



Gérer les points d'accès S3

Workload Factory for NetApp Console

NetApp
October 07, 2026

Sommaire

- Gérer les points d'accès S3 1
 - Créez des points d'accès S3 pour un volume dans NetApp Workload Factory 1
 - Gérez les points d'accès S3 pour un volume dans NetApp Workload Factory 2
 - Modifier les points d'accès S3 pour un volume 2
 - Afficher les détails du point d'accès S3 pour un volume 3
 - Supprimez les points d'accès S3 pour un volume dans NetApp Workload Factory 3
- Configurez l'infrastructure de la table Journal pour NetApp Workload Factory 4
 - À propos de cette tâche 4
 - Avant de commencer 5
 - Configurer l'infrastructure de la table de journalisation 7
 - Dépannage de la configuration de l'infrastructure pour la table de journal 8
 - Référence des autorisations pour la configuration de la table du journal 11

Gérer les points d'accès S3

Créez des points d'accès S3 pour un volume dans NetApp Workload Factory

Créez et associez des points d'accès S3 à un volume dans NetApp Workload Factory.

À propos de cette tâche

Amazon FSx for NetApp ONTAP permet aux systèmes de fichiers NFS et SMB d'accéder aux données S3 et de se connecter aux services AWS comme Amazon Bedrock, SageMaker, Athena, AWS Glue, et plus encore. Vous pouvez connecter les services AWS à toutes vos données de stockage d'objets.

Associez des points d'accès S3 aux volumes NFS et SMB dans un système de fichiers FSx for ONTAP afin que les services AWS accèdent aux fichiers comme s'ils se trouvaient dans un compartiment S3. Lors de l'association du point d'accès, définissez un ID unique, sélectionnez le type d'accès aux fichiers (UNIX ou Windows) et ajoutez un nom d'utilisateur pour l'autorisation d'accès.

Après avoir attaché le point d'accès S3, il apparaît dans la console de gestion AWS avec un alias unique. Utilisez cet alias comme nom de compartiment S3 pour les services AWS, tels qu'Amazon Bedrock, afin d'accéder aux fichiers dans le volume FSx for ONTAP.

Vous pouvez attacher plusieurs points d'accès S3 à un seul volume FSx for ONTAP, chacun avec un niveau d'accès unique, pour vous connecter à plusieurs services AWS.

Avant de commencer

Veuillez remplir les conditions suivantes avant de commencer.

- Vous devez disposer d'un volume existant avec un point d'accès "[Créer un volume avec un point d'accès S3](#)"
- Vous devez "[accorder des identifiants avec la politique d'autorisation *operations and remediation*](#)" dans Workload Factory pour accomplir cette tâche.

Étapes

1. Connectez-vous au "[NetApp Console](#)".
2. Sélectionnez le menu , **Charges de travail > Explorateur de volumes**.
3. Sélectionnez le menu des actions du volume que vous souhaitez utiliser, puis sélectionnez **Actions avancées**, puis **Gérer les points d'accès S3**.
4. Sur la page Gérer les points d'accès S3, sélectionnez **Créer et associer point d'accès S3**.
5. Sur la page **Créer et connecter un point d'accès S3**, fournissez les informations suivantes :
 - **Nom du point d'accès S3** : Saisissez le nom du point d'accès S3.
 - **Utilisateur** : Sélectionnez un utilisateur existant ayant accès au volume ou créez un nouvel utilisateur.
 - **Type d'utilisateur** : sélectionnez **UNIX** ou **Windows** comme type d'utilisateur.
 - **Configuration réseau** : Sélectionnez **Internet** ou **Virtual private cloud (VPC)**. Le type de réseau choisi détermine si le point d'accès est accessible depuis Internet ou s'il est limité à un VPC spécifique. Pour utiliser la fonction Journal table, vous devez sélectionner **Internet** comme configuration réseau.
 - **Tableau d'inventaire** : Facultatif. Nécessite la getObject autorisation. Activez le tableau d'inventaire

sur le volume pour générer des métadonnées pour tous les objets accessibles au point d'accès S3 et des frais de requête AWS S3 s'appliquent. Consultez ["Documentation tarifaire Amazon S3"](#) pour plus d'informations. Le tableau est mis à jour toutes les 24 heures.

- **Étiquettes de point d'accès S3** : Vous pouvez éventuellement ajouter jusqu'à 50 étiquettes ou en supprimer.

6. Sélectionnez **Créer**.

Informations connexes

Vous pouvez, en option, utiliser la fonctionnalité de table de journal avec les points d'accès S3 dans Workload Factory. L'infrastructure de la table de journal capture et stocke les journaux d'audit des événements d'accès utilisateur et des opérations sur les objets via les points d'accès de volume Amazon FSx for ONTAP. Pour activer la fonctionnalité de table de journal, vous devez configurer l'infrastructure AWS nécessaire, y compris AWS CloudTrail, AWS CloudWatch, les compartiments AWS S3, les groupes de journaux AWS CloudWatch et les rôles et politiques AWS Identity and Access Management (IAM). ["Configurez l'infrastructure de la table de journalisation pour NetApp Workload Factory"](#).

Autres sujets connexes :

["Modifiez ou supprimez les points d'accès S3 pour un volume dans NetApp Workload Factory"](#)

Gérez les points d'accès S3 pour un volume dans NetApp Workload Factory

Mettez à jour les détails du point d'accès S3 ou supprimez les points d'accès S3 d'un volume dans NetApp Workload Factory.

Vous pouvez également activer ou désactiver la **table d'inventaire** pour le point d'accès. La table d'inventaire génère des métadonnées pour tous les objets accessibles au point d'accès S3 et engendre des coûts de requête AWS S3. Consultez ["Documentation tarifaire Amazon S3"](#) pour plus d'informations.

Modifier les points d'accès S3 pour un volume

Modifiez les points d'accès S3 pour un volume dans NetApp Workload Factory.

Étapes

1. Connectez-vous au ["NetApp Console"](#).
2. Sélectionnez le menu , **Charges de travail > Stockage > Explorateur de volumes**.
3. Sélectionnez le menu actions du volume pour lequel vous souhaitez modifier les points d'accès S3, puis sélectionnez **Actions avancées**, puis **Gérer les points d'accès S3**.
4. Depuis l'écran **Gérer les points d'accès S3**, sélectionnez le menu actions, puis sélectionnez **Modifier point d'accès**.
5. Apportez les mises à jour, puis sélectionnez **Appliquer**.

Pour configurer l'infrastructure de la fonctionnalité de table de journal, vous devez sélectionner **Internet** comme configuration réseau pour le point d'accès S3. ["Découvrez comment configurer l'infrastructure de la table Journal pour NetApp Workload Factory"](#).

Afficher les détails du point d'accès S3 pour un volume

Consultez les détails du point d'accès S3, tels que l'alias, l'ARN et l'URI S3. Avec les tables d'inventaire et de journal activées, vous pouvez consulter les métadonnées et les journaux d'audit des événements d'accès utilisateur et des opérations sur les objets à travers les points d'accès S3.

À propos de cette tâche

Lorsque la table d'inventaire est activée sur le volume, vous pouvez consulter les détails du point d'accès, de la table d'inventaire et du compartiment de table des points d'accès S3 existants associés au volume. Le système fournit également un lien vers la table d'inventaire dans la console de gestion AWS.

Lorsque la table de journal est activée, Workload Factory génère des journaux sur les points d'accès dans un tableau pour votre référence. Le tableau inclut les événements CloudTrail, les traces (un enregistrement des activités AWS), les filtres CloudTrail, les groupes de journaux CloudWatch, et plus encore.

Vous pouvez copier les détails du point d'accès pour les utiliser dans d'autres applications.

Étapes

1. Connectez-vous au ["NetApp Console"](#).
2. Sélectionnez le menu , **Charges de travail > Stockage > Explorateur de volumes**.
3. Sélectionnez le menu Actions du volume dont vous souhaitez afficher les détails, puis sélectionnez **Actions avancées**, et enfin **Afficher les détails**.

Les détails apparaissent sous quatre onglets : **Point d'accès**, **Tableau d'inventaire**, **Tableau de journal** et **Table bucket**.

4. Si le statut des tables d'inventaire ou de journal est activé, mais que vous ne disposez pas de l'`get:Object` autorisation, suivez les instructions de la boîte de dialogue pour ajouter l'autorisation requise.
5. Lorsque le statut de la table de journal est en attente, vous devez fournir l'CloudTrail ARN pour connecter la table de journal à l'infrastructure créée. Suivez les instructions pour déployer la pile CloudFormation à l'aide de l'AWS CLI ou de la console de gestion AWS, puis retournez à la console NetApp Workload Factory pour saisir l'CloudTrail ARN.

Supprimez les points d'accès S3 pour un volume dans NetApp Workload Factory

Supprimez les points d'accès S3 existants d'un volume dans NetApp Workload Factory.

Étapes

1. Connectez-vous au ["NetApp Console"](#).
2. Sélectionnez le menu , **Charges de travail > Stockage > Explorateur de volumes**.
3. Sélectionnez le menu actions du volume pour lequel vous souhaitez gérer les points d'accès S3, puis sélectionnez **Actions avancées**, puis **Gérer les points d'accès S3**.
4. Sélectionnez le menu des actions pour le point d'accès S3 à supprimer, puis sélectionnez **Supprimer**.
5. Dans la boîte de dialogue **Supprimer un point d'accès S3**, sélectionnez **Supprimer** pour supprimer le point d'accès S3 du volume.

Workload Factory ne supprime pas la table d'inventaire ni la table de journal, mais vous pouvez les supprimer manuellement depuis la console de gestion AWS.

- ["Configurer l'infrastructure de la table de journalisation"](#)

Configurez l'infrastructure de la table Journal pour NetApp Workload Factory

Configurez l'infrastructure de la table Journal pour capturer et stocker les journaux d'audit des événements d'accès utilisateur et des opérations sur les objets via les points d'accès de volume Amazon FSx for ONTAP. Plusieurs étapes sont nécessaires pour configurer l'infrastructure des services AWS tels que AWS CloudTrail, AWS CloudWatch, AWS S3 Buckets, AWS CloudWatch log group, AWS Identity and Access Management (IAM) et AWS S3 Tables afin que les événements de journalisation transitent correctement par le pipeline et soient lus par Workload Factory.

À propos de cette tâche

La fonctionnalité de table Journal enregistre les événements du plan de données S3 (PutObject, GetObject, DeleteObject, etc.) pour les points d'accès S3 FSx for ONTAP surveillés. Elle utilise une chaîne de services AWS déployée dans votre compte AWS. Lorsque vous configurez correctement l'infrastructure, elle se connecte au point d'accès du volume FSx for ONTAP et établit le pipeline qui capture les événements d'audit d'accès utilisateur et d'opérations sur les objets dans la table Journal.

Le tableau suivant répertorie les services AWS qui font partie de l'infrastructure, leurs modèles de noms de ressources respectifs et le rôle du service dans le pipeline.

Service AWS	Modèle de nom de ressource	But
AWS CloudFormation	netapp-metadata-*	Déploie toute l'infrastructure sous forme de pile
Compartiment S3 AWS	netapp-metadata-cloudtrail-events-logs-{uuid}	Stocke les fichiers journaux bruts CloudTrail
AWS CloudTrail	netapp-metadata-journal-data-events-trail-{uuid}	Capture les événements de données S3 pour des points d'accès spécifiques
Groupe de journaux AWS CloudWatch	netapp-metadata-journal-data-events-{uuid}	Reçoit les événements CloudTrail sous forme d'entrées de journal structurées
Rôles IAM	- netapp-metadata-cloudtrail-cw-role-{uuid} - rôle d'intégration des métadonnées S3 de NetApp{uuid}	Intégration active
ObservabilityAdmin	S3TableIntegration	Bridges CloudWatch Logs dans une table S3 Tables
Tables S3	compartiment aws-cloudwatch → logs.aws_cloudtrail__data	Stocke des événements structurés et interrogeables CloudTrail au format Iceberg

Le {uuid} est un identifiant aléatoire de 8 caractères généré lors de la création du modèle.

Avant de commencer

Pour activer la fonctionnalité de tableau de journal, procédez comme suit :

- Disposez d'un volume existant avec un point d'accès ["Créer un volume avec un point d'accès S3"](#)
- Configurez le réseau sur **Internet** pour le point d'accès S3. ["Modifier la configuration réseau du point d'accès S3"](#).
- ["Accorder les autorisations d'opérations et de correction"](#) à vos identifiants NetApp Workload Factory.
- Ajoutez les autorisations de stratégie IAM suivantes au compte AWS que vous utilisez pour exécuter le déploiement CloudFormation afin de configurer la table Journal.

▼ Autorisations de stratégie IAM pour la configuration de la table Journal

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CFNStack",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource": "arn:aws:cloudformation:*:*:stack/netapp-
metadata-*/*"
    },
    {
      "Sid": "StarResources",
      "Effect": "Allow",
      "Action": [
        "cloudformation:GetTemplateSummary",
        "cloudtrail:DescribeTrails",
        "logs:DescribeLogGroups",
        "logs:ListSourcesForS3TableIntegration",
        "observabilityadmin:CreateS3TableIntegration",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:TagResource",
        "observabilityadmin:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3Bucket",
      "Effect": "Allow",
```

```

        "Action": [
            "s3:CreateBucket",
            "s3:PutBucketPolicy",
            "s3:PutBucketTagging"
        ],
        "Resource": "arn:aws:s3:::netapp-metadata-*"
    },
    {
        "Sid": "IAMRoles",
        "Effect": "Allow",
        "Action": [
            "iam:CreateRole",
            "iam:PutRolePolicy",
            "iam:TagRole",
            "iam:GetRole"
        ],
        "Resource": "arn:aws:iam::*:role/netapp-metadata-*"
    },
    {
        "Sid": "PassRole",
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::*:role/netapp-metadata-*",
        "Condition": {
            "StringEquals": {
                "iam:PassedToService": [
                    "cloudtrail.amazonaws.com",
                    "logs.amazonaws.com"
                ]
            }
        }
    },
    {
        "Sid": "CloudTrail",
        "Effect": "Allow",
        "Action": [
            "cloudtrail:CreateTrail",
            "cloudtrail:StartLogging",
            "cloudtrail:AddTags",
            "cloudtrail:PutEventSelectors"
        ],
        "Resource": "arn:aws:cloudtrail::*:trail/netapp-metadata-*"
    },
    {
        "Sid": "CWLogGroup",

```

```

    "Effect": "Allow",
    "Action": [
        "logs:CreateLogGroup",
        "logs>DeleteLogGroup",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
        "logs:AssociateSourceToS3TableIntegration"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:netapp-metadata-*"
  },
  {
    "Sid": "S3Table",
    "Effect": "Allow",
    "Action": [
        "s3tables:CreateTableBucket",
        "s3tables:PutTableBucketEncryption",
        "s3tables:PutTableBucketPolicy"
    ],
    "Resource": "arn:aws:s3tables:*:*:bucket/aws-cloudwatch"
  }
]
}

```

Configurer l'infrastructure de la table de journalisation

Configurez l'infrastructure pour capturer les événements du service AWS à partir du point d'accès S3 dans la table de journal.

Étapes

1. Connectez-vous au ["NetApp Console"](#).
2. Sélectionnez le menu  **Workloads > Storage > FSx for ONTAP**.
3. Dans **FSx for ONTAP**, sélectionnez le menu Actions du système de fichiers contenant le volume à mettre à jour, puis sélectionnez **Gérer**.
4. Depuis l'aperçu du système de fichiers, sélectionnez l'onglet **Volumes**.
5. Dans l'onglet Volumes, sélectionnez le menu actions du volume pour lequel vous souhaitez gérer les points d'accès S3, puis sélectionnez **Advanced actions**, puis **Manage S3 access points**.
6. Depuis l'écran **Gérer les points d'accès S3**, sélectionnez le menu actions, puis sélectionnez **Modifier point d'accès**.
7. Dans la boîte de dialogue **Modifier le point d'accès S3**, assurez-vous que la configuration réseau est définie sur **Internet**.
8. Suivez les instructions de la boîte de dialogue pour configurer l'infrastructure de la fonctionnalité de table de journal.
9. Téléchargez le modèle CloudFormation.
10. Déployez la pile CloudFormation dans votre compte AWS.

- a. Enregistrez le modèle JSON dans un fichier.
 - b. Déployez le modèle à l'aide de l'AWS CLI ou de la console de gestion AWS.
 - c. Attendez que la pile atteigne `CREATE_COMPLETE` le statut.
 - d. Récupérez l'CloudTrail ARN à partir des sorties de la pile.
11. Retournez à la console Workload Factory et revenez au volume pour gérer les points d'accès S3.
 12. Sélectionnez **Afficher les détails** dans le menu des actions de volume.
 13. Dans l'onglet **Tableau de journal**, saisissez l'ARN CloudTrail.
 14. Sélectionnez **Appliquer**.

Si l'une des étapes échoue, [Dépanner la configuration de l'infrastructure pour la table de journal](#) ou contactez le support NetApp pour obtenir de l'aide.

Dépannage de la configuration de l'infrastructure pour la table de journal

Vous pouvez utiliser la console de gestion AWS ou l'AWS CLI pour résoudre les problèmes survenant lors du déploiement de la pile CloudFormation et des ressources qu'elle crée.

Après avoir résolu le problème, soumettez à nouveau l'ARN CloudTrail pour redémarrer la configuration de la table de journalisation.

Échecs de déploiement courants CloudFormation

Autorisations IAM insuffisantes

Le rôle/utilisateur chargé du déploiement requiert des autorisations spécifiques. Consultez [Avant de commencer](#) pour la politique complète.

Si la pile échoue avec une `AccessDenied` ou `InsufficientPermission` erreur, vérifiez les événements de la pile et recherchez l'autorisation manquante dans le champ `ResourceStatusReason`.

Limite CloudTrail

AWS impose une limite par défaut de 5 trails par région. Si le compte a déjà 5 trails, the `FsxDataEventTrail` la ressource échouera avec : `Maximum number of trails (5) exceeded`. Vous pouvez vérifier le nombre de trails au niveau régional avec la commande suivante :

```
aws cloudtrail describe-trails \
  --no-include-shadow-trails \
  --region <region> \
  --query "length(trailList) "
```

Options de résolution

- Option 1 : Supprimer un trail inutilisé dans la région pour libérer de l'espace.
- Option 2 : Utiliser un trail existant. Supprimez les ressources `FsxDataEventTrail`, `CloudTrailBucket`, `CloudTrailBucketPolicy` et `CloudTrailToCloudWatchRole` du modèle avant de redéployer la pile CloudFormation. Transmettez ensuite l'ARN de votre trail existant lors de l'étape d'initialisation. Le trail existant doit avoir un groupe de journaux CloudWatch configuré, une `S3TableIntegration` associée à ce groupe de journaux, et enregistrer des événements de données.

L'intégration des tables S3 existe déjà

Si le compte possède déjà une intégration S3TableIntegration pour la source de données aws_cloudtrail, la ressource LogsToS3TableIntegration échouera.

Résolution

Supprimez les LogsToS3TableIntegration et S3TableIntegrationRole ressources du modèle avant de redéployer la pile CloudFormation. Le système utilise automatiquement l'intégration existante si vous la configurez pour les événements de données aws_cloudtrail.

Pour vérifier l'existence d'une intégration :

```
aws observabilityadmin list-s3-table-integrations --region <your-region>
```

Le nom du compartiment S3 existe déjà

Le nom du compartiment netapp-metadata-cloudtrail-events-logs-{uuid} est unique au niveau mondial. En cas de collision, redemandez le modèle pour obtenir un nouvel UUID.

Le rôle IAM existe déjà

Si un déploiement partiel précédent a laissé des rôles IAM avec le netapp-metadata-* modèle de nom, la création du rôle échouera. Supprimez d'abord les rôles orphelins :

```
aws iam delete-role-policy \
  --role-name netapp-metadata-cloudtrail-cw-role-<uuid> \
  --policy-name <policy-name>
aws iam delete-role \
  --role-name netapp-metadata-cloudtrail-cw-role-<uuid>
```

Échecs après l'activation de la table Journal

Après la soumission de l'CloudTrail ARN, Workload Factory valide l'ensemble du pipeline de ressources en envoyant automatiquement un seed, ou événement de test. En cas de succès, l'événement seed arrive dans la table S3 Tables. Le test prend environ 10 minutes.

Si la validation du test échoue, vous pourriez recevoir l'un des messages d'erreur suivants :

Message d'erreur	Signification
La table aws_cloudtrail__data n'a pas été créée dans {bucket}. Vérifiez les autorisations s3table.	S3TableIntegration n'a pas créé la table gérée par CloudWatch. Le pipeline entre les journaux CloudWatch et les tables S3 est interrompu.
La table existe, mais l'événement initial du journal n'apparaît pas. Vérifiez les autorisations CloudTrail et CloudWatch.	La table existe, mais l'événement initial spécifique n'a jamais été reçu. Le pipeline est interrompu entre CloudTrail et la table S3 Tables.
Échec de la configuration du journal. ...	Une erreur s'est produite lors de l'exécution du processus d'amorçage/d'interrogation en arrière-plan. Vérifiez le message suivant pour plus de détails.

Étapes de résolution

Lorsque le journal atteint l'état FAILED, suivez l'événement initial à travers les différentes étapes du pipeline pour identifier précisément où il s'est arrêté. Chaque étape correspond à une ressource AWS spécifique créée par le template.

1. Vérifiez le compartiment S3 CloudTrail.

Le processus enregistre les journaux d'événements bruts dans le compartiment S3 `netapp-metadata-cloudtrail-events-logs`. Consultez les fichiers journaux récents.

Si aucun fichier journal n'existe, alors CloudTrail n'enregistre pas les événements. Vérifiez les points suivants :

- La piste est en cours de journalisation (`IsLogging: true`)
- Les sélecteurs d'événements avancés incluent l'ARN du point d'accès correct
- Les sélecteurs d'événements avancés incluent les filtres pour `eventCategory = Data` et `resources.type = AWS::S3::AccessPoint`

2. Vérifiez le groupe de journaux CloudWatch.

Le trail transmet également les événements au groupe de journaux CloudWatch. Le nom du groupe de journaux commence par `netapp-metadata-journal-data-events-<uuid>`.

- Si le groupe de journaux est vide, alors CloudTrail ne transmet pas d'événements à CloudWatch. Vérifiez que le `CloudTrailToCloudWatchRole` rôle IAM existe et dispose des autorisations `logs:CreateLogStream` et `logs:PutLogEvents`, et que le trail est configuré avec le `CloudWatchLogsLogGroupArn` et le `CloudWatchLogsRoleArn` corrects.
- Si l'événement initial apparaît dans le groupe de journaux, le problème se situe en aval — passez à l'étape 3.

3. Consultez le tableau des tables S3 (`aws-cloudwatch`).

L'intégration `S3TableIntegration` crée automatiquement un compartiment de table appelé `aws-cloudwatch` et alimente une table sous `logs.aws_cloudtrail__data`. Cette table n'est créée qu'après le traitement du premier événement.

- Si le compartiment de table `aws-cloudwatch` n'existe pas, alors il manque des autorisations pour `S3TableIntegrationRole`. Il a besoin de `s3tables:CreateTableBucket`, `s3tables:PutTableBucketEncryption` et `s3tables:PutTableBucketPolicy` — toutes limitées à `arn:aws:s3tables:*:*:bucket/aws-cloudwatch`.
- Si le compartiment de table existe mais `logs.aws_cloudtrail__data` n'existe pas, alors l'intégration ne route pas les événements. L'intégration doit afficher `Status: ACTIVE` et inclure `aws_cloudtrail` comme source de journal.
- Si la table existe mais que l'événement initial n'y figure pas, il est possible que ce dernier soit encore en transit. L'ingestion des tables S3 présente une certaine latence. Attendez encore quelques minutes. Si cela n'apparaît toujours pas après 15 à 20 minutes, l'intégration est peut-être interrompue.

4. Interrogez directement l'événement initial.

- Ouvrez les tables S3 dans la console de gestion AWS.
- Accédez au compartiment de tables `aws-cloudwatch` → table `aws_cloudtrail__data` et utilisez le bouton **Aperçu** pour exécuter une requête rapide directement dans le navigateur.

- c. Si l'événement est présent dans le tableau mais que le journal affiche toujours `FAILED`, il se peut que la fenêtre d'interrogation ait expiré avant l'arrivée de l'événement.

Une fois le problème résolu, retournez à la console Workload Factory. Réessayez [initialisation de la configuration de la table de journal](#) en soumettant à nouveau l'ARN de Trail.

1. Si l'installation continue d'échouer, contactez le support NetApp pour obtenir de l'aide.

Référence des autorisations pour la configuration de la table du journal

Le rôle IAM qui déploie la pile CloudFormation pour activer la fonctionnalité de table Journal nécessite les autorisations suivantes. Consultez [Avant de commencer](#) pour une politique JSON copiable avec les autorisations requises.

Opérations de pile

Autorisation	Ressource	Pourquoi
cloudformation:CreateStack	arn:aws:cloudformation:*:*:stack/netapp-metadata-/*	Créer la pile
cloudformation:DescribeStacks	arn:aws:cloudformation:*:*:stack/netapp-metadata-/*	Surveiller l'état de la pile
cloudformation:DescribeStackEvents	arn:aws:cloudformation:*:*:stack/netapp-metadata-/*	Diagnostiquer les défaillances au niveau des ressources cloudformation : GetTemplateSummary * Validation préalable du modèle

CloudTrail

Autorisation	Ressource	Pourquoi
cloudtrail:CreateTrail	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	Créer le trail
cloudtrail:StartLogging	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	Activer la journalisation
cloudtrail:AddTags	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	Appliquer l'étiquette d'identification
cloudtrail:PutEventSelectors	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	Configurer la capture des événements de données
cloudtrail:DescribeTrails	*	Résoudre l'ARN de trail pour la sortie de la pile

S3

Autorisation	Ressource	Pourquoi
s3:CreateBucket	arn:aws:s3:::netapp-metadata-*	Créer le compartiment de journalisation CloudTrail

Autorisation	Ressource	Pourquoi
s3:PutBucketPolicy	arn:aws:s3:::netapp-metadata-*	Autoriser à CloudTrail d'écrire des journaux
s3:PutBucketTagging	arn:aws:s3:::netapp-metadata-*	Appliquer l'étiquette d'identification

IAM

Autorisation	Ressource	Pourquoi
iam:CreateRole	arn:aws:iam::*:role/netapp-metadata-*	Créer les deux rôles IAM
iam:PutRolePolicy	arn:aws:iam::*:role/netapp-metadata-*	Joindre les politiques en ligne
iam:TagRole	arn:aws:iam::*:role/netapp-metadata-*	Appliquer l'étiquette d'identification
iam:GetRole	arn:aws:iam::*:role/netapp-metadata-*	Confirmer que le rôle est actif
iam:PassRole	arn:aws:iam::*:role/netapp-metadata-* (condition : PassedToService = cloudtrail.amazonaws.com, logs.amazonaws.com)	Transmettre les rôles à CloudTrail et CloudWatch Logs

Journaux CloudWatch

Autorisation	Ressource	Pourquoi
journaux:CreateLogGroup	arn:aws:logs:*:*:log-group:netapp-metadata-*	Créer le groupe de journalisation
journaux>DeleteLogGroup	arn:aws:logs:*:*:log-group:netapp-metadata-*	Nettoyer le groupe de journaux si la création a échoué
journaux:PutRetentionPolicy	arn:aws:logs:*:*:log-group:netapp-metadata-*	Définir une durée de conservation de 30 jours
journaux:TagResource	arn:aws:logs:*:*:log-group:netapp-metadata-*	Appliquer l'étiquette d'identification
logs:AssociateSourceToS3TableIntegration	arn:aws:logs:*:*:log-group:netapp-metadata-*	Lier la source CloudTrail aux tables S3
journaux :DescribeLogGroups	*	Vérifier l'existence du groupe de journaux
logs:ListSourcesForS3TableIntegration	*	Confirmer l'association d'intégration

ObservabilityAdmin

Autorisation	Ressource	Pourquoi
observabilityadmin:CreateS3TableIntegration	*	Créer le pont CloudWatch → Tables S3
observabilityadmin:GetS3TableIntegration	*	Confirmer que l'intégration est active
observabilityadmin:TagResource	*	Appliquer l'étiquette d'identification
observabilityadmin:ListTagsForResource	*	Détection de dérive

Tables S3

Autorisation	Ressource	Pourquoi
s3tables:CreateTableBucket	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	Créer le compartiment S3 Tables (via integration role)
s3tables:PutTableBucketEncryption	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	Configurer le chiffrement AES256
s3tables:PutTableBucketPolicy	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	Autoriser l'accès aux journaux CloudWatch

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.