Découvrez les bases

Setup and administration

NetApp
February 02, 2026

Sommaire

Découvrez les bases

En savoir plus sur NetApp Workload Factory

NetApp Workload Factory est une puissante plate-forme de gestion du cycle de vie conçue pour vous aider à optimiser vos charges de travail à l'aide d' Amazon FSx for NetApp ONTAP . Les charges de travail qui peuvent être rationalisées à l'aide de Workload Factory et de FSx pour ONTAP incluent les bases de données, les migrations VMware vers VMware Cloud sur AWS, les chatbots IA, etc.

Une *charge de travail* englobe une combinaison de ressources, de code et de services ou d'applications, conçue pour servir un objectif commercial. Cela peut aller d'une application destinée aux clients à un processus back-end. Les charges de travail peuvent impliquer un sous-ensemble de ressources au sein d'un seul compte AWS ou s'étendre sur plusieurs comptes.

Amazon FSx for NetApp ONTAP fournit des volumes de stockage NFS, SMB/CIFS et iSCSI entièrement gérés et natifs AWS pour les applications stratégiques, les bases de données, les conteneurs, les magasins de données VMware Cloud et les fichiers utilisateur. Vous pouvez gérer FSx pour ONTAP via Workload Factory et en utilisant des outils de gestion AWS natifs.

Caractéristiques

La plateforme Workload Factory offre les fonctionnalités majeures suivantes.

Stockage flexible et à faible coût

Découvrez, déployez et gérez les systèmes de fichiers Amazon FSX pour NetApp ONTAP dans le cloud. FSX pour ONTAP allie toutes les capacités d'ONTAP à un service géré AWS natif pour une expérience de cloud hybride homogène.

Migrez les environnements vSphere sur site vers VMware Cloud on AWS

VMware Cloud on AWS migration Advisor vous permet d'analyser les configurations actuelles de vos serveurs virtuels dans les environnements vSphere sur site, de générer un plan de déploiement des infrastructures de serveurs virtuels recommandées dans VMware Cloud on AWS et d'utiliser les systèmes de fichiers Amazon FSX for NetApp ONTAP personnalisés en tant que datastores externes.

Gestion du cycle de vie des bases de données

Découvrez les workloads de bases de données et analysez les économies réalisées avec Amazon FSX pour NetApp ONTAP ; tirez parti des avantages liés au stockage et aux applications lors de la migration de bases de données SQL Server vers FSX pour le stockage ONTAP ; déployez des serveurs, des bases de données et des clones de bases de données SQL qui mettent en œuvre les meilleures pratiques des fournisseurs ; utilisez un co-pilote Infrastructure-Code pour automatiser les opérations ; et surveillez et optimisez en continu les environnements SQL Server pour améliorer les performances, la disponibilité, la protection et la rentabilité

Développement d'un chatbot par IA

Utilisez vos systèmes de fichiers FSX pour ONTAP pour stocker les sources du chatbot de votre entreprise et les bases de données du moteur d'IA. Vous pouvez ainsi intégrer les données non structurées de votre entreprise dans une application de chatbot

Calculateurs d'économies pour réduire les coûts

Analysez vos déploiements actuels qui utilisent le stockage Amazon Elastic Block Store (EBS), Elastic File System (EFS) ou le serveur de fichiers Amazon FSX pour Windows pour voir les économies que vous pouvez réaliser en adoptant Amazon FSX pour NetApp ONTAP. Vous pouvez également utiliser le calculateur pour effectuer un scénario de simulation pour un déploiement futur que vous prévoyez.

Comptes de service pour promouvoir l'automatisation

Utilisez des comptes de service pour automatiser les opérations NetApp Workload Factory de manière sécurisée et fiable. Les comptes de service offrent une automatisation fiable et durable sans aucune restriction de gestion des utilisateurs et sont plus sécurisés car ils fournissent uniquement un accès API.

Demandez-moi l'assistant IA

Posez des questions à l'assistant IA sur la gestion et l'exploitation des systèmes de fichiers FSx for ONTAP . À l'aide du protocole de contexte de modèle (MCP), Ask Me s'interface en toute sécurité avec des environnements externes et interroge les outils API pour fournir des réponses adaptées à votre environnement de stockage spécifique.

Fournisseurs cloud pris en charge

Workload Factory vous permet de gérer le stockage cloud et d'utiliser les fonctionnalités de charge de travail dans Amazon Web Services.

Sécurité

La sécurité de NetApp Workload Factory est une priorité absolue pour NetApp. Toutes les charges de travail de Workload Factory s'exécutent sur Amazon FSx for NetApp ONTAP. En plus de tout "Fonctionnalités de sécurité AWS"NetApp Workload Factory a reçu "Conformité SOC2 de type 1, conformité SOC2 de type 2 et conformité HIPAA".

Amazon FSx for NetApp ONTAP pour NetApp Workload Factory est un"Solution AWS pour le déploiement d'applications d'entreprise" qui a été créé avec les meilleures pratiques bien architecturées à l'esprit.

Le coût

L'utilisation de Workload Factory est gratuite. Le coût que vous payez à Amazon Web Services (AWS) dépend des services de stockage et de charge de travail que vous prévoyez de déployer. Cela inclut le coût d' Amazon FSx for NetApp ONTAP , l'infrastructure VMware Cloud sur AWS, les services AWS, etc.

Comment fonctionne Workload Factory

Workload Factory comprend une console Web fournie via la couche SaaS, un compte, des modes opérationnels qui contrôlent l'accès à votre parc cloud, des liens qui fournissent une connectivité séparée entre Workload Factory et un compte AWS, et bien plus encore.

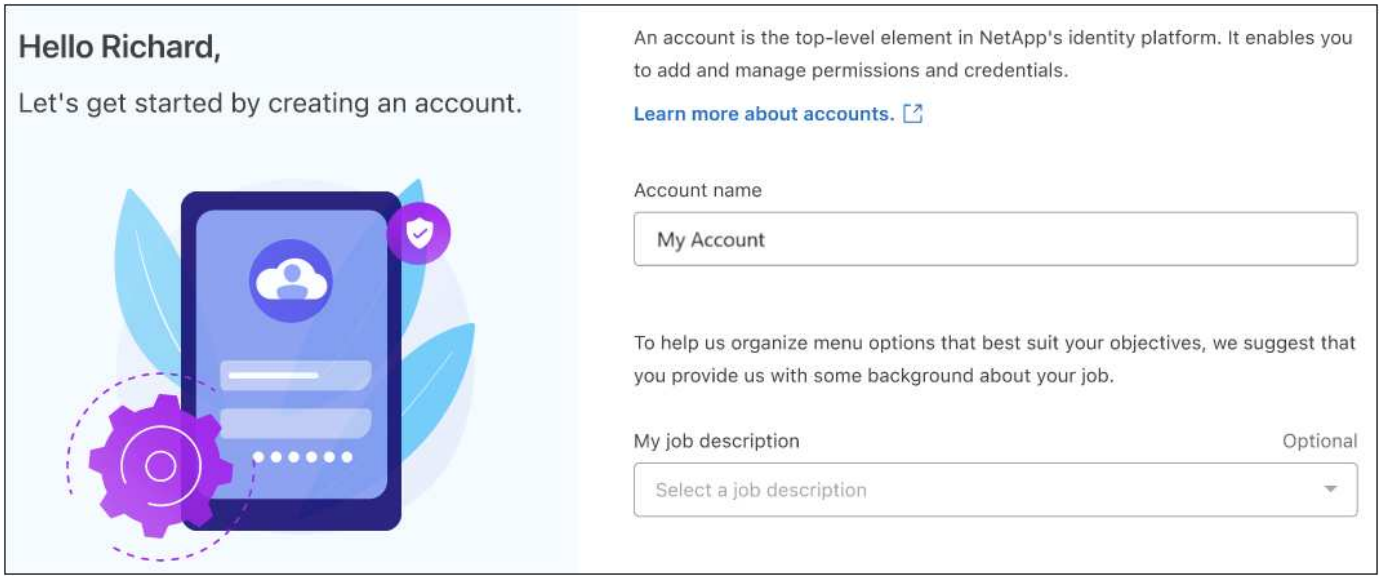
Services à la demande

Workload Factory est accessible via le"Console NetApp Workload Factory" et le"Console NetApp" . Ces expériences SaaS vous permettent d'accéder automatiquement aux dernières fonctionnalités dès leur sortie et de basculer facilement entre vos comptes et liens Workload Factory.

"Découvrez-en plus sur les différentes expériences de console"

Comptes

Lorsque vous vous connectez à Workload Factory pour la première fois, vous êtes invité à créer un compte. Ce compte vous permet d'organiser vos ressources, vos charges de travail et l'accès aux charges de travail de votre organisation à l'aide d'informations d'identification.



Lorsque vous créez un compte, vous êtes l'utilisateur *account admin* unique pour ce compte.

Si votre entreprise a besoin d'une gestion de compte ou d'utilisateurs supplémentaire, contactez-nous via le chat interne au produit.

Si vous utilisez la console NetApp , vous appartiendrez déjà à un compte, car Workload Factory exploite les comptes NetApp .

Comptes de service

Un compte de service agit comme un « utilisateur » qui peut effectuer des appels API autorisés vers NetApp Workload Factory à des fins d'automatisation. Cela facilite la gestion de l'automatisation car vous n'avez pas besoin de créer des scripts d'automatisation basés sur le compte utilisateur d'une personne réelle qui peut quitter l'entreprise à tout moment. Tous les titulaires de compte dans Workload Factory sont considérés comme des administrateurs de compte. Les administrateurs de compte peuvent créer et supprimer plusieurs comptes de service.

"Découvrez comment gérer des comptes de service"

Autorisations

Workload Factory propose des politiques d'autorisation flexibles qui vous permettent de contrôler précisément l'accès à votre environnement cloud et d'attribuer une confiance progressive à Workload Factory en fonction de vos politiques informatiques.

"Découvrez-en plus sur les politiques d'autorisation de Workload Factory"

Liens de connectivité

Un lien Workload Factory crée une relation de confiance et une connectivité entre Workload Factory et un ou plusieurs systèmes de fichiers FSx for ONTAP . Cela vous permet de surveiller et de gérer certaines

fonctionnalités du système de fichiers directement à partir des appels d'API REST ONTAP qui ne sont pas disponibles via l'API Amazon FSx for ONTAP .

Vous n'avez pas besoin d'un lien pour démarrer avec Workload Factory, mais dans certains cas, vous devrez créer un lien pour déverrouiller toutes les fonctionnalités et capacités de charge de travail de Workload Factory.

Les liens exploitent actuellement AWS Lambda.

"En savoir plus sur les liens"

Automatisation de la Codebox

Codebox est un copilote d'infrastructure en tant que code (IaC) qui aide les développeurs et les ingénieurs DevOps à générer le code nécessaire pour exécuter toute opération prise en charge par Workload Factory. Les formats de code incluent l'API REST Workload Factory, AWS CLI et AWS CloudFormation.

Codebox est aligné sur les modes de fonctionnement de Workload Factory (*basic*, *read-only* et *read/write*) et définit un chemin clair pour la préparation à l'exécution ainsi qu'un catalogue d'automatisation pour une réutilisation future rapide.

Le volet Codebox affiche le processus IAC généré par une opération de flux de tâches spécifique et associé à un assistant graphique ou à une interface de conversation. Même si Codebox prend en charge le codage couleur et la recherche pour faciliter la navigation et l'analyse, il ne permet pas de modifier. Vous ne pouvez copier ou enregistrer que dans le catalogue d'automatisation.

"En savoir plus sur Codebox"

Calculateurs d'économies

Workload Factory propose des calculateurs d'économies vous permettant de comparer les coûts de vos environnements de stockage, de vos bases de données ou de vos charges de travail VMware sur les systèmes de fichiers FSx pour ONTAP avec ceux d'autres services Amazon. En fonction de vos besoins en stockage, vous constaterez peut-être que les systèmes de fichiers FSx pour ONTAP constituent l'option la plus rentable pour vous.

- "Découvrez comment explorer les économies pour vos environnements de stockage"
- "Découvrez comment réaliser des économies pour vos charges de travail de base de données"
- "Découvrez comment réaliser des économies sur vos charges de travail VMware."

Charges de travail bien architecturées

Workload Factory vous aide à maintenir et à exploiter des configurations de stockage et de bases de données fiables, sécurisées, efficaces et économiques, conformes au cadre AWS Well-Architected. Workload Factory analyse quotidiennement les déploiements FSx à la recherche de systèmes de fichiers ONTAP , de serveurs SQL Server et de bases de données Oracle afin de fournir des informations sur les erreurs de configuration potentielles et de recommander des actions manuelles ou automatisées pour résoudre les problèmes.

"Apprenez-en davantage sur les charges de travail bien architecturées."

Outils pour utiliser NetApp Workload Factory

Vous pouvez utiliser NetApp Workload Factory avec les outils suivants :

- **Console Workload Factory** : La console Workload Factory fournit une vue visuelle et holistique de vos applications et projets.
- * Console NetApp * : la console NetApp fournit une expérience d'interface hybride afin que vous puissiez utiliser Workload Factory avec d'autres services de données NetApp .
- **Demandez-moi** : utilisez l'assistant IA Ask me pour poser des questions et en savoir plus sur Workload Factory sans quitter la console Workload Factory. Accédez à Demandez-moi depuis le menu d'aide de Workload Factory.
- **CloudShell CLI** : Workload Factory inclut une CLI CloudShell pour gérer et exploiter les environnements AWS et NetApp sur plusieurs comptes à partir d'une seule CLI basée sur un navigateur. Accédez à CloudShell depuis la barre supérieure de la console Workload Factory.
- **API REST** : utilisez les API REST de Workload Factory pour déployer et gérer vos systèmes de fichiers FSx for ONTAP et d'autres ressources AWS.
- **CloudFormation** : utilisez le code AWS CloudFormation pour effectuer les actions que vous avez définies dans la console Workload Factory afin de modéliser, provisionner et gérer les ressources AWS et tierces de la pile CloudFormation dans votre compte AWS.
- **Fournisseur Terraform NetApp Workload Factory** : utilisez Terraform pour créer et gérer les workflows d'infrastructure générés dans la console Workload Factory.

Les API REST

Workload Factory vous permet d'optimiser, d'automatiser et d'exploiter vos systèmes de fichiers FSx for ONTAP pour des charges de travail spécifiques. Chaque charge de travail expose une API REST associée. Collectivement, ces charges de travail et API forment une plate-forme de développement flexible et extensible que vous pouvez utiliser pour administrer vos systèmes de fichiers FSx for ONTAP .

L'utilisation des API REST de Workload Factory présente plusieurs avantages :

- Les API sont basées sur la technologie REST et les bonnes pratiques actuelles. Les principales technologies incluent HTTP et JSON.
- L'authentification Workload Factory est basée sur la norme OAuth2. NetApp s'appuie sur l'implémentation du service Auth0.
- La console Web Workload Factory utilise les mêmes API REST principales, ce qui garantit une cohérence entre les deux chemins d'accès.

"Consultez la documentation de l'API REST de Workload Factory"

Expériences de la console

NetApp Workload Factory est accessible via deux consoles Web. Découvrez comment accéder à Workload Factory à l'aide de la console Workload Factory et de la console NetApp .

- * Console NetApp * : offre une expérience hybride où vous pouvez gérer vos systèmes de fichiers FSx for ONTAP et vos charges de travail exécutées sur Amazon FSx for NetApp ONTAP au même endroit.
- **Console Workload Factory** : offre une expérience Workload Factory dédiée axée sur les charges de travail exécutées sur Amazon FSx for NetApp ONTAP.

Accéder à Workload Factory dans la console NetApp

Vous pouvez accéder à Workload Factory depuis la NetApp Console. En plus d'utiliser Workload Factory pour les fonctionnalités de stockage et de gestion des charges de travail AWS, vous pouvez également accéder à d'autres services de données tels que NetApp Copy and Sync, et bien plus encore.

Étapes

1. Connectez-vous à la"Console NetApp" .
2. Dans le menu de la console NetApp , sélectionnez **Charges de travail**, puis **Vue d'ensemble**.

Accéder à Workload Factory dans la console Workload Factory

Vous pouvez accéder à Workload Factory depuis la console Workload Factory.

Étape

1. Connectez-vous à la"Console Workload Factory" .

Autorisations pour NetApp Workload Factory

Pour utiliser les fonctionnalités et services de NetApp Workload Factory, vous devez fournir des autorisations afin que Workload Factory puisse effectuer des opérations dans votre environnement cloud.

Pourquoi utiliser des autorisations

Lorsque vous accordez des autorisations, Workload Factory associe à l'instance une stratégie lui permettant de gérer les ressources et les processus au sein de ce compte AWS. Cela permet à Workload Factory d'exécuter diverses opérations, depuis la découverte de vos environnements de stockage jusqu'au déploiement de ressources AWS telles que des systèmes de fichiers dans la gestion du stockage ou des bases de connaissances pour les charges de travail GenAI.

Pour les charges de travail de base de données, par exemple, lorsque Workload Factory reçoit les autorisations requises, il analyse toutes les instances EC2 dans un compte et une région donnés et filtre toutes les machines Windows. Si l'agent AWS Systems Manager (SSM) est installé et en cours d'exécution sur l'hôte et que la mise en réseau de System Manager est correctement configurée, Workload Factory peut accéder à la machine Windows et vérifier si le logiciel SQL Server est installé ou non.

Autorisations par charge de travail

Chaque charge de travail utilise des autorisations pour effectuer certaines tâches dans Workload Factory. Les autorisations sont regroupées en politiques d'autorisation définies. Faites défiler jusqu'à la charge de travail que vous utilisez pour en savoir plus sur les politiques d'autorisation, le JSON copiable pour les politiques d'autorisation et un tableau qui répertorie toutes les autorisations, leur objectif, où elles sont utilisées et quelles politiques d'autorisation les prennent en charge.

Autorisations de stockage

Les politiques IAM disponibles pour le stockage fournissent les autorisations dont Workload Factory a besoin pour gérer les ressources et les processus au sein de votre environnement de cloud public.

Le stockage propose les politiques d'autorisation suivantes :

- **Visualisation, planification et analyse** : visualisez les systèmes de fichiers FSx pour ONTAP , informez-vous sur l'état du système, obtenez une analyse détaillée de vos systèmes et explorez les économies possibles.
- **Opérations et correction** : Effectuez des tâches opérationnelles telles que l'ajustement de la capacité du système de fichiers et la résolution des problèmes liés à la configuration de votre système de fichiers.
- **Création et suppression de systèmes de fichiers** : Créez et supprimez des systèmes de fichiers FSx pour ONTAP et des machines virtuelles de stockage.

Consultez les politiques IAM requises :

Règles IAM pour le stockage

Vue, planification et analyse

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeSharedVpcConfiguration",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "elasticfilesystem:DescribeFileSystems",
        "ce:GetCostAndUsage",
        "ce:GetTags",
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Opérations et assainissement

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateVolume",
        "fsx:DeleteVolume",
        "fsx:UpdateFileSystem",
```

```
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume",
        "fsx:CreateBackup",
        "fsx:CreateVolumeFromBackup",
        "fsx:DeleteBackup",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:CreateAndAttachS3AccessPoint",
        "fsx:DetachAndDeleteS3AccessPoint",
        "s3:CreateAccessPoint",
        "s3:DeleteAccessPoint",
        "s3:GetObjectTagging",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:InvokeModel",
        "bedrock:ListInferenceProfiles",
        "bedrock:GetInferenceProfile",
        "s3tables:CreateTableBucket",
        "s3tables:ListTables",
        "s3tables:GetTable",
        "s3tables:GetTableMetadataLocation",
        "s3tables:CreateTable",
        "s3tables:GetNamespace",
        "s3tables:PutTableData",
        "s3tables:CreateNamespace",
        "s3tables:GetTableData",
        "s3tables:ListNamespaces",
        "s3tables:ListTableBuckets",
        "s3tables:GetTableBucket",
        "s3tables:UpdateTableMetadataLocation",
        "s3tables:ListTagsForResource",
        "s3tables:TagResource",
        "s3:GetObjectTagging",
        "s3:ListBucket"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Création et suppression de systèmes de fichiers

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateFileSystem",
        "fsx:CreateStorageVirtualMachine",
        "fsx:DeleteFileSystem",
        "fsx:DeleteStorageVirtualMachine",
        "fsx:TagResource",
        "fsx:UntagResource",
        "kms:CreateGrant",
        "iam:CreateServiceLinkedRole",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumeStatus",
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/AppCreator": "NetappFSxWF"
        }
      }
    },
```

```
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Le tableau suivant affiche les autorisations pour le stockage.

Tableau des autorisations pour le stockage

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Créez un système de fichiers FSX pour ONTAP	fsx:CreateFileSystem	Déploiement	Création et suppression de systèmes de fichiers
Créez un groupe de sécurité pour un système de fichiers FSX pour ONTAP	ec2:CreateSecurityGroup	Déploiement	Création et suppression de systèmes de fichiers
Ajoutez des balises à un groupe de sécurité pour un système de fichiers FSX pour ONTAP	ec2:CreateTags	Déploiement	Création et suppression de systèmes de fichiers
Autoriser la sortie et l'entrée de groupe de sécurité pour un système de fichiers FSX pour ONTAP	ec2:AuthoreSecurityGroupEgress	Déploiement	Création et suppression de systèmes de fichiers
	ec2:AuthoreSecurityGroupIngress	Déploiement	Création et suppression de systèmes de fichiers
Le rôle attribué permet la communication entre FSX pour ONTAP et d'autres services AWS	iam:CreateServiceLinkedRole	Déploiement	Création et suppression de systèmes de fichiers

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Obtenez des détails pour remplir le formulaire de déploiement du système de fichiers FSX pour ONTAP	ec2 : descriptif	• Déploiement • Découvrez les économies	Création et suppression de systèmes de fichiers
	ec2:DescribeSubnets	• Déploiement • Découvrez les économies	Création et suppression de systèmes de fichiers
	ec2:descriptifs des groupes de sécurité	• Déploiement • Découvrez les économies	Création et suppression de systèmes de fichiers
	ec2:DescribeRoutetables	• Déploiement • Découvrez les économies	Création et suppression de systèmes de fichiers
	ec2:DescribeNetworkinterfaces	• Déploiement • Découvrez les économies	Création et suppression de systèmes de fichiers
	ec2:DescribeVolumeStatus	• Déploiement • Découvrez les économies	Création et suppression de systèmes de fichiers

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Obtenez des détails de clé KMS et utilisez-les pour le chiffrement FSX for ONTAP	Kms:CreateGrant	Déploiement	Création et suppression de systèmes de fichiers
	Km:DescribeKey	Déploiement	Création et suppression de systèmes de fichiers
	Km:ListKeys	Déploiement	Création et suppression de systèmes de fichiers
	Kms:Listalas	Déploiement	Création et suppression de systèmes de fichiers
Obtenez les détails des volumes des instances EC2	ec2:Describvolumes	• Inventaire • Découvrez les économies	Vue, planification et analyse
Obtenez les détails des instances EC2	ec2:descriptifs	Découvrez les économies	Vue, planification et analyse
Décrivez Elastic File System dans le calculateur d'économies	Elasticfilesystem:DescribeFileSystems	Découvrez les économies	Vue, planification et analyse
Répertoriez les balises des ressources FSX pour ONTAP	fsx:ListTagsForResource	Inventaire	Vue, planification et analyse
Gestion des entrées et sorties de groupes de sécurité pour un système de fichiers FSX pour ONTAP	ec2 : RevokeSecurityGroupIngress	Les opérations de gestion	Création et suppression de systèmes de fichiers
	ec2 : Révoquer la sortie du groupe de sécurité	Les opérations de gestion	Création et suppression de systèmes de fichiers
	ec2:DeleteSecurityGroup	Les opérations de gestion	Création et suppression de systèmes de fichiers

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Créez, affichez et gérez les ressources du système de fichiers FSX pour ONTAP			

	fsx:DescribeBackups	Les opérations de gestion	Vue, planification et analyse
Objectif	**Action**	**Cas d'utilisation**	**Politique d'autorisation**
	fsx:Créer une sauvegarde	Les opérations de gestion	Opérations et assainissement
	fsx:Créer un volume à partir d'une sauvegarde	Les opérations de gestion	Opérations et assainissement
	fsx:Supprimer la sauvegarde	Les opérations de gestion	Opérations et assainissement
Obtenez des metrics de système de fichiers et de volume	cloudwatch:GetMetricData	Les opérations de gestion	Vue, planification et analyse
	cloudwatch:GetMetricStatistics	Les opérations de gestion	Vue, planification et analyse
Simulez les opérations de workload pour valider les autorisations disponibles et les comparer avec les autorisations de compte AWS requises	iam:SimulatePrincipalPolicy	Déploiement	Tous
Fournir des informations basées sur l'IA pour les événements FSx pour ONTAP EMS	Bedrock:ListeInferenceProfiles	FSx pour l'analyse ONTAP EMS	Opérations et assainissement
	bedrock:GetInferenceProfile	FSx pour l'analyse ONTAP EMS	Opérations et assainissement
	bedrock:InvokeModelWithResponseStream	FSx pour l'analyse ONTAP EMS	Opérations et assainissement
	Bedrock:modèle de facturation	FSx pour l'analyse ONTAP EMS	Opérations et assainissement
Obtenez des données sur les coûts et l'utilisation des systèmes de fichiers FSx pour ONTAP à partir d'AWS Cost Explorer.	ce:GetCostAndUsage	Analyse des coûts et de l'utilisation	Vue, planification et analyse
	ce:GetTags	Analyse des coûts et de l'utilisation	Vue, planification et analyse
Créez un point d'accès S3 et attachez-le à un système de fichiers FSx for ONTAP	fsx:CreateAndAttachS3AccessPoint	Gestion des points d'accès S3	Opérations et assainissement
Détachez un point d'accès S3 d'un système de fichiers FSx for ONTAP et supprimez-le	fsx:DetachAndDeleteS3AccessPoint	Gestion des points d'accès S3	Opérations et assainissement
Créez un point d'accès S3 pour la gestion simplifiée des accès au compartiment	s3:CreateAccessPoint	Gestion des points d'accès S3	Opérations et assainissement

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Supprimer un point d'accès S3	s3:DeleteAccessPoint	Gestion des points d'accès S3	Opérations et assainissement
Ajouter des balises à un point d'accès S3	s3:TagResource	Gestion des points d'accès S3	Opérations et assainissement
Lister et afficher les tags sur un point d'accès S3	s3:ListTagsForResource	Gestion des points d'accès S3	Opérations et assainissement
Supprimer les balises d'un point d'accès S3	s3:UntagResource	Gestion des points d'accès S3	Opérations et assainissement
Découvrir des objets dans un compartiment de point d'accès S3	s3:ListBucket	Opérations sur le compartiment S3	Opérations et assainissement
Lister, créer et décrire les compartiments de table S3	s3tables:ListTableBuckets s3tables:CreateTableBucket s3tables:GetTableBucket	Gestion des compartiments de table S3	Opérations et assainissement
Lister, créer et récupérer des tables S3	s3tables:ListTables s3tables:CreateTable s3tables:GetTable	Opérations sur la table S3	Opérations et assainissement
Lire l'emplacement des métadonnées de la table	s3tables:GetTableMetadataLocation	Opérations sur les métadonnées des tables S3	Opérations et assainissement
Mettre à jour l'emplacement des métadonnées du tableau	s3tables:UpdateTableMetadataLocation	Opérations sur les métadonnées des tables S3	Opérations et assainissement
Lister, créer et récupérer les espaces de noms de tables	s3tables:ListNamespaces s3tables:CreateNamespace s3tables:GetNamespace	Opérations sur l'espace de noms S3	Opérations et assainissement
Lire les données du tableau (select, scan)	s3tables:GetTableData	Opérations sur les données de table S3	Opérations et assainissement
Écrire les données du tableau (insérer)	s3tables:PutTableData	Opérations sur les données de table S3	Opérations et assainissement
Lister les étiquettes sur une table d'inventaire (obtenir FSx for ONTAP, identifiants de VM de stockage, de volume)	s3tables:ListTagsForResource	Opérations d'étiquetage de table S3	Opérations et assainissement

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Étiqueter une table d'inventaire pour la recherche dans NetApp Workload Factory	s3tables:TagResource	Opérations d'étiquetage de table S3	Opérations et assainissement
Récupérer l'étiquetage des objets via point d'accès	s3:GetObjectTagging	Opérations sur les objets S3	Opérations et assainissement

Autorisations pour les charges de travail de la base de données

Les politiques IAM disponibles pour les charges de travail de base de données fournissent les autorisations dont Workload Factory a besoin pour gérer les ressources et les processus au sein de votre environnement de cloud public.

Les bases de données proposent les politiques d'autorisation suivantes :

- **Visualisation, planification et analyse** : Consultez l'inventaire des ressources de la base de données, informez-vous sur l'état de vos ressources, examinez l'analyse de l'architecture de vos configurations de base de données et explorez les économies possibles, obtenez une analyse du journal des erreurs et explorez les économies.
- **Opérations et correction** : Effectuez les tâches opérationnelles pour vos ressources de base de données et corrigez les problèmes liés aux configurations de base de données et au système de stockage de fichiers FSx sous-jacent pour ONTAP .
- **Création d'hôtes de base de données** : Déployez les hôtes de base de données et le système de stockage de fichiers FSx sous-jacent pour ONTAP conformément aux meilleures pratiques.

Sélectionnez votre mode opérationnel pour afficher les politiques IAM requises :

Politiques IAM pour les charges de travail de base de données

Vue, planification et analyse

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CommonGroup",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:GetMetricData",
                "sns:ListTopics",
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "ec2:DescribeRegions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeInstanceTypeOfferings",
                "ec2:DescribeSnapshots",
                "ec2:DescribeVolumes",
                "ec2:DescribeAddresses",
                "kms:ListAliases",
                "kms:ListKeys",
                "kms:DescribeKey",
                "cloudformation:ListStacks",
                "cloudformation:DescribeAccountLimits",
                "ds:DescribeDirectories",
                "fsx:DescribeVolumes",
                "fsx:DescribeBackups",
                "fsx:DescribeStorageVirtualMachines",
                "fsx:DescribeFileSystems",
                "servicequotas:ListServiceQuotas",
                "ssm:GetParametersByPath",
                "ssm:GetCommandInvocation",
                "ssm:SendCommand",
                "ssm:GetConnectionStatus",
                "ssm:DescribePatchBaselines",
                "ssm:DescribeInstancePatchStates",
                "ssm:ListCommands",
                "ssm:DescribeInstanceInformation",
```

```
                "fsx:ListTagsForResource",
                "logs:DescribeLogGroups",
                "bedrock:GetFoundationModelAvailability",
                "bedrock:ListInferenceProfiles"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "SSMParameterStore",
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameter",
                "ssm:GetParameters",
                "ssm:PutParameter",
                "ssm:DeleteParameters"
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/netapp/wlmdb/*"
        },
        {
            "Sid": "SSMResponseCloudWatch",
            "Effect": "Allow",
            "Action": [
                "logs:GetLogEvents",
                "logs:PutRetentionPolicy"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:netapp/wlmdb/*"
        }
    ]
}
```

Opérations et assainissement

```
[
    {
        "Sid": "FSxRemediation",
        "Effect": "Allow",
        "Action": [
            "fsx:UpdateFileSystem",
            "fsx:UpdateVolume"
        ],
        "Resource": "*"
    },
    {
        "Sid": "EC2Remediation",
        "Effect": "Allow",
        "Action": [
            "ec2:StartInstances",
            "ec2:ModifyInstanceAttribute",
            "ec2:StopInstances"
        ],
        "Resource": "*",
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/aws:cloudformation:stack-name":
"WLMDB*"
            }
        }
    }
]
```

Création d'un hôte de base de données

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2TagGroup",
            "Effect": "Allow",
            "Action": [
                "ec2:AllocateAddress",
                "ec2:AllocateHosts",
                "ec2:AssignPrivateIpAddresses",
                "ec2:AssociateAddress",
                "ec2:AssociateRouteTable",
                "ec2:AssociateSubnetCidrBlock",
                "ec2:AssociateVpcCidrBlock",
                "ec2:AttachInternetGateway",
```

```
                "ec2:AttachNetworkInterface",
                "ec2:AttachVolume",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateVolume",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DetachNetworkInterface",
                "ec2:DetachVolume",
                "ec2:DisassociateAddress",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DisassociateRouteTable",
                "ec2:DisassociateSubnetCidrBlock",
                "ec2:DisassociateVpcCidrBlock",
                "ec2:ModifyInstancePlacement",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:ModifySubnetAttribute",
                "ec2:ModifyVolume",
                "ec2:ModifyVolumeAttribute",
                "ec2:ReleaseAddress",
                "ec2:ReplaceRoute",
                "ec2:ReplaceRouteTableAssociation",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/aws:cloudformation:stack-
name": "WLMDB*"
                }
            }
        },
        {
            "Sid": "FSxNGroup",
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/aws:cloudformation:stack-
name": "WLMDB*"
```

```
                }
            }
        },
        {
            "Sid": "CreationGroup",
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DescribeStackEvents",
                "cloudformation:DescribeStacks",
                "cloudformation:ValidateTemplate",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateLaunchTemplateVersion",
                "ec2:CreateNetworkInterface",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVpcEndpoint",
                "ec2:RunInstances",
                "ec2:DescribeTags",
                "ec2:DescribeLaunchTemplates",
                "ec2:ModifyVpcAttribute",
                "fsx:CreateFileSystem",
                "fsx:CreateStorageVirtualMachine",
                "fsx:CreateVolume",
                "fsx:DescribeFileSystemAliases",
                "kms:CreateGrant",
                "kms:DescribeCustomKeyStores",
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:GetLogGroupFields",
                "logs:GetLogRecord",
                "logs:ListLogDeliveries",
                "logs:PutLogEvents",
                "logs:TagResource",
                "sns:Publish",
                "ssm:PutComplianceItems",
                "ssm:PutConfigurePackageResult",
                "ssm:PutInventory",
                "ssm:UpdateAssociationStatus",
                "ssm:UpdateInstanceAssociationStatus",
                "ssm:UpdateInstanceInformation",
                "ssmmessages:CreateControlChannel",
                "ssmmessages:CreateDataChannel",
                "ssmmessages:OpenControlChannel",
```

```
                "ssmmessages:OpenDataChannel",
                "compute-optimizer:GetEnrollmentStatus",
                "compute-optimizer:PutRecommendationPreferences",
                "compute-
optimizer:GetEffectiveRecommendationPreferences",
                "compute-optimizer:GetEC2InstanceRecommendations",
                "autoscaling:DescribeAutoScalingGroups",
                "autoscaling:DescribeAutoScalingInstances",
                "iam:GetPolicy",
                "iam:GetPolicyVersion",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:GetUser"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ArnGroup",
            "Effect": "Allow",
            "Action": [
                "cloudformation:SignalResource"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:stack/WLMDB*",
                "arn:aws:logs:*:*:log-group:WLMDB*"
            ]
        },
        {
            "Sid": "IAMGroup1",
            "Effect": "Allow",
            "Action": [
                "iam:AddRoleToInstanceProfile",
                "iam:CreateInstanceProfile",
                "iam:DeleteInstanceProfile",
                "iam:PutRolePolicy",
                "iam:RemoveRoleFromInstanceProfile"
            ],
            "Resource": [
                "arn:aws:iam::*:instance-profile/*",
                "arn:aws:iam::*:role/WLMDB*"
            ]
        },
        {
            "Sid": "IAMGroup2",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
```

```
            "Resource": [
                "arn:aws:iam::*:instance-profile/*",
                "arn:aws:iam::*:role/WLMDB*"
            ],
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "ec2.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMGroup3",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::*:instance-profile/*",
                "arn:aws:iam::*:role/WLMDB*"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ec2.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMGroup4",
            "Effect": "Allow",
            "Action": "iam:CreateRole",
            "Resource": "arn:aws:iam::*:role/WLMDB*"
        }
    ]
}
```

Le tableau suivant affiche les autorisations pour les charges de travail de la base de données.

Tableau des autorisations pour les charges de travail de la base de données

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Obtenez des statistiques métriques pour FSx pour ONTAP, EBS et FSx pour Windows File Server et pour des recommandations d'optimisation de calcul	cloudwatch:GetMetricStatistics	• Inventaire • Découvrez les économies	Vue, planification et analyse
Collectez les indicateurs de performances enregistrés dans Amazon CloudWatch à partir des nœuds SQL enregistrés. Les données sont générées dans les graphiques de tendances de performances sur l'écran de gestion des instances pour les instances SQL enregistrées.	cloudwatch:GetMetricData	Inventaire	Vue, planification et analyse
Obtenez les détails des instances EC2	ec2:descriptifs	• Inventaire • Découvrez les économies	Vue, planification et analyse
	ec2:Décrivez des Keypaires	Déploiement	Vue, planification et analyse
	ec2:DescribeNetworkinterfaces	Déploiement	Vue, planification et analyse
	ec2:DescribeInstanceTypes	• Déploiement • Découvrez les économies	Vue, planification et analyse

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Remplissez le formulaire de déploiement FSX pour ONTAP	ec2 : descriptif	• Déploiement • Inventaire	Vue, planification et analyse
	ec2:DescribeSubnets	• Déploiement • Inventaire	Vue, planification et analyse
	ec2:descriptifs des groupes de sécurité	Déploiement	Vue, planification et analyse
	ec2:descriptifs	Déploiement	Vue, planification et analyse
	ec2:régions descriptives	Déploiement	Vue, planification et analyse
	ec2:DescribeRoutetables	• Déploiement • Inventaire	Vue, planification et analyse
Procurez-vous des terminaux VPC existants pour déterminer si de nouveaux terminaux doivent être créés avant les déploiements	ec2:DescribeVpcEndpoints	• Déploiement • Inventaire	Vue, planification et analyse
Créez des terminaux VPC s'ils n'existent pas pour les services requis, quelle que soit la connectivité du réseau public sur les instances EC2	ec2:CreateVpcEndpoint	Déploiement	Création d'un hôte de base de données
Obtenir les types d'instances disponibles dans la région pour les nœuds de validation (t2.micro/t3.micro)	ec2:DécribeInstanceTypeOfferings	Déploiement	Vue, planification et analyse
Obtenez les détails des copies Snapshot de chaque volume EBS associé à des fins d'estimation de la tarification et des économies	ec2:snapshots descriptifs	Découvrez les économies	Vue, planification et analyse

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Découvrez en détail chaque volume EBS attaché pour estimer la tarification et les économies	ec2:Describvolumes	• Inventaire • Découvrez les économies	Vue, planification et analyse
Obtenez des détails de clé KMS pour FSX for ONTAP File System Encryption	Kms:Listalas	Déploiement	Vue, planification et analyse
	Km:ListKeys	Déploiement	Vue, planification et analyse
	Km:DescribeKey	Déploiement	Vue, planification et analyse
Obtenez la liste des piles CloudFormation exécutées dans l'environnement pour vérifier la limite de quota	Cloudformation:ListSacks	Déploiement	Vue, planification et analyse
Vérifiez les limites des comptes pour les ressources avant de déclencher le déploiement	Cloudformation:DescribeAccount Limits	Déploiement	Vue, planification et analyse
Obtenez la liste des Active Directory gérés par AWS dans la région	ds:DescribeDirectories	Déploiement	Vue, planification et analyse

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Obtenez des listes et des détails sur les volumes, les sauvegardes, les SVM, les systèmes de fichiers dans les zones de disponibilité des fichiers et les balises pour le système de fichiers FSX pour ONTAP	fsx:Describevolumes	• Inventaire • Découvrez les économies	Vue, planification et analyse
	fsx:DescribeBackups	• Inventaire • Découvrez les économies	Vue, planification et analyse
	fsx:DescribeStockVirtualMachines	• Déploiement • Les opérations de gestion • Inventaire	Vue, planification et analyse
	fsx:DescribeFileSystems	• Déploiement • Les opérations de gestion • Inventaire • Découvrez les économies	Vue, planification et analyse
	fsx:ListTagsForResource	Les opérations de gestion	Vue, planification et analyse
Obtenez les limites de quota de service pour CloudFormation et VPC / Créez des secrets dans un compte utilisateur pour les informations d'identification fournies pour SQL, le domaine et FSx pour ONTAP	Servicecotas:ListServiceQuotas	Déploiement	Vue, planification et analyse
Utilisez la requête SSM pour obtenir la liste mise à jour des régions FSX pour ONTAP prises en charge	ssm:GetParametersByPath	Déploiement	Vue, planification et analyse

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Interroger la réponse SSM après l'envoi de la commande pour les opérations de gestion post-déploiement	ssm:GetCommandInvocation	• Les opérations de gestion • Inventaire • Découvrez les économies • Optimisation	Vue, planification et analyse
Envoyer des commandes via SSM aux instances EC2 pour la découverte et la gestion	ssm:SendCommand	• Les opérations de gestion • Inventaire • Découvrez les économies • Optimisation	Vue, planification et analyse
Obtenir l'état de connectivité SSM sur les instances après le déploiement	ssm:GetConnectionStatus	• Les opérations de gestion • Inventaire • Optimisation	Vue, planification et analyse
Extraire l'état d'association SSM pour un groupe d'instances EC2 gérées (nœuds SQL)	ssm:DescribeInstanceinformation	Inventaire	Vue, planification et analyse
Obtenez la liste des lignes de base de correctifs disponibles pour l'évaluation des correctifs du système d'exploitation	ssm:DescribePatchBasines	Optimisation	Vue, planification et analyse
Obtenez l'état des correctifs sur les instances Windows EC2 pour l'évaluation des correctifs du système d'exploitation	ssm:DescribeInstancePatchStates	Optimisation	Vue, planification et analyse

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Répertoriez les commandes exécutées par AWS Patch Manager sur les instances EC2 pour la gestion des correctifs du système d'exploitation	ssm:ListCommands	Optimisation	Vue, planification et analyse
Vérifiez si le compte est inscrit à AWS Compute Optimizer	Optimiseur-calcul:GetInscriptStatus	• Découvrez les économies • Optimisation	Création d'un hôte de base de données
Mettez à jour une préférence de recommandation existante dans AWS Compute Optimizer afin d'adapter les suggestions aux charges de travail SQL Server	Compute-Optimizer:PutrecommandationPreferences	• Découvrez les économies • Optimisation	Création d'un hôte de base de données
Obtenir les préférences de recommandation en vigueur pour une ressource donnée à partir d'AWS Compute Optimizer	Compute-Optimizer:GetEffectiveRecommandation Preferences	• Découvrez les économies • Optimisation	Création d'un hôte de base de données
Recommandations générées par AWS Compute Optimizer pour les instances Amazon Elastic Compute Cloud (Amazon EC2	Compute-Optimizer:GetEC2InstanceRecommendations	• Découvrez les économies • Optimisation	Création d'un hôte de base de données

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Vérifiez l'association de l'instance aux groupes de mise à l'échelle automatique	Mise à l'échelle automatique:DescribeAutoScalingGroups	• Découvrez les économies • Optimisation	Création d'un hôte de base de données
	Mise à l'échelle automatique:DescribeAutoScatingInstances	• Découvrez les économies • Optimisation	Création d'un hôte de base de données
Obtenez, répertoriez, créez et supprimez les paramètres SSM pour les informations d'identification d'utilisateur AD, FSX pour ONTAP et SQL utilisées lors du déploiement ou gérées dans votre compte AWS	ssm:getParameter [1]	• Déploiement • Les opérations de gestion • Inventaire	Vue, planification et analyse
	ssm:GetParameters [1]	• Déploiement • Les opérations de gestion • Inventaire	Vue, planification et analyse
	ssm:PutParameter [1]	• Déploiement • Les opérations de gestion	Vue, planification et analyse
	ssm:DeleteParameters [1]	• Déploiement • Les opérations de gestion	Vue, planification et analyse

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Associez des ressources réseau aux nœuds SQL et aux nœuds de validation, et ajoutez des adresses IP secondaires supplémentaires aux nœuds SQL	ec2:AllocateAddress [1]	Déploiement	Création d'un hôte de base de données
	ec2:AllocateHosts [1]	Déploiement	Création d'un hôte de base de données
	ec2:AssignPrivateIpAddresses [1]	Déploiement	Création d'un hôte de base de données
	ec2:adresse associate[1]	Déploiement	Création d'un hôte de base de données
	ec2:AssociateRouteTable [1]	Déploiement	Création d'un hôte de base de données
	ec2:AssociateSubnetCidrBlock [1]	Déploiement	Création d'un hôte de base de données
	ec2:AssociateVpcCidrBlock [1]	Déploiement	Création d'un hôte de base de données
	ec2:AttachInternetGateway [1]	Déploiement	Création d'un hôte de base de données
	ec2:AttachNetworkinterface [1]	Déploiement	Création d'un hôte de base de données
Reliez les volumes EBS nécessaires aux nœuds SQL pour le déploiement	ec2 : AttachVolume	Déploiement	Création d'un hôte de base de données
Associez des groupes de sécurité et modifiez les règles aux instances EC2 provisionnées.	ec2:AuthoreSecurityGroupEgress	Déploiement	Création d'un hôte de base de données
	ec2:AuthoreSecurityGroupIngress	Déploiement	Création d'un hôte de base de données
Créez des volumes EBS requis pour les nœuds SQL pour le déploiement	ec2 : CreateVolume	Déploiement	Création d'un hôte de base de données

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Supprimez les nœuds de validation temporaires créés de type t2.micro et pour la restauration ou la nouvelle tentative des nœuds SQL EC2 défaillants	ec2:DeleteNetworkinterface	Déploiement	Création d'un hôte de base de données
	ec2:DeleteSecurityGroup	Déploiement	Création d'un hôte de base de données
	ec2:DeleteTags	Déploiement	Création d'un hôte de base de données
	ec2:DeleteVolume	Déploiement	Création d'un hôte de base de données
	ec2:DetachNetworkinterface	Déploiement	Création d'un hôte de base de données
	ec2 : DetachVolume	Déploiement	Création d'un hôte de base de données
	ec2:DisassociateAddress	Déploiement	Création d'un hôte de base de données
	ec2:DisassociateIamInstanceProfile	Déploiement	Création d'un hôte de base de données
	ec2:DisassociateRouteTable	Déploiement	Création d'un hôte de base de données
	ec2:DisassociateSubnetCidrBlock	Déploiement	Création d'un hôte de base de données
	ec2:DisassociateVpcCidrBlock	Déploiement	Création d'un hôte de base de données

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Modifier les attributs des instances SQL créées. Applicable uniquement aux noms commençant par WLMDB.	ec2:ModimodificaceAttribute	Déploiement	Opérations et assainissement
	ec2:ModifyInstanceplacement	Déploiement	Création d'un hôte de base de données
	ec2:ModilyNetworkInterfaceAttribute	Déploiement	Création d'un hôte de base de données
	ec2:ModifySubnetAttribute	Déploiement	Création d'un hôte de base de données
	ec2 : Modifier le volume	Déploiement	Création d'un hôte de base de données
	ec2:ModimodityVolumeAttribute	Déploiement	Création d'un hôte de base de données
	ec2:ModifyVpcAttribute	Déploiement	Création d'un hôte de base de données
Dissocier et détruire les instances de validation	ec2:adresse de version	Déploiement	Création d'un hôte de base de données
	ec2:ReplaceRoute	Déploiement	Création d'un hôte de base de données
	ec2:ReplaceRouteTableAssociation	Déploiement	Création d'un hôte de base de données
	ec2 : RevokeSecurityGroupEgress	Déploiement	Création d'un hôte de base de données
	ec2 : RevokeSecurityGroupIngress	Déploiement	Création d'un hôte de base de données
Démarrez les instances déployées	ec2:déclarations de début	Déploiement	Opérations et assainissement
Arrêtez les instances déployées	ec2:StopInances	Déploiement	Opérations et assainissement

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Balisez les valeurs personnalisées pour les ressources Amazon FSX pour NetApp ONTAP créées par WLMDB pour obtenir des détails de facturation lors de la gestion des ressources	fsx:TagResource [1]	• Déploiement • Les opérations de gestion	Création d'un hôte de base de données
Créez et validez le modèle CloudFormation pour le déploiement	Cloudformation:CreateStack	Déploiement	Création d'un hôte de base de données
	Cloudformation:DescribeStackEvents	Déploiement	Création d'un hôte de base de données
	Cloudformation:DescribeSacks	Déploiement	Création d'un hôte de base de données
	Cloudformation:ListSacks	Déploiement	Vue, planification et analyse
	Déformation:ValidéeTemplate	Déploiement	Création d'un hôte de base de données
Créez des modèles de pile imbriqués pour réessayer et restaurer	ec2:CreateLaunchTemplate	Déploiement	Création d'un hôte de base de données
	ec2:CreateLaunchTemplateVersion	Déploiement	Création d'un hôte de base de données
Gérer les balises et la sécurité du réseau sur les instances créées	ec2:CreateNetworkinterface	Déploiement	Création d'un hôte de base de données
	ec2:CreateSecurityGroup	Déploiement	Création d'un hôte de base de données
	ec2:CreateTags	Déploiement	Création d'un hôte de base de données
Consultez les détails de l'instance pour le provisionnement	ec2:Décrire les adresses	Déploiement	Vue, planification et analyse
	ec2 : Décrire les modèles de lancement	Déploiement	Vue, planification et analyse

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Démarrez les instances créées	ec2:RunInstances	Déploiement	Création d'un hôte de base de données
Créez les ressources FSX pour ONTAP requises pour le provisionnement. Pour les systèmes FSX for ONTAP existants, un nouveau SVM est créé pour héberger les volumes SQL.	fsx:CreateFileSystem	Déploiement	Création d'un hôte de base de données
	fsx:CreateStorageVirtualmachine	Déploiement	Création d'un hôte de base de données
	fsx:CreateVolume	• Déploiement • Les opérations de gestion	Création d'un hôte de base de données
Découvrez les détails de FSX pour ONTAP	fsx:Décrire les alias du système de fichiers	Déploiement	Création d'un hôte de base de données
Redimensionnez le système de fichiers FSX pour ONTAP pour optimiser la marge du système de fichiers	fsx:système de fichiers de mise à jour	Optimisation	Opérations et assainissement
Redimensionnez les volumes pour corriger la taille des lecteurs du journal et de la base de données de temps	fsx:UpdateVolume	Optimisation	Opérations et assainissement
Obtenez des détails de clé KMS et utilisez-les pour le chiffrement FSX for ONTAP	Kms:CreateGrant	Déploiement	Création d'un hôte de base de données
	kms : Décrire les magasins de clés personnalisés	Déploiement	Création d'un hôte de base de données
	Km:GenerateDataKey	Déploiement	Création d'un hôte de base de données

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Créez des journaux CloudWatch pour les scripts de validation et de provisionnement s'exécutant sur les instances EC2	Journaux:CreateLogGroup	Déploiement	Création d'un hôte de base de données
	Journaux:CreateLogStream	Déploiement	Création d'un hôte de base de données
	journaux : GetLogGroupFields	Déploiement	Création d'un hôte de base de données
	journaux : GetLogRecord	Déploiement	Création d'un hôte de base de données
	Journaux:ListLogDeliveries	Déploiement	Création d'un hôte de base de données
	Journaux:PutLogEvents	• Déploiement • Les opérations de gestion	Création d'un hôte de base de données
	Journaux:TagResource	Déploiement	Création d'un hôte de base de données
Workload Factory bascule vers les journaux Amazon CloudWatch pour l'instance SQL en cas de troncature de sortie SSM	Journaux:GetLogEvents	• Évaluation du stockage (optimisation) • Inventaire	Vue, planification et analyse
Autoriser Workload Factory à obtenir les groupes de journaux actuels et vérifier que la conservation est définie pour les groupes de journaux créés par Workload Factory	Journaux:DescribeLogGroups	• Évaluation du stockage (optimisation) • Inventaire	Vue, planification et analyse
Autoriser Workload Factory à définir une politique de conservation d'un jour pour les groupes de journaux créés par Workload Factory afin d'éviter l'accumulation inutile de flux de journaux pour les sorties de commande SSM	Journaux:PutRetentionPolicy	• Évaluation du stockage (optimisation) • Inventaire	Vue, planification et analyse

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Dressez la liste des sujets SNS des clients et publiez-les sur le service SNS backend WLMDB ainsi que sur le service SNS des clients si cette option est sélectionnée	sns:ListTopics	Déploiement	Vue, planification et analyse
	sns:publier	Déploiement	Création d'un hôte de base de données
Autorisations SSM requises pour exécuter le script de découverte sur les instances SQL provisionnées et pour récupérer la dernière liste des régions AWS prises en charge par FSX pour ONTAP.	ssm:PutCompianceItems	Déploiement	Création d'un hôte de base de données
	ssm:PutConfigurePackageResult	Déploiement	Création d'un hôte de base de données
	ssm:PutInventory	Déploiement	Création d'un hôte de base de données
	ssm:UpdateAssociationStatus	Déploiement	Création d'un hôte de base de données
	ssm:UpdateInstanceAssociationStatus	Déploiement	Création d'un hôte de base de données
	ssm:UpdateInstanceinformation	Déploiement	Création d'un hôte de base de données
	ssmmessages:Créer un canal de contrôle	Déploiement	Création d'un hôte de base de données
	ssmmessages : Créer un canal de données	Déploiement	Création d'un hôte de base de données
	ssmmessages : OpenControlChannel	Déploiement	Création d'un hôte de base de données
	ssmmessages : OpenDataChannel	Déploiement	Création d'un hôte de base de données
Pile de signal CloudFormation en cas de succès ou d'échec.	Formation du nuage:SignalResource [1]	Déploiement	Création d'un hôte de base de données
Ajoutez le rôle EC2 créé par le modèle au profil d'instance d'EC2 pour permettre aux scripts sur EC2 d'accéder aux ressources requises pour le déploiement.	iam:AddRoleToInstanceProfile	Déploiement	Création d'un hôte de base de données

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Créez un profil d'instance pour EC2 et associez le rôle EC2 créé.	iam:CreateInstanceProfile	Déploiement	Création d'un hôte de base de données
Créez un rôle EC2 via un modèle avec les autorisations répertoriées ci-dessous	iam:CreateRole	Déploiement	Création d'un hôte de base de données
Créer un rôle lié au service EC2	iam:CreateServiceLinkedRole [2]	Déploiement	Création d'un hôte de base de données
Supprimez le profil d'instance créé lors du déploiement, spécifiquement pour les nœuds de validation	iam:DeleteInstanceProfile	Déploiement	Création d'un hôte de base de données
Obtenez les détails du rôle et de la stratégie pour déterminer les écarts d'autorisation et les valider pour le déploiement	iam:GetPolicy	Déploiement	Création d'un hôte de base de données
	iam:GetPolicyVersion	Déploiement	Création d'un hôte de base de données
	iam:GetRole	Déploiement	Création d'un hôte de base de données
	iam:GetRolePolicy	Déploiement	Création d'un hôte de base de données
	iam:GetUser	Déploiement	Création d'un hôte de base de données
Transmettre le rôle créé à l'instance EC2	iam:PassRole [3]	Déploiement	Création d'un hôte de base de données
Ajoutez une règle avec les autorisations requises au rôle EC2 créé	iam:PutRolePolicy	Déploiement	Création d'un hôte de base de données
Détacher le rôle du profil d'instance EC2 provisionné	iam:RemoveRoleFromInstanceProfile	Déploiement	Création d'un hôte de base de données
Simulez les opérations de workload pour valider les autorisations disponibles et les comparer avec les autorisations de compte AWS requises	iam:SimulatePrincipalPolicy	Déploiement	Tous

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Obtenez les modèles de base disponibles pour l'analyse des journaux d'erreurs.	Bedrock:GetFoundationModelAvailability	Analyse du journal des erreurs	Vue, planification et analyse
Liste des profils d'interface disponibles dans Amazon Bedrock pour l'analyse des journaux d'erreurs	Bedrock:ListeInferenceProfiles	Analyse du journal des erreurs	Vue, planification et analyse

1. L'autorisation est limitée aux ressources commençant par WLMDB.
2. "iam:CreateServiceLinkedRole" limité par "iam:AWSServiceName": "ec2.amazonaws.com"*
3. "iam:PassRole" limité par "iam:PassedToService": "ec2.amazonaws.com"*

Autorisations pour les workloads GenAI

Les stratégies IAM pour les charges de travail VMware fournissent les autorisations dont Workload Factory for VMware a besoin pour gérer les ressources et les processus au sein de votre environnement de cloud public en fonction du mode opérationnel dans lequel vous opérez.

Les politiques IAM de GenAI ne sont disponibles qu'avec les autorisations de lecture/écriture :

- **Lecture/Écriture** : exécute et automatise les opérations dans AWS en votre nom, avec les informations d'identification attribuées qui disposent des autorisations nécessaires et validées pour l'exécution.

Règles IAM pour les workloads GenAI

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CloudformationGroup",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks"
      ],
      "Resource": "arn:aws:cloudformation:*:*:stack/wlmai*/*"
    },
    {
      "Sid": "EC2Group",
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/aws:cloudformation:stack-name": "wlmai*"
        }
      }
    },
    {
      "Sid": "EC2DescribeGroup",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:RevokeSecurityGroupEgress",
```

```
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMGroup",
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:CreateInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:PutRolePolicy",
        "iam:GetRolePolicy",
        "iam:GetRole",
        "iam:TagRole"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMGroup2",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid": "FSXNGroup",
      "Effect": "Allow",
      "Action": [
        "fsx:DescribeVolumes",
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "FSXNGroup2",
      "Effect": "Allow",
      "Action": [
        "fsx:UntagResource",
```

```
        "fsx:TagResource"
      ],
      "Resource": [
        "arn:aws:fsx:*:*:volume/*/*",
        "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
      ]
    },
    {
      "Sid": "SSMParameterStore",
      "Effect": "Allow",
      "Action": [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource": "arn:aws:ssm:*:*:parameter/netapp/wlmai/*"
    },
    {
      "Sid": "SSM",
      "Effect": "Allow",
      "Action": [
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
      ],
      "Resource": "arn:aws:ssm:*:*:parameter/aws/service/*"
    },
    {
      "Sid": "SSMMessages",
      "Effect": "Allow",
      "Action": [
        "ssm:GetCommandInvocation"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SSMCommandDocument",
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand"
      ],
      "Resource": [
        "arn:aws:ssm:*:*:document/AWS-RunShellScript"
      ]
    },
    {
      "Sid": "SSMCommandInstance",
      "Effect": "Allow",
```

```
      "Action": [
        "ssm:SendCommand",
        "ssm:GetConnectionStatus"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringLike": {
          "ssm:resourceTag/aws:cloudformation:stack-name": "wlmai-*"
        }
      }
    },
    {
      "Sid": "KMS",
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SNS",
      "Effect": "Allow",
      "Action": [
        "sns:Publish"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudWatch",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudWatchAiEngine",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
        "logs:DescribeLogStreams"
```

```
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/netapp/wlmai*"
    },
    {
      "Sid": "CloudWatchAiEngineLogStream",
      "Effect": "Allow",
      "Action": [
        "logs:GetLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/netapp/wlmai*:*"
    },
    {
      "Sid": "BedrockGroup",
      "Effect": "Allow",
      "Action": [
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:InvokeModel",
        "bedrock:ListFoundationModels",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:PutModelInvocationLoggingConfiguration",
        "bedrock:ListInferenceProfiles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudWatchBedrock",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:TagResource"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/bedrock*"
    },
    {
      "Sid": "BedrockLoggingAttachRole",
      "Effect": "Allow",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::*:role/NetApp_AI_Bedrock*"
    },
    {
      "Sid": "BedrockLoggingIamOperations",
```

```
      "Effect": "Allow",
      "Action": [
        "iam:CreatePolicy"
      ],
      "Resource": "*"
    },
    {
      "Sid": "QBusiness",
      "Effect": "Allow",
      "Action": [
        "qbusiness:ListApplications"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Le tableau suivant fournit des détails sur les autorisations pour les charges de travail GenAI.

Tableau des autorisations pour les charges de travail GenAI

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Créez une pile de formation cloud pour les moteurs d'IA pendant les opérations de déploiement et de reconstruction	Cloudformation:CreateStack	Déploiement	Lecture/écriture
Créez la pile de formation cloud du moteur d'IA	Cloudformation:DescribeSacks	Déploiement	Lecture/écriture
Répertoriez les régions de l'assistant de déploiement de moteur ai	ec2:régions descriptives	Déploiement	Lecture/écriture
Afficher les balises du moteur ai	ec2:Etiquettes descriptives	Déploiement	Lecture/écriture
Lister les buckets S3	s3:ListAllMyseaux	Déploiement	Lecture/écriture
Répertoriez les terminaux VPC avant la création de la pile du moteur d'IA	ec2:CreateVpcEndpoint	Déploiement	Lecture/écriture
Créez un groupe de sécurité de moteur d'IA lors des opérations de déploiement et de reconstruction lors de la création de la pile du moteur d'IA	ec2:CreateSecurityGroup	Déploiement	Lecture/écriture
Balisez les ressources créées par la création d'une pile de moteur d'IA pendant les opérations de déploiement et de reconstruction	ec2:CreateTags	Déploiement	Lecture/écriture
Publier des événements cryptés sur le back-end WLMAI à partir de la pile de moteur ai	Km:GenerateDataKey	Déploiement	Lecture/écriture
	Km:déchiffrer	Déploiement	Lecture/écriture
Publier des événements et des ressources personnalisées sur le backend WLMAI à partir de la pile ai-Engine	sns:publier	Déploiement	Lecture/écriture
Répertorier les VPC pendant l'assistant de déploiement du moteur d'IA	ec2 : descriptif	Déploiement	Lecture/écriture
Répertoriez les sous-réseaux dans l'assistant de déploiement du moteur ai	ec2:DescribeSubnets	Déploiement	Lecture/écriture
Obtenez des tables de routage lors du déploiement et de la reconstruction d'un moteur d'IA	ec2:DescribeRoutetables	Déploiement	Lecture/écriture

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Répertoriez les paires de clés pendant l'assistant de déploiement de moteur d'IA	ec2:Décrivez des Keypaires	Déploiement	Lecture/écriture
Liste des groupes de sécurité lors de la création de la pile du moteur d'IA (pour rechercher les groupes de sécurité sur les terminaux privés)	ec2:descriptifs des groupes de sécurité	Déploiement	Lecture/écriture
Procurez-vous des terminaux VPC pour déterminer si un doit être créé pendant le déploiement du moteur d'IA	ec2:DescribeVpcEndpoints	Déploiement	Lecture/écriture
Répertoriez les applications Amazon Q Business	Qbusiness:ListApplications	Déploiement	Lecture/écriture
Répertoriez les instances pour connaître l'état du moteur ai	ec2:descriptifs	Dépannage	Lecture/écriture
Répertoriez les images lors de la création de la pile du moteur d'IA pendant les opérations de déploiement et de reconstruction	ec2:descriptifs	Déploiement	Lecture/écriture
Créez et mettez à jour l'instance d'IA et le groupe de sécurité de terminal privé lors de la création de la pile d'instance d'IA lors des opérations de déploiement et de reconstruction	ec2 : RevokeSecurityGroupEgress	Déploiement	Lecture/écriture
	ec2 : RevokeSecurityGroupIngress	Déploiement	Lecture/écriture
Exécutez le moteur d'IA lors de la création de la pile dans le cloud pendant les opérations de déploiement et de reconstruction	ec2:RunInstances	Déploiement	Lecture/écriture
Associez un groupe de sécurité et modifiez les règles du moteur d'IA lors de la création de la pile lors des opérations de déploiement et de reconstruction	ec2:AuthoreSecurityGroupEgress	Déploiement	Lecture/écriture
	ec2:AuthoreSecurityGroupIngress	Déploiement	Lecture/écriture
Lancez une demande de discussion sur l'un des modèles de base	Bedrock:InvoieModelWithResponseStream	Déploiement	Lecture/écriture
Commencez la discussion/l'intégration de la demande pour les modèles de base	Bedrock:modèle de facturation	Déploiement	Lecture/écriture
Affiche les modèles de base disponibles dans une région	Bedrock:ListFoundationModels	Déploiement	Lecture/écriture

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Obtenez des informations sur un modèle de base	Bedrock:GetFoundationModel	Déploiement	Lecture/écriture
Vérifiez l'accès au modèle de base	Bedrock:GetFoundationModelAvailability	Déploiement	Lecture/écriture
Vérifiez qu'il est nécessaire de créer un groupe de journaux Amazon CloudWatch pendant les opérations de déploiement et de reconstruction	Journaux:DescribeLogGroups	Déploiement	Lecture/écriture
Obtenez des régions qui prennent en charge FSX et Amazon Bedrock pendant l'assistant du moteur d'IA	ssm:GetParametersByPath	Déploiement	Lecture/écriture
Obtenez la dernière image Amazon Linux pour le déploiement du moteur d'IA lors des opérations de déploiement et de reconstruction	ssm:GetParameters	Déploiement	Lecture/écriture
Obtenir la réponse SSM de la commande envoyée au moteur ai	ssm:GetCommandInvocation	Déploiement	Lecture/écriture
Vérifier la connexion SSM au moteur ai	ssm:SendCommand	Déploiement	Lecture/écriture
	ssm:GetConnectionStatus	Déploiement	Lecture/écriture
Créez un profil d'instance de moteur d'IA lors de la création de la pile lors des opérations de déploiement et de reconstruction	iam:CreateRole	Déploiement	Lecture/écriture
	iam:CreateInstanceProfile	Déploiement	Lecture/écriture
	iam:AddRoleToInstanceProfile	Déploiement	Lecture/écriture
	iam:PutRolePolicy	Déploiement	Lecture/écriture
	iam:GetRolePolicy	Déploiement	Lecture/écriture
	iam:GetRole	Déploiement	Lecture/écriture
	iam:TagRole	Déploiement	Lecture/écriture
	iam:PassRole	Déploiement	Lecture/écriture
Simulez les opérations de workload pour valider les autorisations disponibles et les comparer avec les autorisations de compte AWS requises	iam:SimulatePrincipalPolicy	Déploiement	Lecture/écriture
Répertoriez les systèmes de fichiers FSX pour ONTAP au cours de l'assistant de création de la base de connaissances	fsx:Describevolumes	Création d'une base de connaissances	Lecture/écriture

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Répertoriez les volumes du système de fichiers FSX pour ONTAP au cours de l'assistant « Créer une base de connaissances »	fsx:DescribeFileSystems	Création d'une base de connaissances	Lecture/écriture
Gérer les bases de connaissances sur le moteur d'IA pendant les opérations de reconstruction	fsx:ListTagsForResource	Dépannage	Lecture/écriture
Répertoriez les machines virtuelles de stockage du système de fichiers FSX pour ONTAP au cours de l'assistant « Créer une base de connaissances »	fsx:DescribeStockVirtualMachines	Déploiement	Lecture/écriture
Déplacez la base de connaissances vers une nouvelle instance	fsx:UntagResource	Dépannage	Lecture/écriture
Gérez la base de connaissances sur le moteur d'IA pendant la reconstruction	fsx:TagResource	Dépannage	Lecture/écriture
Enregistrez les secrets SSM (jeton ECR, informations d'identification CIFS, clés de compte de service de location) de manière sécurisée	ssm:getParameter	Déploiement	Lecture/écriture
	ssm:PutParameter	Déploiement	Lecture/écriture
Envoyez les journaux du moteur d'IA au groupe de journaux Amazon CloudWatch pendant les opérations de déploiement et de reconstruction	Journaux:CreateLogGroup	Déploiement	Lecture/écriture
	Journaux:PutRetentionPolicy	Déploiement	Lecture/écriture
Envoyez les journaux du moteur d'IA au groupe de journaux Amazon CloudWatch	Journaux:TagResource	Dépannage	Lecture/écriture
Obtenir la réponse SSM d'Amazon CloudWatch (lorsque la réponse est trop longue)	Journaux:DescribeLogStreams	Dépannage	Lecture/écriture
Obtenez la réponse SSM d'Amazon CloudWatch	Journaux:GetLogEvents	Dépannage	Lecture/écriture
Créez un groupe de journaux Amazon CloudWatch pour les journaux Amazon Bedrock lors de la création de la pile lors des opérations de déploiement et de reconstruction	Journaux:CreateLogGroup	Déploiement	Lecture/écriture
	Journaux:PutRetentionPolicy	Déploiement	Lecture/écriture
	Journaux:TagResource	Déploiement	Lecture/écriture

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Liste des profils d'inférence pour le modèle	Bedrock:ListeInferenceProfiles	Dépannage	Lecture/écriture

Autorisations pour les workloads VMware

VMware Workloads propose les politiques d'autorisation suivantes :

- **Visualisation, planification et analyse** : Consultez l'inventaire des environnements de virtualisation EVS, obtenez une analyse détaillée de vos systèmes et explorez les économies possibles.
- **Déploiement et connectivité des banques de données** : Déployez les configurations de machines virtuelles recommandées sur les clusters Amazon EVS, Amazon EC2 ou VMware Cloud on AWS vSphere et utilisez des systèmes de fichiers Amazon FSx for NetApp ONTAP comme banques de données externes.

Sélectionnez la stratégie d'autorisation pour afficher les stratégies IAM requises :

Règles IAM pour workloads VMware

Vue, planification et analyse

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRegions",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeDhcpOptions",
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases",
        "secretsmanager:ListSecrets",
        "evs:ListEnvironments",
        "evs:GetEnvironment",
        "evs:ListEnvironmentVlans"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Déploiement et connectivité du datastore

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack"
      ],
      "Resource": "*"
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateFileSystem",
        "fsx:DescribeFileSystems",
        "fsx:CreateStorageVirtualMachine",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:CreateVolume",
        "fsx:DescribeVolumes",
        "fsx:TagResource",
        "sns:Publish",
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:CreateGrant"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances",
        "ec2:DescribeInstances",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeImages"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Le tableau suivant fournit des détails sur les autorisations pour les charges de travail VMware.

Tableau des autorisations pour les workloads VMware

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Associez des groupes de sécurité et modifiez les règles pour les nœuds provisionnés	ec2:AuthoreSecurityGroupIngress	Déploiement	Déploiement et connectivité du datastore
Création de volumes EBS	fsx:CreateVolume	Déploiement	Déploiement et connectivité du datastore
Balisez les valeurs personnalisées des ressources FSX pour NetApp ONTAP créées par les workloads VMware	fsx:TagResource	Déploiement	Déploiement et connectivité du datastore
Créez et validez le modèle CloudFormation	Cloudformation:CreateStack	Déploiement	Déploiement et connectivité du datastore
Gérer les balises et la sécurité du réseau sur les instances créées	ec2:CreateSecurityGroup	Déploiement	Déploiement et connectivité du datastore
Démarrez les instances créées	ec2:RunInstances	Déploiement	Déploiement et connectivité du datastore
Consultez les détails de l'instance EC2	ec2:descriptifs	Inventaire	Déploiement et connectivité du datastore
Répertoriez les images pendant la création de la pile pendant les opérations de déploiement et de reconstruction	ec2:descriptifs	Inventaire	Déploiement et connectivité du datastore
Afficher les détails de configuration des ensembles d'options DHCP associés aux VPC	ec2 : Décrire les options DHCP	Inventaire	Vue, planification et analyse
Obtenir les VPC dans l'environnement sélectionné pour remplir le formulaire de déploiement	ec2 : descriptif	• Déploiement • Inventaire	Vue, planification et analyse
Obtenez les sous-réseaux dans l'environnement sélectionné pour remplir le formulaire de déploiement	ec2:DescribeSubnets	• Déploiement • Inventaire	Vue, planification et analyse

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Demandez aux groupes de sécurité de l'environnement sélectionné de remplir le formulaire de déploiement	ec2:descriptifs des groupes de sécurité	Déploiement	Vue, planification et analyse
Obtenez les zones de disponibilité dans un environnement sélectionné	ec2:DescribeAvailabilityzones	• Déploiement • Inventaire	Vue, planification et analyse
Obtenez les régions avec la prise en charge d'Amazon FSX pour NetApp ONTAP	ec2:régions descriptives	Déploiement	Vue, planification et analyse
Obtenez les alias de clés KMS à utiliser pour le cryptage Amazon FSX for NetApp ONTAP	Kms:Listalas	Déploiement	Vue, planification et analyse
Obtenez des clés KMS à utiliser pour Amazon FSX for NetApp ONTAP Encryption	Km:ListKeys	Déploiement	Vue, planification et analyse
Obtenez les détails d'expiration des clés KMS à utiliser pour le chiffrement Amazon FSX for NetApp ONTAP	Km:DescribeKey	Déploiement	Vue, planification et analyse
Lister les secrets dans AWS Secrets Manager	gestionnaire de secrets : Lister les secrets	Inventaire	Vue, planification et analyse
Obtenez une liste des environnements d'Amazon EVS	evs:ListEnvironments	Inventaire	Vue, planification et analyse
Obtenez des informations détaillées sur un environnement Amazon EVS spécifique	evs:GetEnvironment	Inventaire	Vue, planification et analyse
Lister les VLAN associés à un environnement Amazon EVS	evs:ListEnvironmentVlans	Inventaire	Vue, planification et analyse

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Créez des ressources Amazon FSX pour NetApp ONTAP requises pour le provisionnement	fsx:CreateFileSystem	Déploiement	Déploiement et connectivité du datastore
	fsx:CreateStorageVirtualmachine	Déploiement	Déploiement et connectivité du datastore
	fsx:CreateVolume	• Déploiement • Les opérations de gestion	Déploiement et connectivité du datastore
Découvrez les détails sur Amazon FSX pour NetApp ONTAP	fsx:décrire*	• Déploiement • Inventaire • Les opérations de gestion • Découvrez les économies	Déploiement et connectivité du datastore
Obtenez des détails de clés KMS et utilisez-les pour le chiffrement Amazon FSX for NetApp ONTAP	Kms:CreateGrant	Déploiement	Déploiement et connectivité du datastore
	Km:décrire*	Déploiement	Vue, planification et analyse
	Km:liste*	Déploiement	Vue, planification et analyse
	Km:déchiffrer	Déploiement	Déploiement et connectivité du datastore
	Km:GenerateDataKey	Déploiement	Déploiement et connectivité du datastore

Objectif	Action	Cas d'utilisation	Politique d'autorisation
Répertoriez les sujets SNS des clients et publiez-les sur le service SNS back-end de WLMVMC ainsi que sur le service SNS des clients si cette option est sélectionnée	sns:publier	Déploiement	Déploiement et connectivité du datastore
Simulez les opérations de workload pour valider les autorisations disponibles et les comparer avec les autorisations de compte AWS requises	iam:SimulatePrincipalPolicy	Déploiement	• Déploiement et connectivité du datastore • Vue, planification et analyse

Journal des modifications

Lorsque des autorisations sont ajoutées et supprimées, nous les noterons dans les sections ci-dessous.

1er février 2025

Les autorisations suivantes ont été ajoutées à la charge de travail de stockage :

- `s3:TagResource`
- `s3:ListTagsForResource`
- `s3:UntagResource`
- `s3tables:CreateTableBucket`
- `s3tables:ListTables`
- `s3tables:GetTable`
- `s3tables:GetTableMetadataLocation`
- `s3tables:CreateTable`
- `s3tables:GetNamespace`
- `s3tables:PutTableData`
- `s3tables:CreateNamespace`
- `s3tables:GetTableData`
- `s3tables:ListNamespaces`
- `s3tables:ListTableBuckets`
- `s3tables:GetTableBucket`

- `s3tables:UpdateTableMetadataLocation`
- `s3tables:ListTagsForResource`
- `s3tables:TagResource`
- `s3:GetObjectTagging`
- `s3:ListBucket`

04 décembre 2025

Les autorisations suivantes ont été ajoutées à la charge de travail de stockage :

- `fsx:CreateAndAttachS3AccessPoint`
- `fsx:DetachAndDeleteS3AccessPoint`
- `s3:CreateAccessPoint`
- `s3:DeleteAccessPoint`

27 novembre 2025

Les autorisations suivantes ont été ajoutées à la charge de travail de stockage :

- `bedrock:ListInferenceProfiles`
- `bedrock:GetInferenceProfile`
- `bedrock:InvokeModelWithResponseStream`
- `bedrock:InvokeModel`

2 novembre 2025

Les politiques d'autorisation « lecture seule » et « lecture/écriture » ont été remplacées dans les charges de travail de stockage, de base de données et VMware afin d'offrir une plus grande granularité et une plus grande flexibilité dans l'attribution des autorisations.

5 octobre 2025

Les autorisations suivantes ont été supprimées de GenAI et sont désormais gérées par le moteur GenAI :

- `bedrock:GetModelInvocationLoggingConfiguration`
- `bedrock:PutModelInvocationLoggingConfiguration`
- `iam:AttachRolePolicy`
- `iam:PassRole`
- `iam:CreatePolicy`

29 juin 2025

L'autorisation suivante est désormais disponible en mode *lecture seule* pour les bases de données : `cloudwatch:GetMetricData` .

3 juin 2025

L'autorisation suivante est désormais disponible en mode *lecture/écriture* pour GenAI : `s3:ListAllMyBuckets` .

4 mai 2025

L'autorisation suivante est désormais disponible en mode *lecture/écriture* pour GenAI : `qbusiness:ListApplications` .

Les autorisations suivantes sont désormais disponibles en mode *lecture seule* pour les bases de données :

- `logs:GetLogEvents`
- `logs:DescribeLogGroups`

L'autorisation suivante est désormais disponible en mode *lecture/écriture* pour les bases de données : `logs:PutRetentionPolicy` .

2 avril 2025

L'autorisation suivante est désormais disponible en mode *lecture seule* pour les bases de données : `ssm:DescribeInstanceInformation` .

30 mars 2025

Mise à jour des autorisations de charge de travail GenAI

Les autorisations suivantes sont désormais disponibles en mode lecture/écriture pour GenAI :

- `bedrock:PutModelInvocationLoggingConfiguration`
- `iam:AttachRolePolicy`
- `iam:PassRole`
- `iam:createPolicy`
- `bedrock:ListInferenceProfiles`

L'autorisation suivante a été supprimée du *mode lecture/écriture* pour GenAI : `Bedrock:GetFoundationModel` .

iam:mise à jour des autorisations SimulatePrincipalPolicy

Le `iam:SimulatePrincipalPolicy` L'autorisation fait partie de toutes les stratégies d'autorisation de charge de travail si vous activez la vérification automatique des autorisations lors de l'ajout d'informations d'identification de compte AWS supplémentaires ou de l'ajout d'une nouvelle capacité de charge de travail à partir de la console Workload Factory. L'autorisation simule les opérations de charge de travail et vérifie si vous disposez des autorisations de compte AWS requises avant de déployer des ressources à partir de Workload Factory. L'activation de cette vérification réduit le temps et les efforts dont vous pourriez avoir besoin pour nettoyer les ressources des opérations ayant échoué et pour ajouter les autorisations manquantes.

2 mars 2025

L'autorisation suivante est désormais disponible en mode *lecture/écriture* pour GenAI : `bedrock:GetFoundationModel` .

3 février 2025

L'autorisation suivante est désormais disponible en mode *lecture seule* pour les bases de données : `iam:SimulatePrincipalPolicy` .