



Créer des ressources de base de données

Workload Factory for NetApp Console

NetApp
October 07, 2026

Sommaire

- Créer des ressources de base de données 1
 - Créer un serveur Microsoft SQL Server dans NetApp Workload Factory pour les bases de données 1
 - À propos de cette tâche 1
 - Avant de commencer 2
 - Étape 1 : Créer un serveur de base de données 2
 - Étape 2 : Activer la connexion à distance sur Microsoft SQL Server 10
 - Créer un serveur PostgreSQL dans NetApp Workload Factory pour bases de données 10
 - À propos de cette tâche 11
 - Avant de commencer 11
 - Créer un serveur PostgreSQL 11
 - Créer une base de données Microsoft SQL dans NetApp Workload Factory for Databases 17
 - Créer une base de données 18
 - Créer un clone sandbox dans NetApp Workload Factory for Databases 19

Créer des ressources de base de données

Créer un serveur Microsoft SQL Server dans NetApp Workload Factory pour les bases de données

La création d'un nouveau Microsoft SQL Server, ou hôte de base de données, dans Workload Factory for Databases nécessite le déploiement d'un système de fichiers FSx for ONTAP et des ressources pour Active Directory.

À propos de cette tâche

Avant de créer un Microsoft SQL Server à partir de Workload Factory, renseignez-vous sur les types de déploiement du stockage disponibles pour la configuration de l'hôte de base de données, la configuration des E/S multichemins Microsoft, le déploiement Active Directory, les détails de mise en réseau et les exigences requises pour mener à bien cette opération.

Après le déploiement, vous devrez [activer la connexion à distance sur Microsoft SQL Server](#).

Déploiements de systèmes de fichiers FSx for ONTAP

La création d'un nouveau Microsoft SQL Server nécessite un système de fichiers FSx for ONTAP comme système de stockage principal. Vous pouvez utiliser un système de fichiers FSx for ONTAP existant ou créer un nouveau système de fichiers. Si vous sélectionnez un système de fichiers FSx for ONTAP existant comme système de stockage principal de votre serveur de base de données, nous créons une nouvelle machine virtuelle de stockage pour les charges de travail Microsoft SQL Server.

Les systèmes de fichiers FSx for ONTAP ont deux modèles de déploiement Microsoft SQL Server : *Failover Cluster Instance (FCI)* ou *Standalone*. Différentes ressources sont créées pour le système de fichiers FSx for ONTAP selon le modèle de déploiement FSx for ONTAP que vous sélectionnez.

- **Déploiement de l'instance de cluster de basculement (FCI) Microsoft SQL** : un système de fichiers FSx for NetApp ONTAP à zones de disponibilité multiples est déployé lorsqu'un nouveau système de fichiers FSx for ONTAP est sélectionné pour le déploiement FCI. Des volumes et des LUN distincts sont créés pour les fichiers de données, de journalisation et tempdb pour un déploiement FCI. Un volume et un LUN supplémentaires sont créés pour le quorum ou le disque témoin du cluster Windows.
- **Déploiement autonome de Microsoft SQL** : un système de fichiers FSx for ONTAP à zone de disponibilité unique est créé lors de la création d'un nouveau Microsoft SQL Server. En outre, des volumes et des LUN distincts sont créés pour les fichiers de données, de journaux et de tempdb.

Configuration des E/S multichemins de Microsoft

Les deux modèles de déploiement de Microsoft SQL Server nécessitent la création d'un LUN à l'aide du protocole de stockage iSCSI. Workload Factory configure Microsoft Multi-path I/O (MPIO) lors de la configuration des LUN pour SQL Server sur FSx for ONTAP. MPIO est configuré selon les bonnes pratiques d'AWS et de NetApp.

Pour plus d'informations, consultez "[Déploiements de haute disponibilité de SQL Server utilisant Amazon FSx for NetApp ONTAP](#)".

Active Directory

Les opérations suivantes se produisent pour Active Directory (AD) lors du déploiement :

- Un nouveau compte de service Microsoft SQL est créé dans le domaine si vous ne fournissez pas de

compte de service SQL existant.

- Le cluster Windows, les noms d'hôte des nœuds et le nom FCI Microsoft SQL sont ajoutés comme ordinateurs gérés au compte de service Microsoft SQL.
- L'entrée du cluster Windows dispose des autorisations nécessaires pour ajouter des ordinateurs au domaine.

Groupes de sécurité Active Directory gérés par l'utilisateur

Si vous sélectionnez « Active Directory géré par l'utilisateur » lors du déploiement de Microsoft SQL Server dans Workload Factory, vous devez fournir un groupe de sécurité qui autorise le trafic entre les instances EC2 et le service d'annuaire pour le déploiement. Contrairement à AWS Managed Microsoft AD, Workload Factory n'associe pas automatiquement le groupe de sécurité pour Active Directory géré par l'utilisateur.

Restauration des ressources

Si vous décidez de restaurer vos ressources Domain Name System (DNS), les enregistrements de ressources dans AD et DNS ne sont pas supprimés automatiquement. Vous pouvez supprimer les enregistrements du serveur DNS et d'AD comme suit.

- Pour un AD géré par l'utilisateur, commencez par ["supprimer l'ordinateur AD"](#). Ensuite, connectez-vous au serveur DNS depuis le gestionnaire DNS et ["supprimer les enregistrements de ressources DNS"](#).
- Pour AWS Managed Microsoft AD, ["installer les outils d'administration AD"](#). Ensuite, ["supprimer l'ordinateur AD"](#). Enfin, connectez-vous au serveur DNS depuis le gestionnaire DNS et ["supprimer les enregistrements de ressources DNS"](#).

Avant de commencer

Assurez-vous de disposer des prérequis suivants avant de créer un nouvel hôte de base de données.

Identifiants et autorisations

Vous devez ["accorder les autorisations de création de l'hôte de base de données"](#) dans votre compte AWS pour créer un nouvel hôte de base de données dans Workload Factory.

Active Directory

Pour vous connecter à Active Directory, vous devez disposer d'un accès administrateur avec les autorisations nécessaires pour effectuer les opérations suivantes :

- Rejoignez le domaine
- Créer des objets d'ordinateur
- Créer des objets dans l'unité d'organisation (UO) par défaut
- Lire toutes les propriétés
- Accorder à l'utilisateur du domaine les droits d'administrateur local sur les nœuds AD
- Créez un utilisateur de service Microsoft SQL Server dans l'AD, s'il n'existe pas déjà

Étape 1 : Créer un serveur de base de données

Vous pouvez utiliser les modes de déploiement *Création rapide* ou *Création avancée* pour effectuer cette tâche dans Workload Factory avec les autorisations du mode *Automate*. Vous pouvez également utiliser les outils suivants disponibles dans Codebox : API REST, AWS CLI, AWS CloudFormation et Terraform. ["Apprenez à utiliser Codebox pour l'automatisation"](#).



Lorsque vous utilisez Terraform depuis Codebox, le code que vous copiez ou téléchargez masque `fsxadmin` et `vsadmin` les mots de passe. Vous devrez les saisir à nouveau lors de l'exécution du code. Vous devrez également inclure les autorisations suivantes pour le compte utilisateur, en plus des autorisations du mode *Automate* : `iam:TagRole` et `iam:TagInstanceProfile`. ["Apprenez à utiliser Terraform depuis Codebox"](#).

Lors du déploiement, Workload Factory active CredSSP pour la délégation des identifiants aux scripts de provisionnement de SQL. Lorsque la délégation CredSSP est bloquée pour tous les ordinateurs du domaine par la stratégie de groupe, le déploiement échoue. Après le déploiement, Workload Factory désactive CredSSP.

Création rapide



Dans *Création rapide*, FCI est le modèle de déploiement par défaut, Windows 2016 est la version Windows par défaut et SQL 2019 Standard Edition est la version SQL par défaut.

Étapes

1. Connectez-vous au ["NetApp Console"](#).
2. Sélectionnez le menu , **Charges de travail > Bases de données**.
3. Dans la vue d'ensemble des bases de données, sélectionnez **Deploy host**, puis sélectionnez **Microsoft SQL Server** dans le menu.
4. Sélectionnez **Création rapide**.
5. Dans les **paramètres AWS**, indiquez les informations suivantes :

- a. **Identifiants AWS** : Sélectionnez les identifiants AWS disposant des autorisations d'automatisation pour déployer le nouvel hôte de base de données.

Les identifiants AWS disposant des autorisations de *création d'hôte de base de données* permettent à Workload Factory de déployer et de gérer le nouvel hôte de base de données depuis votre compte AWS dans workload factory.

Les identifiants AWS disposant des autorisations *view, planning, and analysis* permettent à Workload Factory de générer un modèle CloudFormation que vous pouvez utiliser dans la console AWS CloudFormation.

Si vous n'avez pas d'identifiants AWS associés à Workload Factory et que vous souhaitez créer le nouveau serveur dans Workload Factory, suivez **l'option 1** pour accéder à la page des identifiants. Ajoutez manuellement les identifiants requis et les autorisations de *création d'hôte de base de données* pour les charges de travail de base de données.

Si vous souhaitez remplir le formulaire de création d'un nouveau serveur dans Workload Factory afin de télécharger un modèle de fichier YAML complet pour le déploiement dans AWS CloudFormation, suivez **l'option 2** pour vous assurer que vous disposez des autorisations requises pour créer le nouveau serveur dans AWS CloudFormation. Ajoutez manuellement les informations d'identification requises ainsi que les autorisations de consultation, de planification et d'analyse pour les charges de travail de base de données.

Vous pouvez également télécharger depuis Codebox un modèle de fichier YAML partiellement rempli afin de créer la pile en dehors de Workload Factory, sans informations d'identification ni autorisations. Sélectionnez **CloudFormation** dans la liste déroulante de Codebox pour télécharger le fichier YAML.

b. **Région et VPC** : Sélectionnez une région et un réseau VPC.

Assurez-vous que les sous-réseaux de déploiement sont associés à des points de terminaison d'interface existants et que les groupes de sécurité autorisent l'accès via le protocole HTTPS (443) vers les sous-réseaux sélectionnés.

Les points de terminaison d'interface de service AWS (SQS, FSx, EC2, CloudWatch, CloudFormation, SSM) et le point de terminaison de passerelle S3 sont créés lors du déploiement s'ils ne sont pas trouvés.

Les attributs DNS du VPC `EnableDnsSupport` et `EnableDnsHostnames` sont modifiés pour activer la résolution des adresses de point de terminaison s'ils ne sont pas déjà définis sur `true`.

Lors de l'utilisation d'un DNS inter-VPC, le groupe de sécurité des points de terminaison sur l'autre VPC où réside le DNS doit autoriser le port 443 vers les sous-réseaux de déploiement. Dans le cas contraire, vous devez fournir un résolveur DNS à partir du VPC local lors de la jonction à un Active Directory inter-VPC. Dans un environnement comportant plusieurs contrôleurs de domaine répliqués, si certains contrôleurs de domaine ne sont pas accessibles depuis le sous-réseau, vous pouvez **Rediriger vers CloudFormation** et saisir `Preferred domain controller` pour vous connecter à Active Directory.

c. **Zones de disponibilité** : Sélectionnez les zones de disponibilité et les sous-réseaux en fonction du modèle de déploiement de l'instance de cluster de basculement (FCI).



Les déploiements FCI ne sont pris en charge que sur les configurations FSx for ONTAP à zones de disponibilité multiples (MAZ).

- i. Dans le champ **Configuration du cluster - Nœud 1**, sélectionnez la zone de disponibilité principale pour la configuration MAZ FSx for ONTAP dans le menu déroulant **Zone de disponibilité** et un sous-réseau de la zone de disponibilité principale dans le menu déroulant **Sous-réseau**.
 - ii. Dans le champ **Configuration du cluster - Nœud 2**, sélectionnez la zone de disponibilité secondaire pour la configuration MAZ FSx for ONTAP dans le menu déroulant **Zone de disponibilité** et un sous-réseau de la zone de disponibilité secondaire dans le menu déroulant **Sous-réseau**.
6. Dans les **Paramètres de l'application**, saisissez un nom d'utilisateur et un mot de passe pour les **Identifiants de base de données**.

Pour les comptes GovCloud, saisissez la valeur du paramètre AWS SSM ARN au format suivant : `{fsx:{"username":"fsxadmin","password":"pass"}}`.

La valeur est disponible dans le Parameter Store, sous Détails du paramètre, dans la console de gestion AWS. Le type du paramètre AWS SSM doit être « Chaîne sécurisée » avec le nom au format `/netapp/wlmdb/<anyname>`. En savoir plus sur la récupération des paramètres SSM depuis ["Documentation AWS GovCloud"](#).

7. Sous **Connectivité**, fournissez les éléments suivants :

a. **Paire de clés** : Sélectionnez une paire de clés.

b. **Active Directory** :

- i. Dans le champ **Nom de domaine**, sélectionnez ou saisissez un nom pour le domaine.

A. Pour les annuaires Active Directory gérés par AWS, les noms de domaine apparaissent

dans le menu déroulant.

B. Pour un Active Directory géré par l'utilisateur, saisissez un nom dans le champ **Rechercher et ajouter**, puis cliquez sur **Ajouter**.

- ii. Dans le champ **Adresse DNS**, saisissez l'adresse IP DNS du domaine. Vous pouvez ajouter jusqu'à 3 adresses IP.

Pour les annuaires Active Directory gérés par AWS, la ou les adresse(s) IP du DNS apparaissent dans le menu déroulant.

- iii. Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur du domaine Active Directory.
- iv. Dans le champ **Mot de passe**, saisissez un mot de passe pour le domaine Active Directory.

Pour les comptes GovCloud, saisissez la valeur ARN du paramètre AWS SSM pour les informations d'identification Active Directory au format suivant :

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Le type du paramètre AWS SSM doit être « Chaîne sécurisée » avec le nom au format `/netapp/wlmdb/<anyname>`. En savoir plus sur la récupération des paramètres SSM depuis ["Documentation AWS GovCloud"](#).

8. Dans la section **Paramètres d'infrastructure**, veuillez indiquer les informations suivantes :

- a. **Système FSx for ONTAP** : Créez un nouveau système de fichiers FSx for ONTAP ou utilisez un système de fichiers FSx for ONTAP existant.

- i. **Créer un nouveau FSx pour ONTAP**: Entrez le nom d'utilisateur et le mot de passe.

Pour les comptes GovCloud, saisissez la valeur ARN du paramètre AWS SSM pour les informations d'identification FSx for ONTAP au format suivant :

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Le type du paramètre AWS SSM doit être « Chaîne sécurisée » avec le nom au format `/netapp/wlmdb/<anyname>`. En savoir plus sur la récupération des paramètres SSM depuis ["Documentation AWS GovCloud"](#).

Un nouveau système de fichiers FSx for ONTAP peut ajouter 30 minutes ou plus au temps d'installation.

- i. **Sélectionnez un FSx pour ONTAP** : Sélectionnez le nom du FSx pour ONTAP et saisissez un nom d'utilisateur et un mot de passe pour le système de fichiers.

Pour les systèmes de fichiers FSx pour ONTAP existants, assurez-vous des points suivants :

- Le groupe de routage associé à FSx pour ONTAP permet d'utiliser les routes vers les sous-réseaux pour le déploiement.
- Le groupe de sécurité autorise le trafic provenant des sous-réseaux utilisés pour le déploiement, notamment sur les ports TCP HTTPS (443) et iSCSI (3260).

- b. **Taille du disque de données**: Saisissez la capacité du disque de données et sélectionnez l'unité de capacité.

9. Résumé:

- a. **Aperçu par défaut** : Consultez les configurations par défaut définies par Quick create.

- b. **Coût estimé** : fournit une estimation des frais que vous pourriez engager si vous déployiez les ressources indiquées.

10. Cliquez sur **Créer**.

Sinon, si vous souhaitez modifier l'un de ces paramètres par défaut dès maintenant, créez le serveur de base de données avec Advanced create.

Vous pouvez également sélectionner **Enregistrer la configuration** pour déployer l'hôte ultérieurement.

Création avancée

Étapes

1. Connectez-vous au "[NetApp Console](#)".
2. Sélectionnez le menu , **Charges de travail > Bases de données**.
3. Dans la vue d'ensemble des bases de données, sélectionnez **Deploy host**, puis sélectionnez **Microsoft SQL Server** dans le menu.
4. Sélectionnez **Création avancée**.
5. Pour le **modèle de déploiement**, sélectionnez **Instance de cluster de basculement** ou **Instance unique**.
6. Dans les **paramètres AWS**, indiquez les informations suivantes :

- a. **Identifiants AWS** : Sélectionnez les identifiants AWS disposant des autorisations d'automatisation pour déployer le nouvel hôte de base de données.

Les identifiants AWS disposant des autorisations de *création d'hôte de base de données* permettent à Workload Factory de déployer et de gérer le nouvel hôte de base de données depuis votre compte AWS dans workload factory.

Les identifiants AWS disposant des autorisations *view, planning, and analysis* permettent à Workload Factory de générer un modèle CloudFormation que vous pouvez utiliser dans la console AWS CloudFormation.

Si vous n'avez pas d'identifiants AWS associés à Workload Factory et que vous souhaitez créer le nouveau serveur dans Workload Factory, suivez **l'option 1** pour accéder à la page des identifiants. Ajoutez manuellement les identifiants requis et les autorisations de *création d'hôte de base de données* pour les charges de travail de base de données.

Si vous souhaitez remplir le formulaire de création d'un nouveau serveur dans Workload Factory afin de télécharger un modèle de fichier YAML complet pour le déploiement dans AWS CloudFormation, suivez **l'option 2** pour vous assurer que vous disposez des autorisations requises pour créer le nouveau serveur dans AWS CloudFormation. Ajoutez manuellement les informations d'identification requises ainsi que les autorisations de consultation, de planification et d'analyse pour les charges de travail de base de données.

Vous pouvez également télécharger depuis Codebox un modèle de fichier YAML partiellement rempli afin de créer la pile en dehors de Workload Factory, sans informations d'identification ni autorisations. Sélectionnez **CloudFormation** dans la liste déroulante de Codebox pour télécharger le fichier YAML.

- b. **Région et VPC** : Sélectionnez une région et un réseau VPC.

Assurez-vous que les groupes de sécurité d'un point de terminaison d'interface existant autorisent l'accès au protocole HTTPS (443) vers les sous-réseaux sélectionnés.

Les points de terminaison d'interface de service AWS (SQS, FSx, EC2, CloudWatch, Cloud Formation, SSM) et le point de terminaison de passerelle S3 sont créés lors du déploiement s'ils ne sont pas trouvés.

Les attributs DNS du VPC `EnableDnsSupport` et `EnableDnsHostnames` sont modifiés pour permettre la résolution des adresses des points de terminaison si ce n'est pas déjà défini sur `true`.

- c. **Zones de disponibilité** : sélectionnez les zones de disponibilité et les sous-réseaux en fonction du modèle de déploiement que vous avez sélectionné. Les sous-réseaux ne doivent pas partager la même table de routage pour assurer une haute disponibilité.



Les déploiements FCI ne sont pris en charge que sur les configurations FSx for ONTAP à zones de disponibilité multiples (MAZ).

- Pour les déploiements à instance unique :
 - Dans le champ **Configuration du cluster - Nœud 1**, sélectionnez une zone de disponibilité dans le menu déroulant **Zone de disponibilité** et un sous-réseau dans le menu déroulant **Sous-réseau**.
- Pour les déploiements FCI :
 - Dans le champ **Configuration du cluster - Nœud 1**, sélectionnez la zone de disponibilité principale pour la configuration MAZ FSx for ONTAP dans le menu déroulant **Zone de disponibilité** et un sous-réseau de la zone de disponibilité principale dans le menu déroulant **Sous-réseau**.
 - Dans le champ **Configuration du cluster - Nœud 2**, sélectionnez la zone de disponibilité secondaire pour la configuration MAZ FSx for ONTAP dans le menu déroulant **Zone de disponibilité** et un sous-réseau de la zone de disponibilité secondaire dans le menu déroulant **Sous-réseau**.

- d. **Groupe de sécurité** : Un groupe de sécurité de charge de travail est créé pour autoriser les ports et protocoles nécessaires à la communication entre les nœuds du cluster Microsoft SQL et Windows. Vous pouvez également sélectionner un ou plusieurs groupes de sécurité.

7. Sous **Application settings**, indiquez les éléments suivants :

- a. Sous **Type d'installation de SQL Server**, sélectionnez **AMI avec licence incluse** ou **Utiliser une AMI personnalisée**.
- i. Si vous sélectionnez **AMI avec licence incluse**, veuillez fournir les informations suivantes :
 - A. **Système d'exploitation** : Sélectionnez **Windows server 2016**, **Windows server 2019** ou **Windows server 2022**.
 - B. **Édition de base de données** : Sélectionnez **SQL Server Standard Edition** ou **SQL Server Enterprise Edition**.
 - C. **Version de la base de données** : Sélectionnez **SQL Server 2016**, **SQL Server 2019** ou **SQL Server 2022**.
 - D. **SQL Server AMI** : Sélectionnez une image AMI SQL Server dans le menu déroulant.
 - ii. Si vous sélectionnez **Utiliser une AMI personnalisée**, sélectionnez une AMI dans le menu déroulant.
- b. **Collation SQL Server** : Sélectionnez un jeu de collation pour le serveur.



Si le jeu de classement sélectionné n'est pas compatible avec l'installation, nous

vous recommandons de sélectionner le classement par défaut « SQL_Latin1_General_CP1_CI_AS ».

- c. **Nom de la base de données** : Saisissez le nom du cluster de bases de données.
- d. **Identifiants de base de données** : Saisissez un nom d'utilisateur et un mot de passe pour un nouveau compte de service ou utilisez les identifiants d'un compte de service existant dans Active Directory.

Facultatif : cochez la case **Utiliser un compte de service géré** pour le compte de service SQL Server. Utilisez cette option si votre environnement utilise un compte de service géré (MSA) ou des comptes de service gérés de groupe (gMSA) où la gestion des mots de passe est assurée par Active Directory.

Pour les comptes GovCloud, saisissez la valeur du paramètre AWS SSM ARN au format suivant : `{fsx:{"username":"fsxadmin","password":"pass"}}`.

La valeur est disponible dans le Parameter Store, sous Détails du paramètre, dans la console de gestion AWS. Le type du paramètre AWS SSM doit être « Chaîne sécurisée » avec le nom au format `/netapp/wlmdb/<anyname>`. En savoir plus sur la récupération des paramètres SSM depuis ["Documentation AWS GovCloud"](#).

8. Sous **Connectivité**, fournissez les éléments suivants :

- a. **Paire de clés** : Sélectionnez une paire de clés pour vous connecter en toute sécurité à votre instance.
- b. **Active Directory** : Veuillez fournir les informations Active Directory suivantes :
 - i. Dans le champ **Nom de domaine**, sélectionnez ou saisissez un nom pour le domaine.
 - A. Pour les annuaires Active Directory gérés par AWS, les noms de domaine apparaissent dans le menu déroulant.
 - B. Pour un Active Directory géré par l'utilisateur, saisissez un nom dans le champ **Rechercher et ajouter**, puis cliquez sur **Ajouter**.
 - ii. Dans le champ **Adresse DNS**, saisissez l'adresse IP DNS du domaine. Vous pouvez ajouter jusqu'à 3 adresses IP.

Pour les annuaires Active Directory gérés par AWS, la ou les adresse(s) IP du DNS apparaissent dans le menu déroulant.

- iii. Saisissez le nom d'utilisateur et le mot de passe du domaine Active Directory.

Pour les comptes GovCloud, saisissez la valeur ARN du paramètre AWS SSM pour les informations d'identification Active Directory au format suivant : `{fsx:{"username":"fsxadmin","password":"pass"}}`. Le type du paramètre AWS SSM doit être « Chaîne sécurisée » avec le nom au format `/netapp/wlmdb/<anyname>`. En savoir plus sur la récupération des paramètres SSM depuis ["Documentation AWS GovCloud"](#).

- iv. **Contrôleur de domaine préféré** : Saisissez éventuellement le contrôleur de domaine préféré à utiliser pour la jonction à Active Directory.
- v. **Chemin d'accès à l'unité organisationnelle préférée** : Vous pouvez également saisir l'unité organisationnelle (UO) préférée à rejoindre dans Active Directory.
- vi. **Groupe Active Directory cible** : saisissez éventuellement le groupe Active Directory cible

auquel ajouter les ordinateurs.

9. Dans la section **Paramètres d'infrastructure**, veuillez indiquer les informations suivantes :

- a. **Type d'instance de base de données** : Sélectionnez le type d'instance de base de données dans le menu déroulant.
- b. **Système FSx for ONTAP** : Créez un nouveau système de fichiers FSx for ONTAP ou utilisez un système de fichiers FSx for ONTAP existant.

- i. **Créer un nouveau FSx pour ONTAP**: Entrez le nom d'utilisateur et le mot de passe.

Pour les comptes GovCloud, saisissez la valeur ARN du paramètre AWS SSM pour les informations d'identification FSx for ONTAP au format suivant :

`{fsx:{ "username": "fsxadmin", "password": "pass" }}`. Le type du paramètre AWS SSM doit être « Chaîne sécurisée » avec le nom au format `/netapp/wlmdb/<anyname>`. En savoir plus sur la récupération des paramètres SSM depuis ["Documentation AWS GovCloud"](#).

Un nouveau système de fichiers FSx for ONTAP peut ajouter 30 minutes ou plus au temps d'installation.

- ii. **Sélectionnez un FSx for ONTAP existant** : sélectionnez le nom de FSx for ONTAP dans le menu déroulant, puis saisissez un nom d'utilisateur et un mot de passe pour le système de fichiers.

Pour les systèmes de fichiers FSx pour ONTAP existants, assurez-vous des points suivants :

- Le groupe de routage associé à FSx pour ONTAP permet d'utiliser les routes vers les sous-réseaux pour le déploiement.
- Le groupe de sécurité autorise le trafic provenant des sous-réseaux utilisés pour le déploiement, notamment sur les ports TCP HTTPS (443) et iSCSI (3260).

- c. **Stratégie Snapshot** : Activée par défaut. Des snapshots sont créés quotidiennement et conservés pendant 7 jours.

Les instantanés sont affectés aux volumes créés pour les charges de travail SQL.

- d. **Taille du disque de données**: Saisissez la capacité du disque de données et sélectionnez l'unité de capacité.
- e. **IOPS provisionnées** : sélectionnez **Automatique** ou **Provisionné par l'utilisateur**. Si vous sélectionnez **Provisionné par l'utilisateur**, saisissez la valeur des IOPS.
- f. **Capacité de débit** : Sélectionnez la capacité de débit dans le menu déroulant.

Dans certaines régions, vous pouvez sélectionner une capacité de débit de 4 GBps. Pour provisionner une capacité de débit de 4 GBps, votre système de fichiers FSx for ONTAP doit être configuré avec un minimum de 5 120 Gio de capacité de stockage SSD et 160 000 IOPS SSD.

- g. **Chiffrement** : Sélectionnez une clé de votre compte ou une clé d'un autre compte. Vous devez saisir l'ARN de la clé de chiffrement d'un autre compte.

Les clés de chiffrement personnalisées FSx for ONTAP ne sont pas répertoriées en fonction de l'applicabilité du service. Sélectionnez une clé de chiffrement FSx appropriée. Les clés de chiffrement non FSx entraîneront l'échec de la création du serveur.

Les clés gérées par AWS sont filtrées en fonction de leur applicabilité au service.

- h. **Étiquettes** : Vous pouvez éventuellement ajouter jusqu'à 40 étiquettes.
- i. **Simple Notification Service** : Vous pouvez éventuellement activer le Simple Notification Service (SNS) pour cette configuration en sélectionnant une rubrique SNS pour Microsoft SQL Server dans le menu déroulant.
 - i. Activez le service Simple Notification Service.
 - ii. Sélectionnez un ARN dans le menu déroulant.
- j. **surveillance CloudWatch**: Vous pouvez activer la surveillance CloudWatch si vous le souhaitez.

Nous recommandons d'activer CloudWatch pour le débogage en cas d'échec. Les événements qui apparaissent dans la console AWS CloudFormation sont généraux et n'indiquent pas la cause première. Tous les journaux détaillés sont enregistrés dans le C:\cfn\logs dossier des instances EC2.

Dans CloudWatch, un groupe de journaux est créé avec le nom de la pile. Un flux de journaux pour chaque nœud de validation et nœud SQL apparaît sous le groupe de journaux. CloudWatch affiche la progression du script et fournit des informations pour vous aider à comprendre si et quand le déploiement échoue.

- a. **Restauration des ressources** : Cette fonctionnalité n'est actuellement pas prise en charge.

10. Résumé

- a. **Coût estimé** : fournit une estimation des frais que vous pourriez engager si vous déployiez les ressources indiquées.

11. Cliquez sur **Créer** pour déployer le nouvel hôte de base de données.

Vous pouvez également enregistrer la configuration.

Étape 2 : Activer la connexion à distance sur Microsoft SQL Server

Une fois le serveur déployé, Workload Factory n'active pas la connexion à distance sur Microsoft SQL Server. Pour activer la connexion à distance, procédez comme suit.

Étapes

1. Utilisez l'identité de l'ordinateur pour NTLM en vous référant à "[Sécurité réseau : Autoriser le système local à utiliser l'identité de l'ordinateur pour NTLM](#)" dans la documentation Microsoft.
2. Vérifiez la configuration des ports dynamiques en vous référant à "[Une erreur liée au réseau ou spécifique à l'instance s'est produite lors de l'établissement d'une connexion à SQL Server](#)" la documentation Microsoft.
3. Autorisez l'adresse IP cliente ou le sous-réseau requis dans le groupe de sécurité.

Et ensuite

Maintenant, vous pouvez "[créer une base de données dans Workload Factory for Databases](#)".

Créer un serveur PostgreSQL dans NetApp Workload Factory pour bases de données

La création d'un nouveau serveur PostgreSQL, ou hôte de base de données, dans NetApp Workload Factory for Databases nécessite le déploiement d'un système de

fichiers FSx for ONTAP ainsi que des ressources pour Active Directory.

À propos de cette tâche

Avant de créer un serveur PostgreSQL à partir de Workload Factory, renseignez-vous sur les types de déploiement du stockage disponibles pour la configuration de l'hôte de base de données, les modes de fonctionnement de Workload Factory et les exigences requises pour mener à bien cette opération.

Déploiements de systèmes de fichiers FSx for ONTAP

La création d'un nouveau serveur PostgreSQL nécessite un système de fichiers FSx for ONTAP comme système de stockage principal. Vous pouvez utiliser un système de fichiers FSx for ONTAP existant ou créer un nouveau système de fichiers. Si vous sélectionnez un système de fichiers FSx for ONTAP existant comme système de stockage principal de votre serveur de base de données, nous créons une nouvelle machine virtuelle de stockage pour les charges de travail PostgreSQL.

+ Les systèmes de fichiers FSx for ONTAP disposent de deux modèles de déploiement de serveur PostgreSQL : *High Availability (HA)* ou *single instance*. Différentes ressources sont créées pour le système de fichiers FSx for ONTAP selon le modèle de déploiement FSx for ONTAP que vous sélectionnez.

- **Déploiement Haute disponibilité (HA)** : Un système de fichiers FSx for NetApp ONTAP à zones de disponibilité multiples est déployé lorsqu'un nouveau système de fichiers FSx for ONTAP est sélectionné pour le déploiement HA. Des volumes et des LUN distincts sont créés pour les fichiers de données, de journalisation et de tempdb pour un déploiement HA. Un volume et un LUN supplémentaires sont créés pour le quorum ou le disque témoin du cluster Windows. Le déploiement HA configure la réplication en continu entre les serveurs PostgreSQL principal et secondaire.
- **Déploiement d'une instance unique** : un système de fichiers FSx for ONTAP à zone de disponibilité unique est créé lorsqu'un nouveau serveur PostgreSQL est créé. De plus, des volumes et des LUN distincts sont créés pour les fichiers de données, de journaux et de tempdb.

Avant de commencer

Vous devez disposer de ["accorder les autorisations de création de l'hôte de base de données"](#) dans votre compte AWS pour créer un nouvel hôte de base de données dans Workload Factory.

Créer un serveur PostgreSQL

Vous pouvez utiliser les modes de déploiement *Quick create* ou *Advanced create* pour effectuer cette tâche dans Workload Factory avec les autorisations du mode *Automate*. Vous pouvez également utiliser les outils suivants disponibles dans Codebox : REST API, AWS CLI, AWS CloudFormation et Terraform. ["Apprenez à utiliser Codebox pour l'automatisation"](#).



Lorsque vous utilisez Terraform depuis Codebox, le code que vous copiez ou téléchargez masque `fsxadmin` et `vsadmin` les mots de passe. Vous devrez saisir à nouveau les mots de passe lorsque vous exécuterez le code. Vous devrez inclure les autorisations suivantes pour le compte utilisateur en plus des autorisations du mode *Automate* : `iam:TagRole` et `iam:TagInstanceProfile`. ["Apprenez à utiliser Terraform depuis Codebox"](#).

Création rapide



Dans *Quick create*, HA est le modèle de déploiement par défaut, Windows 2016 est la version Windows par défaut et SQL 2019 Standard Edition est la version SQL par défaut.

Étapes

1. Connectez-vous au "[NetApp Console](#)".
2. Sélectionnez le menu , **Charges de travail > Bases de données**.
3. Dans la vue d'ensemble des bases de données, sélectionnez **Deploy host**, puis **PostgreSQL Server** dans le menu.
4. Sélectionnez **Création rapide**.
5. Sous la rubrique **Zone d'atterrissage**, veuillez indiquer les informations suivantes :

- a. **Identifiants AWS** : Sélectionnez les identifiants AWS disposant des autorisations d'automatisation pour déployer le nouvel hôte de base de données.

Les identifiants AWS disposant des autorisations de *création d'hôte de base de données* permettent à Workload Factory de déployer et de gérer le nouvel hôte de base de données depuis votre compte AWS dans workload factory.

Les identifiants AWS disposant des autorisations *view, planning, and analysis* permettent à Workload Factory de générer un modèle CloudFormation que vous pouvez utiliser dans la console AWS CloudFormation.

Si vous n'avez pas d'identifiants AWS associés à Workload Factory et que vous souhaitez créer le nouveau serveur dans Workload Factory, suivez **l'option 1** pour accéder à la page des identifiants. Ajoutez manuellement les identifiants requis et les autorisations de *création d'hôte de base de données* pour les charges de travail de base de données.

Si vous souhaitez remplir le formulaire de création d'un nouveau serveur dans Workload Factory afin de télécharger un modèle de fichier YAML complet pour le déploiement dans AWS CloudFormation, suivez **l'option 2** pour vous assurer que vous disposez des autorisations requises pour créer le nouveau serveur dans AWS CloudFormation. Ajoutez manuellement les informations d'identification requises ainsi que les autorisations de consultation, de planification et d'analyse pour les charges de travail de base de données.

Vous pouvez également télécharger depuis Codebox un modèle de fichier YAML partiellement rempli afin de créer la pile en dehors de Workload Factory, sans informations d'identification ni autorisations. Sélectionnez **CloudFormation** dans la liste déroulante de Codebox pour télécharger le fichier YAML.

- b. **Région et VPC** : Sélectionnez une région et un réseau VPC.

Assurez-vous que les groupes de sécurité d'un point de terminaison d'interface existant autorisent l'accès au protocole HTTPS (443) vers les sous-réseaux sélectionnés.

Les points de terminaison d'interface de service AWS (SQS, FSx, EC2, CloudWatch, CloudFormation, SSM) et le point de terminaison de passerelle S3 sont créés lors du déploiement s'ils ne sont pas trouvés.

Les attributs DNS du VPC `EnableDnsSupport` et `EnableDnsHostnames` sont modifiés pour activer la résolution des adresses de point de terminaison s'ils ne sont pas déjà définis sur `true`.

- c. **Zones de disponibilité** : Sélectionnez les zones de disponibilité et les sous-réseaux.



Les déploiements HA ne sont pris en charge que sur les configurations FSx for ONTAP à zones de disponibilité multiples (MAZ).

Pour une haute disponibilité, les sous-réseaux ne doivent pas partager la même table de routage.

- i. Dans le champ **Configuration du cluster - Nœud 1**, sélectionnez la zone de disponibilité principale pour la configuration MAZ FSx for ONTAP dans le menu déroulant **Zone de disponibilité** et un sous-réseau de la zone de disponibilité principale dans le menu déroulant **Sous-réseau**.
 - ii. Dans le champ **Configuration du cluster - Nœud 2**, sélectionnez la zone de disponibilité secondaire pour la configuration MAZ FSx for ONTAP dans le menu déroulant **Zone de disponibilité** et un sous-réseau de la zone de disponibilité secondaire dans le menu déroulant **Sous-réseau**.
6. Dans les **Paramètres de l'application**, saisissez un nom d'utilisateur et un mot de passe pour les **Identifiants de base de données**.
 7. Sous **Connectivité**, sélectionnez une paire de clés pour vous connecter en toute sécurité à votre instance.
 8. Dans la section **Paramètres d'infrastructure**, veuillez indiquer les informations suivantes :
 - a. **Système FSx for ONTAP** : Créez un nouveau système de fichiers FSx for ONTAP ou utilisez un système de fichiers FSx for ONTAP existant.

- i. **Créer un nouveau FSx pour ONTAP**: Entrez le nom d'utilisateur et le mot de passe.

Pour les comptes GovCloud, saisissez la valeur ARN du paramètre AWS SSM pour les informations d'identification FSx for ONTAP au format suivant :

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Le type du paramètre AWS SSM doit être « Chaîne sécurisée » avec le nom au format `/netapp/wlmdb/<anyname>`. En savoir plus sur la récupération des paramètres SSM depuis ["Documentation AWS GovCloud"](#).

Un nouveau système de fichiers FSx for ONTAP peut ajouter 30 minutes ou plus au temps d'installation.

- i. **Sélectionnez un FSx for ONTAP existant** : sélectionnez le nom de FSx for ONTAP dans le menu déroulant, puis saisissez un nom d'utilisateur et un mot de passe pour le système de fichiers.

Pour les systèmes de fichiers FSx pour ONTAP existants, assurez-vous des points suivants :

- Le groupe de routage associé à FSx pour ONTAP permet d'utiliser les routes vers les sous-réseaux pour le déploiement.
- Le groupe de sécurité autorise le trafic provenant des sous-réseaux utilisés pour le déploiement, notamment sur les ports TCP HTTPS (443) et iSCSI (3260).

- b. **Taille du disque de données**: Saisissez la capacité du disque de données et sélectionnez l'unité de capacité.

9. Résumé:

- a. **Aperçu par défaut** : Consultez les configurations par défaut définies par Quick create.
- b. **Coût estimé** : fournit une estimation des frais que vous pourriez engager si vous déployiez les ressources indiquées.

10. Cliquez sur **Créer**.

Sinon, si vous souhaitez modifier l'un de ces paramètres par défaut dès maintenant, créez le serveur de base de données avec Advanced create.

Vous pouvez également sélectionner **Enregistrer la configuration** pour déployer l'hôte ultérieurement.

Création avancée

Étapes

1. Connectez-vous au ["NetApp Console"](#).
2. Sélectionnez le menu , **Charges de travail > Bases de données**.
3. Dans la vue d'ensemble des bases de données, sélectionnez **Deploy host**, puis **PostgreSQL Server** dans le menu.
4. Sélectionnez **Création avancée**.
5. Sous **Modèle de déploiement**, sélectionnez **Instance autonome** ou **Haute disponibilité (HA)**.
6. Sous la rubrique **Zone d'atterrissage**, veuillez indiquer les informations suivantes :
 - a. **Identifiants AWS** : Sélectionnez les identifiants AWS disposant des autorisations d'automatisation pour déployer le nouvel hôte de base de données.

Les identifiants AWS disposant des autorisations de *création d'hôte de base de données* permettent à Workload Factory de déployer et de gérer le nouvel hôte de base de données depuis votre compte AWS dans workload factory.

Les identifiants AWS disposant des autorisations *view, planning, and analysis* permettent à Workload Factory de générer un modèle CloudFormation que vous pouvez utiliser dans la console AWS CloudFormation.

Si vous n'avez pas d'identifiants AWS associés à Workload Factory et que vous souhaitez créer le nouveau serveur dans Workload Factory, suivez **l'option 1** pour accéder à la page des identifiants. Ajoutez manuellement les identifiants requis et les autorisations de *création d'hôte de base de données* pour les charges de travail de base de données.

Si vous souhaitez remplir le formulaire de création d'un nouveau serveur dans Workload Factory afin de télécharger un modèle de fichier YAML complet pour le déploiement dans AWS CloudFormation, suivez **l'option 2** pour vous assurer que vous disposez des autorisations requises pour créer le nouveau serveur dans AWS CloudFormation. Ajoutez manuellement les informations d'identification requises ainsi que les autorisations de consultation, de planification et d'analyse pour les charges de travail de base de données.

Vous pouvez également télécharger depuis Codebox un modèle de fichier YAML partiellement rempli afin de créer la pile en dehors de Workload Factory, sans informations d'identification ni autorisations. Sélectionnez **CloudFormation** dans la liste déroulante de Codebox pour télécharger le fichier YAML.

- b. **Région et VPC** : Sélectionnez une région et un réseau VPC.

Assurez-vous que les groupes de sécurité d'un point de terminaison d'interface existant autorisent l'accès au protocole HTTPS (443) vers les sous-réseaux sélectionnés.

Les points de terminaison d'interface de service AWS (SQS, FSx, EC2, CloudWatch, Cloud Formation, SSM) et le point de terminaison de passerelle S3 sont créés lors du déploiement s'ils ne sont pas trouvés.

Les attributs DNS du VPC `EnableDnsSupport` et `EnableDnsHostnames` sont modifiés pour permettre la résolution des adresses des points de terminaison si ce n'est pas déjà défini sur

true.

- c. **Zones de disponibilité** : Sélectionnez les zones de disponibilité et les sous-réseaux.

Pour les déploiements d'instance unique

Dans le champ **Configuration du cluster - Nœud 1**, sélectionnez une zone de disponibilité dans le menu déroulant **Availability zone** et un sous-réseau dans le menu déroulant **Subnet**.

Pour les déploiements HA

- i. Dans le champ **Configuration du cluster - Nœud 1**, sélectionnez la zone de disponibilité principale pour la configuration MAZ FSx for ONTAP dans le menu déroulant **Zone de disponibilité** et un sous-réseau de la zone de disponibilité principale dans le menu déroulant **Sous-réseau**.
 - ii. Dans le champ **Configuration du cluster - Nœud 2**, sélectionnez la zone de disponibilité secondaire pour la configuration MAZ FSx for ONTAP dans le menu déroulant **Zone de disponibilité** et un sous-réseau de la zone de disponibilité secondaire dans le menu déroulant **Sous-réseau**.
- d. **Groupe de sécurité** : Un groupe de sécurité de charge de travail est créé pour autoriser les ports et protocoles requis par PostgreSQL. Vous pouvez également sélectionner un ou plusieurs groupes de sécurité.
7. Sous **Application settings**, indiquez les éléments suivants :
- a. Sélectionnez le **système d'exploitation** dans le menu déroulant.
 - b. Sélectionnez la **version PostgreSQL** dans le menu déroulant.
 - c. **Nom du serveur de base de données** : Saisissez le nom du cluster de base de données.
 - d. **Identifiants de base de données** : Saisissez un nom d'utilisateur et un mot de passe pour un nouveau compte de service ou utilisez les identifiants d'un compte de service existant dans Active Directory.

Pour les comptes GovCloud, saisissez la valeur ARN du paramètre AWS SSM pour les informations d'identification au format suivant :

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Le type du paramètre AWS SSM doit être « Chaîne sécurisée » avec le nom au format `/netapp/wlmdb/<anyname>`. En savoir plus sur la récupération des paramètres SSM depuis ["Documentation AWS GovCloud"](#).

8. Sous **Connectivité**, sélectionnez une paire de clés pour vous connecter en toute sécurité à votre instance.
9. Dans la section **Paramètres d'infrastructure**, veuillez indiquer les informations suivantes :
- a. **Type d'instance de base de données** : Sélectionnez le type d'instance de base de données dans le menu déroulant.
 - b. **Système FSx for ONTAP** : Créez un nouveau système de fichiers FSx for ONTAP ou utilisez un système de fichiers FSx for ONTAP existant.
 - i. **Créer un nouveau FSx pour ONTAP**: Entrez le nom d'utilisateur et le mot de passe.

Pour les comptes GovCloud, saisissez la valeur ARN du paramètre AWS SSM pour les informations d'identification FSx for ONTAP au format suivant :

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Le type du paramètre AWS SSM doit être « Chaîne sécurisée » avec le nom au format `/netapp/wlmdb/<anyname>`.

En savoir plus sur la récupération des paramètres SSM depuis "[Documentation AWS GovCloud](#)".

Un nouveau système de fichiers FSx for ONTAP peut ajouter 30 minutes ou plus au temps d'installation.

- ii. **Sélectionnez un FSx for ONTAP existant** : sélectionnez le nom de FSx for ONTAP dans le menu déroulant, puis saisissez un nom d'utilisateur et un mot de passe pour le système de fichiers.

Pour les systèmes de fichiers FSx pour ONTAP existants, assurez-vous des points suivants :

- Le groupe de routage associé à FSx pour ONTAP permet d'utiliser les routes vers les sous-réseaux pour le déploiement.
 - Le groupe de sécurité autorise le trafic provenant des sous-réseaux utilisés pour le déploiement, notamment sur les ports TCP HTTPS (443) et iSCSI (3260).
- c. **Stratégie Snapshot** : Activée par défaut. Des snapshots sont créés quotidiennement et conservés pendant 7 jours.

Les instantanés sont affectés aux volumes créés pour les charges de travail PostgreSQL.

- d. **Taille du disque de données**: Saisissez la capacité du disque de données et sélectionnez l'unité de capacité.
- e. **IOPS provisionnées** : sélectionnez **Automatique** ou **Provisionné par l'utilisateur**. Si vous sélectionnez **Provisionné par l'utilisateur**, saisissez la valeur des IOPS.
- f. **Capacité de débit** : Sélectionnez la capacité de débit dans le menu déroulant.

Dans certaines régions, vous pouvez sélectionner une capacité de débit de 4 GBps. Pour provisionner une capacité de débit de 4 GBps, votre système de fichiers FSx for ONTAP doit être configuré avec un minimum de 5 120 Gio de capacité de stockage SSD et 160 000 IOPS SSD.

- g. **Chiffrement** : Sélectionnez une clé de votre compte ou une clé d'un autre compte. Vous devez saisir l'ARN de la clé de chiffrement d'un autre compte.

Les clés de chiffrement personnalisées FSx for ONTAP ne sont pas répertoriées en fonction de l'applicabilité du service. Sélectionnez une clé de chiffrement FSx appropriée. Les clés de chiffrement non FSx entraîneront l'échec de la création du serveur.

Les clés gérées par AWS sont filtrées en fonction de leur applicabilité au service.

- h. **Étiquettes** : Vous pouvez éventuellement ajouter jusqu'à 40 étiquettes.
- i. **Service de notification simple** : Vous pouvez activer le Simple Notification Service (SNS) pour cette configuration en sélectionnant un sujet SNS pour PostgreSQL dans le menu déroulant.
 - i. Activez le service Simple Notification Service.
 - ii. Sélectionnez un ARN dans le menu déroulant.
- j. **surveillance CloudWatch**: Vous pouvez activer la surveillance CloudWatch si vous le souhaitez.

Nous recommandons d'activer CloudWatch pour le débogage en cas d'échec. Les événements qui apparaissent dans la console AWS CloudFormation sont généraux et n'indiquent pas la cause première. Tous les journaux détaillés sont enregistrés dans le C:\cfn\logs dossier des instances EC2.

Dans CloudWatch, un groupe de journaux est créé avec le nom de la pile. Un flux de journaux pour chaque nœud de validation et nœud SQL apparaît sous le groupe de journaux. CloudWatch affiche la progression du script et fournit des informations pour vous aider à comprendre si et quand le déploiement échoue.

a. **Restauration des ressources** : Cette fonctionnalité n'est actuellement pas prise en charge.

10. Résumé

a. **Coût estimé** : fournit une estimation des frais que vous pourriez engager si vous déployiez les ressources indiquées.

11. Cliquez sur **Créer** pour déployer le nouvel hôte de base de données.

Vous pouvez également enregistrer la configuration.

Et ensuite

Vous pouvez configurer manuellement les utilisateurs, l'accès distant et les bases de données sur le serveur PostgreSQL déployé.

Créer une base de données Microsoft SQL dans NetApp Workload Factory for Databases

La création d'une nouvelle base de données Microsoft SQL vous permet de gérer la ressource au sein de NetApp Workload Factory for Databases.

À propos de cette tâche

Lors de la création de la base de données, deux nouveaux volumes sont créés dans le système de fichiers FSx for ONTAP, composés de LUN indépendants pour héberger les fichiers de données et de journalisation de la base de données. Les fichiers de la nouvelle base de données sont provisionnés de manière dynamique et ne consomment que quelques Mo de la taille totale allouée à la nouvelle base de données.

Si vous souhaitez isoler le stockage de la base de données, vous pouvez le faire en utilisant un point de montage virtuel. Le point de montage virtuel vous permet de regrouper les bases de données sur quelques lecteurs communs de l'hôte.

La création d'une base de données dans workload factory requiert les autorisations de *consultation*, de *planification* et d'*analyse*. Vous pouvez également copier ou télécharger un modèle de code partiellement rempli pour terminer l'opération en dehors de workload factory. "[Découvrez les autorisations de Workload Factory](#)" pour décider du mode que vous souhaitez utiliser.



Les serveurs Microsoft SQL utilisant le protocole SMB ne prennent pas en charge la création de bases de données.

Avant de commencer

Veuillez remplir les conditions préalables suivantes avant de créer une nouvelle base de données.

- **Identifiants et autorisations** : Vous devez avoir "[Informations d'identification du compte AWS et autorisations opérations et remédiation](#)" pour créer une nouvelle base de données dans Workload Factory.

Vous pouvez également utiliser Codebox pour copier un modèle afin de déployer une base de données en dehors de workload factory à l'aide de l'API REST. "[Découvrez-en plus sur l'automatisation de Codebox](#)".

- **Hôte Windows** : Vous devez disposer de suffisamment de lettres de lecteur disponibles sur le serveur Microsoft SQL Server pour créer de nouveaux lecteurs pour la nouvelle base de données si vous utilisez le mode *Quick create*.
- **Microsoft SQL Server** : vous devez disposer d'un Microsoft SQL Server géré dans workload factory for Databases pour héberger la nouvelle base de données.
- **AWS Systems Manager**: Assurez-vous que le NT Authority\SYSTEM privilège utilisateur est activé sur l'hôte Microsoft SQL via AWS Systems Manager.

Créer une base de données

Vous pouvez utiliser les modes de déploiement *Création rapide* ou *Création avancée* pour effectuer cette tâche dans Workload Factory.

Création rapide

Étapes

1. Connectez-vous au ["NetApp Console"](#).
2. Sélectionnez le menu , **Charges de travail > Bases de données**.
3. Dans le menu Bases de données, sélectionnez **Inventaire**.
4. Dans l'inventaire, sélectionnez **Microsoft SQL Server** comme type de moteur de base de données.
5. Sélectionnez un serveur de base de données avec une instance SQL server gérée dans laquelle créer la base de données.
6. Cliquez sur le menu d'action de l'instance gérée, puis sélectionnez **Créer une base de données utilisateur**.
7. Sur la page Créer une base de données utilisateur, sous Informations sur la base de données, indiquez les éléments suivants :
 - a. **Nom de la base de données** : Veuillez saisir le nom de la base de données.
 - b. **Classement** : Sélectionnez un classement pour la base de données. Le classement par défaut SQL_Latin1_General_CP1_CI_AS" est sélectionné sur Microsoft SQL Server.
8. Dans les paramètres du fichier, veuillez indiquer les informations suivantes :
 - a. **Mode de configuration des fichiers** : Sélectionnez **Création rapide**.
 - b. **Noms de fichiers et chemin**:
 - **Nom du fichier de données** : Saisissez le nom du fichier de données.
 - **Nom du fichier journal**: Saisissez le nom du fichier journal.
 - c. **Taille des fichiers** : Saisissez la taille des données et la taille du journal pour la base de données.
9. Cliquez sur **Créer**.

Sinon, si vous souhaitez modifier dès maintenant l'un de ces paramètres par défaut, remplacez **File settings mode** par **Advanced create**.

Création avancée

Étapes

1. Connectez-vous au ["NetApp Console"](#).

2. Sélectionnez le menu , **Charges de travail > Bases de données**.
3. Dans le menu Bases de données, sélectionnez **Inventaire**.
4. Dans l'inventaire, sélectionnez **Microsoft SQL Server** comme type de moteur de base de données.
5. Sélectionnez un serveur de base de données avec une instance SQL server gérée dans laquelle créer la base de données.
6. Cliquez sur le menu d'action de l'instance gérée, puis sélectionnez **Créer une base de données utilisateur**.
7. Sélectionnez **Créer une base de données utilisateur**.
8. Sur la page Créer une base de données utilisateur, sous Informations sur la base de données, indiquez les éléments suivants :
 - a. **Nom de la base de données** : Veuillez saisir le nom de la base de données.
 - b. **Classement** : Sélectionnez le classement de la base de données. Le classement par défaut « SQL_Latin1_General_CP1_CI_AS » est sélectionné sur Microsoft SQL Server.
9. Dans les paramètres du fichier, veuillez indiquer les informations suivantes :
 - a. **Mode de configuration des fichiers** : Sélectionnez **Création avancée**.
 - b. **Noms de fichiers et chemin**:
 - i. **Fichier de données** : Sélectionnez une lettre de lecteur et saisissez le nom du fichier de données.

Si vous le souhaitez, cochez la case **Point de montage virtuel**.
 - ii. **Fichier journal** : Sélectionnez une lettre de lecteur et saisissez le nom du fichier journal.

Si vous le souhaitez, cochez la case **Point de montage virtuel**.
 - c. **Taille des fichiers** : Saisissez la taille des données et la taille du journal pour la base de données.
10. Cliquez sur **Créer**.

Si vous avez créé l'hôte de la base de données, vous pouvez vérifier la progression de la tâche dans l'onglet **Surveillance des tâches**.

Créer un clone sandbox dans NetApp Workload Factory for Databases

La création d'un clone sandbox d'une base de données dans NetApp Workload Factory for Databases vous permet d'utiliser ce clone pour le développement, les tests, l'intégration, l'analyse, la formation, l'assurance qualité, et bien plus encore sans modifier la base de données source.

À propos de cette tâche

Un clone sandbox est créé à partir de l'instantané le plus récent sur la base de données source. Il peut être cloné sur le même Microsoft SQL Server que la base de données source ou sur un autre Microsoft SQL Server, à condition qu'ils partagent le même système de fichiers FSx for ONTAP.

Avant de commencer

Assurez-vous de remplir les conditions préalables suivantes avant de créer un clone de bac à sable.

- **Identifiants et autorisations** : Vous devez avoir ["Informations d'identification du compte AWS et autorisations opérations et remédiation"](#) pour créer un clone sandbox dans Workload Factory.

Vous pouvez également utiliser le Codebox pour copier un modèle partiellement rempli ou créer un modèle complet afin de pouvoir créer le clone du sandbox en dehors de Workload Factory à l'aide de l'API REST. ["Découvrez-en plus sur l'automatisation de Codebox"](#).

- **Microsoft SQL Server** : vous devez disposer d'un Microsoft SQL Server géré dans Workload Factory for Databases pour héberger le nouveau clone de sandbox.
- **AWS Systems Manager**: Assurez-vous que le NT Authority\SYSTEM privilège utilisateur est activé sur l'hôte Microsoft SQL via AWS Systems Manager.
- **Base de données source** : Vous avez besoin d'une base de données source disponible pour le clone.

Étapes

1. Connectez-vous au ["NetApp Console"](#).
2. Sélectionnez le menu , **Charges de travail > Bases de données**.
3. Dans Databases, sélectionnez l'onglet **Sandboxes**.
4. Dans l'onglet Bacs à sable, sélectionnez **Créer un nouveau bac à sable**.
5. Sur la page Créer un nouvel environnement de test, sous Source de base de données, indiquez les informations suivantes :
 - a. **Hôte de la base de données source** : Sélectionnez l'hôte de la base de données source.
 - b. **Instance de base de données source** : Sélectionnez l'instance de base de données source.
 - c. **Base de données source**: Sélectionnez la base de données source à partir de laquelle effectuer le clonage.
6. Sous « Cible de base de données », indiquez les éléments suivants :
 - a. **Hôte de base de données cible** : Sélectionnez un hôte de base de données cible pour le clone sandbox qui se trouve dans le même VPC et qui possède le même système de fichiers FSx for ONTAP que l'hôte source.
 - b. **Instance de base de données cible** : Sélectionnez l'instance de base de données cible pour le clone de bac à sable.
 - c. **Base de données cible** : Saisissez un nom pour le clone sandbox.
7. **Montage** : Lors du clonage d'une base de données comportant plusieurs fichiers de données et/ou de journalisation, Workload Factory clone tous les fichiers sous la lettre de lecteur attribuée automatiquement ou définie.

Sélectionnez l'une des options suivantes :

- a. **Attribution automatique du point de montage**
- b. **Définir le chemin du point de montage**

Veuillez fournir les informations suivantes pour définir le chemin du point de montage :

- Saisissez la lettre du lecteur pour le chemin d'accès au fichier de données.

- Saisissez la lettre du lecteur correspondant au chemin d'accès du fichier journal.

8. **Définir l'étiquette** : Sélectionnez une étiquette pour définir le clone du bac à sable.

9. Cliquez sur **Créer**.

Pour vérifier l'avancement de la tâche, rendez-vous dans l'onglet **Suivi des tâches**.

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.