ces modifications jusqu'à leur prochain traitement.

Rubriques

- Quand modifier la capacité de débit
- Comment modifier la capacité de débit

- Surveillance des variations de capacité de débit

Quand modifier la capacité de débit

Amazon FSx s'intègre à AmazonCloudWatch, vous permettant de surveiller les niveaux d'utilisation continus du débit de votre système de fichiers. Les performances (débit et IOPS) que vous pouvez générer via votre système de fichiers dépendent des caractéristiques spécifiques de votre charge de travail, ainsi que de la capacité de débit, de la capacité de stockage et du type de stockage de votre système de fichiers. Vous pouvez utiliserCloudWatchdes mesures pour déterminer laquelle de ces dimensions doit être modifiée pour améliorer les performances. Pour plus d'informations, veuillez consulter Surveillance des métriques avec Amazon CloudWatch.

Pour les systèmes de fichiers multi-AZ, le dimensionnement de la capacité de débit entraîne un basculement et une restauration automatiques tandis qu'Amazon FSx remplace les serveurs de fichiers préférés et secondaires. Lors des remplacements de serveurs de fichiers, qui se produisent lors de l'ajustement de la capacité de débit, de la maintenance du système de fichiers et d'une interruption de service imprévue, tout le trafic en cours vers le système de fichiers sera traité par le serveur de fichiers restant. Lorsque le serveur de fichiers remplacé est de nouveau en ligne, FSx pour Windows exécute une tâche de resynchronisation pour s'assurer que les données sont resynchronisées avec le serveur de fichiers nouvellement remplacé.

FSx pour Windows est conçu pour minimiser l'impact de cette activité de resynchronisation sur les applications et les utilisateurs. Toutefois, le processus de resynchronisation implique la synchronisation des données par blocs de grande taille. Cela signifie qu'un gros bloc de données peut nécessiter une synchronisation même si seule une petite partie est mise à jour. Par conséquent, le niveau de resynchronisation dépend non seulement du volume de désabonnement des données, mais également de la nature du taux de désabonnement des données sur le système de fichiers. Si votre charge de travail est lourde en écriture et en IOPS, le processus de synchronisation des données peut prendre plus de temps et nécessiter des ressources de performance supplémentaires.

Votre système de fichiers restera disponible pendant cette période, mais afin de réduire la durée de synchronisation des données, nous vous recommandons de modifier la capacité de débit pendant les périodes d'inactivité lorsque la charge sur votre système de fichiers est minimale. Nous vous recommandons également de vous assurer que votre système de fichiers dispose d'une capacité de débit suffisante pour exécuter la tâche de synchronisation en plus de votre charge de travail, afin de réduire la durée de la synchronisation des données. Enfin, nous vous recommandons de tester l'impact des basculements lorsque votre système de fichiers est moins chargé.

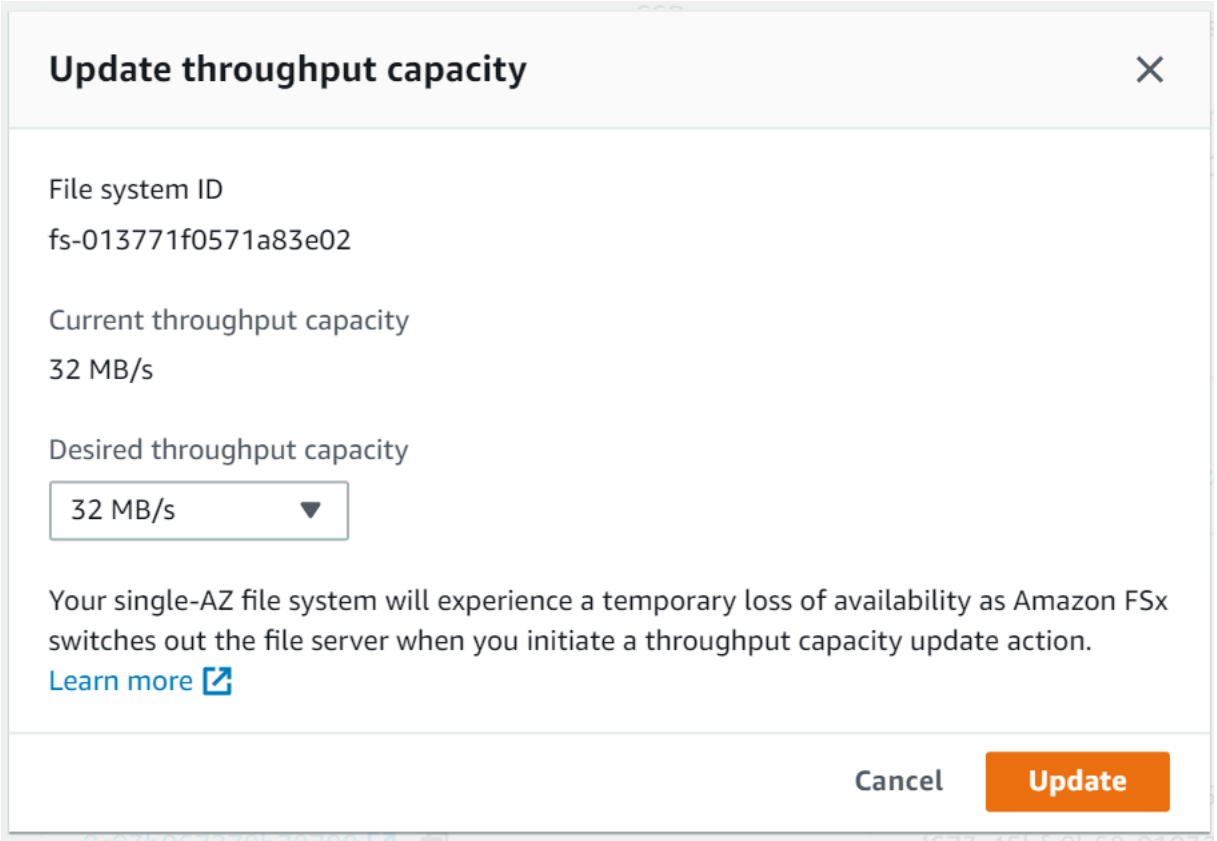
Comment modifier la capacité de débit

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

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

1. Ouvrez la console Amazon FSx à l'adressehttps://console.aws.amazon.com/fsx/.
2. Naviguez versSystèmes de fichiers, puis choisissez le système de fichiers Windows dont vous souhaitez augmenter la capacité de débit.
3. PourActions, choisissezDébit de mise à jour. Ou, dans leRésumépanneau, choisissezMettre à jourà côté du système de fichiersCapacité de débit.

   LeMettre à jour la capacité de débitune fenêtre s'affiche.
4. Choisissez la nouvelle valeur pourCapacité de débitde la liste.



5. ChoisissezMettre à jourpour lancer la mise à jour de la capacité de débit.

> **Note**
>
> Les systèmes de fichiers multi-AZ basculent et retombent lors de la mise à jour du dimensionnement du débit, et sont entièrement disponibles. Les systèmes de fichiers mono-AZ sont indisponibles pendant une très brève période pendant la mise à jour.

6. Vous pouvez suivre la progression de la mise à jour surSystèmes de fichierspage détaillée, dansmises à jouronglet.

   Vous pouvez suivre la progression de la mise à jour à l'aide de la console Amazon FSx,AWS CLI, et l'API. Pour plus d'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, utilisezAWS CLIcommandeupdate-file-system. Définissez les paramètres suivants :

- `--file-system-id`à l'ID du système de fichiers que vous mettez à jour.
- `ThroughputCapacity`à la valeur souhaitée pour mettre à jour le système de fichiers.

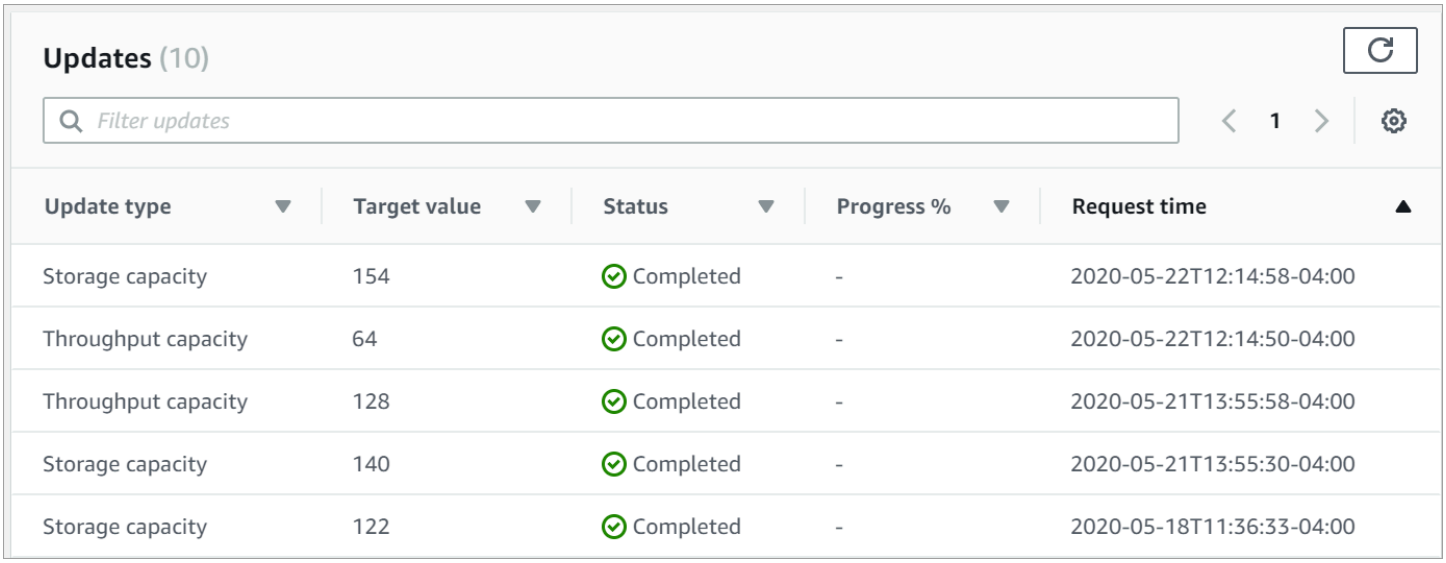
Vous pouvez suivre la progression de la mise à jour à l'aide de la console Amazon FSx,AWS CLI, et l'API. Pour plus d'informations, veuillez consulter Surveillance des variations de capacité de débit.

Surveillance des variations de capacité de débit

Vous pouvez suivre la progression d'une modification de la capacité de débit à l'aide de la console Amazon FSx, de l'API et duAWS CLI.

Surveillance des modifications de la capacité de débit dans la console

Dans lemises à jouronglet dansDétails du système de fichiersfenêtre, vous pouvez afficher 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

La valeur possible estCapacité de débit.

Valeur cible

La valeur à laquelle vous souhaitez modifier la capacité de débit du système de fichiers.

État

État actuel de la mise à jour. Pour les mises à jour de la capacité de débit, les valeurs possibles sont les suivantes :

- En attente— Amazon FSx a reçu la demande de mise à jour, mais n'a pas commencé à la traiter.
- En cours— Amazon FSx est en train de traiter la demande de mise à jour.
- Optimisation mise à jour— Amazon FSx a mis à jour les ressources d'E/S réseau, de processeur et de mémoire du système de fichiers. Le nouveau niveau de performance des E/S sur disque est disponible pour les opérations d'écriture. Lors de vos opérations de lecture, les performances d'E/S du disque se situeront entre le niveau précédent et le nouveau niveau jusqu'à ce que votre système de fichiers ne soit plus dans cet état.
- Terminé— La mise à jour de la capacité de débit s'est terminée avec succès.
- Échoué— 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.

Surveiller les modifications à l'aide duAWS CLIet API

Vous pouvez consulter et surveiller les demandes de modification de la capacité de débit du système de fichiers à l'aide dudescribe-file-systemscommande CLI etDescribeFileSystemsAction de l'API. Le`AdministrativeActions`Le 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,`FILE_SYSTEM_UPDATE`une action administrative est générée.

L'exemple suivant montre l'extrait de réponse d'un`describe-file-systems`Commande CLI. Le système de fichiers a une capacité de débit de 8 Mo/s et la capacité de débit cible de 256 Mo/s.

```
.
.
.
    "ThroughputCapacity": 8,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "WindowsConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Lorsque Amazon FSx termine le traitement de 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`ThroughputCapacity`propriété. Ceci est illustré dans l'extrait de réponse suivant d'undescribe-file-systemsCommande CLI.

```
.
.
.
```

```
    "ThroughputCapacity": 256,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "COMPLETED",
        "TargetFileSystemValues": {
          "WindowsConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Si la modification de la capacité de débit échoue, l'état passe à`FAILED`, et le`FailureDetails`Cette propriété fournit des informations sur l'échec. Pour plus d'informations sur la résolution des problèmes liés aux actions ayant échoué, voirLes mises à jour de capacité de stockage ou de débit échouent.

Baliser vos ressources Amazon FSx

Pour vous aider à gérer vos systèmes de fichiers et autres ressources Amazon FSx, vous pouvez attribuer vos propres métadonnées sous la forme de balises. Les balises vous permettent de classer vos ressources AWS de différentes manières, par exemple, par objectif, par propriétaire ou par environnement. Cette approche 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 balises et vous montre comment les créer.

Rubriques

- Principes de base des étiquettes
- Identification de vos ressources
- Restrictions liées aux balises
- Autorisations et balises

Principes de base des étiquettes

Une balise est une étiquette que vous affectez à une ressource AWS. Chaque balise est constituée d'une clé et d'une valeur facultative que vous définissez.

Les étiquettes vous permettent de classer vos ressources AWS de différentes manières, par exemple, par objectif, par propriétaire ou par environnement. Par exemple, vous pouvez définir pour les systèmes de fichiers Amazon FSx de votre compte un ensemble de balises qui vous aide à suivre le propriétaire et le niveau de stack de chaque instance.

Nous vous recommandons de concevoir un ensemble de clés d'étiquette répondant à vos besoins pour chaque type de ressource. L'utilisation d'un ensemble de clés de balise cohérent facilite la gestion de vos ressources. Vous pouvez rechercher et filtrer les ressources en fonction des balises que vous ajoutez. Pour plus d'informations sur la mise en œuvre d'une stratégie efficace de balisage des ressources, consultez le livre blanc AWS sur les bonnes pratiques en matière de balisage.

Les balises n'ont pas de signification sémantique pour Amazon FSx et sont interprétées strictement comme des chaînes de caractères. De plus, les étiquettes 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, les balises associées à celle-ci seront également supprimées.

Si vous utilisez l'API Amazon FSx, leAWSInterface de ligne de commande, ou unAWSVous pouvez utiliser le`TagResource`Action d'API pour appliquer des balises aux ressources existantes. En outre, certaines actions de création de ressources vous permettent de spécifier des balises pour une ressource lors de la création de cette dernière. Si les balises ne peuvent pas être appliquées au cours de la création de ressources, nous restaurons le processus de création de ressources. Cela permet de s'assurer que les ressources sont créées avec des balises ou qu'elles ne sont pas créées du tout, et qu'aucune ressource ne demeurent sans balise à tout moment. En attribuant des balises aux ressources au moment de la création, vous pouvez supprimer la nécessité d'exécuter des scriptes de balisage personnalisés après la création de ressources. Pour plus d'informations sur la façon de permettre aux utilisateurs de baliser des ressources lors de la création, consultez Accorder l'autorisation de baliser les ressources lors de la création.

Identification de vos ressources

Vous pouvez étiqueter des ressources Amazon FSx qui existent dans votre compte. Si vous utilisez la console Amazon FSx, vous pouvez appliquer des balises aux ressources à l'aide de l'onglet Tags (Balises) de l'écran de ressource concerné. Lorsque vous créez des ressources, vous pouvez appliquer la clé Nom avec une valeur, et vous pouvez appliquer des balises de votre choix lors de la

création d'un nouveau système de fichiers. La console peut organiser des ressources en fonction de la balise Name, mais cette balise n'a pas de signification sémantique pour le service Amazon FSx.

Vous pouvez appliquer des autorisations au niveau des ressources basées sur des balises dans vos stratégies IAM aux actions d'API Amazon FSx qui prennent en charge l'étiquetage à la création, afin de mettre en œuvre un contrôle détaillé des utilisateurs et des groupes qui peuvent baliser des ressources à leur création. Vos ressources sont correctement sécurisées depuis la création. Les balises sont appliquées immédiatement à vos ressources. Les autorisations de niveau ressource basées sur des balises sont donc effectives immédiatement. Vos ressources peuvent être suivies et signalées avec plus de précision. Vous pouvez appliquer l'utilisation du balisage sur les nouvelles ressources et contrôler que les clés et valeurs de balise sont définies sur vos ressources.

Vous pouvez également appliquer des autorisations au niveau des ressources pour le`TagResource`et`UntagResource`Actions d'API Amazon FSx dans vos politiques IAM afin de contrôler les clés et valeurs de balise définies sur vos ressources existantes.

Pour plus d'informations sur l'étiquetage de vos ressources pour la facturation, consultez Utilisation des étiquettes de répartition des coûts dans le AWS Billing Guide de l'utilisateur.

Restrictions liées aux balises

Les restrictions de base suivantes s'appliquent aux balises :

- Nombre maximal de balises par ressource : 50
- Pour chaque ressource, chaque clé de balise doit être unique, et chaque clé de balise peut avoir une seule valeur.
- Longueur de clé maximale : 128 caractères Unicode en UTF-8
- Longueur de valeur maximale : 256 caractères Unicode en UTF-8
- Les caractères autorisés pour les balises Amazon FSx sont les lettres, les chiffres et les espaces représentables en UTF-8, ainsi que les caractères suivants : + - =. _ :/@.
- Les clés et valeurs de balise sont sensibles à la casse.
- Le préfixe `aws:` est réservé à l'utilisation d'AWS. Lorsque la balise possède une clé de balise avec ce préfixe, vous ne pouvez pas modifier ou supprimer sa clé ou sa valeur. 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 basée uniquement sur ses balises ; vous devez spécifier l'identificateur de ressource. Par exemple, pour supprimer un système de

fichiers que vous avez balisé avec une clé de balise appeléeDeleteMe, vous devez utiliser leDeleteFileSystemaction avec l'identificateur 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 votreCompte AWSPas d'autresCompte AWSauront accès à ces balises. Pour le contrôle d'accès aux ressources partagées basé sur des balises, chaqueCompte AWSdoit attribuer son propre ensemble de balises pour contrôler l'accès à la ressource.

Autorisations et balises

Pour plus d'informations sur les autorisations requises pour baliser des ressources Amazon FSx à leur création, consultezAccorder l’autorisation de baliser les ressources lors de la création. Pour plus d'informations sur l'utilisation de balises pour limiter l'accès aux ressources Amazon FSx dans les politiques IAM, consultezUtilisation de balises pour contrôler l'accès à vos ressources Amazon FSx.

Utilisation des fenêtres de maintenance d'Amazon FSx

Amazon FSx pour Windows File Server exécute des correctifs logiciels de routine pour le logiciel Microsoft Windows Server qu'il gère. La fenêtre de maintenance vous permet de contrôler le jour et l'heure de la semaine auxquels les correctifs logiciels sont appliqués. Vous choisissez la fenêtre de maintenance lors de la création du système de fichiers. Si vous n'avez aucune préférence horaire, une fenêtre par défaut de 30 minutes est attribuée.

Le serveur de fichiers FSx pour Windows vous permet d'ajuster votre fenêtre de maintenance 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 soit planifiée au moins une fois tous les 14 jours. Si un correctif est publié et que vous n'avez pas planifié de fenêtre de maintenance dans les 14 jours, FSx pour Windows File Server procède à la maintenance du système de fichiers afin de garantir sa sécurité et sa fiabilité.

Pendant que l'application des correctifs est en cours, attendez-vous à ce que vos systèmes de fichiers mono-AZ ne soient pas disponibles, généralement pendant moins de 20 minutes. Vos systèmes de fichiers Multi-AZ restent disponibles et basculent automatiquement entre le serveur de fichiers préféré et le serveur de fichiers de secours. Pour plus d'informations, veuillez consulter Processus de basculement pour FSx for Windows File Server. Étant donné que l'application de correctifs aux systèmes de fichiers multi-AZ implique un basculement et un retour arrière, tout trafic vers le système de fichiers pendant cette période doit être synchronisé entre le serveur de fichiers

préféré et le serveur de fichiers de secours. Pour réduire le temps consacré à l'application des correctifs, nous vous recommandons de planifier votre fenêtre de maintenance pendant les périodes d'inactivité, lorsque la charge sur votre système de fichiers est minimale.

> **Note**
>
> Pour garantir l'intégrité des données pendant les activités de maintenance, Amazon FSx pour Windows File Server effectue toutes les opérations d'écriture en attente sur les volumes de stockage sous-jacents hébergeant votre système de fichiers avant le début de la maintenance.

Vous pouvez utiliser la console de gestion Amazon FSx,AWS CLI,AWSAPI, ou l'une desAWSSDK pour modifier la fenêtre de maintenance de vos systèmes de fichiers.

Pour modifier la fenêtre de maintenance hebdomadaire (console)

1. Ouvrez la console Amazon FSx à l'adressehttps://console.aws.amazon.com/fsx/.
2. ChoisissezSystèmes de fichiersdans la colonne de navigation de gauche.
3. Choisissez le système de fichiers pour lequel vous souhaitez modifier la fenêtre de maintenance hebdomadaire. La page de détails du système de fichiers s'affiche.
4. ChoisissezAdministrationpour afficher l'administration du système de fichiersRéglagespanneau.
5. ChoisissezMettre à jourpour afficher leModifier la fenêtre de maintenancefenêtre.
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 la maintenance est affichée dansParamètres d'administrationpanneau.

Pour modifier la fenêtre de maintenance hebdomadaire à l'aide duupdate-file-systemCommande CLI, voirProcédure 3 : Mettre à jour un système de fichiers existant.

Meilleures pratiques pour administrer les systèmes de fichiers Amazon FSx

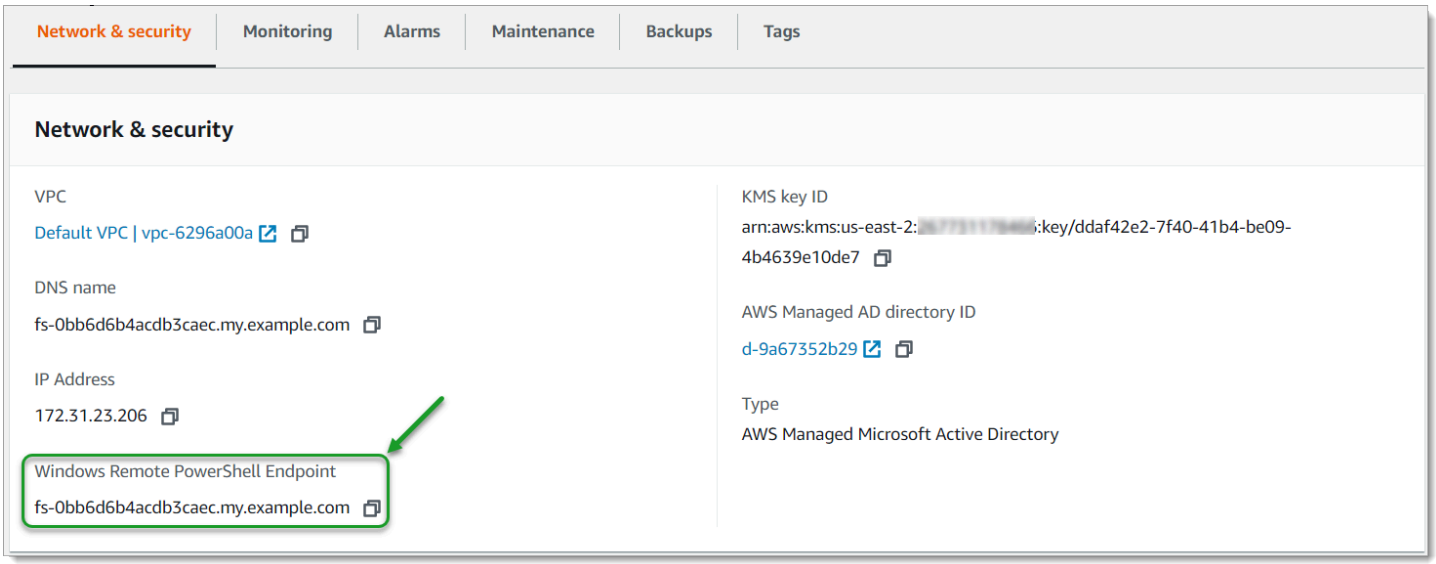
Amazon FSx fournit plusieurs fonctionnalités qui peuvent vous aider à mettre en œuvre les meilleures pratiques pour administrer vos systèmes de fichiers, notamment :

- optimisation de la consommation de stockage
- permettre aux utilisateurs finaux de récupérer des fichiers et des dossiers dans des versions antérieures
- renforcer le chiffrement pour tous les clients connectés

Utilisez la CLI Amazon FSx suivante pour la gestion à distance des PowerShell commandes afin d'implémenter rapidement ces meilleures pratiques sur vos systèmes de fichiers.

Pour exécuter ces commandes, vous devez connaître le Windows Remote PowerShell Endpoint correspondant à votre système de fichiers. Pour trouver ce point de terminaison, procédez comme suit :

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Choisissez votre système de fichiers. Dans l'onglet Réseau et sécurité, localisez le point de PowerShell terminaison Windows Remote, comme indiqué ci-dessous.



Pour plus d'informations, consultez Administration des systèmes de fichiers et Utilisation de l'interface de ligne de commande Amazon FSx pour PowerShell.

Rubriques

- Tâches de configuration administrative ponctuelles
- Tâches d'administration continues pour surveiller votre système de fichiers

Tâches de configuration administrative ponctuelles

Vous trouverez ci-dessous des tâches que vous pouvez configurer rapidement une seule fois pour votre système de fichiers.

Gestion de la consommation de stockage

Utilisez les commandes suivantes pour gérer la consommation de stockage de votre système de fichiers.

- Pour activer la déduplication des données selon le calendrier par défaut, exécutez la commande suivante.

  ```
  Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
   FSxRemoteAdmin -ScriptBlock { Enable-FsxDedup }
  ```

  Vous pouvez éventuellement utiliser la commande suivante pour que la déduplication des données soit opérationnelle sur vos fichiers peu après leur création, sans exiger d'âge minimum pour les fichiers.

  ```
  Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
   FSxRemoteAdmin -ScriptBlock { Set-FSxDedupConfiguration -MinimumFileAgeDays 0 }
  ```

  Pour plus d'informations, consultez Déduplication des données.

- Utilisez la commande suivante pour activer les quotas de stockage utilisateur en mode « Track », uniquement à des fins de reporting et non à des fins d'application.

  ```
  $QuotaLimit = Quota limit in bytes
  $QuotaWarningLimit = Quota warning threshold in bytes
  Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
   FSxRemoteAdmin -ScriptBlock { Enable-FSxUserQuotas -Track -DefaultLimit
   $Using:QuotaLimit -DefaultWarningLimit $Using:QuotaWarningLimit }
  ```

  Pour plus d'informations, consultez Quotas de stockage.

Activer les copies instantanées pour permettre aux utilisateurs finaux de récupérer des fichiers et des dossiers dans des versions antérieures

Activez les clichés instantanés selon le calendrier par défaut (en semaine à 7 h 00 et 12 h 00), comme suit.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxShadowStorage -Default }

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxShadowCopySchedule -Default -Confirm:$False}
```

Pour plus d'informations, consultez Configuration des clichés instantanés pour utiliser le stockage et la planification par défaut.

Appliquer le chiffrement en transit

La commande suivante applique le chiffrement aux clients qui se connectent à votre système de fichiers.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxSmbServerConfiguration -EncryptData $True -
RejectUnencryptedAccess $True -Confirm:$False}
```

Vous pouvez fermer toutes les sessions ouvertes et forcer les clients actuellement connectés à se reconnecter à l'aide du chiffrement.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Close-FSxSmbSession -Confirm:$False}
```

Pour plus d'informations, consultez Gestion du chiffrement en transit et Sessions utilisateur et fichiers ouverts.

Tâches d'administration continues pour surveiller votre système de fichiers

Les tâches continues suivantes vous aident à surveiller l'utilisation du disque de votre système de fichiers, les quotas d'utilisateurs et les fichiers ouverts.

Surveillance de l'état de la déduplication

Surveillez l'état de la déduplication, notamment le taux d'économies réalisé sur votre système de fichiers, comme suit.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -
ConfigurationName FsxRemoteAdmin -ScriptBlock { Get-FSxDedupStatus } | select
 OptimizedFilesCount,OptimizedFilesSize,SavedSpace,OptimizedFilesSavingsRate
```

Surveillance de la consommation de stockage au niveau de l'utilisateur

Obtenez un rapport sur les quotas de stockage actuels des utilisateurs, notamment sur l'espace qu'ils consomment et sur les dépassements de la limite et du seuil d'avertissement.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Get-FSxUserQuotaEntries }
```

Surveillance et fermeture des fichiers ouverts

Gérez les fichiers ouverts en recherchant les fichiers laissés ouverts et en les fermant. Utilisez la commande suivante pour vérifier les fichiers ouverts.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Get-FSxSmbOpenFile}
```

Utilisez la commande suivante pour fermer les fichiers ouverts.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Close-FSxSmbOpenFile -Confirm:$false}
```

Regroupement de plusieurs systèmes de fichiers avec des espaces de noms DFS

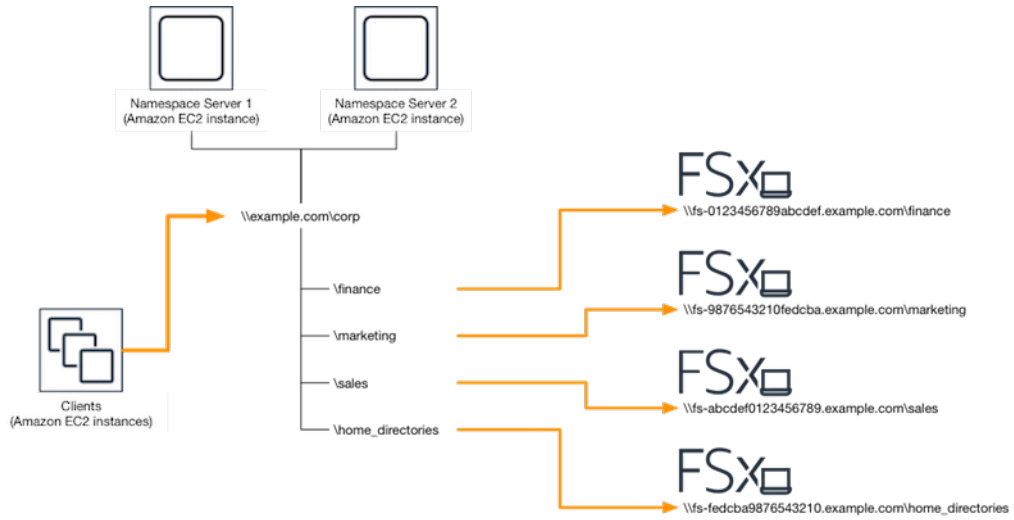
Amazon FSx for Windows File Server prend en charge l'utilisation des espaces de noms DFS (Distributed File System) de Microsoft. Vous pouvez utiliser les espaces de noms DFS pour regrouper les partages de fichiers sur plusieurs systèmes de fichiers dans une structure de dossiers commune (un espace de noms) que vous utilisez pour accéder à l'ensemble de données de fichiers. Les espaces de noms DFS peuvent vous aider à organiser et à unifier l'accès à vos partages de fichiers sur plusieurs systèmes de fichiers. Les espaces de noms DFS peuvent également aider à étendre le stockage des données de fichiers au-delà de ce que chaque système de fichiers prend en charge (64 To) pour les grands ensembles de données de fichiers, jusqu'à des centaines de pétaoctets.

Configuration des espaces de noms DFS pour le regroupement de plusieurs systèmes de fichiers

Vous pouvez utiliser les espaces de noms DFS pour regrouper plusieurs systèmes de fichiers sous un même espace de noms. Dans l'exemple suivant, l'espace de noms basé sur le domaine (example.com \ corp) est créé sur deux serveurs d'espaces de noms, consolidant ainsi les partages de fichiers stockés sur plusieurs systèmes de fichiers Amazon FSx (finance, marketing, ventes, home_directories). Cela permet à vos utilisateurs d'accéder aux partages de fichiers en utilisant un espace de noms commun. Dans ces conditions, ils n'ont pas besoin de spécifier les noms DNS des systèmes de fichiers pour chacun des systèmes de fichiers hébergeant les partages de fichiers.

> **Note**
>
> Amazon FSx ne peut pas être ajouté à la racine du chemin de partage DFS.

Ces étapes vous guident dans la création d'un espace de noms unique (exemple.com \ corp) sur deux serveurs d'espaces de noms. Vous avez également configuré quatre partages de fichiers dans l'espace de noms, chacun redirigeant de manière transparente les utilisateurs vers des partages hébergés sur des systèmes de fichiers Amazon FSx distincts.



Pour regrouper plusieurs systèmes de fichiers dans un espace de noms DFS commun

1. Si aucun serveur d'espace de noms DFS n'est déjà actif, vous pouvez lancer deux serveurs d'espaces de noms DFS à haut niveau de disponibilité à l'aide du modèle Setup-DFSN-Servers.template. AWS CloudFormation 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.
2. Connectez-vous à l'un des serveurs d'espace de noms DFS lancés à l'étape précédente en tant qu'utilisateur du groupe Administrateurs AWS délégués. Pour plus d'informations, consultez la section Connexion à votre instance Windows dans le guide de l'utilisateur Amazon EC2.
3. Accédez à la console de gestion DFS en l'ouvrant. Ouvrez le menu Démarrer et exécutez dfsmgmt.msc. Cela ouvre l'outil d'interface graphique de gestion DFS.
4. Choisissez Action puis Nouvel espace de noms, saisissez le nom d'ordinateur du premier serveur d'espace de noms DFS que vous avez lancé pour Server et choisissez Next.
5. Dans Nom, saisissez l'espace de noms que vous créez (par exemple, corp).
6. Choisissez Modifier les paramètres et définissez les autorisations appropriées en fonction de vos besoins. Choisissez Suivant.
7. Laissez l'option d'espace de noms par défaut basée sur le domaine sélectionnée, laissez l'option Activer le mode Windows Server 2008 sélectionnée, puis choisissez Next.

> **Note**
>
> Le mode Windows Server 2008 est la dernière option disponible pour les espaces de noms.

8. Vérifiez les paramètres de l'espace de noms et choisissez Create.
9. Le nouvel espace de noms étant sélectionné sous Espaces de noms dans la barre de navigation, choisissez Action puis Ajouter un serveur d'espace de noms.
10. Entrez le nom d'ordinateur du deuxième serveur d'espace de noms DFS que vous avez lancé pour le serveur d'espace de noms.
11. Choisissez Modifier les paramètres, définissez les autorisations appropriées en fonction de vos besoins, puis cliquez sur OK.
12. Ouvrez le menu contextuel (clic droit) de l'espace de noms que vous venez de créer, choisissez Nouveau dossier, saisissez le nom du dossier (par exemple, `finance` pour Nom), puis cliquez sur OK.
13. Tapez le nom DNS du partage de fichiers vers lequel vous souhaitez que le dossier DFS Namespace pointe au format UNC (par exemple,**`\\fs-0123456789abcdef0.example.com\finance`**) pour le chemin d'accès au dossier cible, puis cliquez sur OK.
14. Si le partage n'existe pas :
    a. Choisissez Oui pour le créer.
    b. Dans la boîte de dialogue Créer un partage, choisissez Parcourir.
    c. Choisissez un dossier existant ou créez-en un nouveau sous D$, puis cliquez sur OK.
    d. Définissez les autorisations de partage appropriées, puis cliquez sur OK.
15. Dans la boîte de dialogue Nouveau dossier, cliquez sur OK. Le nouveau dossier sera créé sous l'espace de noms.
16. Répétez les quatre dernières étapes pour les autres dossiers que vous souhaitez partager sous le même espace de noms.

Surveillance du serveur de fichiers FSx for Windows

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon FSx et de vos AWS solutions. Vous devez collecter des données de surveillance provenant de toutes les parties de votre AWS solution afin de pouvoir corriger plus facilement une défaillance multipoint, le cas échéant. Toutefois, avant de commencer à surveiller Amazon FSx, vous devez créer un plan de surveillance qui inclut les réponses aux questions suivantes :

- Quels sont les objectifs de la surveillance ?
- Quelles sont les ressources à surveiller ?
- À quelle fréquence les ressources doivent-elles être surveillées ?
- Quels outils de surveillance utiliser ?
- Qui exécute les tâches de supervision ?
- Qui doit être informé en cas de problème ?

Pour plus d'informations sur la journalisation et la surveillance dans FSx for Windows File Server, consultez les rubriques suivantes.

Rubriques

Outils de surveillance

AWS fournit différents outils que vous pouvez utiliser pour surveiller Amazon FSx. Vous pouvez configurer certains de ces outils pour effectuer la surveillance à votre place, tandis que d'autres nécessitent une intervention manuelle. Nous vous recommandons d’automatiser le plus possible les tâches de supervision.

Outils de surveillance automatique

Vous pouvez utiliser les outils de surveillance automatique suivants pour surveiller Amazon FSx et signaler tout problème :

- Amazon CloudWatch Alarms : surveillez une seule métrique sur une période que vous spécifiez et effectuez 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 Simple Notification Service (Amazon SNS) ou à une politique Amazon EC2 Auto Scaling. CloudWatch les alarmes n'appellent pas d'actions simplement parce qu'elles sont dans un état particulier ; l'état doit avoir changé et être maintenu pendant un certain nombre de périodes. Pour plus d'informations, consultez Surveillance des métriques avec Amazon CloudWatch.
- Amazon CloudWatch Logs — Surveillez, stockez et accédez à vos fichiers journaux depuis AWS CloudTrail ou d'autres sources. Pour plus d'informations, consultez Qu'est-ce qu'Amazon CloudWatch Logs ? dans le guide de l'utilisateur d'Amazon CloudWatch Logs.
- AWS CloudTrail Surveillance des journaux : partagez les fichiers journaux entre les comptes, surveillez les fichiers CloudTrail CloudWatch journaux en temps réel en les envoyant à Logs, écrivez des applications de traitement des journaux en Java et vérifiez que vos fichiers journaux n'ont pas changé après leur livraison par CloudTrail. Pour plus d'informations, consultez la section Utilisation des fichiers CloudTrail journaux dans le guide de AWS CloudTrail l'utilisateur.

Outils de surveillance manuelle

Un autre élément important de la surveillance d'Amazon FSx consiste à surveiller manuellement les éléments non couverts par les CloudWatch alarmes Amazon. Les tableaux de bord Amazon FSx et d'autres AWS consoles fournissent une at-a-glance vue d'ensemble de l'état de votre environnement. CloudWatch AWS

Les tableaux de bord de surveillance et de performance de la console Amazon FSx indiquent :

- Avertissements CloudWatch et alarmes actuels de FSx for Windows File Server
- Graphiques présentant un résumé de l'activité du système de fichiers
- Graphiques de la capacité de stockage et de l'utilisation du système de fichiers
- Graphiques des performances des serveurs de fichiers et des volumes de stockage
- CloudWatch alarmes

La page d' CloudWatch accueil indique :

- Alarmes et statuts en cours
- Graphiques des alarmes et des ressources

- Statut d’intégrité du service

En outre, vous pouvez utiliser CloudWatch pour effectuer les opérations suivantes :

- Créez des tableaux de bord personnalisés pour surveiller les services que vous utilisez.
- Données de métriques de graphiques pour résoudre les problèmes et découvrir les tendances.
- Recherchez et parcourez tous les indicateurs de vos AWS ressources.
- Créer et Modifier des alarmes pour être informé des problèmes.

Pour plus d'informations sur le tableau de bord de surveillance et de performance d'Amazon FSx, consultez. Comment utiliser les métriques de FSx for Windows File Server

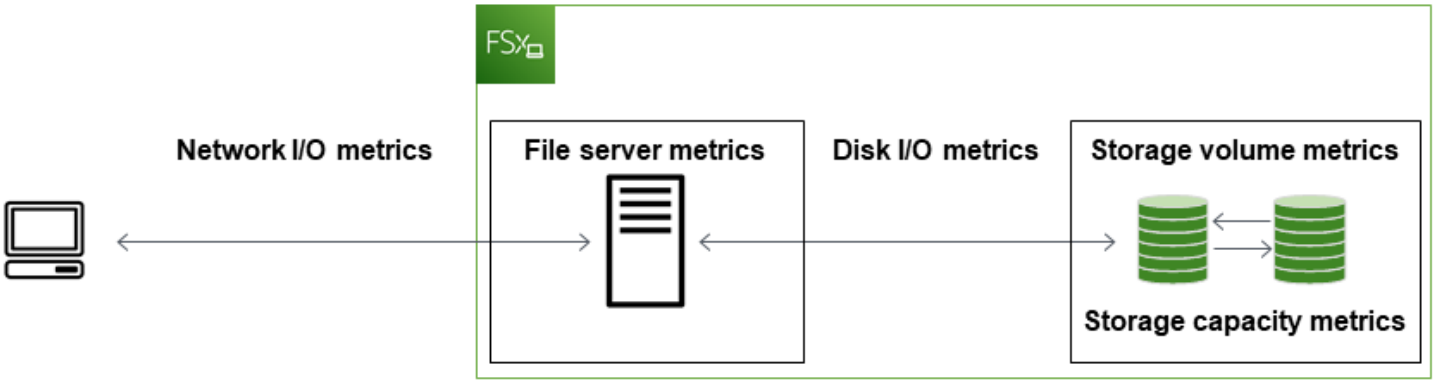
Surveillance des métriques avec Amazon CloudWatch

Vous pouvez surveiller les systèmes de fichiers FSx for Windows File Server à l'aide d' CloudWatchAmazon, qui collecte et traite les données brutes de FSx for Windows File Server en indicateurs lisibles quasiment en temps réel. Ces statistiques sont conservées pendant une période de 15 mois, afin que vous puissiez accéder aux informations historiques et avoir un aperçu des performances de votre application Web ou de votre système de fichiers.

FSx for Windows File Server CloudWatch publie des métriques dans les domaines suivants :

- Les métriques d'E/S réseau mesurent l'activité entre les clients accédant au système de fichiers et au serveur de fichiers.
- Les métriques du serveur de fichiers mesurent l'utilisation du débit du réseau, le processeur et la mémoire du serveur de fichiers, ainsi que le débit disque du serveur de fichiers et l'utilisation des IOPS.
- Les métriques d'E/S du disque mesurent l'activité entre le serveur de fichiers et les volumes de stockage.
- Les mesures du volume de stockage mesurent l'utilisation du débit du disque pour les volumes de stockage sur disque dur et l'utilisation des IOPS pour les volumes de stockage SSD.
- Les indicateurs de capacité de stockage mesurent l'utilisation du stockage, y compris les économies de stockage réalisées grâce à la déduplication des données.

Le schéma suivant illustre un système de fichiers FSx for Windows File Server, ses composants et les domaines métriques.



Par défaut, Amazon FSx for Windows File Server envoie des données métriques CloudWatch à des intervalles d'une minute, avec les exceptions suivantes qui sont émises à intervalles de 5 minutes :

- `FileServerDiskThroughputBalance`
- `FileServerDiskIopsBalance`

Pour plus d'informations CloudWatch, consultez Qu'est-ce qu'Amazon CloudWatch ? dans le guide de CloudWatch l'utilisateur Amazon.

Les métriques peuvent ne pas être publiées pour les systèmes de fichiers mono-AZ pendant la maintenance du système de fichiers ou le remplacement des composants de l'infrastructure, et pour les systèmes de fichiers multi-AZ pendant le basculement et le retour en arrière entre les serveurs de fichiers principal et secondaire.

Certaines CloudWatch métriques Amazon FSx sont signalées sous forme d'octets bruts. Les octets ne sont pas arrondis à la décimale ou à un multiple binaire de l'unité.

Rubriques

- Métriques et dimensions
- Comment utiliser les métriques de FSx for Windows File Server
- Avertissements et recommandations en matière de performances
- Accès aux métriques du serveur de fichiers FSx for Windows
- Création d' CloudWatch alarmes pour surveiller Amazon FSx

Métriques et dimensions

FSx for Windows File Server publie les métriques suivantes dans `AWS/FSx` l'espace de noms d' CloudWatch Amazon pour tous les systèmes de fichiers :

- `DataReadBytes`
- `DataWriteBytes`
- `DataReadOperations`
- `DataWriteOperations`
- `MetadataOperations`
- `FreeStorageCapacity`

FSx for Windows File Server publie les métriques décrites ci-dessous dans l'espace de noms d' CloudWatch Amazon pour `AWS/FSx` les systèmes de fichiers configurés avec une capacité de débit d'au moins 32 Mo/s.

Rubriques

- Métriques d'E/S réseau FSx pour Windows
- Métriques du serveur de fichiers FSx pour Windows
- Métriques d'E/S de disque FSx pour Windows
- Mesures du volume de stockage de FSx pour Windows
- Mesures de capacité de stockage de FSx pour Windows
- Dimensions de FSx pour Windows

Métriques d'E/S réseau FSx pour Windows

L'`AWS/FSx`espace de noms inclut les métriques d'E/S réseau suivantes.

Métrique	Description
`DataReadBytes`	Nombre d'octets pour les opérations de lecture pour les clients accédant au système de fichiers. Unités : octets

Métrique	Description
	Statistiques valides : `Sum`
`DataWriteBytes`	Nombre d'octets pour les opérations d'écriture pour les clients accédant au système de fichiers. Unités : octets Statistiques valides : `Sum`
`DataReadOperations`	Nombre d'opérations de lecture pour les clients accédant au système de fichiers. Unités : nombre Statistiques valides : `Sum`
`DataWriteOperations`	Nombre d'opérations d'écriture pour les clients accédant au système de fichiers. Unités : nombre Statistiques valides : `Sum`
`MetadataOperations`	Nombre d'opérations de métadonnées pour les clients accédant au système de fichiers. Unités : nombre Statistiques valides : `Sum`
`ClientConnections`	Nombre de connexions actives entre les clients et le serveur de fichiers. Unités : nombre

Métriques du serveur de fichiers FSx pour Windows

L'`AWS/FSx`espace de noms inclut les métriques de serveur de fichiers suivantes.

Métrique	Description
`NetworkThroughputUtilization`	Débit réseau pour les clients accédant au système de fichiers, en pourcentage de la limite allouée. Unités : pourcentage
`CPUUtilization`	Pourcentage d'utilisation des ressources du processeur de votre serveur de fichiers. Unités : pourcentage
`MemoryUtilization`	Pourcentage d'utilisation des ressources de mémoire de votre serveur de fichiers. Unités : pourcentage
`FileServerDiskThroughputUtilization`	Débit du disque entre votre serveur de fichiers et ses volumes de stockage, en pourcentage de la limite allouée déterminée par la capacité de débit. Unités : pourcentage
`FileServerDiskThroughputBalance`	Pourcentage de crédits de rafale disponibles pour le débit du disque entre votre serveur de fichiers et ses volumes de stockage. Valable pour les systèmes de fichiers configurés avec une capacité de débit inférieure ou égale à 256 Mo/s. Unités : pourcentage
`FileServerDiskIopsUtilization`	Les IOPS du disque entre votre serveur de fichiers et les volumes de stockage, en pourcentage de la limite allouée déterminée par la capacité de débit. Unités : pourcentage
`FileServerDiskIopsBalance`	Pourcentage de crédits en rafale disponibles pour les IOPS de disque entre votre serveur de fichiers et ses volumes de stockage. Valable pour les systèmes de

Métrique	Description
	fichiers configurés avec une capacité de débit inférieure ou égale à 256 Mo/s. Unités : pourcentage

Métriques d'E/S de disque FSx pour Windows

L'espace de `AWS/FSx` noms inclut les métriques d'E/S de disque suivantes.

Métrique	Description
`DiskReadBytes`	Nombre d'octets pour les opérations de lecture qui accèdent aux volumes de stockage. Unités : octets Statistiques valides : somme
`DiskWriteBytes`	Nombre d'octets pour les opérations d'écriture qui accèdent aux volumes de stockage. Unités : octets Statistiques valides : somme
`DiskReadOperations`	Nombre d'opérations de lecture pour le serveur de fichiers accédant aux volumes de stockage. Unités : nombre Statistiques valides : `Sum`
`DiskWriteOperations`	Nombre d'opérations d'écriture pour le serveur de fichiers accédant aux volumes de stockage. Unités : nombre Statistiques valides : `Sum`

Mesures du volume de stockage de FSx pour Windows

L'`AWS/FSx`espace de noms inclut les métriques de volume de stockage suivantes.

Métrique	Description
`DiskThroughputUtilization`	(Disque dur uniquement) Débit du disque entre votre serveur de fichiers et ses volumes de stockage, en pourcentage de la limite allouée déterminée par les volumes de stockage. Unités : pourcentage
`DiskThroughputBalance`	(Disque dur uniquement) Pourcentage de crédits de rafale disponibles pour le débit du disque pour les volumes de stockage. Unités : pourcentage
`DiskIopsUtilization`	(SSD uniquement) Les IOPS du disque entre votre serveur de fichiers et les volumes de stockage, en pourcentage de la limite d'IOPS allouée déterminée par les volumes de stockage. Unités : pourcentage

Mesures de capacité de stockage de FSx pour Windows

L'`AWS/FSx`espace de noms inclut les mesures de capacité de stockage suivantes.

Métrique	Description
`FreeStorageCapacity`	La quantité de capacité de stockage disponible. Unités : octets Statistiques valides : `Average`, `Minimum`

Métrique	Description
`StorageCapacityUtilization`	Capacité de stockage physique utilisée en pourcentage de la capacité de stockage totale. Unités : pourcentage
`DeduplicationSavedStorage`	La quantité d'espace de stockage économisée par la déduplication des données, si elle est activée. Unités : octets

Dimensions de FSx pour Windows

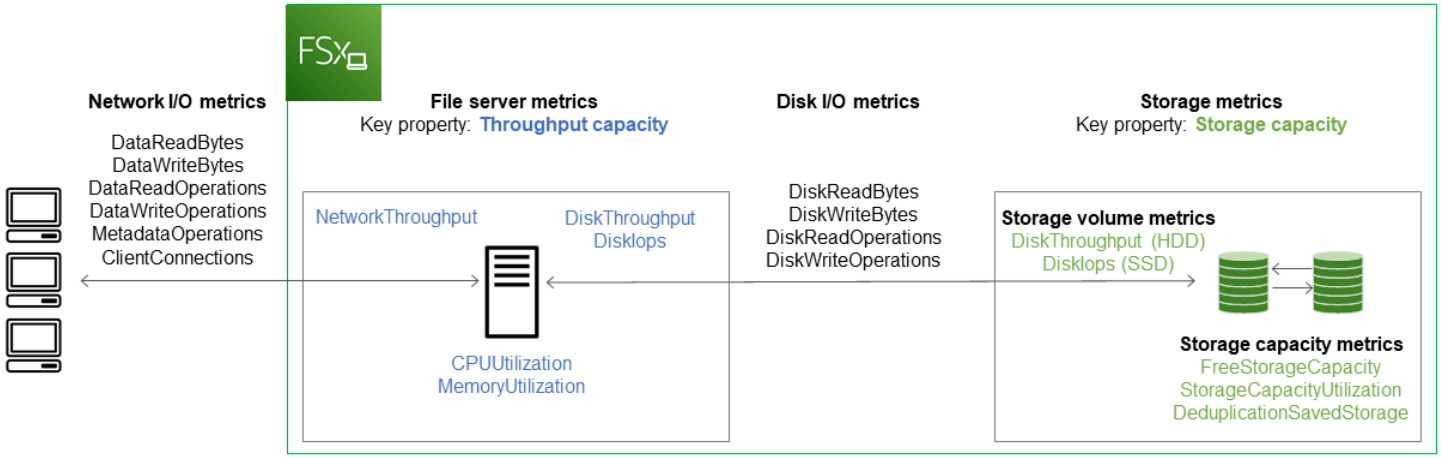
Les métriques de FSx for Windows File Server utilisent `FSx` l'espace de noms et fournissent des métriques pour une seule dimension,. `FileSystemId` Vous pouvez trouver l'ID d'un système de fichiers à l'aide de la describe-file-systems AWS CLI commande ou de la commande DescribeFileSystemsAPI. Un identifiant de système de fichiers prend la forme *`fs-0123456789abcdef0`*.

Comment utiliser les métriques de FSx for Windows File Server

Chaque système de fichiers Amazon FSx comporte deux composants architecturaux principaux :

- Le serveur de fichiers qui fournit des données aux clients accédant au système de fichiers.
- Les volumes de stockage qui hébergent les données dans votre système de fichiers.

FSx for Windows File Server fournit des statistiques permettant de suivre CloudWatch les performances et l'utilisation des ressources du serveur de fichiers et des volumes de stockage de votre système de fichiers. Le schéma suivant illustre un système de fichiers Amazon FSx avec ses composants architecturaux, ainsi que les CloudWatch indicateurs de performance et de ressources disponibles pour la surveillance. La propriété clé affichée pour un ensemble de mesures est la propriété du système de fichiers qui détermine la capacité de ces mesures. Le réglage de cette propriété modifie les performances du système de fichiers pour cet ensemble de mesures.



Utilisez le panneau de surveillance et de performance de la console Amazon FSx pour consulter les métriques du CloudWatch serveur de fichiers FSx for Windows décrites dans le tableau suivant.

Panneau de surveillance et de performance	Comment puis-je...	Diagramme	Métriques pertinentes
	... déterminer le nombre total d'IOPS de mon système de fichiers ?	Nombre total d'E/S par seconde	SOMME (`DataReadOperations + DataWriteOperations +MetadataOperations`) /Période (en secondes)
Récapitulatif	... déterminer le débit total de mon système de fichiers ?	Débit total	SOMME (`DataReadBytes +DataWriteBytes`) /Période (en secondes)
	... déterminer la capacité de stockage disponible sur mon système de fichiers ?	Capacité de stockage	`FreeStorageCapacity`

Panneau de surveillance et de performance	Comment puis-je...	Diagramme	Métriques pertinentes
		disponible	
	... déterminer le nombre de connexions établies entre les clients et le serveur de fichiers ?	Connexions client	`ClientConnections`
	... déterminer la quantité d'espace disque physique utilisé en pourcentage de la capacité de stockage totale du système de fichiers ?	Utilisation de la capacité de stockage	`StorageCapacityUtilization`
Stockag	... déterminer la quantité d'espace disque physique économisée par la déduplication des données ?	Stockage sauvegardé grâce à la déduplication des données	`DeduplicationSavedStorage`
Performances - Serveur de fichiers	... déterminer le débit réseau pour les clients accédant au système de fichiers, en pourcentage du débit provisionné du système de fichiers ?	Utilisation du débit du réseau	`NetworkThroughputUtilization`

Panneau de surveillance et de performance	Comment puis-je...	Diagramme	Métriques pertinentes
	... déterminer le débit du disque entre le serveur de fichiers et ses volumes de stockage, en pourcentage de la limite allouée déterminée par la capacité de débit ?	Utilisation du débit du disque	`FileServerDiskThroughputUtilization`
	... déterminer le pourcentage de crédits de rafale disponibles pour le débit du disque entre le serveur de fichiers et ses volumes de stockage ?	Balance en rafale du débit du disque	`FileServerDiskThroughputBalance`
	... déterminer le nombre d'IOPS sur le disque entre le serveur de fichiers et les volumes de stockage, en pourcentage de la limite allouée déterminée par la capacité de débit ?	Utilisation des IOPS sur disque	`FileServerDiskIopsUtilization`
	... déterminer le pourcentage de crédits de rafale disponibles pour les IOPS de disque entre le serveur de fichiers et les volumes de stockage ?	Balance en rafale des IOPS sur le disque	`FileServerDiskIopsBalance`
	... déterminer le pourcentage d'utilisation du processeur du serveur de fichiers ?	Utilisation de l’UC	`CPUUtilization`
	... déterminer le pourcentage d'utilisation de la mémoire du serveur de fichiers ?	Utilisation de la mémoire	`MemoryUtilization`

Panneau de surveillance et de performance	Comment puis-je...	Diagramme	Métriques pertinentes
Performances — Volumes de stockage	... déterminer le débit pour les opérations qui accèdent aux volumes de stockage, en pourcentage de la limite allouée déterminée par la capacité de stockage du disque dur ?	Utilisation du débit du disque (HDD)	`DiskThroughputUtilization`
	... déterminer le pourcentage de crédits de rafale disponibles pour le débit pour les opérations qui accèdent aux volumes de stockage sur disque dur ?	Balance en rafale du débit du disque (HDD)	`DiskThroughputBalance`
	... déterminer les IOPS pour les opérations qui accèdent aux volumes de stockage, en pourcentage de la limite allouée déterminée par la capacité de stockage SSD ?	Utilisation des IOPS sur le disque (SSD)	`DiskIopsUtilization`

> **Note**
>
> Nous vous recommandons de maintenir une utilisation moyenne de la capacité de débit inférieure à 50 % afin de disposer d'une capacité de débit inutilisée suffisante pour faire face aux pics inattendus de votre charge de travail, ainsi que pour toutes les opérations de stockage Windows en arrière-plan (telles que la synchronisation du stockage, la déduplication ou les clichés instantanés).

Avertissements et recommandations en matière de performances

FSx pour Windows fournit des avertissements de performance pour les systèmes de fichiers configurés avec une capacité de débit d'au moins 32 Mo/s. Amazon FSx affiche un avertissement pour un ensemble de CloudWatch métriques chaque fois que l'une de ces métriques approche ou dépasse un seuil prédéterminé pour plusieurs points de données consécutifs. Ces avertissements vous fournissent des recommandations pratiques que vous pouvez utiliser pour optimiser les performances de votre système de fichiers.

Les avertissements sont accessibles dans plusieurs zones du tableau de bord de surveillance et de performance. Tous les avertissements de performance actifs ou récents d'Amazon FSx et toutes les CloudWatch alarmes configurées pour le système de fichiers présentant un état ALARM apparaissent dans le panneau Surveillance et performances de la section Résumé. L'avertissement apparaît également dans la section du tableau de bord affichant le graphique métrique.

Vous pouvez créer des CloudWatch alarmes pour toutes les métriques Amazon FSx. Pour plus d'informations, consultez Création d' CloudWatch alarmes 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.

S'il existe un avertissement pour cette métrique	Faites ceci
Débit du réseau — utilisation	Augmenter la capacité de débit
Serveur de fichiers > Nombre d'E/S par seconde sur disque : utilisation	
Serveur de fichiers > Débit du disque — utilisation	
Serveur de fichiers > IOPS sur disque - balance en rafale	

S'il existe un avertissement pour cette métrique	Faites ceci
Serveur de fichiers > Débit du disque — équilibre en rafale	
Utilisation de la capacité de stockage	Augmenter la capacité de stockage
Volume de stockage > Débit du disque — utilisation (HDD)	Augmenter la capacité de stockage ou passer au type de stockage SDD
Volume de stockage > Débit du disque — balance de rafale (HDD)	
Volume de stockage > Nombre d'E/S par seconde du disque : utilisation (SSD)	Augmentez le nombre d'IOPS sur SSD

> **Note**
>
> Certains événements du système de fichiers peuvent consommer les ressources de performance des E/S du disque et potentiellement déclencher des avertissements de performance. Par exemple :
>
> - La phase d'optimisation de la mise à l'échelle de la capacité de stockage peut générer une augmentation du débit du disque, comme décrit dans Augmentation de la capacité de stockage et des performances du système de fichiers
> - Pour les systèmes de fichiers multi-AZ, des événements tels que l'augmentation de la capacité de débit, le remplacement du matériel ou l'interruption de la zone de disponibilité entraînent des événements de basculement et de retour en arrière automatiques. Toute modification de données survenant pendant cette période doit être synchronisée entre les serveurs de fichiers principal et secondaire, et Windows Server exécute une tâche de synchronisation des données susceptible de consommer des ressources d'E/S de disque. Pour plus d’informations, consultez Gestion de la capacité de débit.

Pour plus d'informations sur les performances du système de fichiers, consultezPerformances de FSx for Windows File Server.

Accès aux métriques du serveur de fichiers FSx for Windows

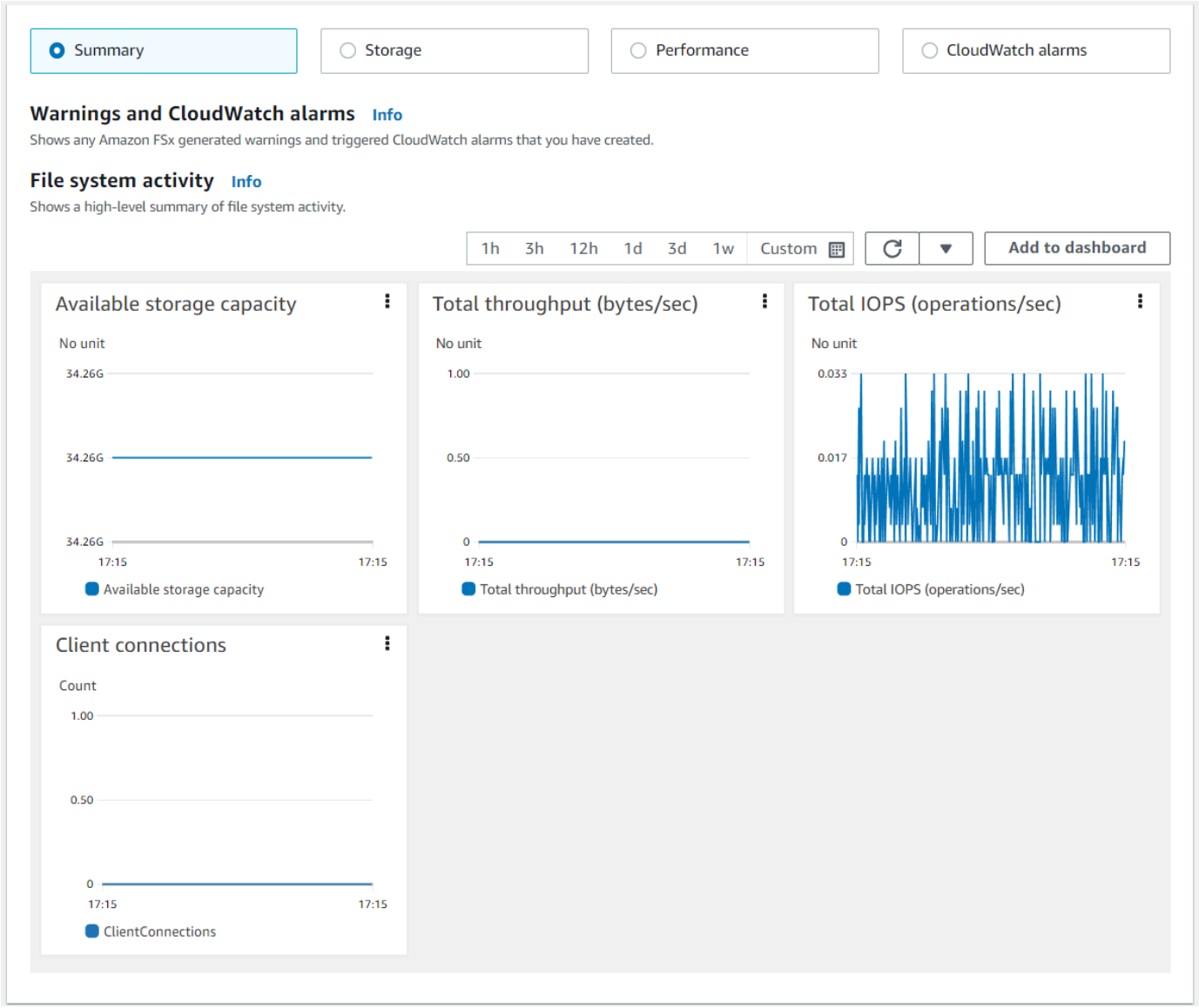
Vous pouvez consulter les métriques Amazon FSx de la CloudWatch manière suivante.

- La console Amazon FSx.
- La CloudWatch console.
- La CloudWatch CLI (interface de ligne de commande).
- L' CloudWatch API.

Les procédures suivantes décrivent comment accéder aux métriques de votre système de fichiers à l'aide de ces différents outils.

Pour consulter les métriques du système de fichiers à l'aide de la console Amazon FSx

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Pour afficher la page de détails du système de fichiers, sélectionnez Systèmes de fichiers dans le volet de navigation.
3. Choisissez le système de fichiers dont vous souhaitez consulter les métriques.
4. Pour afficher les graphiques des indicateurs du système de fichiers, sélectionnez Surveillance et performances dans le deuxième panneau.

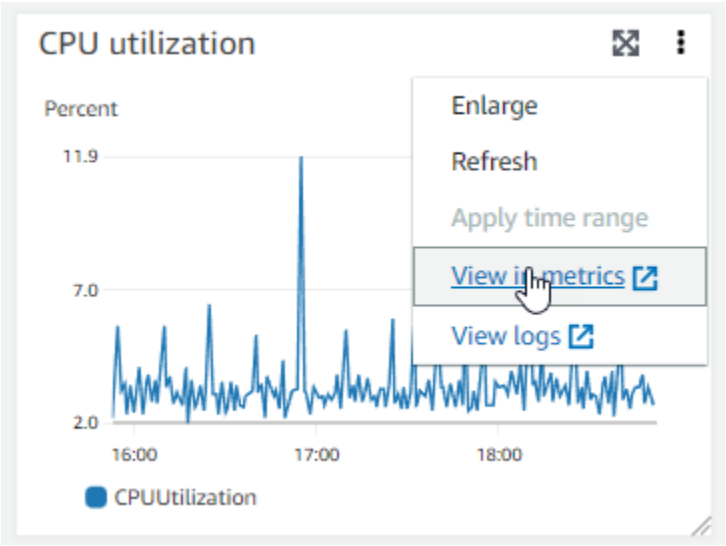


- Les mesures récapitulatives sont affichées par défaut, indiquant tous les avertissements et CloudWatch alarmes actifs ainsi que les mesures d'activité du système de fichiers.
- Choisissez Stockage pour afficher la capacité de stockage et les indicateurs d'utilisation.
- Choisissez Performance pour 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 le système de fichiers.

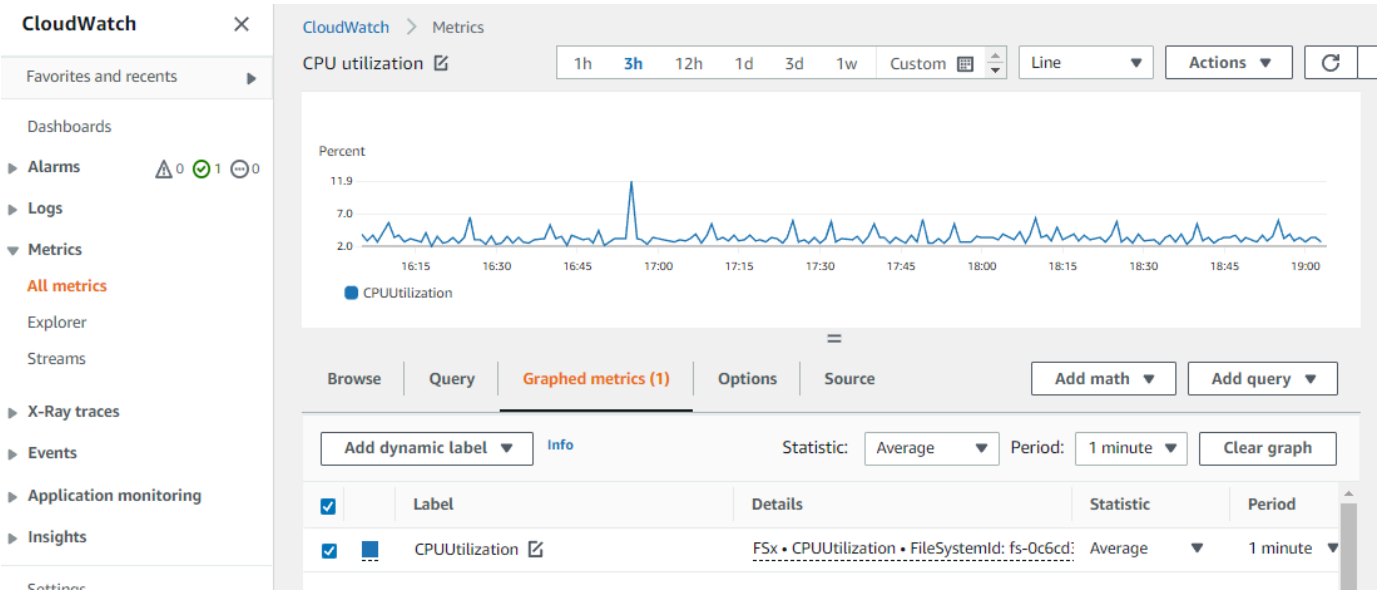
Pour plus d'informations, consultez Comment utiliser les métriques de FSx for Windows File Server.

Pour afficher les métriques dans la CloudWatch console

1. Pour consulter une métrique du système de fichiers sur la page Metrics de la CloudWatch console Amazon, accédez à la métrique dans le panneau Monitoring & performance de la console Amazon FSx.
2. Choisissez Afficher dans les métriques dans le menu Actions en haut à droite du graphique des métriques, comme illustré dans l'image suivante.



Cela ouvre la page Mesures dans la CloudWatch console, qui affiche le graphique des métriques, comme illustré dans l'image suivante.



Pour ajouter des métriques à un CloudWatch tableau de bord

1. Pour ajouter un ensemble de mesures du système de fichiers FSx pour Windows à un tableau de bord de la CloudWatch console, choisissez l'ensemble de mesures (résumé, stockage ou performances) dans le panneau Monitoring & performance de la console Amazon FSx.
2. Choisissez Ajouter au tableau de bord dans le coin supérieur droit du panneau, cela ouvre la CloudWatch console.
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.

Pour accéder aux métriques depuis AWS CLI

- Utilisez la commande `list-metrics` avec l'espace de noms `--namespace "AWS/FSx"`. Pour plus d'informations, consultez la référence de la commande AWS CLI.

Utilisation de l' CloudWatch API

Pour accéder aux métriques depuis l' CloudWatch API

- Appelez `GetMetricStatistics`. Pour plus d'informations, consultez Amazon CloudWatch API Reference.

Création d' CloudWatch alarmes pour surveiller Amazon FSx

Vous pouvez créer une CloudWatch alarme qui envoie un message Amazon SNS lorsque l'alarme change d'état. Une alarme surveille une seule métrique pendant une durée que vous définissez et exécute une ou plusieurs actions en fonction de la valeur de la métrique par rapport à un seuil donné pendant un certain nombre de périodes. L'action est une notification envoyée à une rubrique Amazon SNS ou à une politique Auto Scaling.

Les alarmes déclenchent des actions uniquement pour les changements d'état prolongés. CloudWatch les alarmes n'appellent pas d'actions simplement parce qu'elles sont dans un état particulier ; l'état doit avoir changé et être maintenu pendant un certain nombre de périodes. Vous pouvez créer une alarme à partir de la console Amazon FSx ou de la CloudWatch console.

Les procédures suivantes décrivent comment créer des alarmes pour Amazon FSx à l'aide de la console et de l' AWS CLI API.

Pour définir des alarmes à l'aide de la console Amazon FSx

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation, choisissez Systèmes de fichiers, puis choisissez le système de fichiers pour lequel vous souhaitez créer l'alarme.
3. Choisissez le menu Actions, puis sélectionnez Afficher les détails.
4. Sur la page Résumé, sélectionnez Surveillance et performances.
5. Choisissez les CloudWatch alarmes.
6. Choisissez Créer une CloudWatch alarme. Vous êtes ensuite redirigé vers la console CloudWatch.
7. Choisissez Select metrics, puis Next.
8. Dans la section Metrics, choisissez FSX.
9. Choisissez File System Metrics, choisissez la métrique pour laquelle vous souhaitez définir l'alarme, puis sélectionnez Select metric.
10. Dans la section Conditions, choisissez les conditions que vous souhaitez pour l'alarme, puis cliquez sur Suivant.

> **Note**
>
> Les métriques ne peuvent pas être publiées pendant la maintenance du système de fichiers pour les systèmes de fichiers mono-AZ, ou pendant le basculement et le retour en arrière vers ou depuis les serveurs principaux ou secondaires pour les systèmes de fichiers multi-AZ. 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 SNS lorsque l'état d'alarme déclenche l'action, choisissez un état d'alarme pour Chaque fois que cet état d'alarme est activé.

Pour sélectionner une rubrique SNS, choisissez une rubrique SNS existante. Si vous sélectionnez Create topic, 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 valeurs Name, Description et Whenever de la métrique, puis choisissez Next.
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. Connectez-vous à la CloudWatch console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Choisissez Créer une alarme pour démarrer l'assistant de création d'alarme.
3. Choisissez FSx Metrics, puis parcourez les métriques Amazon FSx pour trouver la métrique sur laquelle vous souhaitez placer une alarme. Pour afficher uniquement les métriques Amazon FSx dans cette boîte de dialogue, recherchez l'ID du système de fichiers de votre système de fichiers. Sélectionnez la métrique sur laquelle créer une alarme, puis sélectionnez Suivant.
4. Indiquez les valeurs Name, Description et Whenever pour la métrique.
5. Si vous souhaitez vous CloudWatch envoyer un e-mail lorsque l'état d'alarme est atteint, pour Chaque fois que cette alarme est atteinte, choisissez State is ALARM. Pour Envoyer une notification à, sélectionnez une rubrique SNS existante. Si vous sélectionnez Create topic, 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.

> **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.

6. À ce stade, la zone d'aperçu de l'alarme vous permet de prévisualiser l'alarme que vous êtes sur le point de créer. Sélectionnez Create Alarm (Créer une alerte).

Pour régler une alarme à l'aide du AWS CLI

- Appelez `put-metric-alarm`. Pour plus d'informations, consultez la référence de la commande AWS CLI.

Pour configurer une alarme à l'aide de l' CloudWatch API

- Appelez `PutMetricAlarm`. Pour plus d'informations, consultez Amazon CloudWatch API Reference.

Enregistrement des appels d'API Amazon FSx for Windows File Server en utilisantAWS CloudTrail

Amazon FSx for Windows File Server est intégré àAWS CloudTrail, un service qui fournit un registre des actions réalisées par un utilisateur, un rôle ou unAWSservice dans Amazon FSx. CloudTrail capture tous les appels d'API pour Amazon FSx en tant qu'événements. Ces captures incluent les appels de la console Amazon FSx et les appels de code vers les opérations d'API Amazon FSx. Si vous créez un journal d'activité, vous pouvez activer la livraison continue de CloudTrail événements dans un compartiment Amazon S3, y compris les événements pour Amazon FSx. Si vous ne configurez pas de journal de suivi, vous pouvez toujours afficher les événements les plus récents dans le CloudTrail Console dansHistorique de l'événement. Utilisation des informations collectées par CloudTrail, vous pouvez déterminer quelle demande a été faite à Amazon FSx, de l'adresse IP à partir de laquelle la demande a été effectuée, de l'auteur et de la requête, ainsi que d'autres détails.

En savoir plus sur CloudTrail, consultez leAWS CloudTrailGuide de l'utilisateur.

Informations Amazon FSx dans CloudTrail

CloudTrail est activé sur votreCompte AWSlors de la création de ce dernier. Lorsqu'une activité a lieu dans Amazon FSx, elle est enregistrée dans un CloudTrail événement avec d'autresAWSEvénements de serviceHistorique de l'événement. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, veuillez consulter la rubriqueAffichage d'événements avec CloudTrail Historique de l'événement.

Pour un enregistrement continu des événements dans votreCompte AWS, y compris des événements pour Amazon FSx, créez un journal d'activité. UNsentierpermet CloudTrail pour livrer des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal d'activité consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Simple Storage Service (Amazon S3) de votre choix. En outre, vous pouvez configurer d'autresAWSservices pour analyser plus en profondeur les données d'événement collectées dans CloudTrail journaux. Pour en savoir plus, consultez les ressources suivantes :

- Présentation de la création d'un journal d'activité
- CloudTrail Intégrations et services pris en charge par
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception CloudTrail fichiers journaux de plusieurs régionsetRéception CloudTrail fichiers journaux de plusieurs comptes

Toutes les actions Amazon FSx sont enregistrées par CloudTrail et sont documentés dans leRéférence de l'API Amazon FSx. Par exemple, les appels vers le`CreateFileSystem`,`CreateBackup`et`TagResource`les actions génèrent des entrées dans CloudTrail fichiers journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre service AWS.

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Présentation des entrées des fichiers journaux Amazon FSx

Un journal d'activité est une configuration qui permet d'envoyer des événements sous forme de fichiers journaux à un compartiment Simple Storage Service (Amazon S3) que vous spécifiez. CloudTrail Les fichiers journaux peuvent contenir une ou plusieurs entrées de journal. Un événement représente une demande individuelle émise à partir d'une source quelconque et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail Les fichiers journaux ne constituent pas une pile ordonnée retraçant les appels d'API publics. Ils ne suivent aucun ordre précis.

L'exemple suivant montre un CloudTrail entrée de journal qui montre`TagResource`opération lorsqu'une balise pour un système de fichiers est créée 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 un CloudTrail entrée de journal qui montre`UntagResource`action 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"
}
```

Performances de FSx for Windows File Server

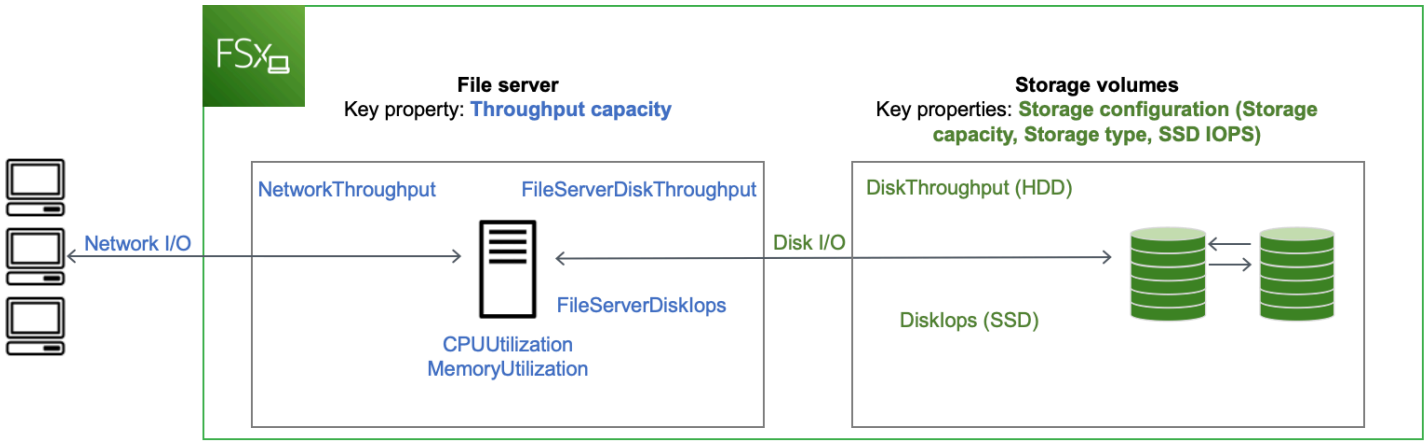
FSx for Windows File Server propose des options de configuration du système de fichiers répondant à de nombreux besoins en termes de performances. Vous trouverez ci-dessous une présentation des performances du système de fichiers Amazon FSx, avec une discussion sur les options de configuration des performances disponibles et des conseils utiles en matière de performances.

Rubriques

Performances du système de fichiers

Chaque système de fichiers FSx for Windows File Server se compose d'un serveur de fichiers Windows avec lequel les clients communiquent et d'un ensemble de volumes de stockage, ou disques, attachés au serveur de fichiers. Chaque serveur de fichiers utilise un cache rapide en mémoire pour améliorer les performances des données les plus fréquemment consultées.

Le schéma suivant illustre la manière dont les données sont accessibles à partir d'un système de fichiers FSx for Windows File Server.



Lorsqu'un client accède à des données stockées dans le cache en mémoire, les données sont transmises directement au client demandeur sous forme d'E/S réseau. Le serveur de fichiers n'a pas besoin de le lire ou de l'écrire sur le disque. Les performances de cet accès aux données sont déterminées par les limites d'E/S du réseau et par la taille du cache en mémoire.

Lorsqu'un client accède à des données qui ne sont pas dans le cache, le serveur de fichiers les lit ou les écrit sur le disque sous forme d'E/S de disque. Les données sont ensuite transmises du serveur de fichiers au client sous forme d'E/S réseau. Les performances de cet accès aux données sont déterminées par les limites d'E/S du réseau ainsi que par les limites d'E/S du disque.

Les performances des E/S réseau et le cache en mémoire du serveur de fichiers sont déterminés par la capacité de débit du système de fichiers. Les performances d'E/S du disque sont déterminées par la combinaison de la capacité de débit et de la configuration du stockage. Les performances d'E/S de disque maximales, qui correspondent au débit du disque et aux niveaux d'IOPS du disque, que votre système de fichiers peut atteindre sont les plus faibles des valeurs suivantes :

- Le niveau de performance des E/S de disque fourni par votre serveur de fichiers, en fonction de la capacité de débit que vous sélectionnez pour votre système de fichiers.
- Le niveau de performance des E/S du disque fourni par votre configuration de stockage (capacité de stockage, type de stockage et niveau d'IOPS SSD que vous sélectionnez pour votre système de fichiers).

Considérations supplémentaires relatives aux performances

Les performances du système de fichiers sont généralement mesurées par sa latence, son débit et ses opérations d'E/S par seconde (IOPS).

Latence

Les serveurs de fichiers FSx for Windows File Server utilisent un cache rapide en mémoire pour obtenir des latences constantes inférieures à la milliseconde pour les données auxquelles on accède activement. Pour les données qui ne se trouvent pas dans le cache en mémoire, c'est-à-dire pour les opérations de fichiers qui doivent être traitées en effectuant des E/S sur les volumes de stockage sous-jacents, Amazon FSx fournit des latences de fonctionnement des fichiers inférieures à la milliseconde avec le stockage sur disque dur (SSD) et des latences à un chiffre en millisecondes avec le stockage sur disque dur (HDD).

Débit et IOPS

Les systèmes de fichiers Amazon FSx fournissent jusqu'à 2 Gbit/s et 80 000 IOPS partout où Régions AWS Amazon FSx est disponible, et 12 Gbit/s de débit et 400 000 IOPS dans l'est des États-Unis (Virginie du Nord), l'ouest des États-Unis (Oregon), l'est des États-Unis (Ohio), l'Europe (Irlande), l'Asie-Pacifique (Tokyo) et l'Asie-Pacifique (Singapour). Le débit et les IOPS spécifiques que votre charge de travail peut générer sur votre système de fichiers dépendent de la capacité de débit, de la capacité de stockage et du type de stockage de votre système de fichiers, ainsi que de la nature de votre charge de travail, notamment de la taille de l'ensemble de travail actif.

Performances pour un seul client

Avec Amazon FSx, vous pouvez atteindre le débit total et les niveaux d'IOPS de votre système de fichiers à partir d'un seul client qui y accède. Amazon FSx prend en charge le multicanal pour les PME. Cette fonctionnalité lui permet de fournir un débit pouvant atteindre plusieurs Gbit/s et des centaines de milliers d'IOPS pour un seul client accédant à votre système de fichiers. SMB Multicanal utilise plusieurs connexions réseau entre le client et le serveur simultanément pour agréger la bande passante réseau afin d'optimiser l'utilisation. Bien qu'il existe une limite théorique au nombre de connexions SMB prises en charge par Windows, cette limite se chiffre en millions, et vous pouvez pratiquement avoir un nombre illimité de connexions SMB.

Performance en rafale

Les charges de travail basées sur des fichiers sont généralement élevées, caractérisées par des périodes courtes et intenses d'E/S élevées avec de longs temps d'inactivité entre les rafales. Pour prendre en charge les charges de travail élevées, outre les vitesses de base qu'un système de fichiers peut supporter 24 heures sur 24, 7 jours sur 7, Amazon FSx permet d'atteindre des vitesses plus élevées pendant des périodes de temps, à la fois pour les opérations d'E/S réseau et d'E/S

sur disque. Amazon FSx utilise un mécanisme de crédit d'E/S pour allouer le débit et les IOPS en fonction de l'utilisation moyenne. Les systèmes de fichiers accumulent des crédits lorsque leur débit et leur utilisation d'IOPS sont inférieurs à leurs limites de base, et peuvent utiliser ces crédits lorsqu'ils effectuent des opérations d'E/S.

Impact de la capacité de débit sur les performances

La capacité de débit détermine les performances du système de fichiers dans les catégories suivantes :

- E/S réseau : vitesse à laquelle le serveur de fichiers peut transmettre les données des fichiers aux clients qui y accèdent.
- Processeur et mémoire du serveur de fichiers : ressources disponibles pour le traitement des données de fichiers et l'exécution d'activités en arrière-plan, telles que la déduplication des données et les clichés instantanés.
- E/S sur disque : vitesse à laquelle le serveur de fichiers peut prendre en charge les E/S entre le serveur de fichiers et les volumes de stockage.

Les tableaux suivants fournissent des informations détaillées sur les niveaux maximaux d'E/S réseau (débit et IOPS) et d'E/S sur disque (débit et IOPS) que vous pouvez atteindre avec chaque configuration de capacité de débit allouée, ainsi que sur la quantité de mémoire disponible pour la mise en cache et la prise en charge des activités d'arrière-plan telles que la déduplication des données et les clichés instantanés. Bien que vous puissiez sélectionner des niveaux de capacité de débit inférieurs à 32 mégaoctets par seconde (Mo/s) lorsque vous utilisez l'API ou la CLI Amazon FSx, gardez à l'esprit que ces niveaux sont destinés aux charges de travail de test et de développement, et non aux charges de travail de production.

> **Note**
>
> Notez que les niveaux de capacité de débit supérieurs ou égaux à 4 608 Mbit/s ne sont pris en charge que dans les régions suivantes : USA Est (Virginie du Nord), USA Ouest (Oregon), USA Est (Ohio), Europe (Irlande), Asie-Pacifique (Tokyo) et Asie-Pacifique (Singapour).

E/S réseau et mémoire

Capacité de débit FSx (mégaoctets par seconde)	Débit du réseau (mégaoctets par seconde)		IOPS du réseau	Mémoire (Go)
	Base de référence	Burst (quelques minutes par jour)		
32	32	600	Milliers	4
64	64	600	Dizaines de milliers	8
128	150	1 250		8
256	300	1 250	Des centaines de milliers	16
512	600	1 250		32
1,024	1 500	–		72
2 048	3 125	–		144
4 608	9 375	–	Des millions	192
6 144	12 500	–		256
9 216	18 750	–		384
12 288	21 250	–		512

E/S de disque

Capacité de débit FSx (mégaoctets par seconde)	Débit du disque (mégaoctets par seconde)		IOPS sur disque	
	Base de référence	Burst (30 minutes par jour)	Base de référence	Burst (30 minutes par jour)
32	32	260	2 KM	12 000
64	64	350	4K	16 000
128	128	600	6 KM	20 KM
256	256	600	10 000	20 KM
512	512	–	20 KM	–
1,024	1,024	–	40 000	–
2 048	2 048	–	80 000	–
4 608	4 608	–	150 000	–
6 144	6 144	–	200 000	–
9 216	9 216 [1]	–	300 K [1]	–
12 288	12 288 [1]	–	400 K [1]	–

> **Note**
>
> [1] Si vous disposez d'un système de fichiers multi-AZ avec une capacité de débit de 9 216 ou 12 288 Mo/s, les performances seront limitées à 9 000 Mo/s et 262 500 IOPS pour le trafic d'écriture uniquement. Sinon, pour le trafic de lecture sur tous les systèmes de fichiers multi-AZ, le trafic de lecture et d'écriture sur tous les systèmes de fichiers mono-AZ et tous les

autres niveaux de capacité de débit, votre système de fichiers prendra en charge les limites de performances indiquées dans le tableau.

Choisir le bon niveau de capacité de débit

Lorsque vous créez un système de fichiers à l'aide de la console de gestion Amazon Web Services, Amazon FSx sélectionne automatiquement le niveau de capacité de débit recommandé pour votre système de fichiers en fonction de la capacité de stockage que vous configurez. Bien que la capacité de débit recommandée soit suffisante pour la plupart des charges de travail, vous avez la possibilité d'annuler la recommandation et de sélectionner une capacité de débit spécifique pour répondre aux besoins de votre application. Par exemple, si votre charge de travail nécessite le transfert de 1 Gbit/s de trafic vers votre système de fichiers, vous devez sélectionner une capacité de débit d'au moins 1 024 Mbit/s.

Vous devez également tenir compte des fonctionnalités que vous prévoyez d'activer sur votre système de fichiers pour décider du niveau de débit à configurer. Par exemple, l'activation des clichés instantanés peut vous obliger à augmenter votre capacité de débit jusqu'à trois fois votre charge de travail prévue afin de garantir que le serveur de fichiers puisse conserver les clichés instantanés avec la capacité de performance d'E/S disponible. Si vous activez la déduplication des données, vous devez déterminer la quantité de mémoire associée à la capacité de débit de votre système de fichiers et vous assurer que cette quantité de mémoire est suffisante pour la taille de vos données.

Vous pouvez ajuster la capacité de débit à la hausse ou à la baisse à tout moment après l'avoir créée. Pour plus d’informations, consultez Gestion de la capacité de débit.

Vous pouvez surveiller l'utilisation des ressources de performance du serveur de fichiers par votre charge de travail et obtenir des recommandations sur la capacité de débit à sélectionner en consultant l'onglet Surveillance et performances > Performances de votre console Amazon FSx. Nous vous recommandons de procéder à des tests dans un environnement de pré-production pour vous assurer que la configuration que vous avez sélectionnée répond aux exigences de performance de votre charge de travail. Pour les systèmes de fichiers multi-AZ, nous vous recommandons également de tester l'impact du processus de basculement qui se produit lors de la maintenance du système de fichiers, des modifications de capacité de débit et des interruptions de service imprévues sur votre charge de travail, ainsi que de vous assurer que vous disposez d'une capacité de débit suffisante pour éviter tout impact sur les performances lors de tels événements. Pour plus d’informations, consultez Accès aux métriques du serveur de fichiers FSx for Windows.

Impact de la configuration du stockage sur les performances

La capacité de stockage, le type de stockage et le niveau d'IOPS du SSD de votre système de fichiers ont tous un impact sur les performances d'E/S disque de votre système de fichiers. Vous pouvez configurer ces ressources pour fournir les niveaux de performance souhaités pour votre charge de travail.

Vous pouvez augmenter la capacité de stockage et adapter les IOPS des SSD à tout moment. Pour plus d'informations, consultez Gestion de la capacité de stockage et Gestion des IOPS sur SSD. Vous pouvez également mettre à niveau votre système de fichiers du type de stockage HDD au type de stockage SSD. Pour plus d'informations, consultez Gestion du type de stockage.

Votre système de fichiers fournit les niveaux par défaut de débit de disque et d'IOPS suivants :

Type de stockage	Débit du disque (Mbits/s par TiB de stockage)	IOPS sur disque (IOPS par TiB de stockage)
SSD	750	3 000*
HDD	12 lignes de base ; 80 rafales (jusqu'à un maximum de 1 Gbit/s par système de fichiers)	12 lignes de base ; 80 rafales

> **Note**
>
> *Pour les systèmes de fichiers dotés d'un type de stockage SSD, vous pouvez fournir des IOPS supplémentaires jusqu'à un ratio maximum de 500 IOPS par GiB de stockage et de 400 000 IOPS par système de fichiers.

Performance du disque dur en rafale

Pour les volumes de stockage sur disque dur, Amazon FSx utilise un modèle de bucket en rafale pour des raisons de performances. La taille du volume détermine le débit de base du volume, qui correspond à la vitesse à laquelle le volume accumule des crédits de débit. La taille du volume détermine également le débit de transmission en rafales du volume, qui correspond à la vitesse à laquelle vous pouvez utiliser des crédits lorsqu'ils sont disponibles. Les gros volumes ont un débit de

base et de transmission en rafales plus élevé. Plus votre volume a de crédits, plus longtemps il est en mesure d'assurer la transmission des I/O en rafales.

Le débit disponible d'un volume de stockage sur disque dur est exprimé par la formule suivante :

```
(Volume size) × (Credit accumulation rate per TiB) = Throughput
```

Pour un volume de disque dur de 1 To, le débit en rafale est limité à 80 Mo/s, le compartiment se remplit de crédits à 12 Mo/s et peut contenir jusqu'à 1 TiB de crédits.

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 configuré avec 2 TiB de capacité de stockage sur disque dur et 32 Mo/s de capacité de débit possède les niveaux de débit suivants :

- Débit réseau : 32 Mbits/s en mode de référence et 600 Mbits/s en rafale (voir le tableau des capacités de débit)
- Débit du disque : 24 Mo/s en ligne de base et 160 Mo/s en rafale, ce qui correspond à la valeur la plus faible des deux valeurs suivantes :
  - les niveaux de débit du disque de 32 Mo/s en ligne de base et de 260 Mo/s en rafale pris en charge par le serveur de fichiers, sur la base de la capacité de débit du système de fichiers
  - les niveaux de débit du disque de 24 Mo/s en ligne de base (12 Mo/s par To* 2 TiB) et de 160 Mo/s en rafale (80 Mo/s par TiB* 2 TiB) pris en charge par les volumes de stockage, en fonction du type et de la capacité de stockage

Votre charge de travail accédant au système de fichiers pourra donc atteindre un débit de base de 32 Mo/s et un débit en rafale de 600 Mo/s pour les opérations de fichiers effectuées sur des données activement consultées mises en cache dans le cache en mémoire du serveur de fichiers, et jusqu'à 24 Mo/s de débit de référence et 160 Mo/s de débit en rafale pour les opérations de fichiers devant être acheminées jusqu'au disque, par exemple en raison de défaillances du cache.

Mesurer les performances à l'aide de CloudWatch métriques

Vous pouvez utiliser Amazon CloudWatch pour mesurer et surveiller le débit et les IOPS de votre système de fichiers. Pour plus d'informations, consultez Surveillance des métriques avec Amazon CloudWatch.

Résolution des problèmes de performances

Pour obtenir de l'aide pour résoudre les problèmes de performances courants, consultezRésolution des problèmes de performances du système de fichiers.

Procédure pas à pas Amazon FSx

Vous trouverez ci-dessous un certain nombre de procédures pas à pas orientées tâches qui vous guident à travers divers processus.

Rubriques

Procédure 1 : Conditions préalables à la prise en main

Avant de pouvoir terminer l'exercice de démarrage, une instance Amazon EC2 basée sur Microsoft Windows doit déjà être jointe à votreAWS Directory Serviceannuaire. Vous devez également être connecté à l'instance via le protocole Bureau à distance Windows en tant qu'utilisateur administrateur de votre annuaire. La procédure suivante vous montre comment effectuer ces actions préalables nécessaires.

Rubriques

Étape 1 : Configurer Active Directory

Avec Amazon FSx, vous pouvez utiliser un stockage de fichiers entièrement géré pour les charges de travail Windows. De même,AWS Directory Servicefournit des répertoires entièrement gérés à utiliser dans le déploiement de votre charge de travail. Si vous avez déjà un domaine AD d'entreprise

exécuté dansAWSdans un Virtual Private Cloud (VPC) utilisant des instances EC2, vous pouvez activer l'authentification et le contrôle d'accès basés sur les utilisateurs. Pour ce faire, établissez une relation de confiance entre votreAWSMicrosoft AD géré et votre domaine d'entreprise. Pour l'authentification Windows dans Amazon FSx, vous n'avez besoin que d'une confiance de forêt directionnelle unidirectionnelle, où leAWSla forêt gérée fait confiance à la forêt du domaine d'entreprise.

Votre domaine d'entreprise joue le rôle du domaine de confiance, et leAWS Directory Servicedomaine géré joue le rôle du domaine de confiance. Les demandes d'authentification validées se déplacent entre les domaines dans une seule direction, ce qui permet aux comptes de votre domaine d'entreprise de s'authentifier par rapport aux ressources partagées dans le domaine géré. Dans ce cas, Amazon FSx interagit uniquement avec le domaine géré. Le domaine géré transmet ensuite les demandes d'authentification à votre domaine d'entreprise.

> **Note**
>
> Vous pouvez également utiliser un type d'approbation externe avec Amazon FSx pour les domaines approuvés.

Votre groupe de sécurité Active Directory doit activer l'accès entrant à partir du groupe de sécurité du système de fichiers Amazon FSx.

Pour créer unAWSServices d'annuaire pour Microsoft AD

- Si ce n'est pas le cas, utilisez l'AWS Directory Servicepour créer votreAWSAnnuaire géré Microsoft AD. Pour de plus amples informations, veuillez consulterCréation de votreAWSAnnuaire Managed Microsoft ADdans leAWS Directory ServiceGuide d'administration.

  > **Important**
  >
  > N'oubliez pas le mot de passe que vous attribuez à votre utilisateur Admin. Vous en aurez besoin plus tard dans cet exercice de démarrage. Si vous oubliez le mot de passe, vous devez répéter les étapes de cet exercice avec le nouveauAWS Directory Serviceannuaire et utilisateur Admin.

- Si vous avez déjà un AD, créez une relation d'approbation entre votreAWSMicrosoft AD géré et votre AD existant. Pour de plus amples informations, veuillez consulter Quand créer une relation d'approbation dans le Guide d'administration AWS Directory Service.

Étape 2 : Lancer une instance Windows dans la console Amazon EC2

Vous pouvez lancer une instance Windows à l'aide de l'AWS Management Consolecomme décrit dans la procédure suivante. Cela a pour but de vous aider à lancer rapidement votre première instance, de sorte qu'elle ne couvre pas toutes les options possibles. Pour plus d'informations sur les options avancées, consultez Lancement d'une instance.

Pour lancer une instance

1. Ouvrez la console Amazon EC2 sur https://console.aws.amazon.com/ec2/.
2. Sur le tableau de bord de la console, sélectionnez Launch Instance.
3. La page Choose an Amazon Machine Image (AMI) affiche une liste de configurations de base nommées Amazon Machine Images (AMI) qui servent de templates pour votre instance. Sélectionnez l'AMI pour Windows Server 2016 Base ou Windows Server 2012 R2 Base. Notez que ces AMI sont indiquées comme « Éligible à l'offre gratuite ».
4. Sur la page Choisir un type d'instance, vous pouvez sélectionner la configuration matérielle de votre instance. Sélectionnez le type `t2.micro` qui est sélectionné par défaut. Notez que ce type d'instance est éligible pour l'offre gratuite.
5. Sélectionnez Vérifier et lancer afin de laisser l'assistant compléter les autres paramètres de configuration pour vous.
6. Dans la pageExaminer le lancement d'instancepage, sousGroupes de sécurité, un groupe de sécurité apparaît que l'assistant a créé et sélectionné pour vous. Vous pouvez utiliser ce groupe de sécurité ou choisir le groupe de sécurité que vous avez créé lors de la configuration à l'aide des étapes suivantes :

   a. Sélectionnez Edit security groups.

   b. Sur la page Configure Security Group, vérifiez que Select an existing security group est sélectionné.

   c. Choisissez votre groupe de sécurité dans la liste des groupes de sécurité existants, puis sélectionnez Vérifier et lancer.
7. Sur la page Review Instance Launch, sélectionnez Launch.
8. Lorsque vous êtes invité à choisir une paire de clés, sélectionnez Choisir une paire de clés existante, puis sélectionnez la paire de clés que vous avez créée lors de la configuration.

   Sinon, vous pouvez créer une nouvelle paire de clés. Sélectionnez Créer une nouvelle paire de clés, entrez un nom pour la paire de clés, puis sélectionnez Télécharger une paire de clés. C'est

la seule occasion pour vous d'enregistrer votre fichier clé privé. Veillez donc à télécharger la paire de clés. Enregistrez le fichier de clé privée en lieu sûr. Vous devez fournir le nom de votre paire de clés quand vous lancez une instance, ainsi que la clé privée correspondante chaque fois que vous vous connectez à l'instance.

> **Warning**
>
> Ne sélectionnez pas l'option Continuer sans paire de clés. Si vous lancez votre instance sans une paire de clés, vous ne pourrez pas vous y connecter.

Lorsque vous êtes prêt, cochez la case de confirmation, puis sélectionnez Launch Instances.

9. Une page de confirmation indique que l'instance est en cours de lancement. Sélectionnez View Instances pour fermer la page de confirmation et revenir à la console.
10. Sur l'écran Instances, vous pouvez afficher le statut du lancement. Il suffit de peu de temps pour lancer une instance. Lorsque vous lancez une instance, son état initial est `pending`. Une fois que l'instance a démarré, son état devient `running` et elle reçoit un nom DNS public. (Si la colonne DNS public (IPv4) est masquée, sélectionnez l'icône Afficher / Masquer les colonnes (icône en forme d'engrenage) dans le coin supérieur droit de la page, puis sélectionnez DNS public (IPv4).)
11. Cela peut prendre quelques minutes avant que l'instance soit prête pour que vous puissiez vous y connecter. Vérifiez que votre instance a réussi ses contrôles de statut ; vous pouvez voir cette information dans la colonne Status Checks.

> **Important**
>
> Notez l'ID du groupe de sécurité créé lors du lancement de cette instance. Vous en aurez besoin lors de la création de votre système de fichiers Amazon FSx.

Maintenant que votre instance est lancée, vous pouvez vous connecter à votre instance.

Étape 3 : Se connecter à votre instance

Pour vous connecter à une instance Windows, vous devez récupérer le mot de passe administrateur initial, puis spécifier ce mot de passe lorsque vous vous connectez à votre instance à l'aide du Bureau à distance.

Le nom du compte administrateur dépend de la langue du système d'exploitation. Par exemple, pour l'anglais c'est Administrateur, pour le français c'est Administrateur, et pour le portugais c'est Administrador. Pour plus d'informations, consultez Noms localisés pour le compte administrateur dans Windows dans le Wiki Microsoft TechNet.

Si vous avez joint votre instance à un domaine, vous pouvez vous connecter à votre instance à l'aide des informations d'identification de domaine que vous avez définies dansAWS Directory Service. Sur l'écran de connexion Bureau à distance, n'utilisez pas le nom de l'ordinateur local ni le mot de passe généré. Au lieu de cela, utilisez le nom d'utilisateur complet de l'administrateur et le mot de passe de ce compte. Par exemple : **`corp.example.com\Admin`**.

La licence pour le système d'exploitation Windows Server autorise deux connexions à distance simultanées à des fins administratives. La licence pour Windows Server est incluse dans le prix de votre instance Windows. Si vous avez besoin de plus de deux connexions à distance simultanées, vous devez acheter une licence de Services de bureau à distance (RDS). Si vous tentez une troisième connexion, une erreur se produit. Pour de plus amples informations, veuillez consulterConfigurer le nombre de connexions distantes simultanées autorisées pour une connexion.

Pour vous connecter à votre instance de Windows en utilisant un client RDP

1. Dans la console Amazon EC2, sélectionnez l'instance, puis choisissez Se connecter.
2. DansConnectez-vous à votre instance, choisissezObtenir le mot(Cela prend quelques minutes après le lancement de l'instance pour que le mot de passe soit disponible).
3. Choisissez Parcourir et accédez au fichier de clé privée que vous avez créé lorsque vous avez lancé l'instance. Sélectionnez le fichier, puis choisissez Ouvrir pour copier tout le contenu du fichier dans le champ Contenu.
4. Choisissez Déchiffrer le mot de passe. La console affiche le mot de passe administrateur par défaut de l'instance dans leConnectez-vous à votre instance, remplaçant le lien versObtenir le motaffiché précédemment avec le mot de passe réel.
5. Enregistrez le mot de passe administrateur par défaut ou copiez-le dans le Presse-papiers. Vous en aurez besoin pour vous connecter à l'instance.
6. Sélectionnez Télécharger le fichier Bureau à distance. Votre navigateur vous invite à ouvrir ou enregistrer le fichier .rdp. L'une ou l'autre option convient. Lorsque vous avez terminé, vous pouvez choisirFermerpour rejeter leConnectez-vous à votre instanceboîte de dialogue.

   - Si vous avez ouvert le fichier .rdp, vous verrez la boîte de dialogue Connexion Bureau à distance.

- Si vous avez enregistré le fichier .rdp, accédez à votre répertoire de téléchargements, et ouvrez le fichier .rdp pour afficher la boîte de dialogue.

7. Vous pouvez obtenir un avertissement indiquant que l'éditeur de la connexion à distance est inconnu. Vous pouvez continuer à vous connecter à votre instance.
8. Lorsque vous y êtes invité, connectez-vous à l'instance, à l'aide du compte administrateur du système d'exploitation et du mot de passe que vous avez enregistrés ou copiés précédemment. Si votre Connexion Bureau à distance dispose déjà d'un compte administrateur configuré, vous devrez peut-être choisir l'option Utiliser un autre compte et saisir le nom d'utilisateur et le mot de passe manuellement.

   > **Note**
   >
   > Les opérations de copier et coller du contenu peuvent endommager les données. Si vous rencontrez une erreur « Échec du mot de passe » à la connexion, essayez de saisir le mot de passe manuellement.

9. En raison de la nature des certificat auto-signés, vous pouvez obtenir un avertissement indiquant que le certificat de sécurité ne peut pas être authentifié. Utilisez les étapes suivantes pour vérifier l'identité de l'ordinateur distant ou cliquez simplement sur Oui ou sur Continuer pour poursuivre si vous faites confiance au certificat.

   a. Si vous utilisez Connexion Bureau à distance depuis un PC Windows, sélectionnez Afficher le certificat. Si vous utilisez Bureau à distance Microsoft sur un Mac, sélectionnez Afficher le certificat.

   b. Choisissez l'onglet Détails et faites défiler l'écran jusqu'à l'entrée Empreinte sur un PC Windows ou l'entrée Empreintes SHA1 sur un Mac. Il s'agit de l'identifiant unique du certificat de sécurité de l'ordinateur distant.

   c. Dans la console Amazon EC2, sélectionnez l'instance, puis Actions et Obtenir le journal système.

   d. Dans la sortie du journal système, recherchez une entrée intitulée `RDPCERTIFICATE-THUMBPRINT`. Si cette valeur correspond à l'empreinte du certificat, vous avez vérifié l'identité de l'ordinateur distant.

   e. Si vous utilisez Connexion Bureau à distance depuis un PC Windows, retournez à la boîte de dialogue Certificat, puis cliquez sur OK. Si vous utilisez Bureau à distance Microsoft sur un Mac, retournez à la boîte de dialogue vérifier certificat et sélectionnez Continuer.

f. [Windows] Sélectionnez Oui dans la fenêtre Connexion Bureau à distance pour vous connecter à votre instance.

Maintenant que vous êtes connecté à votre instance, vous pouvez lier l'instance à votreAWS Directory Serviceannuaire.

Étape 4 : Joignez votre instance à votreAWS Directory Serviceannuaire

La procédure suivante vous montre comment lier manuellement une instance Amazon EC2 Windows existante à votreAWS Directory Serviceannuaire.

Pour joindre une instance Windows à votreAWS Directory Serviceannuaire

1. Connect à l'instance à l'aide de n'importe quel client de protocole Bureau à distance.
2. Ouvrez la boîte de dialogue des propriétés TCP/IPv4 sur l'instance.

   a. OuvrirConnexions réseau.

   > **Tip**
   >
   > Vous pouvez ouvrirConnexions réseaudirectement en exécutant ce qui suit à partir d'une invite de commandes sur l'instance.
   >
   > ```
   > %SystemRoot%\system32\control.exe ncpa.cpl
   > ```

   b. Ouvrez le menu contextuel (clic droit) pour toute connexion réseau activée, puis choisissezPropriétés.

   c. Dans la boîte de dialogue Propriétés de la connexion, ouvrez (double clic)Protocole Internet Version 4.
3. (Facultatif) SélectionnezUtilisez les adresses suivantes du serveur DNS, modifiez laServeur DNS préféréetServeur DNS auxiliaireadresses aux adresses IP duAWS Directory Service—serveurs DNS fournis, et choisissezOK..
4. Ouverture d'Propriétés de systèmeboîte de dialogue pour l'instance, choisissez leNom de l'ordinateuret choisissezModification.

> **Tip**
>
> Vous pouvez ouvrir lePropriétés de systèmeen exécutant ce qui suit à partir d'une invite de commandes sur l'instance.
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. DansMembre de, choisissezDomaine, saisissez le nom complet de votreAWS Directory Service, puis choisissezOK..
6. Lorsque vous êtes invité à fournir le nom et le mot de passe de l'administrateur de domaine, saisissez le nom d'utilisateur et le mot de passe du compte administrateur.

> **Note**
>
> Vous pouvez entrer soit le nom complet de votre domaine, soit le NetBios name, suivi d'une barre oblique inverse (\), puis par le nom d'utilisateur, dans ce cas,Administrateur. Par exemple,corp.example.com \ AdminouCorp \ Admin.

7. Lorsque vous avez reçu le message vous accueillant dans le domaine, redémarrez l'instance pour que les modifications prennent effet.
8. Reconnectez-vous à votre instance via RDP et connectez-vous à l'instance à l'aide du nom d'utilisateur et du mot de passe de votreAWS Directory Serviceutilisateur Admin de l'annuaire.

Maintenant que votre instance a été jointe au domaine, vous êtes prêt à créer votre système de fichiers Amazon FSx. Vous pouvez ensuite terminer les autres tâches de l'exercice de démarrage. Pour plus d'informations, consultez Commencer à utiliser Amazon FSx for Windows File Server.

Procédure 2 : Création d'un système de fichiers à partir d'une sauvegarde

Avec Amazon FSx, vous pouvez créer un système de fichiers à partir d'une sauvegarde. Dans ce cas, vous pouvez modifier l'un des éléments suivants pour mieux s'adapter au cas d'utilisation que vous avez pour votre système de fichiers nouvellement créé :

- Type de stockage

- Capacité de débit
- VPC
- Zone de disponibilité
- Sous-réseau
- Groupes de sécurité VPC
- Configuration d'Active Directory
- AWS KMSClé de chiffrement
- Heure de démarrage automatique quotidienne de la sauvegarde
- Fenêtre de maintenance hebdomadaire

La procédure suivante vous guide à travers le processus de création d'un système de fichiers à partir d'une sauvegarde. Avant de créer ce système de fichiers, vous devez avoir une sauvegarde existante. Pour de plus amples informations, veuillez consulterUtilisation des sauvegardes

Pour créer un système de fichiers à partir d'une sauvegarde existante

1. Ouvrez la console Amazon FSx à l'adressehttps://console.aws.amazon.com/fsx/.
2. Dans la liste de navigation à droite, choisissezSauvegardes.
3. Dans le tableau de bord, choisissez la sauvegarde que vous souhaitez utiliser pour créer un nouveau système de fichiers.

   > **Note**
   >
   > Vous ne pouvez restaurer votre sauvegarde que sur un système de fichiers de la même capacité de stockage que l'original. Vous pouvez augmenter la capacité de stockage de votre système de fichiers restauré une fois qu'il est disponible. Pour plus d'informations, consultez Gestion de la capacité de stockage.

4. Choisissez Restore backup. L'assistant de création d'un système de fichiers démarre.
5. Choisissez les paramètres que vous souhaitez modifier pour ce nouveau système de fichiers. Le type de stockage est défini surSSDpar défaut, mais vous pouvez le changer enDISQUE DURdans les conditions suivantes :

   - Le type de déploiement du système de fichiers estMulti-AZouMono-AZ 2.
   - La capacité de stockage est d'au moins 2 000 GiB.

6. ChoisissezRésumé de l'évaluationpour vérifier vos paramètres avant de créer le système de fichiers.
7. Choisissez Create file system (Créer un système de fichiers).

Vous avez maintenant créé avec succès votre nouveau système de fichiers à partir d'une sauvegarde existante.

Procédure 3 : Mettre à jour un système de fichiers existant

Il y a trois éléments que vous pouvez mettre à jour avec les procédures de cette procédure. Tous les autres éléments de votre système de fichiers que vous pouvez mettre à jour, vous pouvez le faire à partir de la console. Ces procédures supposent que vous avez leAWS CLIinstallé et configuré sur votre ordinateur local. Pour de plus amples informations, veuillez consulterInstalletConfigurationdans leAWS Command Line InterfaceGuide de l'utilisateur.

- AutomaticBackupRetentionDays— le nombre de jours durant lesquels les sauvegardes automatiques pour votre système de fichiers doivent être retenues.
- DailyAutomaticBackupStartTime— heure de la journée en heure universelle coordonnée (UTC) à laquelle la fenêtre de sauvegarde automatique quotidienne doit démarrer. La fenêtre est de 30 minutes à partir de cette heure spécifiée. Cette fenêtre ne peut pas chevaucher la fenêtre de sauvegarde de maintenance hebdomadaire.
- WeeklyMaintenanceStartTime— l'heure de la semaine à laquelle vous souhaitez que la fenêtre de maintenance démarre. Le jour 1 est lundi, 2 est mardi, et ainsi de suite. La fenêtre est de 30 minutes à partir de cette heure spécifiée. Cette fenêtre ne peut pas chevaucher la fenêtre de sauvegarde automatique quotidienne.

Les procédures suivantes expliquent comment mettre à jour votre système de fichiers avec leAWS CLI.

Pour mettre à jour la durée de conservation des sauvegardes automatiques pour votre système de fichiers

1. Ouvrez une invite de commande ou un terminal sur votre ordinateur.
2. Exécutez la commande suivante, en remplaçant l'ID du système de fichiers par l'ID de votre système de fichiers et le nombre de jours pendant lesquels vous souhaitez conserver vos sauvegardes automatiques.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration AutomaticBackupRetentionDays=30
```

Pour mettre à jour la fenêtre de sauvegarde quotidienne de votre système de fichiers

1. Ouvrez une invite de commande ou un terminal sur votre ordinateur.
2. Exécutez la commande suivante, en remplaçant l'ID du système de fichiers par l'ID de votre système de fichiers et l'heure à laquelle vous souhaitez commencer la fenêtre.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration DailyAutomaticBackupStartTime=01:00
```

Pour mettre à jour la fenêtre de maintenance hebdomadaire de votre système de fichiers

1. Ouvrez une invite de commande ou un terminal sur votre ordinateur.
2. Exécutez la commande suivante, en remplaçant l'ID du système de fichiers par l'ID de votre système de fichiers et la date et l'heure par lesquelles vous souhaitez commencer la fenêtre.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration WeeklyMaintenanceStartTime=1:01:30
```

Procédure pas à pas 4 : utilisation d'Amazon FSx avec Amazon AppStream 2.0

En prenant en charge le protocole SMB (Server Message Block), Amazon FSx for Windows File Server permet d'accéder à votre système de fichiers à partir d'instances Amazon EC2AWS, VMware Cloud on WorkSpaces, Amazon et Amazon AppStream 2.0. AppStream 2.0 est un service de streaming d'applications entièrement géré. Vous gérez de manière centralisée vos applications de bureau sur la AppStream version 2.0 et vous les envoyez en toute sécurité à un navigateur sur n'importe quel ordinateur. Pour plus d'informations sur la AppStream version 2.0, consultez le Guide d'administration d'Amazon AppStream 2.0. Pour obtenir des instructions sur la manière de rationaliser la gestion de vos images et de vos flottes Amazon AppStream 2.0, consultez le billet deAWS blog Créer automatiquement des images Windows AppStream 2.0 personnalisées.

Utilisez cette procédure pas à pas comme un guide expliquant comment utiliser Amazon FSx AppStream 2.0 pour deux cas d'utilisation : fournir un stockage persistant personnel à chaque utilisateur et fournir un dossier partagé entre les utilisateurs pour accéder aux fichiers courants.

Fournir un stockage persistant personnel à chaque utilisateur

Vous pouvez utiliser Amazon FSx pour fournir à chaque utilisateur de votre organisation un lecteur de stockage unique dans le cadre de sessions de streaming AppStream 2.0. Un utilisateur sera autorisé à accéder uniquement à son dossier. Le lecteur est automatiquement monté au début d'une session de streaming et les fichiers ajoutés ou mis à jour sur le lecteur sont automatiquement conservés entre les sessions de streaming.

Vous devez effectuer trois procédures pour effectuer cette tâche.

Pour créer des dossiers de base pour les utilisateurs du domaine à l'aide d'Amazon FSx

1. Créez un système de fichiers Amazon FSx. Pour plus d'informations, veuillez consulter Commencer à utiliser Amazon FSx for Windows File Server.
2. Une fois le système de fichiers disponible, créez un dossier pour chaque utilisateur du domaine AppStream 2.0 au sein de votre système de fichiers Amazon FSx. L'exemple suivant utilise le nom d'utilisateur de domaine de l'utilisateur comme nom du dossier correspondant. Cela signifie que vous pouvez créer le nom UNC du partage de fichiers pour le mapper facilement à l'aide de la variable d'environnement Windows`%username%`.
3. Partagez chacun de ces dossiers en tant que dossier partagé. Pour plus d'informations, veuillez consulter Gestion des partages de fichiers sur les systèmes de fichiers FSx for Windows File Server.

Pour lancer un générateur d'images AppStream 2.0 joint à un domaine

1. Connectez-vous à la console AppStream 2.0 : https://console.aws.amazon.com/appstream2
2. Choisissez Directory Configs dans le menu de navigation et créez un objet Directory Config. Pour plus d'informations, consultez la section Utilisation d'Active Directory avec la AppStream version 2.0 du Guide d'administration d'Amazon AppStream 2.0.
3. Choisissez Images, Image Builder, puis lancez un nouveau générateur d'images.
4. Choisissez l'objet Configuration de répertoire créé précédemment dans l'assistant Image Builder pour joindre l'instance Image Builder à votre domaine Active Directory.

5. Lancez l'instance Image Builder dans le même VPC que celui de votre système de fichiers Amazon FSx. Assurez-vous d'associer le générateur d'images au mêmeAWS Managed Microsoft AD répertoire que celui auquel votre système de fichiers Amazon FSx est joint. Les groupes de sécurité VPC que vous associez au générateur d'images doivent autoriser l'accès à votre système de fichiers Amazon FSx.
6. Une fois le générateur d'images disponible, connectez-vous au générateur d'images et connectez-vous à l'aide de votre compte d'administrateur de domaine.
7. Installez vos applications.

Pour associer des partages de fichiers Amazon FSx à la AppStream version 2.0

1. Dans le générateur d'images, créez un script batch à l'aide de la commande suivante et enregistrez-le dans un emplacement de fichier connu (par exemple : C:\Scripts\map -fs.bat). L'exemple suivant utilise S : comme lettre de lecteur pour mapper le dossier partagé sur votre système de fichiers Amazon FSx. Vous utilisez le nom DNS de votre système de fichiers Amazon FSx ou un alias DNS associé au système de fichiers dans ce script, que vous pouvez obtenir depuis la vue détaillée du système de fichiers de la console Amazon FSx.

   Si vous utilisez le nom DNS du système de fichiers :

   ```
   @echo off
   net use S: /delete
   net use S: \\file-system-DNS-name\users\%username%
   ```

   Si vous utilisez un alias DNS associé au système de fichiers :

   ```
   @echo off
   net use S: /delete
   net use S: \\fqdn-DNS-alias\users\%username%
   ```

2. Ouvrez une PowerShell invite et exécutez`gpedit.msc`.
3. Dans Configuration utilisateur, choisissez Paramètres Windows, puis Logon.
4. Accédez au script batch que vous avez créé à la première étape de cette procédure et choisissez-le.
5. Dans Configuration de l'ordinateur, sélectionnez Modèles d'administration Windows, Système, puis Stratégie de groupe.

6. Choisissez la politique Configurer le délai du script d'ouverture de session. Activez la politique et réduisez le délai à`0`. Ce paramètre permet de garantir que le script de connexion de l'utilisateur est exécuté immédiatement lorsque l'utilisateur démarre une session de streaming.
7. Créez votre image et attribuez-la à une flotte AppStream 2.0. Assurez-vous de joindre également la flotte AppStream 2.0 au même domaine Active Directory que celui que vous avez utilisé pour le générateur d'images. Lancez la flotte dans le même VPC que celui qu'utilise votre système de fichiers Amazon FSx. Les groupes de sécurité VPC que vous associez à la flotte doivent fournir un accès à votre système de fichiers Amazon FSx.
8. Lancez une session de streaming à l'aide du SSO SAML. Pour vous connecter à une flotte associée à Active Directory, configurez la fédération d'authentification unique à l'aide d'un fournisseur SAML. Pour plus d'informations, consultez la section Accès par authentification unique à la AppStream version 2.0 à l'aide de SAML 2.0 dans le Guide d'administration d'Amazon AppStream 2.0.
9. Votre partage de fichiers Amazon FSx est mappé à la lettre S : drive lors de la session de streaming.

Fourniture d'un dossier partagé entre les utilisateurs

Vous pouvez utiliser Amazon FSx pour fournir un dossier partagé aux utilisateurs de votre organisation. Un dossier partagé peut être utilisé pour conserver les fichiers communs (par exemple, des fichiers de démonstration, des exemples de code, des manuels d'instructions, etc.) nécessaires à tous les utilisateurs.

Vous devez effectuer trois procédures pour effectuer cette tâche.

Pour créer un dossier partagé à l'aide d'Amazon FSx

1. Créez un système de fichiers Amazon FSx. Pour plus d'informations, veuillez consulter Commencer à utiliser Amazon FSx for Windows File Server.
2. Chaque système de fichiers Amazon FSx inclut un dossier partagé par défaut auquel vous pouvez accéder à l'adresse \ \ *File-System-DNS-Name* \ share, ou \ \ *FQDN-DNS-Alias* \ *share si vous utilisez des alias* DNS. Vous pouvez utiliser le partage par défaut ou créer un autre dossier partagé. Pour plus d'informations, veuillez consulter Gestion des partages de fichiers sur les systèmes de fichiers FSx for Windows File Server.

Pour lancer un générateur d'images AppStream 2.0

1. Depuis la console AppStream 2.0, lancez un nouveau générateur d'images ou connectez-vous à un générateur d'images existant. Lancez le générateur d'images dans le même VPC que celui utilisé par votre système de fichiers Amazon FSx. Les groupes de sécurité VPC que vous associez au générateur d'images doivent autoriser l'accès à votre système de fichiers Amazon FSx.
2. Une fois le générateur d'images disponible, connectez-vous au générateur d'images en tant qu'utilisateur administrateur.
3. Installez ou mettez à jour vos applications en tant qu'administrateur.

Pour lier le dossier partagé à la AppStream version 2.0

1. Créez un script batch, comme décrit dans la procédure précédente, pour monter automatiquement le dossier partagé chaque fois qu'un utilisateur lance une session de streaming. Pour terminer le script, vous avez besoin du nom DNS du système de fichiers ou d'un alias DNS associé au système de fichiers (que vous pouvez obtenir depuis la vue détaillée du système de fichiers dans la console Amazon FSx), ainsi que des informations d'identification pour accéder au dossier partagé.

   Si vous utilisez le nom DNS du système de fichiers :

   ```
   @echo off
   net use S: /delete
   net use S: \\file-system-DNS-name\share /user:username password
   ```

   Si vous utilisez un alias DNS associé au système de fichiers :

   ```
   @echo off
   net use S: /delete
   net use S: \\fqdn-DNS-alias\share /user:username password
   ```

2. Créez une politique de groupe pour exécuter ce script batch à chaque ouverture de session utilisateur. Vous pouvez suivre les instructions comme indiqué dans la section précédente.
3. Créez votre image et attribuez-la à votre flotte.

4. Lancez une session de streaming. Vous devriez maintenant voir le dossier partagé automatiquement mappé à la lettre du lecteur.

Procédure pas à pas 5 : Utilisation d'alias DNS pour accéder à votre système de fichiers

FSx for Windows File Server fournit un nom DNS (Domain Name System) par défaut pour chaque système de fichiers que vous pouvez utiliser pour accéder aux données de votre système de fichiers. Vous pouvez également accéder à vos systèmes de fichiers à l'aide d'un alias DNS de votre choix. Avec les alias DNS, vous pouvez continuer à utiliser les noms DNS existants pour accéder aux données stockées sur Amazon FSx lors de la migration du stockage du système de fichiers sur site vers Amazon FSx, sans avoir à mettre à jour d'outils ou d'applications. Vous pouvez associer jusqu'à 50 alias DNS à un système de fichiers à la fois.

Pour accéder à vos systèmes de fichiers Amazon FSx à l'aide d'alias DNS, vous devez effectuer les trois étapes suivantes :

1. Associez des alias DNS à votre système de fichiers Amazon FSx.
2. Configurez les noms principaux de service (SPN) pour l'objet informatique de votre système de fichiers. (Cela est nécessaire pour obtenir l'authentification Kerberos lorsque vous accédez à votre système de fichiers à l'aide d'alias DNS.)
3. Mettez à jour ou créez un enregistrement DNS CNAME pour le système de fichiers et l'alias DNS.

Rubriques

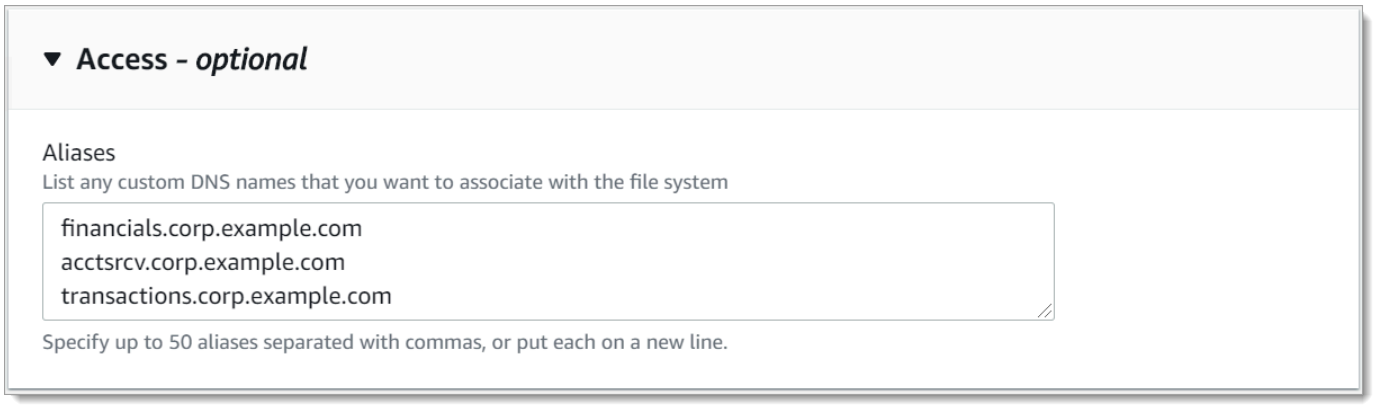
Étape 1 : associer des alias DNS à votre système de fichiers Amazon FSx

Vous pouvez associer des alias DNS aux systèmes de fichiers FSx for Windows File Server existants, lorsque vous créez de nouveaux systèmes de fichiers ou lorsque vous créez un nouveau système de fichiers à partir d'une sauvegarde à l'aide de la console, de la CLI et de l'API Amazon

FSx. Si vous créez un alias avec un autre nom de domaine, entrez le nom complet, y compris le domaine parent, pour associer un alias.

Cette procédure décrit comment associer des alias DNS lors de la création d'un nouveau système de fichiers à l'aide de la console Amazon FSx. Pour plus d'informations sur l'association d'alias DNS aux systèmes de fichiers existants, et pour plus de détails sur l'utilisation de la CLI et de l'API, consultezGestion des alias DNS.

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Suivez la procédure de création d'un nouveau système de fichiers décrite dans Créez votre système de fichiers la section Mise en route.
3. Dans la section Accès - facultatif de l'assistant de création de système de fichiers, entrez les alias DNS que vous souhaitez associer à votre système de fichiers.



   Respectez les consignes suivantes lorsque vous spécifiez des alias DNS :

   - Doit être formaté en tant que nom de domaine complet (FQDN)*hostname.domain*, par exemple,. `accounting.example.com`
   - Peut contenir des caractères alphanumériques et des tirets (-).
   - Il ne peut pas commencer ni se terminer par un trait d'union.
   - Il peut commencer par un caractère numérique.

   Pour les noms d'alias DNS, Amazon FSx stocke les caractères alphabétiques sous forme de lettres minuscules (a-z), quelle que soit la manière dont vous les spécifiez : lettres majuscules, lettres minuscules ou lettres correspondantes sous forme de codes d'échappement.
4. Pour les préférences de maintenance, apportez les modifications souhaitées.

5. Dans la section Balises - facultatif, ajoutez les balises dont vous avez besoin, puis choisissez Next.
6. Vérifiez la configuration du système de fichiers qui s'affiche sur la page Create file system (Créer un système de fichiers). Choisissez Créer un système de fichiers pour créer le système de fichiers.

   Lorsque votre nouveau système de fichiers sera disponible, passez à l'étape 2.

Étape 2 : Configuration des noms principaux de service (SPN) pour Kerberos

Nous vous recommandons d'utiliser l'authentification et le chiffrement basés sur Kerberos lors du transit avec Amazon FSx. Kerberos fournit l'authentification la plus sécurisée pour les clients qui accèdent à votre système de fichiers.

Pour activer l'authentification Kerberos pour les clients qui accèdent à Amazon FSx à l'aide d'un alias DNS, vous devez ajouter des noms principaux de service (SPN) correspondant à l'alias DNS sur l'objet informatique Active Directory de votre système de fichiers Amazon FSx. Un SPN ne peut être associé qu'à un seul objet informatique Active Directory à la fois. Si vous avez déjà configuré des SPN pour le nom DNS pour l'objet informatique Active Directory de votre système de fichiers d'origine, vous devez d'abord les supprimer.

Deux SPN sont requis pour l'authentification Kerberos :

```
HOST/alias
HOST/alias.domain
```

Si l'alias est le cas`finance.domain.com`, les deux SPN requis sont les suivants :

```
HOST/finance
HOST/finance.domain.com
```

> **Note**
>
> Vous devez supprimer tous les SPN HOST existants correspondant à l'alias DNS sur l'objet informatique Active Directory avant de créer de nouveaux SPN HOST pour l'objet informatique Active Directory (AD) de votre système de fichiers Amazon FSx. Les tentatives

de définition de SPN pour votre système de fichiers Amazon FSx échoueront si un SPN pour l'alias DNS existe dans l'AD.

Les procédures suivantes décrivent comment effectuer les opérations suivantes :

- Recherchez tous les noms SPN d'alias DNS existants sur l'objet informatique Active Directory du système de fichiers d'origine.
- Supprimez les SPN existants trouvés, le cas échéant.
- Créez de nouveaux alias DNS SPN pour l'objet informatique Active Directory de votre système de fichiers Amazon FSx.

Pour installer le module PowerShell Active Directory requis

1. Connectez-vous à une instance Windows jointe à l'Active Directory auquel votre système de fichiers Amazon FSx est joint.
2. Ouvrez PowerShell en tant qu'administrateur.
3. Installez le module PowerShell Active Directory à l'aide de la commande suivante.

```
Install-WindowsFeature RSAT-AD-PowerShell
```

Pour rechercher et supprimer des alias DNS SPN existants sur l'objet informatique Active Directory du système de fichiers d'origine

1. Trouvez tous les SPN existants à l'aide des commandes suivantes. *alias_fqdn*Remplacez-le par l'alias DNS que vous avez associé au système de fichiers à l'étape 1.

```
## Find SPNs for original file system's AD computer object
$ALIAS = "alias_fqdn"
SetSPN /Q ("HOST/" + $ALIAS)
SetSPN /Q ("HOST/" + $ALIAS.Split(".")[0])
```

2. Supprimez les SPN HOST existants renvoyés à l'étape précédente à l'aide de l'exemple de script suivant.

   - *alias_fqdn*Remplacez-le par l'alias DNS complet que vous avez associé au système de fichiers à l'étape 1.

- *file_system_DNS_name*Remplacez-le par le nom DNS du système de fichiers d'origine.

```
## Delete SPNs for original file system's AD computer object
$Alias = "alias_fqdn"
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})

SetSPN /D ("HOST/" + ${Alias}) ${FSxAdComputer}.Name
SetSPN /D ("HOST/" + ${Alias}.Split(".")[0]) ${FSxAdComputer}.Name
```

3. Répétez les étapes précédentes pour chaque alias DNS que vous avez associé au système de fichiers à l'étape 1.

Pour définir des SPN sur l'objet informatique Active Directory de votre système de fichiers Amazon FSx

1. Définissez de nouveaux SPN pour votre système de fichiers Amazon FSx en exécutant les commandes suivantes.

   - *file_system_DNS_name*Remplacez-le par le nom DNS attribué par Amazon FSx au système de fichiers.

     Pour trouver le nom DNS de votre système de fichiers sur la console Amazon FSx, choisissez Systèmes de fichiers, choisissez votre système de fichiers, puis choisissez le volet Réseau et sécurité sur la page de détails du système de fichiers.

     Vous pouvez également obtenir le nom DNS dans la réponse à l'opération de l'API DescribeFileSystems.

   - *alias_fqdn*Remplacez-le par l'alias DNS complet que vous avez associé au système de fichiers à l'étape 1.

```
## Set SPNs for FSx file system AD computer object
$FSxDnsName = "file_system_DNS_name"
$Alias = "alias_fqdn"
$FileSystemHost = (Resolve-DnsName $FSxDnsName | Where Type -eq 'A')
[0].Name.Split(".")[0]
```

```
$FSxAdComputer = (Get-AdComputer -Identity $FileSystemHost)

##Use one of the following commands, not both:
Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-
AdditionalDnsHostname"="$Alias"}
##Or
SetSpn /S ("HOST/" + $Alias.Split('.')[0]) $FSxAdComputer.Name
SetSpn /S ("HOST/" + $Alias) $FSxAdComputer.Name
```

> **Note**
>
> La définition d'un SPN pour votre système de fichiers Amazon FSx échouera si un SPN pour l'alias DNS existe dans l'AD pour l'objet informatique du système de fichiers d'origine. Pour plus d'informations sur la recherche et la suppression de SPN existants, consultezPour rechercher et supprimer des alias DNS SPN existants sur l'objet informatique Active Directory du système de fichiers d'origine.

2. Vérifiez que les nouveaux SPN sont configurés pour l'alias DNS à l'aide de l'exemple de script suivant. Assurez-vous que la réponse inclut deux SPN HOST `HOST/`*`alias`* et`HOST/`*`alias_fqdn`*, comme décrit précédemment dans cette procédure.

   *`file_system_DNS_name`*Remplacez-le par le nom DNS attribué par Amazon FSx à votre système de fichiers. Pour trouver le nom DNS de votre système de fichiers sur la console Amazon FSx, choisissez Systèmes de fichiers, choisissez votre système de fichiers, puis choisissez le volet Réseau et sécurité sur la page de détails du système de fichiers.

   Vous pouvez également obtenir le nom DNS dans la réponse à l'opération de l'API DescribeFileSystems.

   ```
   ## Verify SPNs on FSx file system AD computer object
   $FileSystemDnsName = "file_system_dns_name"
   $FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
   [0].Name.Split(".")[0]
   $FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})
   SetSpn /L ${FSxAdComputer}.Name
   ```

3. Répétez les étapes précédentes pour chaque alias DNS que vous avez associé au système de fichiers à l'étape 1.

Pour plus d'informations sur la manière d'obliger les clients à utiliser l'authentification et le chiffrement Kerberos lors de la connexion à votre système de fichiers Amazon FSx, consultez. Application de l'authentification Kerberos à l'aide de GPO

Étape 3 : Mettre à jour ou créer un enregistrement DNS CNAME pour le système de fichiers

Après avoir correctement configuré les SPN pour votre système de fichiers, vous pouvez passer à Amazon FSx en remplaçant chaque enregistrement DNS résolu dans le système de fichiers d'origine par un enregistrement DNS correspondant au nom DNS par défaut du système de fichiers Amazon FSx.

Les modules `dnsserver` et `activedirectory` Windows sont nécessaires pour exécuter les commandes présentées dans cette section.

Pour installer les applets de commande requis PowerShell

1. Connectez-vous à une instance Windows jointe à l'Active Directory à laquelle votre système de fichiers Amazon FSx est joint en tant qu'utilisateur membre d'un groupe disposant d'autorisations d'administration DNS (administrateurs de systèmes de noms de domaine AWSAWS délégués dans AWS Managed Active Directory, administrateurs de domaine ou autre groupe auquel vous avez délégué des autorisations d'administration DNS dans votre Active Directory autogéré).

   Pour plus d'informations, consultez la section Connexion à votre instance Windows dans le guide de l'utilisateur Amazon EC2.
2. Ouvrez PowerShell en tant qu'administrateur.
3. Le module PowerShell DNS Server est nécessaire pour exécuter les instructions de cette procédure. Installez-le à l'aide de la commande suivante.

   ```
   Install-WindowsFeature RSAT-DNS-Server
   ```

Pour mettre à jour ou créer un nom DNS personnalisé pour votre système de fichiers Amazon FSx

1. Connectez-vous à votre instance Amazon EC2 en tant qu'utilisateur membre d'un groupe disposant d'autorisations d'administration DNS (administrateurs de systèmes de noms de domaine AWS délégués dans AWS Managed Active Directory, administrateurs de domaines ou

autre groupe auquel vous avez délégué des autorisations d'administration DNS dans votre Active Directory autogéré).

Pour plus d'informations, consultez la section Connexion à votre instance Windows dans le guide de l'utilisateur Amazon EC2.

2. À l'invite de commande, exécutez le script suivant. Ce script migre tous les enregistrements DNS CNAME existants vers votre système de fichiers Amazon FSx. Si aucun n'est trouvé, il crée un nouvel enregistrement DNS CNAME pour l'alias DNS *alias_fqdn* qui correspond au nom DNS par défaut de votre système de fichiers Amazon FSx.

   Pour exécuter le script :

   - *alias_fqdn*Remplacez-le par l'alias DNS que vous avez associé au système de fichiers.
   - Remplacez *file_system_DNS_name* par le nom DNS qu'Amazon FSx a attribué au système de fichiers.

```
$Alias="alias_fqdn"
$FSxDnsName="file_system_dns_name"
$AliasHost=$Alias.Split('.')[0]
$ZoneName=((Get-WmiObject Win32_ComputerSystem).Domain)
$DnsServerComputerName = (Resolve-DnsName $ZoneName -Type NS | Where Type -eq 'A' |
 Select -ExpandProperty Name) | Select -First 1
foreach ($computer in $DnsServerComputerName)
{
Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName $computer -
HostNameAlias $FSxDnsName -ZoneName $ZoneName
}
```

3. Répétez l'étape précédente pour chaque alias DNS que vous avez associé au système de fichiers à l'étape 1.

Vous avez maintenant ajouté une valeur DNS CNAME pour votre système de fichiers Amazon FSx avec l'alias DNS. Vous pouvez désormais utiliser l'alias DNS pour accéder à vos données.

> **Note**
>
> Lors de la mise à jour d'un enregistrement DNS CNAME pour qu'il pointe vers un système de fichiers Amazon FSx précédemment pointé vers un autre système de fichiers, les clients peuvent ne pas être en mesure de se connecter au système de fichiers pendant une courte

période. Lorsque le cache DNS du client est actualisé, il doit pouvoir se connecter à l'aide de l'alias DNS. Pour plus d'informations, consultez Impossible d'accéder au système de fichiers à l'aide d'un alias DNS.

Application de l'authentification Kerberos à l'aide de GPO

Vous pouvez appliquer l'authentification Kerberos lors de l'accès au système de fichiers en définissant les objets de stratégie de groupe (GPO) suivants dans votre Active Directory :

- Restreindre le NTLM : trafic NTLM sortant vers des serveurs distants - Utilisez ce paramètre de stratégie pour refuser ou auditer le trafic NTLM sortant d'un ordinateur vers un serveur distant exécutant le système d'exploitation Windows.
- Restreindre le protocole NTLM : ajoutez des exceptions de serveur distant pour l'authentification NTLM - Utilisez ce paramètre de stratégie pour créer une liste d'exceptions des serveurs distants sur lesquels les appareils clients sont autorisés à utiliser l'authentification NTLM si le paramètre de stratégie Sécurité du réseau : restreindre le trafic NTLM : trafic NTLM sortant vers les serveurs distants est configuré.

1. Connectez-vous à une instance Windows jointe à l'Active Directory auquel votre système de fichiers Amazon FSx est joint en tant qu'administrateur. Si vous configurez un Active Directory autogéré, appliquez ces étapes directement à votre Active Directory.
2. Choisissez Démarrer, Outils d'administration, puis Gestion des politiques de groupe.
3. Choisissez Group Policy Objects.
4. Si votre objet de stratégie de groupe n'existe pas déjà, créez-le.
5. Localisez la sécurité réseau existante : Restreindre le protocole NTLM : politique relative au trafic NTLM sortant vers les serveurs distants. (S'il n'existe aucune stratégie, créez-en une nouvelle.) Dans l'onglet Paramètres de sécurité locaux, ouvrez le menu contextuel (clic droit) et choisissez Propriétés.
6. Choisissez Refuser tout.
7. Choisissez Appliquer pour enregistrer le paramètre de sécurité.
8. Pour définir des exceptions pour les connexions NTLM à des serveurs distants spécifiques pour le client, recherchez le lien Sécurité du réseau : Restreindre le protocole NTLM : ajouter des exceptions de serveur distant.

Ouvrez le menu contextuel (clic droit) et choisissez Propriétés dans l'onglet Paramètres de sécurité locaux.

9. Entrez le nom des serveurs à ajouter à la liste d'exceptions.
10. Choisissez Appliquer pour enregistrer le paramètre de sécurité.

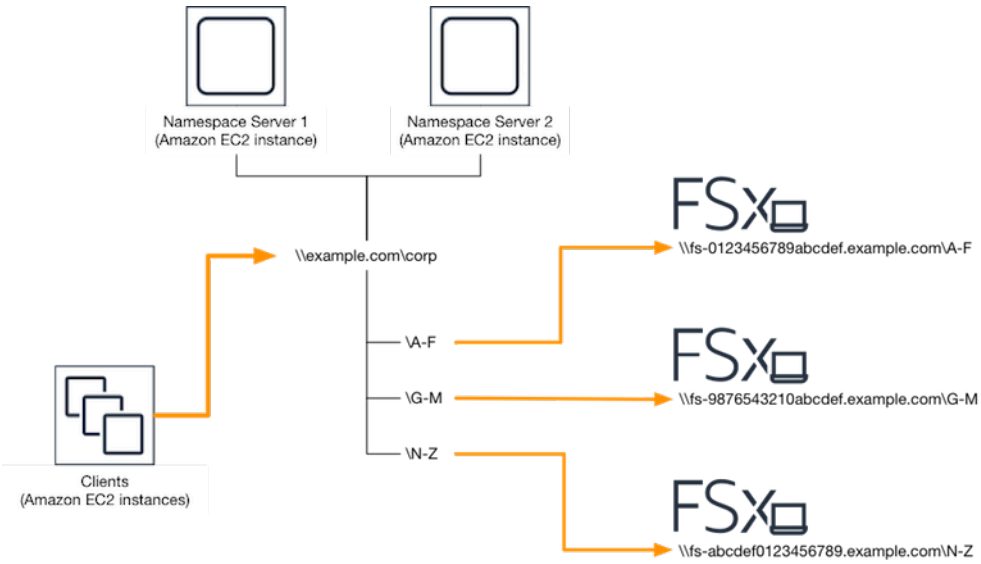
Procédure pas à pas 6 : augmenter les performances grâce aux shards

Amazon FSx for Windows File Server prend en charge l'utilisation du système de fichiers distribué Microsoft (DFS). En utilisant les espaces de noms DFS, vous pouvez augmenter les performances (en lecture et en écriture) pour répondre aux charges de travail intensives en termes d'E/S en répartissant les données de vos fichiers sur plusieurs systèmes de fichiers Amazon FSx. Dans le même temps, vous pouvez toujours présenter une vue unifiée sous un espace de noms commun à vos applications. Cette solution consiste à diviser les données de vos fichiers en ensembles de données ou fragments plus petits et à les stocker dans différents systèmes de fichiers. Les applications accédant à vos données à partir de plusieurs instances peuvent atteindre des niveaux de performance élevés en lisant et en écrivant sur ces partitions en parallèle.

Vous pouvez utiliser cette solution lorsque votre charge de travail nécessite un accès en lecture/écriture uniformément réparti aux données de vos fichiers (par exemple, si chaque sous-ensemble d'instances de calcul accède à une partie différente de vos données de fichier).

Configuration des espaces de noms DFS pour des performances évolutives

La procédure suivante vous guide tout au long de la création d'une solution DFS sur Amazon FSx pour des performances évolutives. Dans cet exemple, les données stockées dans l'espace de noms de l'*`entreprise`* sont découpées par ordre alphabétique. Les fichiers de données « A-F », « G-M » et « N-Z » sont tous stockés sur des partages de fichiers différents. En fonction du type de données, de la taille des E/S et du modèle d'accès aux E/S, vous devez décider de la meilleure façon de partager vos données sur plusieurs partages de fichiers. Choisissez une convention de partitionnement qui répartit les E/S de manière uniforme sur tous les partages de fichiers que vous prévoyez d'utiliser. N'oubliez pas que chaque espace de noms prend en charge jusqu'à 50 000 partages de fichiers et des centaines de pétaoctets de capacité de stockage au total.



Pour configurer les espaces de noms DFS pour des performances évolutives

1. Si aucun serveur d'espace de noms DFS n'est déjà actif, vous pouvez lancer deux serveurs d'espaces de noms DFS à haut niveau de disponibilité à l'aide du modèle Setup-DFSN-Servers.template. AWS CloudFormation 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.
2. Connectez-vous à l'un des serveurs d'espace de noms DFS lancés à l'étape précédente en tant qu'utilisateur du groupe Administrateurs AWS délégués. Pour plus d'informations, consultez la section Connexion à votre instance Windows dans le guide de l'utilisateur Amazon EC2.
3. Accédez à la console de gestion DFS. Ouvrez le menu Démarrer et exécutez dfsmgmt.msc. Cela ouvre l'outil d'interface graphique de gestion DFS.
4. Choisissez Action puis Nouvel espace de noms, saisissez le nom d'ordinateur du premier serveur d'espace de noms DFS que vous avez lancé pour Server et choisissez Next.
5. Dans Nom, saisissez l'espace de noms que vous créez (par exemple, corp).
6. Choisissez Modifier les paramètres et définissez les autorisations appropriées en fonction de vos besoins. Choisissez Suivant.
7. Laissez l'option d'espace de noms par défaut basée sur le domaine sélectionnée, laissez l'option Activer le mode Windows Server 2008 sélectionnée, puis choisissez Next.

> **Note**
>
> Le mode Windows Server 2008 est la dernière option disponible pour les espaces de noms.

8. Vérifiez les paramètres de l'espace de noms et choisissez Create.
9. Le nouvel espace de noms étant sélectionné sous Espaces de noms dans la barre de navigation, choisissez Action puis Ajouter un serveur d'espace de noms.
10. Entrez le nom d'ordinateur du deuxième serveur d'espace de noms DFS que vous avez lancé pour le serveur d'espace de noms.
11. Choisissez Modifier les paramètres, définissez les autorisations appropriées en fonction de vos besoins, puis cliquez sur OK.
12. Ouvrez le menu contextuel (clic droit) de l'espace de noms que vous venez de créer, choisissez Nouveau dossier, entrez le nom du dossier pour la première partition (par exemple, **`A-F`** pour Nom), puis choisissez Ajouter.
13. Tapez le nom DNS du partage de fichiers hébergeant cette partition au format UNC (par exemple,**`\\fs-0123456789abcdef0.example.com\A-F`**) pour Path to folder target et cliquez sur OK.
14. Si le partage n'existe pas :
    a. Choisissez Oui pour le créer.
    b. Dans la boîte de dialogue Créer un partage, choisissez Parcourir.
    c. Choisissez un dossier existant ou créez-en un nouveau sous D$, puis cliquez sur OK.
    d. Définissez les autorisations de partage appropriées, puis cliquez sur OK.
15. La cible du dossier étant désormais ajoutée pour la partition, cliquez sur OK.
16. Répétez les quatre dernières étapes pour les autres partitions que vous souhaitez ajouter au même espace de noms.

Procédure 7 : Copie d'une sauvegarde vers une autreRégion AWS

Avec Amazon FSx, vous pouvez copier une sauvegarde existante au sein de celle-ciCompte AWSà un autreRégion AWS(copie de sauvegarde entre régions) ou sur la mêmeRégion AWS(copie de sauvegarde dans la région).

La procédure suivante vous guide à travers le processus de création d'une copie d'une sauvegarde à l'intérieur de celle-ci.Compte AWS. Avant de pouvoir créer cette copie de sauvegarde, vous devez disposer d'une sauvegarde existante. Pour plus d'informations, consultez Utilisation des sauvegardes.

Pour copier une sauvegarde existante à l'intérieur de la mêmeCompte AWS(entre régions ou en région)

1. Ouvrez la console Amazon FSx à l'adressehttps://console.aws.amazon.com/fsx/.
2. Dans le volet de navigation, choisissez Sauvegardes.
3. DansSauvegardes, choisissez la sauvegarde que vous voulez copier.
4. Choisissez Copier la sauvegarde. Ce faisant, ouvre leCopie de sauvegardeAssistant.
5. DansRégion de destination, choisissez une destinationRégion AWSpour copier la sauvegarde sur. La destination peut être dans un autreRégion AWSou au sein de la mêmeRégion AWS.
6. (Facultatif) SélectionnezCopie d'étiquettespour copier des balises de la sauvegarde source vers la sauvegarde de destination. Si vous sélectionnezCopie d'étiquetteset ajoutez également des balises à l'étape 8, toutes les balises sont fusionnées.
7. PourChiffrement, choisissez leAWS KMSclé de chiffrement pour chiffrer la sauvegarde copiée.
8. PourBalises - facultatif, saisissez une clé et une valeur pour ajouter des balises à votre sauvegarde copiée. Si vous ajoutez des balises ici et que vous avez également sélectionnéCopie d'étiquettesà l'étape 6, toutes les balises sont fusionnées.
9. Choisissez Copier la sauvegarde.

Vous avez maintenant copié avec succès une sauvegarde dans la mêmeCompte AWSà un autreRégion AWSou au sein de la mêmeRégion AWS.

Sécurité dans Amazon FSx

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture 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 cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le cloud Amazon Web Services. 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 conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon FSx for Windows File Server, AWS consultez la section Services concernés par programme de conformité.
- 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 for Windows File Server. Les rubriques suivantes expliquent comment configurer Amazon FSx pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser les ressources de votre serveur de fichiers Amazon FSx for Windows.

Rubriques

Chiffrement des données dans Amazon FSx

Amazon FSx for Windows File Server prend en charge deux formes de chiffrement pour les systèmes de fichiers : le chiffrement des données en transit et le chiffrement au repos. Le chiffrement des données en transit est pris en charge sur les partages de fichiers mappés sur une instance de calcul compatible avec le protocole SMB 3.0 ou une version ultérieure. Le chiffrement des données au repos est automatiquement activé lors de la création d'un système de fichiers Amazon FSx. Amazon FSx 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.

Quand utiliser le chiffrement ?

Si votre organisation est soumise à des politiques d'entreprise ou des réglementations nécessitant le chiffrement des données et des métadonnées au repos, nous vous recommandons de créer un système de fichiers chiffré en montant votre système de fichiers à l'aide du chiffrement des données en transit.

Pour plus d'informations sur le chiffrement avec Amazon FSx for Windows File Server, consultez les rubriques connexes suivantes :

- Créez votre système de fichiers Amazon FSx for Windows File Server
- Actions, ressources et clés de condition pour Amazon FSx dans le guide de l'utilisateur IAM

Rubriques

Chiffrement au repos

Tous les systèmes de fichiers Amazon FSx sont chiffrés au repos avec des 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. Ces processus sont gérés de manière transparente par Amazon FSx, de sorte que vous n'avez pas à modifier vos applications.

Amazon FSx utilise un algorithme de chiffrement AES-256 conforme aux normes du secteur pour chiffrer les données et métadonnées Amazon FSx au repos. Pour de plus amples informations,

consultez Principes de base du chiffrement dans le Guide du développeur AWS Key Management Service .

> **Note**
>
> L'infrastructure de gestion des AWS clés utilise des algorithmes cryptographiques approuvés par les Federal Information Processing Standards (FIPS) 140-2. Cette infrastructure est conforme aux recommandations NIST (National Institute of Standards and Technology) 800-57.

Comment Amazon FSx utilise AWS KMS

Amazon FSx s'intègre à la gestion AWS KMS des clés. Amazon FSx utilise un AWS KMS key pour chiffrer votre système de fichiers. Vous choisissez la clé KMS utilisée pour chiffrer et déchiffrer les systèmes de fichiers (données et métadonnées). Vous pouvez activer, désactiver ou révoquer les autorisations sur cette clé KMS. Cette clé KMS peut être de l'un des deux types suivants :

- Clé gérée par AWS— Il s'agit de la clé KMS par défaut, dont l'utilisation est gratuite.
- Clé gérée par le client – Il s’agit de la clé KMS la plus souple à utiliser, car vous pouvez configurer ses stratégies de clé et ses octrois pour plusieurs utilisateurs ou services. Pour plus d'informations sur la création de clés gérées par le client, consultez la section Création de clés dans le guide du AWS Key Management Service développeur.

Si vous utilisez une clé 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 gérée par le client, vous pouvez choisir à tout moment à quel moment désactiver, réactiver, supprimer ou révoquer l'accès à votre clé KMS. Pour plus d'informations, consultez Rotating AWS KMS keys dans le guide du AWS Key Management Service développeur.

Le chiffrement et le déchiffrement du système de fichiers au repos sont gérés de manière transparente. Cependant, Compte AWS les identifiants spécifiques à Amazon FSx apparaissent dans vos AWS CloudTrail journaux relatifs aux AWS KMS actions.

Politiques clés d'Amazon FSx pour AWS KMS

Les politiques de clé constituent le principal moyen de contrôler l'accès aux clés KMS. Pour plus d'informations sur les politiques clés, consultez la section Utilisation des politiques clés AWS KMS dans le Guide du AWS Key Management Service développeur.La liste suivante décrit toutes les autorisations AWS KMS associées prises en charge par Amazon FSx pour les systèmes de fichiers chiffrés au repos :

- kms:Encrypt - (Facultatif) Chiffre le texte brut en texte chiffré. Cette autorisation est incluse dans la stratégie de clé par défaut.
- kms:Decrypt - (Obligatoire) Déchiffre le texte chiffré. Le texte chiffré est du texte brut qui a été précédemment chiffré. Cette autorisation est incluse dans la stratégie de clé par défaut.
- kms : ReEncrypt — (Facultatif) Chiffre les données côté serveur avec une nouvelle clé KMS, sans exposer le texte clair des données côté client. Les données sont d'abord déchiffrées, puis chiffrées à nouveau. Cette autorisation est incluse dans la stratégie de clé par défaut.
- kms : GenerateData KeyWithout Plaintext — (Obligatoire) Renvoie une clé de chiffrement des données chiffrée sous une clé KMS. Cette autorisation est incluse dans la politique de clé par défaut sous kms : GenerateData Key*.
- kms : CreateGrant — (Obligatoire) Ajoute une autorisation à une clé pour spécifier qui peut utiliser la clé et dans quelles conditions. Les octrois sont des mécanismes d'autorisation alternatifs aux stratégies de clé. Pour plus d'informations sur les subventions, consultez la section Utilisation des subventions dans le Guide du AWS Key Management Service développeur. Cette autorisation est incluse dans la stratégie de clé par défaut.
- kms : DescribeKey — (Obligatoire) Fournit des informations détaillées sur la clé KMS spécifiée. Cette autorisation est incluse dans la stratégie de clé par défaut.
- kms : ListAliases — (Facultatif) Répertorie tous les alias clés du compte. Lorsque vous utilisez la console pour créer un système de fichiers chiffré, cette autorisation alimente la liste des clés KMS. Nous vous recommandons d'utiliser cette autorisation pour offrir un confort d'utilisation maximal. Cette autorisation est incluse dans la stratégie de clé par défaut.

Chiffrement en transit

Le chiffrement des données en transit est pris en charge sur les partages de fichiers mappés sur une instance de calcul compatible avec le protocole SMB 3.0 ou une version ultérieure. Cela inclut toutes les versions de Windows à partir de Windows Server 2012 et Windows 8, ainsi que tous les clients Linux dotés du client Samba version 4.2 ou ultérieure. Amazon FSx for Windows File Server 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.

Le chiffrement SMB utilise l'algorithme AES-128-GCM ou AES-128-CCM (la variante GCM étant choisie si le client prend en charge SMB 3.1.1) comme algorithme de chiffrement, et assure également l'intégrité des données lors de la signature à l'aide des clés de session Kerberos SMB. L'utilisation de l'AES-128-GCM améliore les performances, par exemple en multipliant par deux les performances lors de la copie de fichiers volumineux via des connexions SMB cryptées.

Pour répondre aux exigences de conformité relatives au chiffrement permanent data-in-transit, vous pouvez limiter l'accès au système de fichiers afin de n'autoriser l'accès qu'aux clients qui prennent en charge le chiffrement des PME. Vous pouvez également activer ou désactiver le chiffrement en transit par partage de fichiers ou pour l'ensemble du système de fichiers. Cela vous permet d'avoir un mélange de partages de fichiers chiffrés et non chiffrés sur le même système de fichiers. Pour en savoir plus encryption-in-transit sur la gestion de votre système de fichiers, consultezGestion du chiffrement en transit.

Contrôle d'accès au niveau des fichiers et des dossiers à l'aide des ACL Windows

Amazon FSx for Windows File Server prend en charge l'authentification basée sur l'identité via le protocole SMB (Server Message Block) via Microsoft Active Directory. Active Directory est le service d'annuaire Microsoft permettant de stocker des informations sur les objets du réseau et de faciliter la recherche et l'utilisation de ces informations par les administrateurs et les utilisateurs. Ces objets incluent généralement des ressources partagées telles que des serveurs de fichiers, des comptes d'utilisateurs et d'ordinateurs du réseau. Pour en savoir plus sur la prise en charge d'Active Directory dans Amazon FSx, consultez. Utilisation de Microsoft Active Directory dans FSx for Windows File Server

Vos instances de calcul jointes à un domaine peuvent accéder aux partages de fichiers Amazon FSx à l'aide des informations d'identification Active Directory. Vous utilisez des listes de contrôle d'accès (ACL) Windows standard pour un contrôle d'accès précis au niveau des fichiers et des dossiers. Les systèmes de fichiers Amazon FSx vérifient automatiquement les informations d'identification des utilisateurs accédant aux données du système de fichiers afin de faire appliquer ces ACL Windows.

Chaque système de fichiers Amazon FSx est fourni avec un partage de fichiers Windows par défaut appelé. `share` Les ACL Windows pour ce dossier partagé sont configurées pour autoriser l'accès en lecture/écriture aux utilisateurs du domaine. Ils permettent également un contrôle total

du groupe d'administrateurs délégués de votre Active Directory qui est délégué pour effectuer des actions administratives sur vos systèmes de fichiers. Si vous intégrez votre système de fichiers à AWS Managed Microsoft AD, ce groupe est constitué d' AWS administrateurs FSx délégués. Si vous intégrez votre système de fichiers à votre configuration Microsoft AD autogérée, ce groupe peut être composé d'administrateurs de domaine. Il peut également s'agir d'un groupe d'administrateurs délégués personnalisé que vous avez spécifié lors de la création du système de fichiers. Pour modifier les ACL, vous pouvez mapper le partage en tant qu'utilisateur membre du groupe d'administrateurs délégués.

> **Warning**
>
> Amazon FSx exige que l'utilisateur du SYSTÈME dispose des autorisations ACL NTFS de contrôle total sur tous les dossiers de votre système de fichiers. Ne modifiez pas les autorisations ACL NTFS pour cet utilisateur sur vos dossiers. Cela peut rendre votre partage de fichiers inaccessible et empêcher les sauvegardes du système de fichiers d'être utilisables.

Liens connexes

- Qu'est-ce que AWS Directory Service ? dans le Guide AWS Directory Service d'administration.
- Créez votre répertoire Microsoft AD AWS géré dans le Guide AWS Directory Service d'administration.
- Quand créer une relation de confiance dans le guide AWS Directory Service d'administration.
- Procédure 1 : Conditions préalables à la prise en main.

Contrôle d'accès au système de fichiers avec Amazon VPC

Vous accédez à votre système de fichiers Amazon FSx via une interface elastic network. Cette interface réseau réside dans le cloud privé virtuel (VPC) basé sur le service Amazon Virtual Private Cloud (Amazon VPC) que vous associez à votre système de fichiers. Vous vous connectez à votre système de fichiers Amazon FSx via son nom de service de noms de domaine (DNS). Le nom DNS correspond à l'adresse IP privée de l'interface elastic network du système de fichiers dans votre VPC. Seules les ressources du VPC associé, les ressources connectées au VPC associé par AWS Direct Connect ou VPN, ou les ressources des VPC homologues peuvent accéder à l'interface réseau de

votre système de fichiers. 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.

FSx for Windows File Server prend en charge le partage VPC, qui vous permet de visualiser, de créer, de modifier et de supprimer des ressources dans un sous-réseau partagé d'un VPC appartenant à un autre compte. AWS Pour de plus amples informations, veuillez consulter Utilisation de VPC partagés dans le Amazon VPC Guide de l'utilisateur.

Groupes de sécurité Amazon VPC

Pour mieux contrôler le trafic réseau passant par les interfaces réseau élastiques de votre système de fichiers au sein de votre VPC, utilisez des groupes de sécurité pour limiter l'accès à vos systèmes de fichiers. Un groupe de sécurité est un pare-feu dynamique qui contrôle le trafic à destination et en provenance des interfaces réseau associées. Dans ce cas, la ressource associée est la ou les interfaces réseau de votre système de fichiers.

Pour utiliser un groupe de sécurité afin de contrôler l'accès à votre système de fichiers Amazon FSx, ajoutez des règles d'entrée et de sortie. Les règles entrantes contrôlent le trafic entrant, tandis que les règles sortantes contrôlent le trafic sortant de votre système de fichiers. Assurez-vous que vous disposez des bonnes règles de trafic réseau dans votre groupe de sécurité pour mapper le partage de fichiers de votre système de fichiers Amazon FSx à un dossier de votre instance de calcul prise en charge.

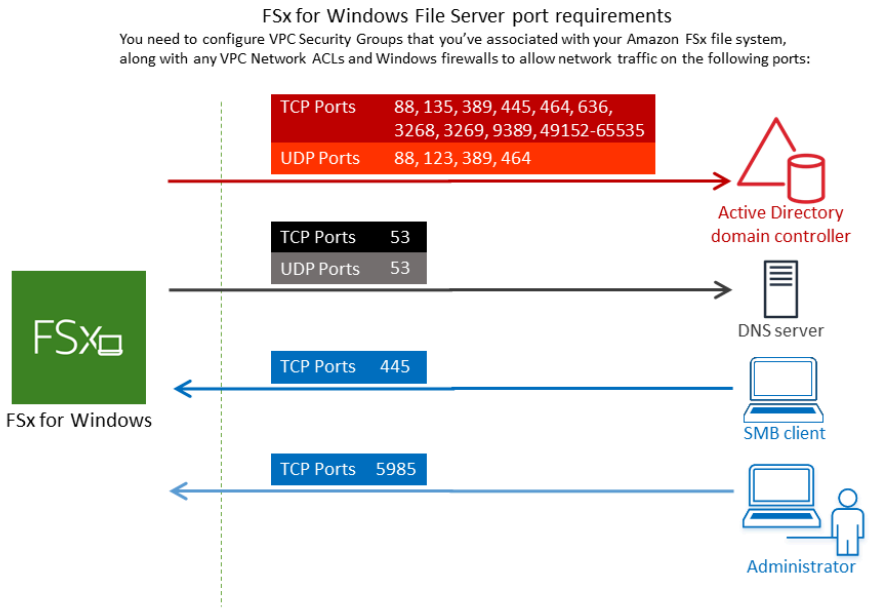
Pour plus d'informations sur les règles des groupes de sécurité, consultez la section Règles des groupes de sécurité dans le guide de l'utilisateur Amazon EC2.

Pour créer un groupe de sécurité pour Amazon FSx

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Sélectionnez Créer un groupe de sécurité.

4. Attribuez un nom et une description au groupe de sécurité.
5. Pour le VPC, choisissez l'Amazon VPC associé à votre système de fichiers pour créer le groupe de sécurité au sein de ce VPC.
6. Ajoutez les règles suivantes pour autoriser le trafic réseau sortant sur les ports suivants :

   a. Pour les groupes de sécurité VPC, le groupe de sécurité par défaut pour votre Amazon VPC par défaut est déjà ajouté à votre système de fichiers dans la console. Assurez-vous que le groupe de sécurité et les ACL du réseau VPC du ou des sous-réseaux sur lesquels vous créez votre système de fichiers FSx autorisent le trafic sur les ports et dans les directions indiquées dans le schéma suivant.



Le tableau suivant identifie le rôle de chaque port.

Protocole	Ports	Rôle
TCP/UDP	53	Système de nom de domaine (DNS)
TCP/UDP	88	Authentification Kerberos
TCP/UDP	464	Changement/définition de mot de passe

Protocole	Ports	Rôle
TCP/UDP	389	Protocole LDAP (Lightweight Directory Access Protocol)
UDP	123	Protocole NTP (Network Time Protocol)
TCP	135	Distributed Computing Environment / End Point Mapper (DCE / EPMAP)
TCP	445	Partage de fichiers SMB avec les services d'annuaire
TCP	636	Protocole LDAP (Lightweight Directory Access Protocol) via TLS/SSL (LDAPS)
TCP	3268	Catalogue mondial Microsoft
TCP	3269	Microsoft Global Catalog via SSL
TCP	5985	WinRM 2.0 (gestion à distance de Microsoft Windows)
TCP	9389	Services Web Microsoft AD DS, PowerShell
TCP	49152 - 65535	Ports éphémères pour RPC

> **Important**
>
> L'autorisation du trafic sortant sur le port TCP 9389 est requise pour les déploiements de systèmes de fichiers mono-AZ 2 et multi-AZ.

b. Assurez-vous que ces règles de trafic sont également reflétées sur les pare-feux qui s'appliquent à chacun des contrôleurs de domaine AD, des serveurs DNS, des clients FSx et des administrateurs FSx.

> **Important**
>
> Alors que les groupes de sécurité Amazon VPC nécessitent que les ports soient ouverts uniquement dans le sens où le trafic réseau est initié, la plupart des pare-feux Windows et des ACL de réseau VPC nécessitent que les ports soient ouverts dans les deux sens.

> **Note**
>
> Si vous avez défini des sites Active Directory, vous devez vous assurer que le ou les sous-réseaux du VPC associé à votre système de fichiers Amazon FSx sont définis dans un site Active Directory et qu'aucun conflit n'existe entre le ou les sous-réseaux de votre VPC et ceux de vos autres sites. Vous pouvez afficher et modifier ces paramètres à l'aide du composant logiciel enfichable MMC Active Directory Sites and Services.

> **Note**
>
> Dans certains cas, vous avez peut-être modifié les règles de votre groupe de AWS Managed Microsoft AD sécurité par rapport aux paramètres par défaut. Si tel est le cas, assurez-vous que ce groupe de sécurité dispose des règles entrantes requises pour autoriser le trafic provenant de votre système de fichiers Amazon FSx. Pour plus d'informations sur les règles de trafic entrant requises, consultez la section AWS Managed Microsoft AD Conditions préalables du Guide d'AWS Directory Service administration.

Maintenant que vous avez créé votre groupe de sécurité, vous pouvez l'associer aux interfaces Elastic Network de votre système de fichiers Amazon FSx.

Pour associer un groupe de sécurité à votre système de fichiers Amazon FSx

1. Ouvrez la console Amazon FSx à l'adresse https://console.aws.amazon.com/fsx/.
2. Sur le tableau de bord, choisissez votre système de fichiers pour en afficher les détails.

3. Choisissez l'onglet Réseau et sécurité, puis choisissez les interfaces réseau de votre système de fichiers ; par exemple, ENI-01234567890123456. Pour les systèmes de fichiers mono-AZ, vous verrez une interface réseau unique. Pour les systèmes de fichiers multi-AZ, vous verrez une interface réseau dans le sous-réseau Preferred et une autre dans le sous-réseau Standby.
4. Pour chaque interface réseau, choisissez l'interface réseau et dans Actions, choisissez Modifier les groupes de sécurité.
5. Dans la boîte de dialogue Modifier les groupes de sécurité, choisissez les groupes de sécurité à utiliser, puis cliquez sur Enregistrer.

Interdire l'accès à un système de fichiers

Pour interdire temporairement à tous les clients l'accès réseau à votre système de fichiers, vous pouvez supprimer tous les groupes de sécurité associés aux interfaces Elastic Network de votre système de fichiers et les remplacer par un groupe dépourvu de règles entrantes/sortantes.

ACL du réseau Amazon VPC

Une autre option pour sécuriser l'accès au système de fichiers au sein de votre VPC consiste à établir des listes de contrôle d'accès réseau (ACL réseau). Les ACL réseau sont distinctes des groupes de sécurité, mais possèdent des fonctionnalités similaires pour ajouter une couche de sécurité supplémentaire aux ressources de votre VPC. Pour plus d'informations sur les ACL réseau, consultez la section ACL réseau dans le guide de l'utilisateur Amazon VPC.

Identity and Access Management pour Amazon FSx for Windows File Server

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

- Gestion des accès à l’aide de politiques
- Comment fonctionne Amazon FSx for Windows File Server avec IAM
- Exemples de politiques basées sur l'identité pour Amazon FSx for Windows File Server
- AWS politiques gérées pour Amazon FSx
- Résolution des problèmes d'identité et d'accès au serveur de fichiers Amazon FSx for Windows
- Utilisation de balises avec Amazon FSx
- Utilisation de rôles liés à un service pour Amazon FSx

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Amazon FSx.

Utilisateur du service : si vous utilisez le service Amazon FSx pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités d'Amazon FSx pour effectuer votre travail, il se peut que vous ayez besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans Amazon FSx, consultez. Résolution des problèmes d'identité et d'accès au serveur de fichiers Amazon FSx for Windows

Administrateur du service — Si vous êtes responsable des ressources Amazon FSx au sein de votre entreprise, vous avez probablement un accès complet à Amazon FSx. C'est à vous de déterminer les fonctionnalités et les ressources d'Amazon FSx auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d’IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec Amazon FSx, consultez. Comment fonctionne Amazon FSx for Windows File Server avec IAM

Administrateur IAM — Si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Amazon FSx. Pour consulter des exemples de politiques basées sur l'identité Amazon FSx que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité pour Amazon FSx for Windows File Server

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 Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, veuillez consulter Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser

l'utilisateur root pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur root et utilisez-les pour effectuer les tâches que seul l'utilisateur root peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez la section Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification du Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations

pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez la section 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, veuillez consulter la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, une fonction 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, l'action que vous effectuez est susceptible de lancer une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Fonction du service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez la section Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Présentation 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 relatives à 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 la section Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs

utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez la section Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Présentation des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonction 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 qui en résultent représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctions d'une organisation, vous pouvez appliquer les politiques de contrôle de service (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de la séance obtenue 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 remplace 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 obtenues 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 fonctionne Amazon FSx for Windows File Server 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 for Windows File Server

Fonctionnalité IAM	Support FSx
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACL	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d'identification temporaires	Oui
Transférer les sessions d'accès	Oui
Fonctions de service	Non
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont FSx et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour FSx

Prend en charge les politiques basées sur une 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 la section Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour FSx

Pour consulter des exemples de politiques basées sur l'identité Amazon FSx, consultez. Exemples de politiques basées sur l'identité pour Amazon FSx for Windows File Server

Politiques basées sur les ressources au sein de FSx

Prend en charge les politiques basées sur une ressource	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment Amazon S3. 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

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources

accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez Différence entre les rôles IAM et les politiques basées sur une ressource dans le Guide de l'utilisateur IAM.

Actions stratégiques pour FSx

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions FSx, consultez la section Actions définies par Amazon FSx for Windows File Server dans le Service Authorization Reference.

Les actions de stratégie dans FSx utilisent le préfixe suivant avant l'action :

```
fsx
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "fsx:action1",
      "fsx:action2"
         ]
```

Pour consulter des exemples de politiques basées sur l'identité Amazon FSx, consultez. Exemples de politiques basées sur l'identité pour Amazon FSx for Windows File Server

Ressources relatives aux politiques pour 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 pour lesquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources FSx et de leurs ARN, consultez la section Ressources définies par Amazon FSx for Windows File Server dans le Service Authorization Reference. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Amazon FSx for Windows File Server.

Pour consulter des exemples de politiques basées sur l'identité Amazon FSx, consultez. Exemples de politiques basées sur l'identité pour Amazon FSx for Windows File Server

Clés de conditions de politique pour FSx

Prise en charge des clés de condition de stratégie spécifiques au service	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition FSx, consultez la section Clés de condition pour Amazon FSx for Windows File Server dans le Service Authorization Reference. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par Amazon FSx for Windows File Server.

Pour consulter des exemples de politiques basées sur l'identité Amazon FSx, consultez. Exemples de politiques basées sur l'identité pour Amazon FSx for Windows File Server

ACL dans FSx

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux

politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec FSx

Prend en charge ABAC (étiquettes dans les politiques)	Oui

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès basé sur les attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec FSx

Prend en charge les informations d'identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Transférer les sessions d'accès pour 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, l'action que vous effectuez est susceptible de lancer 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 FSx

Prend en charge les fonctions de service	Non

Une fonction du service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations pour un rôle de service peut interrompre les fonctionnalités de FSx. Modifiez les rôles de service uniquement lorsque FSx fournit des instructions à cet effet.

Rôles liés à un service pour FSx

Prend en charge les rôles liés à un service.	Oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés aux services Amazon FSx, consultez. Utilisation de rôles liés à un service pour Amazon FSx

Exemples de politiques basées sur l'identité pour Amazon FSx for Windows File Server

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources Amazon FSx. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par FSx, y compris le format des ARN pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour Amazon FSx for Windows File Server dans le Service Authorization Reference.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console FSx
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources Amazon FSx dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour de plus amples informations, consultez Politiques gérées AWS ou Politiques gérées AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder des autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, n'accordez que les autorisations nécessaires à l'exécution de la tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez Politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour de plus amples informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour de plus amples informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console FSx

Pour accéder à la console Amazon FSx for Windows File Server, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux ressources Amazon FSx présentes dans votre. Compte AWS Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console FSx, attachez également la politique `AmazonFSxConsoleReadOnlyAccess` AWS gérée par FSx aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

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": "*"
        }
    ]
}
```

AWS politiques gérées pour Amazon FSx

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation

courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle 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 F SxServiceRolePolicy

Permet à Amazon FSx de gérer les AWS ressources en votre nom. Pour en savoir plus, veuillez consulter Utilisation de rôles liés à un service pour Amazon FSx.

AWS politique gérée : AmazonF SxDeleteServiceLinkedRoleAccess

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 à Amazon FSx de supprimer son rôle lié au service pour l'accès à Amazon S3, utilisé uniquement par Amazon FSx for Lustre.

Détails des autorisations

Cette politique inclut des autorisations permettant `iam` à Amazon FSx d'afficher, de supprimer et de visualiser l'état de suppression des rôles liés au service FSx pour l'accès à Amazon S3.

Pour consulter les autorisations associées à cette politique, consultez AmazonF SxDeleteServiceLinkedRoleAccess dans le Guide de référence des politiques AWS gérées.

AWS politique gérée : AmazonF SxFullAccess

Vous pouvez associer AmazonF SxFullAccess à vos entités IAM. Amazon FSx associe également cette politique à un rôle de service qui permet à Amazon FSx d'effectuer des actions en votre nom.

Fournit un accès complet à Amazon FSx et aux services associés AWS .

Détails des autorisations

Cette politique inclut les autorisations suivantes.

- `fsx`— Permet aux principaux un accès complet pour effectuer toutes les actions Amazon FSx, à l'exception de. `BypassSnaplockEnterpriseRetention`
- `ds`— Permet aux directeurs d'accéder aux informations relatives aux AWS Directory Service annuaires.
- `ec2`
  - Permet aux principaux de créer des balises dans les conditions spécifiées.
  - Fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.
- `iam`— Permet aux principes de créer un rôle lié au service Amazon FSx au nom de l'utilisateur. Cela est nécessaire pour qu'Amazon FSx puisse gérer les AWS ressources au nom de l'utilisateur.
- `logs`— Permet aux principaux de créer des groupes de journaux, des flux de journaux et d'écrire des événements dans des flux de journaux. Cela est nécessaire pour que les utilisateurs puissent surveiller l'accès au système de fichiers FSx for Windows File Server en envoyant des journaux d'accès aux audits CloudWatch à Logs.
- `firehose`— Permet aux directeurs d'écrire des enregistrements sur un Amazon Data Firehose. Cela est nécessaire pour que les utilisateurs puissent surveiller l'accès au système de fichiers FSx for Windows File Server en envoyant des journaux d'accès aux audits à Firehose.

Pour consulter les autorisations associées à cette politique, consultez AmazonF SxFullAccess dans le Guide de référence des politiques AWS gérées.

AWS politique gérée : AmazonF SxConsoleFullAccess

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 des autorisations

Cette politique inclut les autorisations suivantes.

- `fsx`— Permet aux principaux d'effectuer toutes les actions dans la console de gestion Amazon FSx, à l'exception de. `BypassSnaplockEnterpriseRetention`
- `cloudwatch`— Permet aux principaux de consulter les CloudWatch alarmes et les mesures dans la console de gestion Amazon FSx.
- `ds`— Permet aux principaux de répertorier les informations relatives à un AWS Directory Service répertoire.
- `ec2`
  - Permet aux principaux de créer des balises sur les tables de routage, de répertorier les interfaces réseau, les tables de routage, les groupes de sécurité, les sous-réseaux et le VPC associé à un système de fichiers Amazon FSx.
  - Fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.
- `kms`— Permet aux principaux de répertorier les alias des AWS Key Management Service clés.
- `s3`— Permet aux principaux de répertorier certains ou tous les objets d'un compartiment Amazon S3 (jusqu'à 1 000).
- `iam`— Accorde l'autorisation de créer un rôle lié à un service qui permet à Amazon FSx d'effectuer des actions au nom de l'utilisateur.

Pour consulter les autorisations associées à cette politique, consultez AmazonF SxConsoleFullAccess dans le Guide de référence des politiques AWS gérées.

AWS politique gérée : AmazonF SxConsoleReadOnlyAccess

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 des autorisations

Cette politique inclut les autorisations suivantes.

- `fsx`— Permet aux principaux de consulter les informations relatives aux systèmes de fichiers Amazon FSx, y compris toutes les balises, dans la console de gestion Amazon FSx.
- `cloudwatch`— Permet aux principaux de consulter les CloudWatch alarmes et les mesures dans la console de gestion Amazon FSx.
- `ds`— Permet aux principaux de consulter les informations relatives à un AWS Directory Service répertoire dans la console de gestion Amazon FSx.
- `ec2`
  - Permet aux principaux de visualiser les interfaces réseau, les groupes de sécurité, les sous-réseaux et le VPC associé à un système de fichiers Amazon FSx dans la console de gestion Amazon FSx.
  - Fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.
- `kms`— Permet aux principaux d'afficher les alias des AWS Key Management Service clés dans la console de gestion Amazon FSx.
- `log`— Permet aux principaux de décrire les groupes de CloudWatch journaux Amazon Logs associés au compte à l'origine de la demande. Cela est nécessaire pour que les principaux puissent consulter la configuration d'audit d'accès aux fichiers existante pour un système de fichiers FSx for Windows File Server.
- `firehose`— Permet aux principaux de décrire les flux de diffusion Amazon Data Firehose associés au compte à l'origine de la demande. Cela est nécessaire pour que les principaux puissent consulter la configuration d'audit d'accès aux fichiers existante pour un système de fichiers FSx for Windows File Server.

Pour consulter les autorisations associées à cette politique, consultez AmazonF SxConsoleReadOnlyAccess dans le Guide de référence des politiques AWS gérées.

AWS politique gérée : AmazonF SxReadOnlyAccess

Vous pouvez associer la politique `AmazonFSxReadOnlyAccess` à vos identités IAM.

Cette politique accorde des autorisations administratives qui permettent un accès en lecture seule à Amazon FSx.

- `fsx`— Permet aux principaux de consulter les informations relatives aux systèmes de fichiers Amazon FSx, y compris toutes les balises, dans la console de gestion Amazon FSx.
- `ec2`— Fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.

Pour consulter les autorisations associées à cette politique, consultez AmazonF SxReadOnlyAccess dans le Guide de référence des politiques AWS gérées.

Amazon FSx met à jour les politiques gérées AWS

Consultez les informations relatives aux mises à jour des politiques AWS gérées pour Amazon FSx depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page Amazon FSxHistorique du document.

Modification	Description	Date
AmazonF SxServiceRolePolicy — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `ec2:GetSecurityGroupsForVpc` qui permet aux principaux de fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.	9 janvier 2024
AmazonF SxReadOnlyAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `ec2:GetSecurityGroupsForVpc` qui permet aux principaux de fournir une validation améliorée	9 janvier 2024

Modification	Description	Date
	des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.	
AmazonF SxConsole ReadOnlyAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `ec2:GetSecurityGroupsForVpc` qui permet aux principaux de fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.	9 janvier 2024
AmazonF SxFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `ec2:GetSecurityGroupsForVpc` qui permet aux principaux de fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.	9 janvier 2024

Modification	Description	Date
AmazonF SxConsole FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation, `ec2:GetSecurityGroupsForVpc` qui permet aux principaux de fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.	9 janvier 2024
AmazonF SxFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation pour permettre aux utilisateurs d'effectuer une réplication de données entre régions et entre comptes pour FSx pour les systèmes de fichiers OpenZFS.	20 décembre 2023
AmazonF SxConsole FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation pour permettre aux utilisateurs d'effectuer une réplication de données entre régions et entre comptes pour FSx pour les systèmes de fichiers OpenZFS.	20 décembre 2023

Modification	Description	Date
AmazonF SxFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation pour permettre aux utilisateurs d'effectuer une réplication à la demande de volumes pour les systèmes de fichiers FSx pour OpenZFS.	26 novembre 2023
AmazonF SxConsole FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté une nouvelle autorisation pour permettre aux utilisateurs d'effectuer une réplication à la demande de volumes pour les systèmes de fichiers FSx pour OpenZFS.	26 novembre 2023
AmazonF SxFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux utilisateurs d'afficher, d'activer et de désactiver le support VPC partagé pour FSx pour les systèmes de fichiers ONTAP Multi-AZ.	14 novembre 2023
AmazonF SxConsole FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux utilisateurs d'afficher, d'activer et de désactiver le support VPC partagé pour FSx pour les systèmes de fichiers ONTAP Multi-AZ.	14 novembre 2023

Modification	Description	Date
AmazonF SxFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre à Amazon FSx de gérer les configurations réseau pour FSx pour les systèmes de fichiers multi-AZ OpenZFS.	9 août 2023
AWS politique gérée : AmazonF SxServiceRolePolicy — Mise à jour d'une politique existante	Amazon FSx a modifié l'`cloudwatch:PutMetricData` autorisation existante afin qu'Amazon FSx publie les CloudWatch métriques dans l'espace de noms. `AWS/FSx`	24 juillet 2023
AmazonF SxFullAccess — Mise à jour d'une politique existante	Amazon FSx a mis à jour la politique afin de supprimer l'`fsx:*`autorisation et d'ajouter des actions spécifiques`fsx`.	13 juillet 2023
AmazonF SxConsole FullAccess — Mise à jour d'une politique existante	Amazon FSx a mis à jour la politique afin de supprimer l'`fsx:*`autorisation et d'ajouter des actions spécifiques`fsx`.	13 juillet 2023
AmazonF SxFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre à Amazon FSx de gérer les configurations réseau pour FSx pour les systèmes de fichiers multi-AZ OpenZFS.	31 mai 2023

Modification	Description	Date
AmazonF SxConsole ReadOnlyAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux utilisateurs de consulter les indicateurs de performance améliorés et les actions recommandées pour les systèmes de fichiers FSx for Windows File Server dans la console Amazon FSx.	21 septembre 2022
AmazonF SxConsole FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux utilisateurs de consulter les indicateurs de performance améliorés et les actions recommandées pour les systèmes de fichiers FSx for Windows File Server dans la console Amazon FSx.	21 septembre 2022
AmazonF SxReadOnlyAccess — Politique de suivi mise en place	Cette politique accorde un accès en lecture seule à toutes les ressources Amazon FSx et à toutes les balises qui leur sont associées.	4 février 2022
AmazonF SxDeleteServiceLinkedRoleAccess — Politique de suivi mise en place	Cette politique accorde des autorisations administratives qui permettent à Amazon FSx de supprimer son rôle lié au service pour l'accès à Amazon S3.	7 janvier 2022

Modification	Description	Date
AmazonF SxServiceRolePolicy — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre à Amazon FSx de gérer les configurations réseau pour les systèmes de fichiers Amazon FSx for ONTAP. NetApp	2 septembre 2021
AmazonF SxFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre à Amazon FSx de créer des balises sur les tables de routage EC2 pour les appels délimités.	2 septembre 2021
AmazonF SxConsole FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre à Amazon FSx de créer des systèmes de fichiers multi-AZ Amazon FSx pour ONTAP. NetApp	2 septembre 2021
AmazonF SxConsole FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre à Amazon FSx de créer des balises sur les tables de routage EC2 pour les appels délimités.	2 septembre 2021

Modification	Description	Date
AmazonF SxServiceRolePolicy — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre à Amazon FSx de décrire et d'écrire dans les flux de journaux Logs. CloudWatch Cela est nécessaire pour que les utilisateurs puissent consulter les journaux d'audit d'accès aux fichiers pour les systèmes de fichiers FSx for Windows File Server à CloudWatch l'aide des journaux.	8 juin 2021
AmazonF SxServiceRolePolicy — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre à Amazon FSx de décrire et d'écrire dans les flux de diffusion Amazon Data Firehose. Cela est nécessaire pour que les utilisateurs puissent consulter les journaux d'audit d'accès aux fichiers d'un système de fichiers FSx for Windows File Server à l'aide d'Amazon Data Firehose.	8 juin 2021

Modification	Description	Date
AmazonF SxFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux principaux de décrire et de créer des groupes de CloudWatch journaux, des flux de journaux et d'écrire des événements dans des flux de journaux. Cela est nécessaire pour que les principaux puissent consulter les journaux d'audit d'accès aux fichiers pour les systèmes CloudWatch de fichiers FSx for Windows File Server à l'aide des journaux.	8 juin 2021
AmazonF SxFullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux principaux de décrire et d'écrire des enregistrements dans un Amazon Data Firehose. Cela est nécessaire pour que les utilisateurs puissent consulter les journaux d'audit d'accès aux fichiers d'un système de fichiers FSx for Windows File Server à l'aide d'Amazon Data Firehose.	8 juin 2021

Modification	Description	Date
AmazonF SxConsole FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux principaux de décrire les groupes de CloudWatch journaux Amazon Logs associés au compte à l'origine de la demande. Cela est nécessaire pour que les principaux puissent choisir un groupe de CloudWatch journaux Logs existant lors de la configuration de l'audit d'accès aux fichiers pour un système de fichiers FSx for Windows File Server.	8 juin 2021
AmazonF SxConsole FullAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux principaux de décrire les flux de diffusion Amazon Data Firehose associés au compte à l'origine de la demande. Cela est nécessaire pour que les principaux puissent choisir un flux de diffusion Firehose existant lors de la configura tion de l'audit d'accès aux fichiers pour un système de fichiers FSx for Windows File Server.	8 juin 2021

Modification	Description	Date
AmazonF SxConsole ReadOnlyAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux principaux de décrire les groupes de CloudWatch journaux Amazon Logs associés au compte à l'origine de la demande. Cela est nécessaire pour que les principaux puissent consulter la configuration d'audit d'accès aux fichiers existante pour un système de fichiers FSx for Windows File Server.	8 juin 2021
AmazonF SxConsole ReadOnlyAccess — Mise à jour d'une politique existante	Amazon FSx a ajouté de nouvelles autorisations pour permettre aux principaux de décrire les flux de diffusion Amazon Data Firehose associés au compte à l'origine de la demande. Cela est nécessaire pour que les principaux puissent consulter la configuration d'audit d'accès aux fichiers existante pour un système de fichiers FSx for Windows File Server.	8 juin 2021

Modification	Description	Date
Amazon FSx a commencé à suivre les modifications	Amazon FSx a commencé à suivre les modifications apportées à ses politiques AWS gérées.	8 juin 2021

Résolution des problèmes d'identité et d'accès au serveur de fichiers Amazon FSx for Windows

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Amazon FSx et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans FSx
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources FSx

Je ne suis pas autorisé à effectuer une action dans 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 de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Amazon FSx.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Amazon FSx. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction du 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 stratégies 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 de connexion.

Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources FSx

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Amazon FSx prend en charge ces fonctionnalités, consultez. Comment fonctionne Amazon FSx for Windows File Server avec IAM
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.

- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des stratégies basées sur les ressources pour l'accès intercompte, veuillez consulter Différence entre les rôles IAM et les stratégies basées sur les ressources dans le Guide de l'utilisateur IAM.

Utilisation de balises avec Amazon FSx

Vous pouvez utiliser des balises pour contrôler l'accès aux ressources Amazon FSx et pour implémenter le contrôle d'accès basé sur les attributs (ABAC). Les utilisateurs doivent être autorisés à appliquer des balises aux ressources Amazon FSx lors de leur création.

Accorder l'autorisation de baliser les ressources lors de la création

Certaines actions de l'API Amazon FSx qui créent des ressources vous permettent de spécifier des balises lors de la création de la ressource. Vous pouvez utiliser des 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 permettre aux utilisateurs d'attribuer des balises aux ressources au moment de la création, ils doivent avoir les autorisations d'utiliser l'action qui crée la ressource (par exemple, `fsx:CreateFileSystem` ou `fsx:CreateBackup`). Si les balises sont spécifiées dans l'action de création de ressources, Amazon effectue une autorisation supplémentaire sur l'action `fsx:TagResource` pour 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 suivant illustre une politique qui permet aux utilisateurs de créer des systèmes de fichiers et d'appliquer des balises aux systèmes de fichiers lors de leur création dans un système spécifique Compte AWS.

```
{
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/*"
    }
  ]
}
```

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 uniquement évaluée si les balises sont appliquées pendant l'action de création de ressources. Par conséquent, un utilisateur qui est autorisé à créer une ressource (en supposant qu'il n'existe aucune condition de balisage) n'a pas besoin des autorisations d'utiliser l'action `fsx:TagResource` si aucune balise n'est spécifié dans la demande. Toutefois, si l'utilisateur essaie de créer une ressource avec des balises, la demande échoue s'il n'a pas les autorisations d'utiliser l'action `fsx:TagResource`.

Pour plus d'informations sur le balisage des ressources Amazon FSx, consultez. Baliser vos ressources Amazon FSx Pour plus d'informations sur l'utilisation de balises pour contrôler l'accès aux ressources FSx, consultez. Utilisation de balises pour contrôler l'accès à vos ressources Amazon FSx

Utilisation de balises pour contrôler l'accès à vos ressources Amazon FSx

Pour contrôler l'accès aux ressources et aux actions Amazon FSx, vous pouvez utiliser des politiques AWS Identity and Access Management (IAM) basées sur des balises. Vous pouvez fournir le contrôle de deux manières :

1. Contrôlez l'accès aux ressources Amazon FSx en fonction des balises présentes sur ces ressources.
2. Contrôlez quelles balises peuvent être transmises dans une condition de demande IAM.

Pour plus d'informations sur l'utilisation des balises pour contrôler l'accès aux AWS ressources, consultez la section Contrôle de l'accès à l'aide de balises dans le guide de l'utilisateur IAM. Pour plus d'informations sur le balisage des ressources Amazon FSx lors de leur création, consultez. Accorder l’autorisation de baliser les ressources lors de la création Pour plus d’informations sur le balisage des ressources, consultez Baliser vos ressources Amazon FSx.

Contrôle de l'accès en fonction des balises sur une ressource

Pour contrôler les actions qu'un utilisateur ou un rôle peut effectuer sur une ressource Amazon FSx, vous pouvez utiliser des balises sur la ressource. Par exemple, vous pouvez autoriser ou refuser des opérations d'API spécifiques sur une ressource de système de fichiers en fonction de la paire clé-valeur de la balise sur la ressource.

Example policy — Créez un système de fichiers lorsque vous fournissez une balise spécifique

Cette politique permet à l'utilisateur de créer un système de fichiers uniquement lorsqu'il le balise avec une paire clé-valeur spécifique, dans cet exemple,`key=Department, value=Finance`.

```
{
    "Effect": "Allow",
    "Action": [
        "fsx:CreateFileSystem",
        "fsx:TagResource"
    ],
    "Resource": "arn:aws:fsx:region:account-id:file-system/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/Department": "Finance"
        }
    }
```

```
}
```

Example politique — Créez des sauvegardes uniquement des systèmes de fichiers Amazon FSx avec une balise spécifique

Cette politique permet aux utilisateurs de créer des sauvegardes uniquement des systèmes de fichiers marqués avec la paire clé-valeur`key=Department, value=Finance`, et la sauvegarde sera créée avec la balise`Deparment=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }

    ]
}
```

Example politique — Création d'un système de fichiers avec une balise spécifique à partir de sauvegardes avec une balise spécifique

Cette politique permet aux utilisateurs de créer des systèmes de fichiers étiquetés avec `Department=Finance` uniquement à partir de sauvegardes étiquetées avec`Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example politique — Supprime les systèmes de fichiers avec des 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"
                }
            }
        }
    ]
}
```

Utilisation de rôles liés à un service pour Amazon FSx

Amazon FSx for Windows File Server AWS Identity and Access Management utilise des rôles 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 à un service sont prédéfinis par Amazon FSx et incluent toutes les autorisations requises par le service pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration d'Amazon FSx, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Amazon FSx définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul Amazon FSx peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos ressources Amazon FSx, car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez Services AWS qui fonctionnent 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.

La politique d'autorisation des rôles permet à Amazon FSx d'effectuer les actions suivantes sur toutes les ressources applicables AWS :

Vous ne pouvez pas associer AmazonF SxServiceRolePolicy à vos entités IAM. Cette politique est associée à un rôle lié à un service qui permet à FSx de gérer les AWS ressources en votre nom. Pour de plus amples informations, veuillez consulter Utilisation de rôles liés à un service pour Amazon FSx.

Pour les mises à jour de cette politique, voir Amazon F SxServiceRolePolicy

Cette politique accorde des autorisations administratives qui permettent à FSx de gérer les AWS ressources pour le compte de l'utilisateur.

Détails des autorisations

Les autorisations de SxServiceRolePolicy rôle AmazonF sont définies par la politique SxServiceRolePolicy AWS gérée par AmazonF. AmazonF SxServiceRolePolicy dispose des autorisations suivantes :

> **Note**
>
> AmazonF SxServiceRolePolicy est utilisé par tous les types de systèmes de fichiers Amazon FSx ; certaines des autorisations répertoriées peuvent ne pas s'appliquer à FSx pour Windows.

- `ds`— Permet à FSx d'afficher, d'autoriser et de supprimer les applications de votre répertoire. AWS Directory Service
- `ec2`— Permet à FSx d'effectuer les opérations suivantes :
  - Affichez, créez et dissociez les interfaces réseau associées à un système de fichiers Amazon FSx.
  - Affichez une ou plusieurs adresses IP élastiques associées à un système de fichiers Amazon FSx.

  - Affichez les VPC, les groupes de sécurité et les sous-réseaux Amazon associés à un système de fichiers Amazon FSx.
  - Fournir une validation améliorée des groupes de sécurité de tous les groupes de sécurité pouvant être utilisés avec un VPC.
  - Créez une autorisation permettant à un utilisateur AWS autorisé d'effectuer certaines opérations sur une interface réseau.
- `cloudwatch`— Permet à FSx de publier des points de données métriques CloudWatch sous l'espace de noms AWS /FSx.
- `route53`— Permet à FSx d'associer un Amazon VPC à une zone hébergée privée.
- `logs`— Permet à FSx de décrire et d'écrire dans les flux de CloudWatch journaux Logs. Cela permet aux utilisateurs d'envoyer les journaux d'audit d'accès aux fichiers d'un système de fichiers FSx for Windows File Server vers CloudWatch un flux de journaux.
- `firehose`— Permet à FSx de décrire et d'écrire dans les flux de diffusion Amazon Data Firehose. Cela permet aux utilisateurs de publier les journaux d'audit d'accès aux fichiers d'un système de fichiers FSx for Windows File Server sur un flux de diffusion Amazon Data Firehose.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateFileSystem",
            "Effect": "Allow",
            "Action": [
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
                "ec2:GetSecurityGroupsForVpc",
```

```
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PutMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/FSx"
                }
            }
        },

        {
            "Sid": "TagResourceNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
            "Sid": "ManageNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
```

```
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
        {
            "Sid": "ManageRouteTable",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
        },
        {
            "Sid": "PutCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Sid": "ManageAuditLogs",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:PutRecord",
```

```
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
}
```

Toute mise à jour de cette politique est décrite dansAmazon FSx met à jour les politiques gérées AWS.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Gguide 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 Consoleinterface de ligne de commande IAM ou l'API IAM, Amazon FSx crée le rôle lié au service pour vous.

> **Important**
>
> Ce rôle lié à un service peut apparaître dans votre compte si vous avez effectué une action dans un autre service qui utilise les fonctions prises en charge par ce rôle. Pour de plus amples informations, veuillez consulter Un nouveau rôle est apparu dans mon compte IAM.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez un système de fichiers, Amazon FSx crée à nouveau le rôle lié à un service pour vous.

Modification d'un rôle lié à un service pour Amazon FSx

Amazon FSx ne vous permet pas de modifier le rôle lié au 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 fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n’avez aucune entité inutilisée qui n’est pas surveillée ou gérée activement. Toutefois, vous devez supprimer tous vos systèmes de fichiers et toutes vos sauvegardes avant de pouvoir supprimer manuellement le rôle lié à un service.

> **Note**
>
> Si le service Amazon FSx utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer manuellement le rôle lié à un service à l’aide d’IAM

Utilisez la console IAM, l'interface de ligne de commande IAM ou l'API IAM pour supprimer le rôle lié à un service . Pour plus d'informations, veuillez consulter Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés au service Amazon FSx

Amazon FSx prend en charge l'utilisation de rôles liés à un service dans toutes les régions où le service est disponible. Pour plus d’informations, consultez Régions et Points de terminaison AWS.

Validation de conformité pour Amazon FSx for Windows File Server

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Amazon FSx for Windows File Server et interface des points de terminaison de VPC

Vous pouvez améliorer le niveau de sécurité de votre VPC en configurant Amazon FSx pour utiliser un point de terminaison de VPC d'interface. Les points de terminaison d'un VPC d'interface reposent surAWS PrivateLink, une technologie qui vous permet d'accéder en privé aux API Amazon FSx sans passerelle Internet, périphérique NAT, connexion VPN ouAWS Direct Connectconnexion. Les instances de votre VPC ne nécessitent pas d'adresses IP publiques pour communiquer avec les API Amazon FSx. Le trafic entre votre VPC et Amazon FSx ne quitte pas leAWSréseau.

Chaque point de terminaison de VPC d'interface est représenté par une ou plusieurs interfaces réseau Elastic dans vos sous-réseaux. Une interface réseau fournit une adresse IP privée qui sert de point d'entrée au trafic vers l'API Amazon FSx.

Considérations relatives aux points FSx terminaison d'un VPC de l'interface Amazon

Avant de configurer un point de terminaison de VPC d'interface pour Amazon FSx, veillez à consulterPropriétés et limites des points de terminaison d'un VPC d'interfacedans leAmazon VPC User Guide.

Vous pouvez appeler n'importe quelle opération d'API Amazon FSx à partir de votre VPC. Par exemple, vous pouvez créer un système de fichiers FSx for Windows File Server en appelant le CreateFileSystem API à partir de votre VPC. Pour obtenir la liste complète des API Amazon FSx, consultezActionsdans la référence de l'API Amazon FSx.

Considérations relatives au Homologation

Vous pouvez connecter d'autres VPC au VPC avec des points de terminaison de VPC d'interface à l'aide d'un Appairage de VPC. L'appairage de VPC est une connexion réseau entre deux VPC. Vous pouvez aussi établir une connexion d'appairage de VPC entre vos deux VPC, ou avec un VPC situé dans un autre VPCCompte AWS. Les VPC peuvent également se trouver dans deuxRégions AWS.

Le trafic entre des VPC appairés reste sur le réseau AWS et ne traverse pas l'Internet public. Une fois les VPC appairés, des ressources telles que des instances Amazon Elastic Compute Cloud (Amazon EC2) dans les deux VPC peuvent accéder à l'API Amazon FSx via des points de terminaison de VPC d'interface créés dans celui des VPC.

Création d'un point de terminaison de VPC d'interface pour l'API Amazon FSx

Vous pouvez créer un point de terminaison de VPC pour l'API Amazon FSx à l'aide de la console Amazon VPC ou d'AWS Command Line Interface(AWS CLI). Pour de plus amples informations, veuillez consulterCréation d'un point de terminaison d'un VPC d'interfacedans leAmazon VPC User Guide.

Pour créer un point de terminaison de VPC d'interface pour Amazon FSx, utilisez l'une des méthodes suivantes :

- **`com.amazonaws.region.fsx`**— Crée un point de terminaison pour les opérations d'API Amazon FSx.
- **`com.amazonaws.region.fsx-fips`**— Crée un point de terminaison pour l'API Amazon FSx conforme àNormes FIPS 140-2.

Pour utiliser l'option de DNS privée, vous devez définir le`enableDnsHostnames`et`enableDnsSupport`attributs de votre VPC. Pour de plus amples informations, veuillez consulterAffichage et mise à jour de la prise en charge de DNS pour votre VPCdans leAmazon VPC User Guide.

ExcludesRégions AWSEn Chine, si vous activez le DNS privé pour le point de terminaison, vous pouvez faire des demandes d'API à Amazon FSx avec le point de terminaison d'un VPC en utilisant son nom DNS par défaut pour leRégion AWS, par exemple`fsx.us-east-1.amazonaws.com`. Pour la Chine (Beijing) et Chine (Ningxia)Régions AWS, vous pouvez effectuer des demandes d'API avec le point de terminaison d'un VPC en utilisant`fsx-api.cn-north-1.amazonaws.com.cn`et`fsx-api.cn-northwest-1.amazonaws.com.cn`, respectivement.

Pour de plus amples informations, veuillez consulterAccès à un service via un point de terminaison de VPC d'interfacedans leAmazon VPC User Guide.

Création d'une stratégie de point de terminaison de VPC pour Amazon FSx

Pour contrôler davantage l'accès à l'API Amazon FSx, vous pouvez éventuellement attacher unAWS Identity and Access Management(IAM) à votre point de terminaison de VPC. La stratégie spécifie les éléments suivants :

- Le mandataire 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.

Quotas

Vous trouverez ci-dessous des informations sur les quotas lorsque vous travaillez avec Amazon FSx for Windows File Server.

Rubriques

Les quotas que vous pouvez augmenter

Vous trouverez ci-dessous les quotas pour Amazon FSx for Windows File Server que vous pouvez augmenter Région AWS pour Compte AWS chacun d'entre eux.

Ressource	Par défaut	Description
Systèmes de fichiers Windows	100	Le nombre maximum de systèmes de fichiers Amazon FSx pour Windows Server que vous pouvez créer dans ce compte.
Capacité de débit de Windows	10240	Capacité de débit totale (en Mo/s) autorisée pour tous les systèmes de fichiers Amazon FSx pour Windows de ce compte.
Capacité de stockage sur disque dur Windows	524288	Capacité maximale de stockage sur disque dur (en GiB) autorisée pour tous les systèmes de fichiers Amazon

Ressource	Par défaut	Description
		FSx for Windows File Server de ce compte.
Capacité de stockage SSD Windows	524288	La capacité de stockage SSD maximale (en GiB) autorisée pour tous les systèmes de fichiers Amazon FSx for Windows File Server de ce compte.
Nombre total d'E/S par seconde sur SSD sous Windows	500 000	Le nombre total d'IOPS sur SSD autorisé pour tous les systèmes de fichiers Amazon FSx for Windows File Server de ce compte.
Sauvegardes Windows	500	Le nombre maximum de sauvegardes initiées par l'utilisateur pour tous les systèmes de fichiers Amazon FSx for Windows File Server que vous pouvez avoir dans ce compte.

Pour demander une augmentation de quota

1. Ouvrez la console Service Quotas.
2. Dans le panneau de navigation, choisissez Services AWS.
3. Choisissez Amazon FSx.
4. Choisissez un quota.
5. Choisissez Demander une augmentation de quota, puis suivez les instructions pour demander une augmentation de quota.
6. Pour consulter l'état de la demande de quota, sélectionnez Historique des demandes de quotas dans le volet de navigation de la console.

Pour de plus amples informations, veuillez consulter Demande d’augmentation de quota dans le Guide de l’utilisateur Service Quotas.

Quotas de ressources pour chaque système de fichiers

Vous trouverez ci-dessous les quotas sur les ressources du serveur de fichiers Amazon FSx for Windows pour chaque système de fichiers d'un. Région AWS

Ressource	Limite par système de fichiers
Nombre maximum de tags	50
Durée de conservation maximale pour les sauvegardes automatisées	90 jours
Nombre maximum de demandes de copie de sauvegarde en cours vers une seule région de destination par compte.	5
Capacité de stockage minimale, systèmes de fichiers SSD	32 GiO
Capacité de stockage minimale, systèmes de fichiers HDD	2 000 GiB
Capacité de stockage maximale, SSD et HDD	64 Tio
Nombre minimal d'IOPS sur SSD	96
Nombre maximal d'IOPS sur SSD	400 000
Capacité de débit minimale	8 Mbits/s
Capacité de débit maximale	12 288 Mbits/s
Nombre maximum de partages de fichiers	100 000

Considérations supplémentaires

En outre, notez les éléments suivants :

- Vous pouvez utiliser chaque touche AWS Key Management Service (AWS KMS) sur un maximum de 125 systèmes de fichiers Amazon FSx.
- Pour obtenir une liste des Régions AWS endroits où vous pouvez créer des systèmes de fichiers, consultez Amazon FSx Endpoints and Quotas dans le. Références générales AWS
- Vous mappez vos partages de fichiers à partir d'instances Amazon EC2 dans votre cloud privé virtuel (VPC) avec leurs noms de service de noms de domaine (DNS).

Quotas spécifiques à Microsoft Windows

Pour plus d'informations, consultez la section Limites NTFS sur le Microsoft Windows Dev Center.

Résolution des problèmes liés à Amazon FSx

Utilisez les sections suivantes pour résoudre les problèmes que vous rencontrez avec Amazon FSx.

Si vous rencontrez des problèmes non répertoriés ci-dessous lors de l'utilisation d'Amazon FSx, essayez de poser une question sur le forum Amazon FSx.

Rubriques

Vous ne pouvez pas accéder à votre système de fichiers

L'impossibilité d'accéder à votre système de fichiers peut avoir plusieurs causes, chacune ayant sa propre résolution, comme suit.

Rubriques

- L'utilisateur Active Directory ne dispose pas des autorisations requises
- Autoriser le contrôle total : autorisations ACL NTFS supprimées
- Impossible d'accéder à un système de fichiers à l'aide d'un client local
- Le nouveau système de fichiers n'est pas enregistré dans le DNS
- Impossible d'accéder au système de fichiers à l'aide d'un alias DNS
- Impossible d'accéder au système de fichiers à l'aide d'une adresse IP

L'interface Elastic Network du système de fichiers a été modifiée ou supprimée

Vous ne devez ni modifier ni supprimer l'interface Elastic Network du 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. Créez un nouveau système de fichiers et ne modifiez ni ne supprimez l'interface Amazon FSx Elastic network. Pour plus d'informations, consultez Contrôle d'accès au système de fichiers avec Amazon VPC.

L'adresse IP élastique attachée à l'interface Elastic Network du système de fichiers a été supprimée.

Amazon FSx ne prend pas en charge l'accès aux systèmes de fichiers depuis l'Internet public. Amazon FSx détache automatiquement toute adresse IP élastique, qui est une adresse IP publique accessible depuis Internet, attachée à l'interface réseau élastique d'un système de fichiers. Pour plus d'informations, consultez Clients, méthodes d'accès et environnements pris en charge pour Amazon FSx for Windows File Server.

Le groupe de sécurité du système de fichiers ne possède pas les règles d'entrée ou de sortie 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 de l'instance de calcul ne possède pas les 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.

Instance de calcul non jointe à un Active Directory

Vos instances de calcul ne sont peut-être pas correctement jointes à l'un des deux types d'Active Directory :

- Le AWS Managed Microsoft AD répertoire auquel votre système de fichiers est joint.
- Un annuaire Microsoft Active Directory doté d'une relation d'approbation forestière unidirectionnelle établie avec l' AWS Managed Microsoft AD annuaire.

Assurez-vous que vos instances de calcul sont jointes à l'un des deux types d'annuaires. L'un d'entre eux est le AWS Managed Microsoft AD répertoire auquel votre système de fichiers est joint. L'autre type est un annuaire Microsoft Active Directory doté d'une relation d'approbation forestière unidirectionnelle établie avec l' AWS Managed Microsoft AD annuaire. Pour plus d’informations, consultez Utilisation d'Amazon FSx avec AWS Directory Service for Microsoft Active Directory.

Le partage de fichiers n'existe pas

Le partage de fichiers Microsoft Windows auquel vous essayez d'accéder n'existe pas.

Si vous utilisez un partage de fichiers existant, assurez-vous que le nom DNS du système de fichiers et le nom du partage sont correctement spécifiés. Pour gérer vos partages de fichiers, consultezGestion des partages de fichiers sur les systèmes de fichiers FSx for Windows File Server.

L'utilisateur Active Directory ne dispose pas des autorisations requises

L'utilisateur Active Directory sous lequel vous accédez au partage de fichiers ne dispose pas des autorisations d'accès nécessaires.

Assurez-vous que les autorisations d'accès pour le partage de fichiers et les listes de contrôle d'accès (ACL) Windows pour le dossier partagé autorisent l'accès aux utilisateurs Active Directory qui ont besoin d'y accéder.

Autoriser le contrôle total : autorisations ACL NTFS supprimées

Si vous supprimez les autorisations ACL NTFS Allow Full control pour l'utilisateur SYSTEM sur un dossier que vous avez partagé, ce partage peut devenir inaccessible et les sauvegardes du système de fichiers effectuées à partir de ce point risquent de ne pas être utilisables.

Vous devrez recréer le partage de fichiers concerné. Pour plus d'informations, consultez Gestion des partages de fichiers sur les systèmes de fichiers FSx for Windows File Server. Après avoir recréé le dossier ou le partage, vous pouvez mapper et utiliser les partages de fichiers Windows à partir de vos instances de calcul.

Impossible d'accéder à un système de fichiers à l'aide d'un client local

Vous utilisez votre système de fichiers Amazon FSx sur site via un VPN, et vous utilisez AWS Direct Connect une plage d'adresses IP non privées pour le client sur site.

Amazon FSx prend uniquement en charge l'accès depuis les clients locaux dotés d'adresses IP non privées sur les systèmes de fichiers créés après le 17 décembre 2020.

Si vous devez accéder à votre système de fichiers FSx for Windows File Server créé avant le 17 décembre 2020 à l'aide d'une plage d'adresses IP non privée, vous pouvez créer un nouveau système de fichiers en restaurant une sauvegarde du système de fichiers. Pour plus d'informations, consultez Utilisation des sauvegardes.

Le nouveau système de fichiers n'est pas enregistré dans le DNS

Pour les systèmes de fichiers joints à un Active Directory autogéré, Amazon FSx n'a pas enregistré le DNS du système de fichiers lors de sa création car le réseau du client n'utilise pas le DNS Microsoft.

Amazon FSx n'enregistre pas les systèmes de fichiers dans le DNS si votre réseau utilise un service DNS tiers au lieu du DNS Microsoft. Vous devez configurer manuellement les entrées DNS A pour vos systèmes de fichiers Amazon FSx. Pour les systèmes de fichiers mono-AZ 1, vous devrez ajouter une entrée DNS A ; pour les systèmes de fichiers mono-AZ 2 et multi-AZ, vous devrez ajouter deux entrées DNS A. Suivez la procédure ci-dessous pour obtenir la ou les adresses IP du système de fichiers à utiliser lors de l'ajout manuel des entrées DNS A.

1. Dans le https://console.aws.amazon.com/fsx/, choisissez le système de fichiers dont vous souhaitez obtenir l'adresse IP pour afficher la page de détails du système de fichiers.
2. Dans l'onglet Réseau et sécurité, effectuez l'une des opérations suivantes :

- Pour un système de fichiers mono-AZ 1 :
  - Dans le panneau Subnet, choisissez l'interface réseau élastique affichée sous Network interface pour ouvrir la page Network Interfaces dans Amazon EC2.
  - L'adresse IP du système de fichiers mono-AZ 1 à utiliser est indiquée dans la colonne IP IPv4 privée principale.
- Pour un système de fichiers mono-AZ 2 ou multi-AZ :
  - Dans le panneau Sous-réseau préféré, choisissez l'interface réseau élastique affichée sous Interface réseau pour ouvrir la page Network Interfaces dans Amazon EC2.
  - L'adresse IP du sous-réseau préféré à utiliser est indiquée dans la colonne IP IPv4 privée secondaire.
  - Dans le panneau du sous-réseau Amazon FSx Standby, choisissez l'interface réseau élastique affichée sous Interface réseau pour ouvrir la page Network Interfaces dans la console Amazon EC2.
  - L'adresse IP du sous-réseau de secours à utiliser est indiquée dans la colonne IP IPv4 privée secondaire.

Impossible d'accéder au système de fichiers à l'aide d'un alias DNS

Si vous ne parvenez pas à accéder à un système de fichiers à l'aide d'un alias DNS, suivez la procédure ci-dessous pour résoudre le problème.

1. Vérifiez que l'alias est associé au système de fichiers en effectuant l'une des étapes suivantes :

   a. Utilisation de la console Amazon FSx : choisissez le système de fichiers auquel vous essayez d'accéder. Sur la page des détails du système de fichiers, les alias DNS sont affichés dans l'onglet Réseau et sécurité.

   b. Utilisation de la CLI ou de l'API : utilisez la commande `describe-file-system-aliases`CLI ou l'opération DescribeFileSystemAliasesAPI pour récupérer les alias actuellement associés au système de fichiers.

2. Si l'alias DNS n'est pas répertorié, vous devez l'associer au système de fichiers. Pour plus d'informations, consultez Gestion des alias DNS sur les systèmes de fichiers existants.
3. Si l'alias DNS est associé au système de fichiers, vérifiez que vous avez également configuré les éléments obligatoires suivants :

- Noms principaux de service (SPN) créés correspondant à l'alias DNS sur l'objet informatique Active Directory de votre système de fichiers Amazon FSx.

  Pour plus d'informations, consultez Étape 2 : Configuration des noms principaux de service (SPN) pour Kerberos.

- Création d'un enregistrement DNS CNAME pour l'alias DNS qui correspond au nom DNS par défaut du système de fichiers Amazon FSx.

  Pour plus d'informations, consultez Étape 3 : Mettre à jour ou créer un enregistrement DNS CNAME pour le système de fichiers.

4. Si vous avez créé des SPN valides et un enregistrement DNS CNAME, vérifiez que le DNS du client possède l'enregistrement DNS CNAME qui correspond au système de fichiers approprié.

   a. Exécutez `nslookup` pour confirmer que l'enregistrement existe et qu'il correspond au nom DNS par défaut du système de fichiers.

   b. Si le DNS CNAME correspond à un autre système de fichiers, attendez que le cache DNS du client soit actualisé, puis vérifiez à nouveau l'enregistrement CNAME. Vous pouvez accélérer le processus en vidant le cache DNS du client à l'aide de la commande suivante.

   ```
   ipconfig /flushdns
   ```

5. Si l'enregistrement DNS CNAME correspond au DNS par défaut du système de fichiers Amazon FSx et que le client ne parvient toujours pas à accéder au système de fichiers, Vous ne pouvez pas accéder à votre système de fichiers consultez les étapes de résolution des problèmes supplémentaires.

Impossible d'accéder au système de fichiers à l'aide d'une adresse IP

Si vous ne parvenez pas à accéder à votre système de fichiers à l'aide d'une adresse IP, essayez plutôt d'utiliser le nom DNS ou l'alias DNS associé.

Vous pouvez trouver le nom DNS du système de fichiers et tous les alias DNS associés sur la console Amazon FSx en choisissant Windows File Server, Network & security. Vous pouvez également les trouver dans la réponse de l'opération CreateFileSystemou DescribeFileSystemsAPI. Pour plus d'informations sur l'utilisation des alias DNS, consultezGestion des alias DNS.

- Pour un système de fichiers mono-AZ joint à un Microsoft Active Directory AWS géré, le nom DNS est le suivant.

```
fs-0123456789abcdef0.ad-domain.com
```

- Pour tous les systèmes de fichiers multi-AZ et les systèmes de fichiers mono-AZ joints à un Active Directory autogéré, le nom DNS est le suivant.

```
amznfsxaa11bb22.ad-domain.com
```

La création d'un nouveau système de fichiers Amazon FSx échoue

L'échec d'une demande de création de système de fichiers peut avoir plusieurs causes, comme décrit dans la section suivante.

Rubriques

- Résolution des problèmes liés aux systèmes de fichiers joints à un répertoire Microsoft Active Directory AWS géré
- La création d'un système de fichiers joint à un Active Directory autogéré échoue

Résolution des problèmes liés aux systèmes de fichiers joints à un répertoire Microsoft Active Directory AWS géré

Utilisez les sections suivantes pour résoudre les problèmes liés à la création d'un système de fichiers FSx for Windows File Server joint à votre Active Directory autogéré.

Groupe de sécurité VPC et ACL réseau mal configurés

Assurez-vous que les groupes de sécurité VPC et les ACL réseau sont configurés selon la configuration de groupe de sécurité recommandée. Pour plus d'informations, consultez la section Création de groupes de sécurité.

La création d'un système de fichiers joint à un Active Directory autogéré échoue

Rubriques

- Noms de groupes d'administrateurs de systèmes de fichiers dupliqués
- Les serveurs DNS ou les contrôleurs de domaine sont inaccessibles
- Informations d'identification du compte de service non valides
- Autorisations de compte de service insuffisantes
- Capacité du compte de service dépassée
- Amazon FSx ne peut pas accéder à l'unité organisationnelle (UO)
- Le compte de service ne peut pas accéder au groupe d'administrateurs
- Amazon FSx a perdu la connectivité dans le domaine
- Le compte de service ne dispose pas des autorisations correctes
- Caractères Unicode utilisés dans les paramètres de création

Noms de groupes d'administrateurs de systèmes de fichiers dupliqués

La création d'un système de fichiers joint à votre Active Directory autogéré échoue avec le message d'erreur suivant :

```
File system creation failed. Amazon FSx is unable to apply your Microsoft Active
 Directory configuration with the
specified file system administrators group. Please ensure that your Active Directory
 does not contain multiple domain
groups with the name: domain_group.
```

Amazon FSx n'a pas créé le système de fichiers car plusieurs groupes d'administrateurs portent le même nom dans le domaine.

Si vous ne spécifiez pas de nom de groupe, Amazon FSx essaiera d'utiliser la valeur par défaut « Domain Admins » comme groupe d'administrateurs. La demande échouera si plusieurs groupes utilisent le nom « Administrateurs de domaine » par défaut.

Suivez les étapes ci-dessous pour résoudre le problème.

1. Passez en revue les conditions requises pour joindre votre système de fichiers à votre Active Directory autogéré.
2. Utilisez l'outil de validation Amazon FSx Active Directory pour valider votre configuration Active Directory autogérée avant de créer un système de fichiers FSx for Windows File Server joint à un Active Directory autogéré.

3. Créez un nouveau système de fichiers à l'aide du AWS Management Console ou AWS CLI. Pour plus d'informations, consultez Joindre un système de fichiers Amazon FSx à un domaine Microsoft Active Directory autogéré.
4. Donnez un nom unique au groupe d'administrateurs du système de fichiers dans le domaine de votre Active Directory autogéré.

Les serveurs DNS ou les contrôleurs de domaine sont inaccessibles

La création d'un système de fichiers joint à votre Active Directory autogéré échoue avec le message d'erreur suivant :

```
Amazon FSx can't reach the DNS servers provided or the domain controllers for your
 self-managed directory in Microsoft Active Directory.
File system creation failed. Amazon FSx is unable to communicate with your Microsoft
 Active Directory domain controllers.
This is because Amazon FSx can't reach the DNS servers provided or domain controllers
 for your domain.
To fix this problem, delete your file system and create a new one with valid DNS
 servers and networking configuration that allows
traffic from the file system to the domain controller.
```

Suivez les étapes ci-dessous pour résoudre le problème.

1. Vérifiez que vous avez respecté les conditions requises pour établir la connectivité réseau et le routage entre le sous-réseau dans lequel vous créez un système de fichiers Amazon FSx et votre Active Directory autogéré. Pour plus d'informations, consultez Conditions préalables à l'utilisation d'un Microsoft Active Directory autogéré.

   Utilisez l'outil de validation Active Directory d'Amazon FSx pour tester et vérifier ces paramètres réseau.

   > **Note**
   >
   > Si plusieurs sites Active Directory sont définis, assurez-vous que les sous-réseaux du VPC associé à votre système de fichiers Amazon FSx sont définis dans un site Active Directory et qu'il n'existe aucun conflit d'adresses IP entre les sous-réseaux de votre VPC et ceux de vos autres sites. Vous pouvez afficher et modifier ces paramètres à l'aide du composant logiciel enfichable MMC Active Directory Sites and Services.

2. Vérifiez que vous avez configuré les groupes de sécurité VPC que vous avez associés à votre système de fichiers Amazon FSx, ainsi que toutes les ACL du réseau VPC, pour autoriser le trafic réseau sortant sur tous les ports.

   > **Note**
   >
   > Si vous souhaitez implémenter le moindre privilège, vous pouvez autoriser le trafic sortant uniquement vers les ports spécifiques requis pour la communication avec les contrôleurs de domaine Active Directory. Pour plus d'informations, consultez la documentation de Microsoft Active Directory.

3. Vérifiez que les valeurs des propriétés administratives du serveur de fichiers ou du réseau Microsoft Windows ne contiennent pas de caractères autres que latin-1. Par exemple, la création du système de fichiers échoue si vous utilisez le `Domänen-Admins` nom du groupe d'administrateurs du système de fichiers.
4. Vérifiez que les serveurs DNS et les contrôleurs de domaine de votre domaine Active Directory sont actifs et capables de répondre aux demandes relatives au domaine fourni.
5. Assurez-vous que le niveau fonctionnel de votre domaine Active Directory est Windows Server 2008 R2 ou supérieur.
6. Assurez-vous que les règles de pare-feu des contrôleurs de domaine de votre domaine Active Directory autorisent le trafic provenant de votre système de fichiers Amazon FSx. Pour plus d'informations, consultez la documentation de Microsoft Active Directory.

Informations d'identification du compte de service non valides

La création d'un système de fichiers joint à un Active Directory autogéré échoue avec le message d'erreur suivant :

```
Amazon FSx is unable to establish a connection with your Microsoft Active Directory
 domain controllers
because the service account credentials provided are invalid. To fix this problem,
 delete your file
system and create a new one using a valid service account.
```

Suivez les étapes ci-dessous pour résoudre le problème.

1. Vérifiez que vous entrez uniquement le nom d'utilisateur en tant qu'entrée pour le nom d'utilisateur du compte de service, par exemple dans la configuration autogérée d'Active Directory. `ServiceAcct`

   > **Important**
   >
   > N'incluez PAS de préfixe de domaine (`corp.com\ServiceAcct`) ou de suffixe de domaine (`ServiceAcct@corp.com`) lors de la saisie du nom d'utilisateur du compte de service.
   > N'UTILISEZ PAS le nom distinctif (DN) lors de la saisie du nom d'utilisateur du compte de service (CN=ServiceAcct, OU=example, DC=corp, DC=com).

2. Vérifiez que le compte de service que vous avez fourni existe dans votre domaine Active Directory.
3. 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

   Pour plus d'informations sur la création d'un compte de service doté des autorisations appropriées, consultez Délégation de privilèges à votre compte de service Amazon FSx .

Autorisations de compte de service insuffisantes

La création d'un système de fichiers joint à votre Active Directory autogéré échoue avec le message d'erreur suivant :

```
Amazon FSx is unable to establish a connection with your
Microsoft Active Directory domain controllers. This is because the service account
 provided does not
```

```
have permission to join the file system to the domain with the specified organizational
 unit.
To fix this problem, delete your file system and create a new one using a service
 account with
permission to join the file system to the domain with the specified organizational
 unit.
```

Suivez la procédure ci-dessous pour résoudre le 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

  Pour plus d'informations sur la création d'un compte de service doté des autorisations appropriées, consultez Délégation de privilèges à votre compte de service Amazon FSx .

Capacité du compte de service dépassée

La création d'un système de fichiers joint à votre Active Directory autogéré échoue avec le message d'erreur suivant :

```
Amazon FSx can't establish a connection with your Microsoft Active Directory
domain controllers. This is because the service account provided has reached the
maximum number of computers that it can join to the domain. To fix this problem,
delete your file system and create a new one, supplying a service account that
is able to join new computers to the domain.
```

Pour résoudre le problème, vérifiez que le compte de service que vous avez fourni a atteint le nombre maximum d'ordinateurs qu'il peut associer au domaine. S'il a atteint la limite maximale, créez un nouveau compte de service avec les autorisations appropriées. Utilisez le nouveau compte de

service et créez un nouveau système de fichiers. Pour plus d'informations, consultez Délégation de privilèges à votre compte de service Amazon FSx .

Amazon FSx ne peut pas accéder à l'unité organisationnelle (UO)

La création d'un système de fichiers joint à votre Active Directory autogéré échoue avec le message d'erreur suivant :

```
Amazon FSx can't establish a connection with your Microsoft Active Directory domain
 controller(s).
This is because the organizational unit you specified either doesn't exist or isn't
 accessible
to the service account provided. To fix this problem, delete your file system and
 create a new one specifying an
organizational unit to which the service account can join the file system.
```

Suivez les étapes ci-dessous pour résoudre le problème.

1. Vérifiez que l'unité d'organisation que vous avez fournie se trouve dans votre domaine Active Directory.
2. 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 disposer, au minimum, des autorisations nécessaires pour 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
   - Bénéficiez d'une délégation de contrôle pour créer et 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 Délégation de privilèges à votre compte de service Amazon FSx .

Le compte de service ne peut pas accéder au groupe d'administrateurs

La création d'un système de fichiers joint à votre Active Directory autogéré échoue avec le message d'erreur suivant :

```
Amazon FSx is unable to apply your Microsoft Active Directory configuration. This is
 because the file system
administrators group you provided either doesn't exist or isn't accessible to the
 service account you
provided. To fix this problem, delete your file system and create a new one specifying
 a file
system administrators group in the domain that is accessible to the service account
provided.
```

Suivez les étapes ci-dessous pour résoudre le problème.

1. Assurez-vous de fournir uniquement le nom du groupe sous forme de chaîne pour le paramètre du groupe d'administrateurs.

   > **Important**
   >
   > N'incluez PAS de préfixe de domaine (`corp.com\FSxAdmins`) ou de suffixe de domaine (`FSxAdmins@corp.com`) lorsque vous fournissez le paramètre de nom de groupe.
   > N'UTILISEZ PAS le nom distinctif (DN) du groupe. Un exemple de nom distinctif est CN=FSxAdmins, OU=Example, DC=Corp, DC=com.

2. Assurez-vous que le groupe d'administrateurs fourni existe dans le même domaine Active Directory que celui auquel vous souhaitez joindre le système de fichiers.
3. Si vous n'avez pas fourni de paramètre de groupe d'administrateurs, Amazon FSx tente d'utiliser le `Builtin Domain Admins` groupe dans votre domaine Active Directory. Si le nom de ce groupe a été modifié, ou si vous utilisez un autre groupe pour l'administration du domaine, vous devez fournir ce nom pour le groupe.

Amazon FSx a perdu la connectivité dans le domaine

La création d'un système de fichiers joint à votre Active Directory autogéré échoue avec le message d'erreur suivant :

```
Amazon FSx is unable to apply your Microsoft Active Directory configuration. To fix
 this problem, delete your file system and create a new one
meeting the pre-requisites described in the Amazon FSx user guide.
```

Lors de la création de votre système de fichiers, Amazon FSx a pu accéder aux serveurs DNS et aux contrôleurs de domaine de votre domaine Active Directory, et a réussi à joindre le système de fichiers à votre domaine Active Directory. Cependant, lors de la création du système de fichiers, Amazon FSx a perdu la connectivité ou l'adhésion à votre domaine. Suivez les étapes ci-dessous pour résoudre le problème.

1. Assurez-vous que la connectivité réseau continue d'exister entre votre système de fichiers Amazon FSx et votre Active Directory. Assurez-vous également que le trafic réseau continue d'être autorisé entre eux en utilisant les règles de routage, les règles de groupe de sécurité VPC, les ACL du réseau VPC et les règles de pare-feu des contrôleurs de domaine.
2. Assurez-vous que les objets informatiques créés par Amazon FSx pour vos systèmes de fichiers dans votre domaine Active Directory sont toujours actifs et qu'ils n'ont pas été supprimés ou manipulés d'une autre manière.

Le compte de service ne dispose pas des autorisations correctes

La création d'un système de fichiers joint à votre Active Directory autogéré échoue avec le message d'erreur suivant :

```
File system creation failed. Amazon FSx is unable to establish a connection with your
 Microsoft Active Directory domain controller(s).
This is because the service account provided does not have permission to join the file
 system to the domain with the specified
organizational unit (OU). To fix this problem, delete your file system and create a new
 one using a service account with permission
to create computer objects and reset passwords within the specified organizational
 unit.
```

Assurez-vous d'avoir délégué les autorisations requises au compte de service que vous avez fourni. Suivez les étapes ci-dessous pour résoudre le problème.

Le compte de service doit disposer au minimum des autorisations suivantes :

- Bénéficiez d'une délégation de contrôle pour créer et supprimer des objets informatiques dans l'unité d'organisation à laquelle vous rejoignez le système de fichiers

- Disposez des autorisations suivantes dans l'unité d'organisation pour laquelle vous rejoignez le système de fichiers :
  - Possibilité de réinitialiser les mots de passe
  - Possibilité d'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 (déléguée) de créer et de supprimer des objets informatiques
  - Aptitude validée à lire et à écrire les restrictions du compte
  - Possibilité de modifier les autorisations

  Pour plus d'informations sur la création d'un compte de service doté des autorisations appropriées, consultez Délégation de privilèges à votre compte de service Amazon FSx .

Caractères Unicode utilisés dans les paramètres de création

La création d'un système de fichiers joint à votre Active Directory autogéré échoue avec le message d'erreur suivant :

```
File system creation failed. Amazon FSx is unable to create a file system within the
 specified
Microsoft Active Directory. To fix this problem, please delete your file system and
 create a new one
meeting the pre-requisites described in the FSx for ONTAP User Guide.
```

Amazon FSx ne prend pas en charge les caractères Unicode. Vérifiez qu'aucun des paramètres de création ne comporte de caractères Unicode, tels que des accents. Cela inclut les paramètres qui peuvent être laissés vides lorsqu'une valeur par défaut est renseignée automatiquement. Assurez-vous que les valeurs par défaut correspondantes dans votre Active Directory ne contiennent pas non plus de caractères Unicode.

Si vous rencontrez des problèmes non répertoriés ici lors de l'utilisation d'Amazon FSx, posez une question sur le forum Amazon FSx ou contactez le support Amazon Web Services.

Le système de fichiers est mal configuré

Un système de fichiers FSx for Windows File Server peut se retrouver dans un état mal configuré en raison d'une modification de votre environnement Active Directory. Dans cet état, votre système de

fichiers est actuellement indisponible ou risque de perdre sa disponibilité, et les sauvegardes risquent d'échouer.

L'état Mauvais configuré inclut un message d'erreur et une action corrective recommandée auxquels vous pouvez accéder à l'aide de la console Amazon FSx, de l'API ou. AWS CLI Après avoir pris les mesures correctives, vérifiez que l'état de votre système de fichiers finit par changer en. Notez que cette modification peut prendre plusieurs minutes. `Available`

Votre système de fichiers peut se retrouver dans un état mal configuré pour plusieurs raisons, notamment les suivantes :

- Les adresses IP du serveur DNS ne sont plus valides.
- Les informations d'identification du compte de service ne sont plus valides ou ne disposent pas des autorisations requises.
- Le contrôleur de domaine Active Directory n'est pas accessible en raison de problèmes de connectivité réseau, tels que des groupes de sécurité VPC non valides, une configuration de l'ACL ou de la table de routage du réseau VPC, ou des paramètres de pare-feu du contrôleur de domaine.

(Pour obtenir la liste complète des exigences relatives à Active Directory, consultezConditions préalables à l'utilisation d'un Microsoft Active Directory autogéré. Vous pouvez également vérifier que votre environnement Active Directory est correctement configuré pour répondre à ces exigences en utilisant l'outil de validation Active Directory d'Amazon FSx.)

La résolution de certains de ces problèmes nécessite de mettre à jour directement un ou plusieurs paramètres de la configuration Active Directory de votre système de fichiers, tels que la modification des adresses IP du serveur DNS ou la modification du nom d'utilisateur ou du mot de passe du compte de service. Dans ces cas, votre action corrective impliquera nécessairement d'utiliser la console Amazon FSx, l'API ou de mettre AWS CLI à jour les paramètres de configuration requis.

D'autres problèmes peuvent ne pas nécessiter de modification des paramètres de configuration d'Active Directory, tels que la modification des paramètres de pare-feu de votre contrôleur de domaine ou des groupes de sécurité VPC. Dans ces cas, vous devrez toutefois prendre d'autres mesures avant que le système de fichiers ne le devienne`Available`. Après vous être assuré que votre environnement Active Directory est correctement configuré, sélectionnez le bouton Attempt Recovery à côté de l'état Mauvais configuré dans la console Amazon FSx, ou utilisez `StartMisconfiguredStateRecovery` la commande dans la console Amazon FSx, l'API ou. AWS CLI

Rubriques

Système de fichiers mal configuré : Amazon FSx ne peut accéder ni aux serveurs DNS ni aux contrôleurs de domaine de votre domaine.

Un système de fichiers passe dans un `Misconfigured` état où Amazon FSx ne peut pas communiquer avec votre ou vos contrôleurs de domaine Microsoft Active Directory.

Pour résoudre ce problème, procédez comme suit :

1. Assurez-vous que votre configuration réseau autorise le trafic entre le système de fichiers et le contrôleur de domaine.
2. Utilisez l'outil de validation Amazon FSx Active Directory pour tester et vérifier les paramètres réseau de votre Active Directory autogéré. Pour plus d'informations, consultez Utilisation d'Amazon FSx avec votre Microsoft Active Directory autogéré.
3. Passez en revue la configuration Active Directory autogérée du système de fichiers dans la console Amazon FSx.
4. Pour mettre à jour la configuration Active Directory autogérée du système de fichiers, vous pouvez utiliser la console Amazon FSx.

    a. Dans le volet de navigation, choisissez Systèmes de fichiers, puis le système de fichiers à mettre à jour ; la page de détails du système de fichiers apparaît.

    b. Sur la page des détails du système de fichiers, choisissez Mettre à jour dans l'onglet Réseau et sécurité.

Vous pouvez également utiliser la `update-file-system` commande Amazon FSx CLI ou l'opération API. UpdateFileSystem

Système de fichiers mal configuré : les informations d'identification du compte de service ne sont pas valides

Amazon FSx ne peut pas établir de connexion avec votre ou vos contrôleurs de domaine Microsoft Active Directory. Cela est dû au fait que les informations d'identification du compte de service fournies ne sont pas valides. Pour plus d'informations, consultez Utilisation d'Amazon FSx avec votre Microsoft Active Directory autogéré.

Pour résoudre le problème de configuration, procédez comme suit :

1. Vérifiez que vous utilisez le bon compte de service et que vous utilisez les informations d'identification correctes pour ce compte.
2. Mettez ensuite à jour la configuration du système de fichiers avec le compte de service ou les informations d'identification du compte corrects à l'aide de la console Amazon FSx.

   a. Dans le volet de navigation, choisissez Systèmes de fichiers, puis sélectionnez le système de fichiers mal configuré à mettre à jour.

   b. Sur la page des détails du système de fichiers, choisissez Mettre à jour dans l'onglet Réseau et sécurité.

   Vous pouvez également utiliser l'opération d'API Amazon FSx. `update-file-system` Pour en savoir plus, consultez le document UpdateFileSystemde référence des API Amazon FSx.

Système de fichiers mal configuré : le compte de service fourni n'est pas autorisé à joindre le système de fichiers au domaine

Amazon FSx ne peut pas établir de connexion avec vos contrôleurs de domaine Microsoft Active Directory. Cela est dû au fait que le compte de service fourni n'est pas autorisé à associer le système de fichiers au domaine avec l'unité d'organisation spécifiée.

Pour résoudre le problème de configuration, procédez comme suit :

1. Ajoutez les autorisations requises au compte de service Amazon FSx ou créez un nouveau compte de service avec les autorisations requises. Pour plus d'informations à ce sujet, consultez Délégation de privilèges à votre compte de service Amazon FSx .
2. Mettez ensuite à jour la configuration Active Directory autogérée du système de fichiers avec les nouvelles informations d'identification du compte de service. Pour mettre à jour la configuration, vous pouvez utiliser la console Amazon FSx.

   a. Dans le volet de navigation, choisissez Systèmes de fichiers, puis le système de fichiers à mettre à jour ; la page de détails du système de fichiers apparaît.

   b. Sur la page des détails du système de fichiers, choisissez Mettre à jour dans l'onglet Réseau et sécurité.

   Vous pouvez également utiliser l'opération d'API Amazon FSx. `update-file-system` Pour en savoir plus, consultez le document UpdateFileSystemde référence des API Amazon FSx.

Système de fichiers mal configuré : le compte de service ne peut plus associer d'ordinateurs au domaine

Amazon FSx ne peut pas établir de connexion avec vos contrôleurs de domaine Microsoft Active Directory. Dans ce cas, cela est dû au fait que le compte de service fourni a atteint le nombre maximum d'ordinateurs qu'il peut joindre au domaine.

Pour résoudre le problème de configuration, procédez comme suit :

1. Identifiez un autre compte de service ou créez un nouveau compte de service qui peut associer de nouveaux ordinateurs au domaine.
2. Mettez ensuite à jour la configuration Active Directory autogérée du système de fichiers avec les nouvelles informations d'identification du compte de service à l'aide de la console Amazon FSx.

   a. Dans le volet de navigation, choisissez Systèmes de fichiers, puis le système de fichiers à mettre à jour ; la page de détails du système de fichiers apparaît.

   b. Sur la page des détails du système de fichiers, choisissez Mettre à jour dans l'onglet Réseau et sécurité.

   Vous pouvez également utiliser l'opération d'API Amazon FSx. `update-file-system` Pour en savoir plus, consultez le document UpdateFileSystemde référence des API Amazon FSx.

Système de fichiers mal configuré : le compte de service n'a pas accès à l'unité d'organisation

Amazon FSx ne peut pas établir de connexion avec vos contrôleurs de domaine Microsoft Active Directory car le compte de service fourni n'a pas accès à l'unité d'organisation spécifiée.

Pour résoudre le problème de configuration, procédez comme suit :

1. Identifiez un autre compte de service ou créez un nouveau compte de service ayant accès à l'unité d'organisation.
2. Mettez ensuite à jour la configuration Active Directory autogérée du système de fichiers avec les nouvelles informations d'identification du compte de service.

    a. Dans le volet de navigation, choisissez Systèmes de fichiers, puis le système de fichiers à mettre à jour ; la page de détails du système de fichiers apparaît.

    b. Sur la page des détails du système de fichiers, choisissez Mettre à jour dans l'onglet Réseau et sécurité.

    Vous pouvez également utiliser l'opération d'API Amazon FSx. `update-file-system` Pour en savoir plus, consultez le document UpdateFileSystemde référence des API Amazon FSx.

Résolution des problèmes liés à l'utilisation de Remote Power Shell sur FSx for Windows File Server

Vous pouvez administrer vos systèmes de fichiers FSx for Windows File Server à l'aide de commandes de gestion à PowerShell distance personnalisées.

Rubriques

- La SxSmbShare commande New-F échoue avec une confiance unidirectionnelle
- Vous ne pouvez pas accéder à votre système de fichiers à l'aide de Remote PowerShell

La SxSmbShare commande New-F échoue avec une confiance unidirectionnelle

Amazon FSx ne prend pas en charge l'exécution de la `New-FSxSmbShare` PowerShell commande dans les cas où vous disposez d'une approbation unidirectionnelle et où le domaine dans lequel réside l'utilisateur n'est pas configuré pour approuver le domaine associé au système de fichiers Amazon FSx.

Vous pouvez résoudre ce problème en utilisant l'une des solutions suivantes :

- L'utilisateur exécutant la `New-FSxSmbShare` commande doit se trouver dans le même domaine que le système de fichiers FSx.
- Vous pouvez utiliser l'interface graphique fsmgmt.msc pour créer des partages sur votre système de fichiers. Pour plus d’informations, consultez Gestion des partages de fichiers à l'aide de l'interface graphique des dossiers partagés.

Vous ne pouvez pas accéder à votre système de fichiers à l'aide de Remote PowerShell

L'impossibilité de se connecter à votre système de fichiers à l'aide de Remote peut avoir plusieurs causes PowerShell, chacune ayant sa propre résolution, comme suit.

Pour vous assurer dans un premier temps que vous pouvez vous connecter correctement au Windows Remote PowerShell Endpoint, vous pouvez également exécuter un test de connectivité de base. Par exemple, vous pouvez exécuter la `test-netconnection endpoint -port 5985` commande.

Le groupe de sécurité du système de fichiers ne dispose pas des règles entrantes requises pour autoriser une connexion à distance PowerShell

Le groupe de sécurité du système de fichiers doit disposer d'une règle entrante autorisant le trafic sur le port 5985 afin d'établir une session à distance PowerShell . Pour plus d’informations, consultez Groupes de sécurité Amazon VPC.

Vous avez configuré une approbation externe entre le Microsoft Active Directory AWS géré et votre Active Directory local

Pour utiliser Amazon FSx Remote PowerShell avec l'authentification Kerberos, vous devez configurer une politique de groupe locale sur le client pour l'ordre de recherche dans les forêts. Pour plus d'informations, consultez la documentation Microsoft Configure Kerberos Forest Search Order (KFSO).

Une erreur de localisation de langue se produit lors de la tentative de lancement d'une PowerShell session à distance

Vous devez ajouter ce qui suit `-SessionOption` à votre commande : `-SessionOption (New-PSSessionOption -uiCulture "en-US")`

Voici deux exemples d'utilisation `-SessionOption` lors du lancement d'une PowerShell session à distance sur votre système de fichiers.

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName Windows Remote PowerShell
 Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {fsx-command} -SessionOption
 (New-PSSessionOption -uiCulture "en-US")
```

```
PS C:\Users\delegateadmin> Enter-Pssession -ComputerName Windows Remote PowerShell
 Endpoint -ConfigurationName FsxRemoteAdmin -SessionOption (New-PSSessionOption -
uiCulture "en-US")
```

Impossible de configurer le DFS-R sur un système de fichiers multi-AZ ou mono-AZ 2

Microsoft Distributed File System Replication (DFS-R) n'est pas prise en charge sur les systèmes de fichiers multi-AZ et mono-AZ 2.

Les systèmes de fichiers multi-AZ sont configurés de manière native pour assurer la redondance entre plusieurs zones d'accès. Utilisez le type de déploiement Multi-AZ pour une haute disponibilité dans plusieurs zones de disponibilité. Pour plus d'informations, consultez Disponibilité et durabilité : systèmes de fichiers mono-AZ et multi-AZ.

Les mises à jour de capacité de stockage ou de débit échouent

L'échec des demandes de mise à jour de la capacité de stockage et de débit du système de fichiers peut avoir plusieurs causes, chacune ayant sa propre résolution.

L'augmentation de la capacité de stockage échoue car Amazon FSx ne peut pas accéder à la clé de chiffrement KMS du système de fichiers

Une demande d'augmentation de la capacité de stockage a échoué car Amazon FSx n'a pas pu accéder à la clé de chiffrement du système de fichiers AWS Key Management Service (AWS KMS).

Vous devez vous assurer qu'Amazon FSx a accès à la AWS KMS clé afin d'exécuter l'action administrative. Utilisez les informations suivantes pour résoudre le problème d'accès aux clés.

- Si la clé KMS a été supprimée, vous devez créer un nouveau système de fichiers à partir d'une sauvegarde à l'aide d'une nouvelle clé KMS. Pour plus d’informations, consultez Procédure 2 : Création d'un système de fichiers à partir d'une sauvegarde. Vous pouvez réessayer la demande une fois que le nouveau système de fichiers sera disponible.
- Si la clé KMS est désactivée, réactivez-la, puis réessayez la demande d'augmentation de la capacité de stockage. Pour plus d'informations, consultez la section Activation et désactivation des clés dans le guide du AWS Key Management Service développeur.
- Si la clé n'est pas valide car elle est en attente de suppression, vous devez créer un nouveau système de fichiers à partir d'une sauvegarde à l'aide d'une nouvelle clé KMS. Vous pouvez réessayer la demande une fois que le nouveau système de fichiers sera disponible. Pour plus d’informations, consultez Procédure 2 : Création d'un système de fichiers à partir d'une sauvegarde.
- Si la clé n'est pas valide en raison de son importation en attente, vous devez attendre que l'importation soit terminée, puis réessayer la demande d'augmentation de la capacité de stockage.
- Si la limite d'attribution de la clé a été dépassée, vous devez demander une augmentation du nombre de subventions pour la clé. Pour plus d'informations, consultez la section Quotas de ressources dans le guide du AWS Key Management Service développeur. Lorsque l'augmentation du quota est accordée, réessayez la demande d'augmentation de la capacité de stockage.

La mise à jour de la capacité de stockage ou de débit échoue car l'Active Directory autogéré est mal configuré

La demande de mise à jour de la capacité de stockage ou du débit a échoué car Active Directory autogéré de votre système de fichiers est mal configuré.

Pour résoudre l'état mal configuré spécifique, consultezLe système de fichiers est mal configuré.

L'augmentation de la capacité de stockage échoue en raison d'une capacité de débit insuffisante

La demande d'augmentation de la capacité de stockage a échoué car la capacité de débit du système de fichiers est définie sur 8 Mo/s.

Augmentez la capacité de débit du système de fichiers à un minimum de 16 Mo/s, puis réessayez la demande. Pour plus d'informations, consultez Gestion de la capacité de débit.

La mise à jour de la capacité de débit à 8 Mo/s échoue

Une demande de modification de la capacité de débit d'un système de fichiers à 8 Mo/s a échoué.

Cela peut se produire lorsqu'une demande d'augmentation de capacité de stockage est en attente ou en cours. L'augmentation de la capacité de stockage nécessite un débit minimum de 16 Mo/s. Attendez que la demande d'augmentation de la capacité de stockage soit terminée, puis réessayez la demande de modification de la capacité de débit.

Le passage du type de stockage au disque dur lors de la restauration d'une sauvegarde échoue

La création d'un système de fichiers à partir d'une sauvegarde échoue avec le message d'erreur suivant :

```
Switching storage type to HDD while creating a file system from backup backup_id is not supported because a storage scaling activity was still under way on the source file system to increase storage capacity from less than 2000 GiB when the backup backup_id was taken, and the minimum storage capacity for HDD storage is 2000 GiB.
```

Ce problème se produit lors de la restauration d'une sauvegarde et que vous avez changé le type de stockage de SSD à HDD. La restauration à partir d'une sauvegarde échoue car la sauvegarde que vous restaurez a été effectuée alors qu'une augmentation de la capacité de stockage était toujours en cours sur le système de fichiers d'origine. La capacité de stockage SSD du système de fichiers avant la demande d'augmentation était inférieure à 2 000 GiB, soit la capacité de stockage minimale requise pour créer un système de fichiers HDD.

Suivez la procédure ci-dessous pour résoudre ce problème.

1. Attendez que la demande d'augmentation de la capacité de stockage soit terminée et que le système de fichiers dispose d'au moins 2 000 GiB de capacité de stockage SSD. Pour plus d'informations, consultez Surveillance de l'augmentation de la capacité de stockage.
2. Effectuez une sauvegarde du système de fichiers initiée par l'utilisateur. Pour plus d'informations, consultez Utilisation de sauvegardes initiées par l'utilisateur.
3. Restaurez la sauvegarde initiée par l'utilisateur sur un nouveau système de fichiers à l'aide du stockage sur disque dur. Pour plus d'informations, consultez Restauration des sauvegardes.

Résolution des problèmes de clichés instantanés

Les clichés instantanés peuvent être absents ou inaccessibles pour plusieurs raisons, comme décrit dans la section suivante.

Rubriques

- Les copies instantanées les plus anciennes sont manquantes
- Toutes mes copies instantanées sont manquantes
- Impossible de créer des sauvegardes Amazon FSx ou d'accéder à des copies instantanées sur un système de fichiers récemment restauré ou mis à jour

Les copies instantanées les plus anciennes sont manquantes

Les clichés instantanés les plus anciens sont supprimés dans l'une des situations suivantes :

- Si vous avez 500 clichés instantanés, le cliché instantané suivant remplace le cliché instantané le plus ancien, quel que soit l'espace de stockage restant alloué aux clichés instantanés.

- Si la quantité maximale de stockage de cliché instantané configurée est atteinte, le cliché instantané suivant remplace un ou plusieurs des clichés instantanés les plus anciens, même si vous en avez moins de 500.

Les deux résultats sont un comportement attendu. Si l'espace de stockage alloué aux clichés instantanés est insuffisant, envisagez d'augmenter l'espace que vous avez alloué.

Toutes mes copies instantanées sont manquantes

Une capacité d'E/S insuffisante sur votre système de fichiers (par exemple, parce que vous utilisez du stockage sur disque dur, parce que la capacité de stockage sur disque dur est épuisée ou parce que la capacité de débit est insuffisante) peut entraîner la suppression de tous les clichés instantanés par Windows Server, car celui-ci n'est pas en mesure de conserver les clichés instantanés avec la capacité de performance d'E/S disponible. Tenez compte des recommandations suivantes pour éviter ce problème :

- Si vous utilisez le stockage sur disque dur, utilisez la console Amazon FSx ou l'API Amazon FSx pour passer au stockage SSD. Pour plus d’informations, consultez Gestion du type de stockage.
- Augmentez la capacité de débit du système de fichiers jusqu'à une valeur trois fois supérieure à la charge de travail attendue.
- Assurez-vous que votre système de fichiers dispose d'au moins 320 Mo d'espace libre, en plus de la quantité maximale de stockage de clichés instantanés configurée.
- Planifiez des clichés instantanés lorsque vous vous attendez à ce que votre système de fichiers soit inactif.

Pour plus d’informations, consultez Recommandations relatives aux systèmes de fichiers pour les clichés instantanés.

Impossible de créer des sauvegardes Amazon FSx ou d'accéder à des copies instantanées sur un système de fichiers récemment restauré ou mis à jour

Ce comportement est normal. Amazon FSx reconstruit l'état du cliché instantané sur un système de fichiers récemment restauré et n'autorise pas l'accès aux clichés instantanés ou aux sauvegardes lors de la reconstruction de l'état du cliché instantané.

Résolution des problèmes de performances du système de fichiers

Les performances du système de fichiers dépendent de plusieurs facteurs, notamment le trafic que vous générez vers votre système de fichiers, la manière dont vous le provisionnez et les fonctionnalités activées, telles que la déduplication des données ou les clichés instantanés. Pour plus d'informations sur la compréhension des performances de votre système de fichiers, consultezPerformances de FSx for Windows File Server.

Rubriques

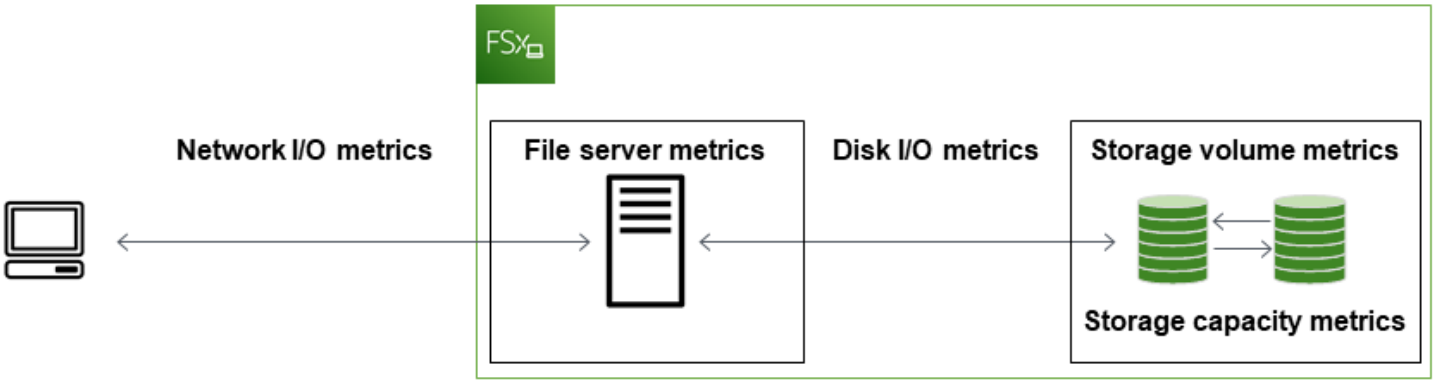
Comment déterminer le débit et les limites d'IOPS pour mon système de fichiers ?

Pour consulter le débit et les limites d'IOPS d'un système de fichiers, reportez-vous au tableau indiquant les niveaux de performance en fonction de la capacité de débit de provisionnement.

Quelle est la différence entre les E/S réseau et les E/S disque ? Pourquoi mes E/S réseau sont-elles différentes de mes E/S sur disque ?

Les systèmes de fichiers Amazon FSx incluent un ou plusieurs serveurs de fichiers qui fournissent des données via le réseau aux clients accédant au système de fichiers. Il s'agit des E/S réseau. Le serveur de fichiers dispose d'un cache rapide en mémoire pour améliorer les performances des données les plus fréquemment consultées. Les serveurs de fichiers génèrent également du trafic vers les volumes de stockage hébergeant les données de votre système de fichiers. Il s'agit des E/

S de disque. Le schéma suivant illustre les E/S de réseau et de disque pour un système de fichiers Amazon FSx.



Pour plus d'informations, consultez Surveillance des métriques avec Amazon CloudWatch.

Pourquoi l'utilisation de mon processeur ou de ma mémoire est-elle élevée, même lorsque mes E/S réseau sont faibles ?

L'utilisation du processeur et de la mémoire du serveur de fichiers dépend non seulement du trafic réseau que vous transportez, mais également des fonctionnalités que vous avez activées sur votre système de fichiers. La façon dont vous configurez et planifiez ces fonctionnalités peut avoir un impact sur l'utilisation du processeur et de la mémoire.

Les tâches de déduplication des données en cours peuvent consommer de la mémoire. Vous pouvez modifier la configuration des tâches de déduplication afin de réduire les besoins en mémoire. Par exemple, vous pouvez limiter l'optimisation pour qu'elle s'exécute sur des types de fichiers ou des dossiers spécifiques, ou définir une taille et un âge de fichier minimaux pour l'optimisation. Nous recommandons également de configurer les tâches de déduplication pour qu'elles s'exécutent pendant les périodes d'inactivité lorsque la charge de votre système de fichiers est minimale. Pour plus d'informations, consultez Déduplication des données.

Si l'énumération basée sur l'accès est activée, vous pouvez constater une utilisation élevée du processeur lorsque vos utilisateurs finaux consultent ou répertorient les partages de fichiers, ou pendant la phase d'optimisation d'une tâche de dimensionnement du stockage. Pour plus d'informations, voir Activer l'énumération basée sur l'accès sur un espace de noms dans la documentation Microsoft Storage.

Qu'est-ce que l'éclatement ? Quelle est la quantité de rafale utilisée par mon système de fichiers ? Que se passe-t-il lorsque les crédits de rafale sont épuisés ?

Les charges de travail basées sur des fichiers sont généralement élevées, caractérisées par des périodes courtes et intenses d'E/S élevées avec des temps d'inactivité entre les rafales. Pour prendre en charge ces types de charges de travail, outre les vitesses de base qu'un système de fichiers peut supporter, Amazon FSx permet d'atteindre des vitesses plus élevées pendant des périodes de temps, à la fois pour les opérations d'E/S réseau et d'E/S sur disque.

Amazon FSx utilise un mécanisme de crédit d'E/S pour allouer le débit et les IOPS en fonction de l'utilisation moyenne. Les systèmes de fichiers accumulent des crédits lorsque leur débit et leur utilisation d'IOPS sont inférieurs à leurs limites de base, et peuvent utiliser ces crédits pour dépasser les limites de base (jusqu'aux limites de rafale) lorsque cela est nécessaire. Pour plus d'informations sur les limites et la durée des rafales pour votre système de fichiers, consultezPerformances de FSx for Windows File Server.

Un avertissement s'affiche sur la page Surveillance et performances. Dois-je modifier la configuration de mon système de fichiers ?

La page Surveillance et performances inclut des avertissements qui indiquent lorsque les récentes demandes de charge de travail ont atteint ou dépassé les limites de ressources déterminées par la façon dont vous avez configuré votre système de fichiers. Cela ne signifie pas nécessairement que vous devez modifier votre configuration, même si votre système de fichiers risque d'être sous-approvisionné pour votre charge de travail si vous ne prenez pas les mesures recommandées.

Si la charge de travail à l'origine de l'avertissement était atypique et que vous ne vous attendez pas à ce qu'elle continue, il peut être prudent de ne rien faire et de surveiller de près votre utilisation à l'avenir. Toutefois, si la charge de travail à l'origine de l'avertissement est typique et que vous vous attendez à ce qu'elle continue, voire s'intensifie, nous vous conseillons de suivre les mesures recommandées pour améliorer les performances du serveur de fichiers (en augmentant la capacité de débit) ou en augmentant les performances du volume de stockage (en augmentant la capacité de stockage ou en passant du stockage sur disque dur au stockage SSD).

> **Note**
>
> Certains événements du système de fichiers peuvent consommer les ressources de performance des E/S du disque et potentiellement déclencher des avertissements de performance. Par exemple :
>
> - La phase d'optimisation de la mise à l'échelle de la capacité de stockage peut générer une augmentation du débit du disque, comme décrit dans Augmentation de la capacité de stockage et des performances du système de fichiers
> - Pour les systèmes de fichiers multi-AZ, des événements tels que l'augmentation de la capacité de débit, le remplacement du matériel ou l'interruption de la zone de disponibilité entraînent des événements de basculement et de retour en arrière automatiques. Toute modification de données survenant pendant cette période doit être synchronisée entre les serveurs de fichiers principal et secondaire, et Windows Server exécute une tâche de synchronisation des données susceptible de consommer des ressources d'E/S de disque. Pour plus d’informations, consultez Gestion de la capacité de débit.

Mes statistiques étaient temporairement absentes, dois-je m'inquiéter ?

Les systèmes de fichiers mono-AZ seront indisponibles pendant la maintenance du système de fichiers, le remplacement des composants de l'infrastructure et lorsqu'une zone de disponibilité n'est pas disponible. Pendant ces périodes, les statistiques ne seront pas disponibles.

Dans un déploiement multi-AZ, Amazon FSx provisionne et gère automatiquement un serveur de fichiers de secours dans une autre zone de disponibilité. En cas de maintenance du système de fichiers ou d'interruption de service imprévue, Amazon FSx bascule automatiquement vers le serveur de fichiers secondaire, ce qui vous permet de continuer à accéder à vos données sans intervention manuelle. Au cours de la brève période au cours de laquelle votre système de fichiers bascule puis revient en panne, les métriques peuvent être temporairement indisponibles.

Informations supplémentaires

Cette section fournit une référence des fonctionnalités Amazon FSx prises en charge mais obsolètes.

Rubriques

Configuration d'un calendrier de sauvegarde personnalisé

Nous vous recommandons AWS Backup de l'utiliser pour configurer un calendrier de sauvegarde personnalisé pour votre système de fichiers. Les informations fournies ici sont fournies à titre de référence si vous devez planifier des sauvegardes plus fréquemment que lorsque vous les utilisez AWS Backup.

Lorsque cette option est activée, Amazon FSx for Windows File Server effectue automatiquement une sauvegarde de votre système de fichiers une fois par jour pendant une fenêtre de sauvegarde quotidienne. Amazon FSx applique une période de rétention que vous spécifiez pour ces sauvegardes automatiques. Il prend également en charge les sauvegardes initiées par l'utilisateur, ce qui vous permet d'effectuer des sauvegardes à tout moment.

Vous trouverez ci-dessous les ressources et la configuration nécessaires pour déployer une planification de sauvegarde personnalisée. La planification des sauvegardes personnalisées effectue des sauvegardes initiées par l'utilisateur sur un système de fichiers Amazon FSx selon un calendrier personnalisé que vous définissez. Par exemple, une fois toutes les six heures, une fois par semaine, etc. Ce script configure également la suppression des sauvegardes antérieures à la période de rétention spécifiée.

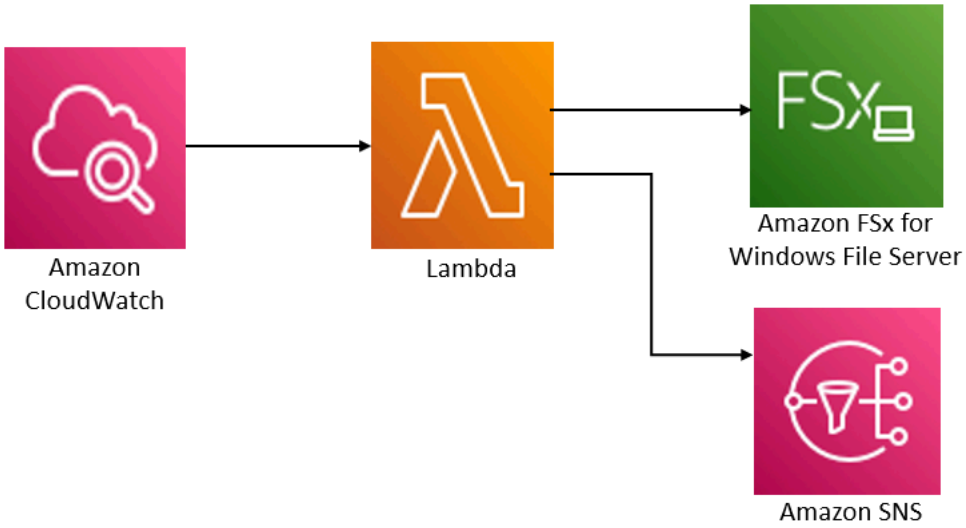
La solution déploie automatiquement tous les composants nécessaires et prend en compte les paramètres suivants :

- Le système de fichiers
- Un modèle de planification CRON pour effectuer des sauvegardes
- Période de conservation des sauvegardes (en jours)
- Les balises de nom de sauvegarde

Pour plus d'informations sur les modèles de planification CRON, consultez la section Expressions de planification pour les règles dans le guide de CloudWatch l'utilisateur Amazon.

Présentation de l’architecture

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



Cette solution effectue les opérations suivantes :

1. Le AWS CloudFormation modèle déploie un CloudWatch événement, une fonction Lambda, une file d'attente Amazon SNS et un rôle IAM. Le rôle IAM autorise la fonction Lambda à appeler les opérations de l'API Amazon FSx.
2. L' CloudWatch événement s'exécute selon un calendrier que vous définissez sous la forme d'un modèle CRON, lors du déploiement initial. Cet événement appelle la fonction Lambda du gestionnaire de sauvegarde de la solution qui appelle l'opération d'API Amazon `CreateBackup` FSx pour lancer une sauvegarde.
3. Le gestionnaire de sauvegarde extrait une liste des sauvegardes existantes initiées par l'utilisateur pour le système de fichiers spécifié à l'aide de. `DescribeBackups` Il supprime ensuite les sauvegardes antérieures à la période de rétention, que vous avez spécifiée lors du déploiement initial.
4. Le gestionnaire de sauvegarde envoie un message de notification à la file d'attente Amazon SNS en cas de sauvegarde réussie si vous choisissez l'option d'être averti lors du déploiement initial. Une notification est toujours envoyée en cas de panne.

AWS CloudFormation modèle

Cette solution permet AWS CloudFormation d'automatiser le déploiement de la solution de planification de sauvegarde personnalisée Amazon FSx. Pour utiliser cette solution, téléchargez le modèle AWS CloudFormation fsx-scheduled-backup.template.

Déploiement automatique

La procédure suivante permet de configurer et de déployer cette solution de planification de sauvegarde personnalisée. Le déploiement prend environ cinq minutes. Avant de commencer, vous devez disposer de l'ID d'un système de fichiers Amazon FSx exécuté dans un Amazon Virtual Private Cloud (Amazon VPC) sur votre compte. AWS Pour plus d'informations sur la création de ces ressources, consultezCommencer à utiliser Amazon FSx for Windows File Server.

> **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.

Pour lancer la pile de solutions de sauvegarde personnalisée

1. Téléchargez le modèle AWS CloudFormation fsx-scheduled-backup.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). Amazon FSx n'est actuellement disponible que de manière spécifique. Régions AWS Vous devez lancer cette solution dans une AWS région où Amazon FSx est disponible. Pour plus d'informations, consultez la section Amazon FSx Régions AWS et les points de terminaison 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
ID du système de fichiers Amazon FSx	Aucune valeur par défaut	ID du système de fichiers que vous souhaitez sauvegarder.
Modèle de planification CRON pour les sauvegardes.	0 0/4 * * ? *	Planification de l'exécution de l' CloudWatch événement, du déclenchement d'une nouvelle sauvegarde et de la suppression des anciennes sauvegardes en dehors de la période de conservation.
Conservation des sauvegardes (jours)	30	Nombre de jours pendant lesquels les sauvegardes initiées par l'utilisateur sont conservées. La fonction Lambda supprime les sauvegardes initiées par l'utilisateur datant de plus de ce nombre de jours.
Nom des sauvegardes	sauvegarde planifiée par l'utilisateur	Le nom de ces sauvegardes, qui apparaît dans la colonne Backup Name de la console de gestion Amazon FSx.
Notifications de sauvegarde	Oui	Choisissez si vous souhaitez être averti lorsque les sauvegardes sont lancées avec succès. Une notification est toujours envoyée en cas d'erreur.

Paramètre	Par défaut	Description
Adresse e-mail	Aucune valeur par défaut	Adresse e-mail pour s'abonner aux notifications SNS.

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.

Options supplémentaires

Vous pouvez utiliser la fonction Lambda créée par cette solution pour effectuer des sauvegardes planifiées personnalisées de plusieurs systèmes de fichiers Amazon FSx. L'ID du système de fichiers est transmis à la fonction Amazon FSx dans le JSON d'entrée pour l' CloudWatch événement. Le JSON par défaut transmis à la fonction Lambda est le suivant, où les valeurs pour `FileSystemId` et `SuccessNotification` sont transmises à partir des paramètres spécifiés lors du lancement de la AWS CloudFormation pile.

```
{
 "start-backup": "true",
 "purge-backups": "true",
 "filesystem-id": "${FileSystemId}",
 "notify_on_success": "${SuccessNotification}"
}
```

Pour planifier des sauvegardes pour un système de fichiers Amazon FSx supplémentaire, créez une autre règle d' CloudWatch événement. Pour ce faire, utilisez la source d'événements Schedule, avec la fonction Lambda créée par cette solution comme cible. Choisissez Constant (texte JSON) sous Configurer l'entrée. À l'entrée JSON, il suffit de remplacer l'ID du système de fichiers Amazon FSx par l'ID du système de fichiers Amazon FSx à sauvegarder. `${FileSystemId}` Remplacez également l'`Yes`un ou `No` l'autre `${SuccessNotification}` dans le JSON ci-dessus.

Les règles d' CloudWatch événement supplémentaires que vous créez manuellement ne font pas partie de la pile de solutions AWS CloudFormation de sauvegarde planifiée personnalisées Amazon FSx. Ils ne sont donc pas supprimés si vous supprimez la pile.

Utilisation de la réplication de systèmes de fichiers distribués Microsoft

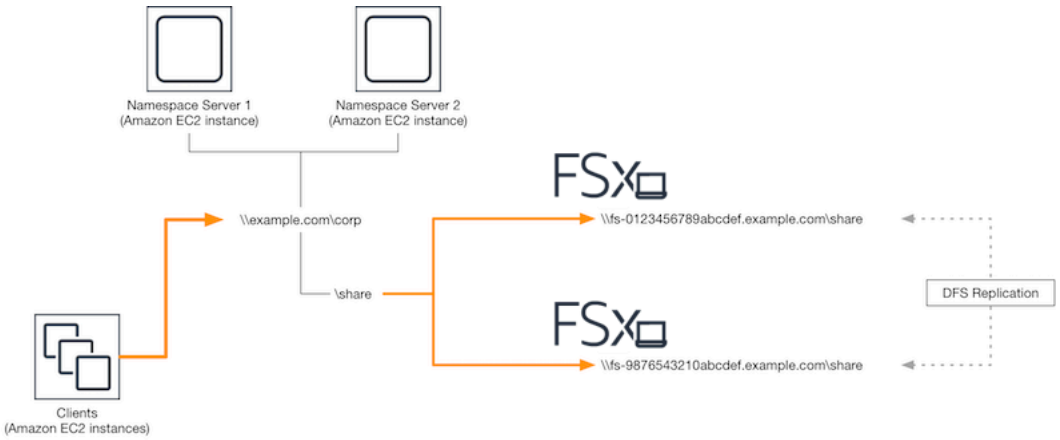
> **Note**
>
> Pour implémenter la haute disponibilité pour un serveur de fichiers FSx for Windows, nous vous recommandons d'utiliser Amazon FSx Multi-AZ. Pour plus d'informations sur Amazon FSx Multi-AZ, consultez Disponibilité et durabilité : systèmes de fichiers mono-AZ et multi-AZ

Amazon FSx prend en charge l'utilisation du système de fichiers distribué Microsoft (DFS) pour les déploiements de systèmes de fichiers dans plusieurs zones de disponibilité (AZ) afin d'obtenir une disponibilité et une durabilité multi-AZ. La réplication DFS vous permet de répliquer automatiquement les données entre deux systèmes de fichiers. À l'aide des espaces de noms DFS, vous pouvez configurer un système de fichiers en tant que système principal et l'autre en tant que système de secours, avec basculement automatique vers le système de secours si le système principal ne répond plus.

Avant d'utiliser la réplication DFS, procédez comme suit :

- Configurez vos groupes de sécurité comme décrit dans Step 8 Getting Started with Amazon FSx.
- Créez deux systèmes de fichiers Amazon FSx dans des zones de disponibilité différentes au sein d'une AWS région. Pour plus d'informations sur la création de vos systèmes de fichiers, consultezÉcrire des données dans votre partage de fichiers.
- Assurez-vous que les deux systèmes de fichiers sont identiques AWS Directory Service for Microsoft Active Directory.
- Une fois les systèmes de fichiers créés, notez leurs identifiants pour plus tard.

Dans les rubriques suivantes, vous trouverez une description de la configuration et de l'utilisation de la réplication DFS et du basculement des espaces de noms DFS entre les zones de disponibilité avec Amazon FSx.



Configuration de la réplication DFS

Vous pouvez utiliser la réplication DFS pour répliquer automatiquement les données entre deux systèmes de fichiers Amazon FSx. Cette réplication est bidirectionnelle, ce qui signifie que vous pouvez écrire dans l'un ou l'autre système de fichiers et que les modifications sont répliquées dans l'autre.

> **Important**
>
> Vous ne pouvez pas utiliser l'interface utilisateur de gestion DFS dans les outils d'administration Microsoft Windows (dfsmgmt.msc) pour configurer la réplication DFS sur votre système de fichiers FSx for Windows File Server.

Pour configurer la réplication DFS (scriptée)

1. Commencez le processus de gestion de DFS en lançant votre instance et en la connectant au Microsoft Active Directory où vous avez rejoint vos systèmes de fichiers Amazon FSx. Pour ce faire, choisissez l'une des procédures suivantes dans le guide AWS Directory Service d'administration :

   - Jonction facile d'une instance EC2 Windows
   - Jonction manuelle d'une instance Windows

2. Connectez-vous à votre instance en tant qu'utilisateur Active Directory membre du groupe des administrateurs du système de fichiers. Dans AWS Managed AD, ce groupe est appelé AWS Administrateurs FSx délégués. Dans votre Microsoft AD autogéré, ce groupe est appelé

Administrateurs de domaine ou le nom personnalisé du groupe d'administrateurs que vous avez indiqué lors de la création.

Cet utilisateur doit également être membre d'un groupe auquel des autorisations d'administration DFS lui ont été déléguées. Dans AWS Managed AD, ce groupe est appelé Administrateurs de systèmes de fichiers distribués AWS délégués. Dans votre AD autogéré, cet utilisateur doit être membre des administrateurs de domaine ou d'un autre groupe auquel vous avez délégué des autorisations d'administration DFS.

Pour plus d'informations, consultez la section Connexion à votre instance Windows dans le guide de l'utilisateur Amazon EC2.

3. Téléchargez le script FSX-DFSR-Setup.ps1 PowerShell .
4. Ouvrez le menu Démarrer et entrez PowerShell. Dans la liste, sélectionnez Windows PowerShell.
5. Exécutez le PowerShell script avec les paramètres spécifiés suivants pour établir la réplication DFS entre vos deux systèmes de fichiers :

   - Les noms du groupe et du dossier de réplication DFS
   - Le chemin local vers le dossier que vous souhaitez répliquer sur vos systèmes de fichiers (par exemple, `D:\share` pour le partage par défaut inclus dans votre système de fichiers Amazon FSx)
   - Les noms DNS des systèmes de fichiers Amazon FSx principal et de secours que vous avez créés lors des étapes préalables

   Example

   ```
   FSx-DFSr-Setup.ps1 -group Group -folder Folder -path ContentPath -
   primary FSxFileSystem1-DNS-Name -standby FSxFileSystem2-DNS-Name
   ```

Pour configurer la réplication DFS (étape par étape)

1. Commencez le processus de gestion de DFS en lançant votre instance et en la connectant au Microsoft Active Directory où vous avez rejoint vos systèmes de fichiers Amazon FSx. Pour ce faire, choisissez l'une des procédures suivantes dans le guide AWS Directory Service d'administration :

- Jonction facile d'une instance EC2 Windows
- Jonction manuelle d'une instance Windows

2. Connectez-vous à votre instance en tant qu'utilisateur Active Directory membre du groupe des administrateurs du système de fichiers. Dans AWS Managed AD, ce groupe est appelé AWS Administrateurs FSx délégués. Dans votre Microsoft AD autogéré, ce groupe est appelé Administrateurs de domaine ou le nom personnalisé du groupe d'administrateurs que vous avez indiqué lors de la création.

   Cet utilisateur doit également être membre d'un groupe auquel des autorisations d'administration DFS lui ont été déléguées. Dans AWS Managed AD, ce groupe est appelé Administrateurs de systèmes de fichiers distribués AWS délégués. Dans votre AD autogéré, cet utilisateur doit être membre des administrateurs de domaine ou d'un autre groupe auquel vous avez délégué des autorisations d'administration DFS.

   Pour plus d'informations, consultez la section Connexion à votre instance Windows dans le guide de l'utilisateur Amazon EC2.

3. Ouvrez le menu Démarrer et entrez PowerShell. Dans la liste, sélectionnez Windows PowerShell.

4. Si les outils de gestion DFS ne sont pas déjà installés, installez-les sur votre instance à l'aide de la commande suivante.

```
Install-WindowsFeature RSAT-DFS-Mgmt-Con
```

5. À l' PowerShell invite, créez un groupe et un dossier de réplication DFS à l'aide des commandes suivantes.

```
$Group = "Name of the DFS Replication group"
$Folder = "Name of the DFS Replication folder"

New-DfsReplicationGroup -GroupName $Group
New-DfsReplicatedFolder -GroupName $Group -FolderName $Folder
```

6. Déterminez le nom de l'ordinateur Active Directory associé à chaque système de fichiers à l'aide des commandes suivantes.

```
$Primary = "DNS name of the primary FSx file system"
$Standby = "DNS name of the standby FSx file system"
```

```
$C1 = (Get-ADObject -Filter "objectClass -eq 'Computer' -and ServicePrincipalName -
eq 'HOST/$Primary'").Name
$C2 = (Get-ADObject -Filter "objectClass -eq 'Computer' -and ServicePrincipalName -
eq 'HOST/$Standby'").Name
```

7. Ajoutez vos systèmes de fichiers en tant que membres du groupe de réplication DFS que vous avez créé à l'aide des commandes suivantes.

```
Add-DfsrMember –GroupName $Group –ComputerName $C1
Add-DfsrMember –GroupName $Group –ComputerName $C2
```

8. Utilisez les commandes suivantes pour ajouter le chemin local (par exemple,`D:\share`) de chaque système de fichiers au groupe de réplication DFS. Dans cette procédure, *`file system 1`* joue le rôle de membre principal, ce qui signifie que son contenu est initialement synchronisé avec l'autre système de fichiers.

```
$ContentPath1 = "Local path to the folder you want to replicate on file system 1"
$ContentPath2 = "Local path to the folder you want to replicate on file system 2"

Set-DfsrMembership –GroupName $Group –FolderName $Folder –ContentPath $ContentPath1
 –ComputerName $C1 –PrimaryMember $True
Set-DfsrMembership –GroupName $Group –FolderName $Folder –ContentPath $ContentPath2
 –ComputerName $C2 –PrimaryMember $False
```

9. Ajoutez une connexion entre les systèmes de fichiers à l'aide de la commande suivante.

```
Add-DfsrConnection –GroupName $Group –SourceComputerName $C1 –
DestinationComputerName $C2
```

Dans les minutes qui suivent, les deux systèmes de fichiers devraient commencer à synchroniser le contenu du système `ContentPath` spécifié ci-dessus.

Configuration des espaces de noms DFS pour le basculement

Vous pouvez utiliser les espaces de noms DFS pour traiter un système de fichiers comme votre système de fichiers principal et l'autre comme votre système de secours. Vous pouvez ainsi configurer le basculement automatique vers le mode veille si le système principal ne répond plus. Les espaces de noms DFS vous permettent de regrouper des dossiers partagés sur différents serveurs en un seul espace de noms, où un chemin de dossier unique peut mener à des fichiers stockés sur plusieurs serveurs. Les espaces de noms DFS sont gérés par des serveurs d'espaces de noms DFS,

qui dirigent les instances de calcul mappant un dossier d'espace de noms DFS vers les serveurs de fichiers appropriés.

Pour configurer des espaces de noms DFS pour le basculement (interface utilisateur)

1. Si aucun serveur d'espace de noms DFS n'est déjà actif, lancez deux serveurs d'espaces de noms DFS à haut niveau de disponibilité à l'aide du modèle Setup-DFSN-Servers.template. AWS CloudFormation 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.
2. Connectez-vous à l'un des serveurs d'espace de noms DFS lancés à l'étape précédente en tant qu'utilisateur du groupe Administrateurs AWS délégués. Pour plus d'informations, consultez la section Connexion à votre instance Windows dans le guide de l'utilisateur Amazon EC2.
3. Ouvrez la console de gestion DFS. Ouvrez le menu Démarrer et lancez`dfsmgmt.msc`. Cela ouvre l'outil d'interface graphique de gestion DFS.
4. Dans Action, choisissez Nouvel espace de noms, entrez le nom d'ordinateur du premier serveur d'espace de noms DFS que vous avez lancé pour Server, puis choisissez Next.
5. Dans Nom, entrez l'espace de noms que vous créez (par exemple,**`corp`**).
6. Choisissez Modifier les paramètres et définissez les autorisations appropriées en fonction de vos besoins. Choisissez Suivant.
7. Conservez l'option d'espace de noms par défaut basée sur le domaine sélectionnée, maintenez l'option Activer le mode Windows Server 2008 sélectionnée et choisissez Next.

   > **Note**
   >
   > Le mode Windows Server 2008 est la dernière option disponible pour les espaces de noms.

8. Vérifiez les paramètres de l'espace de noms et choisissez Create.
9. Lorsque le nouvel espace de noms est sélectionné sous Espaces de noms dans la barre de navigation, choisissez Action, puis Ajouter un serveur d'espace de noms.
10. Pour Namespace server, entrez le nom d'ordinateur du deuxième serveur d'espace de noms DFS que vous avez lancé.
11. Choisissez Modifier les paramètres, définissez les autorisations appropriées en fonction de vos besoins, puis cliquez sur OK.

12. ***Choisissez Ajouter, entrez le nom UNC du partage de fichiers sur le système de fichiers Amazon FSx principal (par exemple \ \ fs-0123456789abcdef0 .example.com \ share) pour Path to folder target, puis cliquez sur OK.***
13. ***Choisissez Ajouter, entrez le nom UNC du partage de fichiers sur le système de fichiers Amazon FSx de secours (par exemple, \ \ fs-fedbca9876543210f .example.com \ share) pour Path to folder target, puis cliquez sur OK.***
14. Dans la fenêtre Nouveau dossier, cliquez sur OK. Le nouveau dossier est créé avec les deux cibles de dossier situées sous votre espace de noms.
15. Répétez les trois dernières étapes pour chaque partage de fichiers que vous souhaitez ajouter à votre espace de noms.

Pour configurer les espaces de noms DFS pour Failover () PowerShell

1. Si aucun serveur d'espace de noms DFS n'est déjà actif, lancez deux serveurs d'espaces de noms DFS à haut niveau de disponibilité à l'aide du modèle Setup-DFSN-Servers.template. AWS CloudFormation 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.
2. Connectez-vous à l'un des serveurs d'espace de noms DFS lancés à l'étape précédente en tant qu'utilisateur du groupe Administrateurs AWS délégués. Pour plus d'informations, consultez la section Connexion à votre instance Windows dans le guide de l'utilisateur Amazon EC2.
3. Ouvrez le menu Démarrer et entrez PowerShell. Windows PowerShell apparaît dans la liste des correspondances.
4. Ouvrez le menu contextuel (clic droit) pour Windows PowerShell et choisissez Exécuter en tant qu'administrateur.
5. Si les outils de gestion DFS ne sont pas encore installés, installez-les sur votre instance à l'aide de la commande suivante.

```
Install-WindowsFeature RSAT-DFS-Mgmt-Con
```

6. Si vous ne possédez pas encore d'espace de noms DFS, vous pouvez en créer un à l'aide des commandes suivantes PowerShell .

```
$NSS1 = computer name of the 1st DFS Namespace server
```

```
$NSS2 = computer name of the 2nd DFS Namespace server

$DNSRoot = fully qualified Active Directory domain name (e.g. mydomain.com)
$Namespace = Namespace name you want to use
$Folder = Folder path you want to use within the Namespace
$FS1FolderTarget = Share path to Folder Target on File System 1
$FS2FolderTarget = Share path to Folder Target on File System 2

$NSS1,$NSS2 | ForEach-Object { Invoke-Command -ComputerName $_ -ScriptBlock { mkdir
 “C:\DFS\${using:Namespace}”;
New-SmbShare -Name ${using:Namespace} -Path “C:\DFS\${using:Namespace}” } }

New-DfsnRoot -Path "\\${DNSRoot}\${Namespace}" -TargetPath "\\${NSS1}.${DNSRoot}\
${Namespace}" -Type DomainV2
New-DfsnRootTarget -Path "\\${DNSRoot}\${Namespace}" -TargetPath "\\${NSS2}.
${DNSRoot}\${Namespace}"
```

7. Pour créer un dossier dans votre espace de noms DFS, vous pouvez utiliser la commande suivante PowerShell. Cela crée un dossier qui dirige les instances de calcul accédant au dossier vers votre système de fichiers Amazon FSx principal par défaut.

```
$FS1 = DNS name of primary FSx file system
New-DfsnFolder -Path “\\${DNSRoot}\${Namespace}\${Folder}" -TargetPath “\\${FS1}\
${FS1FolderTarget}” -EnableTargetFailback $True -ReferralPriorityClass GlobalHigh
```

8. Ajoutez votre système de fichiers Amazon FSx de secours dans le même dossier d'espace de noms DFS. Les instances de calcul qui accèdent au dossier retournent vers ce système de fichiers si elles ne peuvent pas se connecter au système de fichiers Amazon FSx principal.

```
$FS2 = DNS name of secondary FSx file system
New-DfsnFolderTarget -Path “\\${DNSRoot}\${Namespace}\${Folder}" -TargetPath “\\
${FS2}\${FS2FolderTarget}”
```

Vous pouvez désormais accéder à vos données à partir d'instances de calcul en utilisant le chemin distant du dossier DFS Namespace spécifié précédemment. Cela dirige les instances de calcul vers le système de fichiers Amazon FSx principal (et vers le système de fichiers de secours, si le système de fichiers principal ne répond pas).

Par exemple, ouvrez le menu Démarrer et entrez`PowerShell`. Dans la liste, sélectionnez `Windows PowerShell` et exécutez la commande suivante.

```
net use Z: \\${DNSRoot}\${Namespace}\${Folder} /persistent:yes
```

Utilisation de Windows de maintenance et de FSx Multi-AZ

Pour garantir la haute disponibilité de votre déploiement de système de fichiers multi-AZ, nous vous recommandons de choisir des fenêtres de maintenance qui ne se chevauchent pas pour les deux systèmes de fichiers Amazon FSx dans votre déploiement multi-AZ. Cela permet de garantir que les données de vos fichiers restent accessibles à vos applications et à vos utilisateurs pendant les fenêtres de maintenance du système.

> **Note**
>
> Pour autoriser le trafic de réplication DFS à destination et en provenance des systèmes de fichiers, assurez-vous d'ajouter des règles entrantes et sortantes aux groupes de sécurité VPC, comme décrit dans. Groupes de sécurité Amazon VPC

Historique du document

- Version de l'API : 01/03/2018
- Dernière mise à jour de la documentation : 17 janvier 2024

Le tableau suivant décrit les modifications importantes apportées au guide de l'utilisateur Windows d'Amazon FSx. Pour recevoir des notifications en cas de mise à jour de cette documentation, abonnez-vous au flux RSS.

Modification	Description	Date
Support ajouté pour des niveaux d'IOPS plus élevés sur les systèmes de fichiers avec des capacités de débit de 4 Gbit/s et plus	FSx for Windows File Server augmente le nombre maximal d'IOPS de 130 000 à 150 000 pour les systèmes de fichiers dotés d'une capacité de débit de 4 Gbit/s ou plus, de 175 000 à 200 000 pour les systèmes de fichiers dotés d'une capacité de débit de 6 Gbit/s ou plus, de 260 000 à 300 000 pour les systèmes de fichiers dotés d'une capacité de débit de 9 Gbit/s ou plus, et de 350 000 à 400 000 pour les systèmes de fichiers dotés d'une capacité de débit de 12 Gbit/s ou supérieur. Pour plus d'informations, consultez la section Performances de FSx for Windows File Server.	17 janvier 2024
Amazon FSx a mis à jour les politiques gérées AmazonFSxFullAccess, AmazonF, AmazonFSx	Amazon FSx a mis à jour les politiques AmazonFSx FullAccess, AmazonF, AmazonFSxConsoleFu	9 janvier 2024

ConsoleFullAccess, AmazonF SxReadOnlyAccess et SxConsoleReadOnlyAccess AmazonF SxServiceRolePolic y AWS	llAccess, AmazonF SxReadOnlyAccess et SxServiceRolePolicy AmazonF pour SxConsole ReadOnlyAccess ajouter l'autorisation. `ec2:GetSe curityGroupsForVpc` Pour plus d'informations, consultez les mises à jour des politiques AWS gérées par Amazon FSx.	
Amazon FSx a mis à jour les politiques gérées par Amazon F SxFullAccess et Amazon F SxConsoleFullAccess AWS	Amazon FSx a mis à jour les SxConsoleFullAccess politique s d'AmazonF SxFullAccess et d'AmazonF pour ajouter cette action. `ManageCro ssAccountDataRepli cation` Pour plus d'informa tions, consultez les mises à jour des politiques AWS gérées par Amazon FSx.	20 décembre 2023
Amazon FSx a mis à jour les politiques gérées par Amazon F SxFullAccess et Amazon F SxConsoleFullAccess AWS	Amazon FSx a mis à jour les SxConsoleFullAccess politique s d'AmazonF SxFullAccess et d'AmazonF pour ajouter l'autorisation. `fsx:CopyS napshotAndUpdateVo lume` Pour plus d'informa tions, consultez les mises à jour des politiques AWS gérées par Amazon FSx.	26 novembre 2023

Amazon FSx a mis à jour les politiques gérées par Amazon F SxFullAccess et Amazon F SxConsoleFullAccess AWS	Amazon FSx a mis à jour les SxConsoleFullAccess politique s d'AmazonF SxFullAccess et d'AmazonF pour ajouter les autorisations et. `fsx:Descr ibeSharedVPCConfig uration fsx:Updat eSharedVPCConfigur ation` Pour plus d'informa tions, consultez les mises à jour des politiques AWS gérées par Amazon FSx.	14 novembre 2023
Support ajouté pour la mise à jour du type de stockage du système de fichiers	Les systèmes de fichiers FSx for Windows File Server prennent désormais en charge la mise à jour du type de stockage HDD vers le type de stockage SSD. Pour plus d'informations, consultez la section Gestion du type de stockage.	9 août 2023
Support ajouté pour une capacité de débit maximale plus élevée	Les systèmes de fichiers FSx for Windows File Server prennent désormais en charge une capacité de débit allant jusqu'à 12 Gbit/s. Pour plus d'informations, consultez la section Performances de FSx for Windows File Server.	9 août 2023

Support ajouté pour le provisionnement des IOPS sur SSD	Les systèmes de fichiers FSx for Windows File Server prennent désormais en charge le provisionnement d'IOPS sur SSD indépendamment de la capacité de stockage, jusqu'à un maximum de 350 000 IOPS. Pour plus d'informations, consultez la section Gestion des IOPS des SSD.	9 août 2023
Amazon FSx a mis à jour la politique gérée par Amazon SxServiceRolePolicy AWS FSx	Amazon FSx a mis à jour l'`cloudwatch:PutMetricData` autorisation dans AmazonF. SxService RolePolicy Pour plus d'informations, consultez AmazonF. SxServiceRolePolicy	24 juillet 2023
Amazon FSx a mis à jour la politique gérée par Amazon SxFullAccess AWS FSx	Amazon FSx a mis à jour la SxFullAccess politique d'AmazonF afin de supprimer l'`fsx:*`autorisation et d'ajouter des actions spécifiques. `fsx` Pour plus d'informations, consultez la SxFullAccess politique d'AmazonF.	13 juillet 2023
Amazon FSx a mis à jour la politique gérée par Amazon SxConsoleFullAccess AWS FSx	Amazon FSx a mis à jour la SxConsoleFullAccess politique d'AmazonF afin de supprimer l'`fsx:*`autorisation et d'ajouter des actions spécifiques. `fsx` Pour plus d'informations, consultez la SxConsoleFullAccess politique d'AmazonF.	13 juillet 2023

Support ajouté pour les nouvelles CloudWatch métriques pour Amazon FSx for Windows File Server	FSx for Windows File Server fournit désormais des mesures CloudWatch supplémentaires qui surveillent les performances des serveurs de fichiers et des volumes de stockage ainsi que l'utilisation de la capacité. Pour plus d'informations, consultez la section Mesures et dimensions.	22 septembre 2022
Support ajouté pour les avertissements relatifs aux performances du système de fichiers	Amazon FSx affiche désormais des avertissements dans la fenêtre Performances et surveillance lorsqu'un ensemble de CloudWatch métriques approche ou dépasse des seuils prédéterminés pour ces métriques. Chaque avertissement fournit également une recommandation exploitable pour améliorer les performances du système de fichiers. Pour plus d'informations, consultez la section Avertissements et recommandations en matière de performances.	22 septembre 2022

Support ajouté pour une surveillance améliorée des performances du système de fichiers	Le tableau de bord de surveillance du système de fichiers de la console Amazon FSx pour les systèmes de fichiers FSx for Windows File Server inclut de nouvelles sections Résumé, Stockage et Performances. Ces sections présentent des graphiques illustrant CloudWatch les nouvelles mesures qui vous permettent de mieux surveiller les performances. Pour plus d'informations, consultez la section Surveillance des métriques avec CloudWatch.	22 septembre 2022
Support ajouté pour les points de AWS PrivateLink terminaison VPC d'interface.	Vous pouvez désormais utiliser les points de terminaison VPC de l'interface pour accéder à l'API Amazon FSx depuis votre VPC sans envoyer de trafic sur Internet. Pour plus d'informations, consultez Amazon FSx et les points de terminaison VPC d'interface.	5 avril 2022

Support ajouté pour Amazon Kendra	Vous pouvez désormais utiliser votre système de fichiers FSx for Windows File Server comme source de données pour Amazon Kendra, ce qui vous permettra d'indexer et de rechercher des informations contenues dans des documents stockés sur votre système de fichiers. Pour plus d'informations, consultez la section Utilisation de FSx for Windows File Server avec Amazon Kendra.	26 mars 2022
Support ajouté pour l'audit d'accès aux fichiers	Vous pouvez désormais activer l'audit des accès des utilisateurs finaux aux fichiers, aux dossiers et aux partages de fichiers. Vous pouvez choisir d'envoyer les journaux des événements d'audit aux services Amazon CloudWatch Logs ou Amazon Data Firehose. Pour plus d'informations, consultez la section Audit de l'accès aux fichiers.	8 juin 2021

Support ajouté pour la copie de sauvegardes	Vous pouvez désormais utiliser Amazon FSx pour copier des sauvegardes d'un même AWS compte vers un autre Région AWS (copies interrégionales) ou au sein du même compte Région AWS (copies intra-régionales). Pour plus d'informations, consultez la section Copie de sauvegardes.	12 avril 2021
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 celle-ci atteint un seuil que vous spécifiez. Pour plus d'informations, consultez la section Augmenter dynamiquement la capacité de stockage.	17 février 2021

Support ajouté pour l'accès client à l'aide d'adresses IP non privées	Vous pouvez accéder aux systèmes de fichiers FSx for Windows File Server avec des clients locaux utilisant des adresses IP non privées. Pour plus d'informations, consultez la section Environnements pris en charge. Vous pouvez associer le système de fichiers FSx for Windows File Server à un Microsoft Active Directory autogéré avec des serveurs DNS et des contrôleurs de domaine AD qui utilisent des adresses IP non privées. Pour plus d'informations, consultez Utilisation d'Amazon FSx avec votre Microsoft Active Directory autogéré.	17 décembre 2020
Support ajouté pour l'utilisation d'alias DNS	Vous pouvez désormais associer des alias DNS à vos systèmes de fichiers FSx for Windows File Server afin d'accéder aux données de votre système de fichiers. Pour plus d'informations, consultez Gestion des alias DNS et Procédure pas à pas 5 : Utilisation d'alias DNS pour accéder à votre système de fichiers.	9 novembre 2020

Support ajouté pour Amazon Elastic Container Service	Vous pouvez désormais utiliser FSx for Windows File Server avec Amazon ECS. Pour plus d'informations, consultez la section Clients pris en charge.	9 novembre 2020
Amazon FSx est désormais intégré à AWS Backup	Vous pouvez désormais les utiliser AWS Backup pour sauvegarder et restaurer vos systèmes de fichiers FSx en plus d'utiliser les sauvegardes natives d'Amazon FSx. Pour plus d'informations, consultez Utilisation AWS Backup avec Amazon FSx.	9 novembre 2020
Support ajouté pour la mise à l'échelle de la capacité de débit	Vous pouvez désormais modifier la capacité de débit des systèmes de fichiers FSx for Windows File Server existants en fonction de l'évolution de vos exigences en matière de débit. Pour plus d'informations, consultez la section Gestion de la capacité de débit.	1er juin 2020

Support ajouté pour le dimensionnement de la capacité de stockage	Vous pouvez désormais augmenter la capacité de stockage des systèmes de fichiers FSx for Windows File Server existants au fur et à mesure de l'évolution de vos besoins en matière de stockage. Pour plus d'informations, consultez la section Gestion de la capacité de stockage.	1er juin 2020
Support ajouté pour le stockage sur disque dur (HDD)	Le stockage sur disque dur vous offre une flexibilité en termes de prix et de performances lorsque vous utilisez FSx for Windows File Server. Pour plus d'informations, consultez Optimisation des coûts avec Amazon FSx.	26 mars 2020
Support ajouté pour le transfert de fichiers à l'aide de AWS DataSync	Vous pouvez désormais l'utiliser AWS DataSync pour transférer des fichiers vers et depuis votre serveur de fichiers FSx for Windows. Pour plus d'informations, consultez Migrer des fichiers vers Amazon FSx for Windows File Server AWS DataSync à l'aide de	4 février 2020

FSx for Windows File Server prend désormais en charge les tâches supplémentaires d'administration du système de fichiers Windows	Vous pouvez désormais gérer et administrer les partages de fichiers, la déduplication des données, les quotas de stockage et le chiffrement en transit pour vos partages de fichiers à l'aide de la CLI Amazon FSx pour la gestion à distance PowerShell sur. Pour plus d'informations, consultez la section Administration des systèmes de fichiers.	20 novembre 2019
FSx for Windows File Server intègre la prise en charge native du multi-AZ	Vous pouvez utiliser le déploiement multi-AZ pour FSx for Windows File Server afin de créer plus facilement des systèmes de fichiers à haute disponibilité couvrant plusieurs zones de disponibilité (AZ). Pour de plus amples informations, veuillez consulter Disponibilité et durabilité : systèmes de fichiers monoAZ et multi-AZ.	20 novembre 2019

FSx for Windows File Server propose un support pour la gestion des sessions utilisateur et des fichiers ouverts	Vous pouvez désormais utiliser l'outil Shared Folders natif de Microsoft Windows pour gérer les sessions utilisateur et ouvrir des fichiers sur vos systèmes de fichiers FSx for Windows File Server. Pour plus d'informations, consultez la section Gestion des sessions utilisateur et des fichiers ouverts.	17 octobre 2019
Amazon FSx annonce la prise en charge des copies instantanées de Microsoft Windows	Vous pouvez désormais configurer des clichés instantanés de Windows sur vos systèmes de fichiers FSx for Windows File Server. Les copies instantanées permettent à vos utilisateurs d'annuler facilement les modifications apportées aux fichiers et de comparer les versions des fichiers en restaurant les versions précédentes. Pour plus d'informations, consultez la section Utilisation des clichés instantanés.	31 juillet 2019

Amazon FSx publie le support partagé pour Microsoft Active Directory	Vous pouvez désormais associer les systèmes de fichiers FSx for Windows File Server AWS Managed Microsoft AD à des répertoir es situés dans un autre VPC ou dans un Compte AWS autre système de fichiers que le système de fichiers. Pour plus d'informations, consultez Support Active Directory.	25 juin 2019
Amazon FSx propose une prise en charge améliorée de Microsoft Active Directory	Vous pouvez désormais associer les systèmes de fichiers FSx for Windows File Server à vos domaines Microsoft Active Directory autogérés, sur site ou dans le cloud. Pour plus d'informa tions, consultez Support Active Directory.	24 juin 2019
Amazon FSx est conforme à la certification SOC	Amazon FSx a été évalué pour sa conformité à la certification SOC. Pour plus d'informations, consultez la section Sécurité et protection des données.	16 mai 2019
Ajout d'une note de clarifica tion concernant AWS Direct Connect le support des connexions VPN et VPC inter-régions	Les systèmes de fichiers Amazon FSx créés après le 22 février 2019 sont accessibles à l'aide AWS Direct Connect du VPN et du peering VPC interrégional. Pour plus d'informations, consultez la section Méthodes d'accès prises en charge.	25 février 2019

AWS Direct Connect, VPN et prise en charge de la connexion d'appairage VPC inter-régions ajoutée	Vous pouvez désormais accéder aux systèmes de fichiers Amazon FSx for Windows File Server à partir de ressources locales et de ressources d'un autre Amazon VPC ou. Compte AWS Pour plus d'informations, consultez la section Méthodes d'accès prises en charge.	22 février 2019
Amazon FSx est désormais disponible pour tous	Amazon FSx for Windows File Server fournit des serveurs de fichiers Microsoft Windows entièrement gérés, soutenus par un système de fichiers Windows entièrement natif. Amazon FSx for Windows File Server fournit les fonctionn alités, les performances et la compatibilité nécessaires pour transférer et transférer facilement des applications AWS d'entreprise.	28 novembre 2018

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.