Créez un nouveau serveur de base de données

Database workloads

NetApp
March 02, 2026

Sommaire

Créez un nouveau serveur de base de données

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

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

Description de la tâche

Avant de créer un serveur Microsoft SQL Server à partir de Workload Factory, découvrez les types de déploiement de stockage disponibles pour la configuration de l'hôte de base de données, la configuration Microsoft Multi-path I/O, le déploiement Active Directory, les détails de mise en réseau et les exigences pour effectuer cette opération.

Après le déploiement, vous devrez Activez la connexion à distance sur Microsoft SQL Server.

FSX pour les déploiements de systèmes de fichiers ONTAP

La création d'un nouveau serveur Microsoft SQL nécessite un système de fichiers FSX pour ONTAP en tant que système back-end de stockage. Vous pouvez utiliser un système de fichiers FSX pour ONTAP existant ou créer un nouveau système de fichiers. Si vous sélectionnez un système de fichiers FSX pour ONTAP existant comme back-end de stockage du serveur de base de données, nous créons une nouvelle VM de stockage pour les workloads Microsoft SQL.

Les systèmes de fichiers FSX pour ONTAP disposent de deux modèles de déploiement Microsoft SQL Server : *instance de cluster de basculement (FCI)* ou *autonome*. Différentes ressources sont créées pour le système de fichiers FSX pour ONTAP selon le modèle de déploiement de FSX pour ONTAP que vous sélectionnez.

- **Instance de cluster de basculement (FCI) déploiement Microsoft SQL** : un système de fichiers FSX pour NetApp ONTAP à plusieurs zones de disponibilité est déployé lorsqu'un nouveau système de fichiers FSX pour ONTAP est sélectionné pour le déploiement FCI. Des volumes et des LUN distincts sont créés pour les fichiers de données, de journaux et de tempdb pour un déploiement FCI. Un volume et une LUN supplémentaires sont créés pour quorum ou disque témoin pour le cluster Windows.
- **Déploiement autonome de Microsoft SQL** : un système de fichiers FSX pour ONTAP à zone de disponibilité unique est créé lors de la création d'un nouveau serveur Microsoft SQL. De plus, des volumes et des LUN distincts sont créés pour les fichiers de données, de journaux et de tempdb.

Configuration d'E/S multi-chemins Microsoft

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

Pour plus d'informations, reportez-vous à "Déploiements haute disponibilité de SQL Server avec Amazon FSx for NetApp ONTAP" .

Active Directory

Les événements suivants se produisent pour Active Directory (AD) pendant le 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 de nœud et le nom FCI Microsoft SQL sont ajoutés en tant qu'ordinateurs gérés au compte de service Microsoft SQL.
- L'entrée de 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 vers le service d'annuaire pour le déploiement. Workload Factory n'attache pas automatiquement le groupe de sécurité pour Active Directory géré par l'utilisateur comme il le fait pour AWS Managed Microsoft AD.

Restauration des ressources

Si vous décidez de restaurer vos ressources DNS (Domain Name System), 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 AD géré par l'utilisateur, d'abord "Retirez l'ordinateur AD". Ensuite, connectez-vous au serveur DNS à partir du gestionnaire DNS et "Supprimez les enregistrements de ressources DNS"de .
- Pour Microsoft AD géré par AWS, "Installez les outils d'administration AD". Ensuite, "Retirez l'ordinateur AD". Enfin, connectez-vous au serveur DNS à partir du gestionnaire DNS et "Supprimez les enregistrements de ressources DNS"de .

Avant de commencer

Assurez-vous de disposer des conditions préalables suivantes avant de créer un nouvel hôte de base de données.

Informations d'identification et autorisations

Vous devez "accorder les permissions 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

Lorsque vous vous connectez à Active Directory, vous devez disposer d'un accès administrateur avec des autorisations pour effectuer les opérations suivantes :

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

Étape 1 : création d'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 *Automatiser*. Vous pouvez également utiliser les outils suivants disponibles dans Codebox : API REST, AWS CLI, AWS CloudFormation et Terraform. "Découvrez comment utiliser Codebox pour l'automatisation" .

Lorsque vous utilisez Terraform à partir de Codebox, le code que vous copiez ou téléchargez se cache `fsxadmin` et `vsadmin` passe. Vous devrez saisir à nouveau les mots de passe lorsque vous exécuterez le code. Vous devrez inclure les autorisations suivantes pour le compte d'utilisateur en plus des autorisations *automate* mode : `iam:TagRole` et `iam:TagInstanceProfile`. "Découvrez comment utiliser Terraform à partir de Codebox".

Lors du déploiement, Workload Factory active CredSSP pour la délégation d'informations d'identification aux scripts pour le provisionnement de SQL. Lorsque la délégation CredSSP est bloquée pour tous les ordinateurs du domaine avec la stratégie de groupe, le déploiement échoue. Après le déploiement, Workload Factory désactive CredSSP.

Création rapide

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

Étapes

1. Connectez-vous à l'aide de l'un des "expériences de la console".
2. Dans la mosaïque Bases de données, sélectionnez **Déployer l'hôte**, puis sélectionnez **Microsoft SQL Server** dans le menu.
3. Sélectionnez **création rapide**.
4. Sous **paramètres AWS**, fournissez les informations suivantes :
   a. **Informations d'identification AWS** : sélectionnez les informations d'identification AWS avec des autorisations d'automatisation pour déployer le nouvel hôte de base de données.

      Les informations d'identification AWS avec des autorisations de lecture/écriture permettent à Workload Factory de déployer et de gérer le nouvel hôte de base de données à partir de votre compte AWS dans Workload Factory.

      Les informations d'identification AWS avec des autorisations en lecture seule permettent à Workload Factory de générer un modèle CloudFormation que vous pouvez utiliser dans la console AWS CloudFormation.

      Si vous n'avez pas d'informations d'identification AWS associées à Workload Factory et que vous souhaitez créer le nouveau serveur dans Workload Factory, suivez l'**Option 1** pour accéder à la page Informations d'identification. Ajoutez manuellement les informations d'identification et les autorisations requises pour le mode *lecture/écriture* 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 pouvoir 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 et les autorisations requises pour le mode *lecture* pour les charges de travail de base de données.

      En option, vous pouvez télécharger un modèle de fichier YAML partiellement complété à partir de Codebox pour créer la pile en dehors de Workload Factory sans aucune information d'identification ni autorisation. Sélectionnez **CloudFormation** dans la liste déroulante de la boîte de code 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 aux points de terminaison d'interface existants et que les groupes de sécurité autorisent l'accès au protocole HTTPS (443) aux sous-réseaux sélectionnés.

      Terminaux de l'interface de services AWS (SQS, FSX, EC2, CloudWatch, CloudFormation, SSM) et le noeud final de la passerelle S3 sont créés pendant le déploiement s'ils sont introuvables.

      Les attributs DNS VPC `EnableDnsSupport` et `EnableDnsHostnames` sont modifiés pour activer la résolution de l'adresse du terminal 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 de l'autre VPC où réside le DNS doit autoriser le port 443 pour les sous-réseaux de déploiement. Dans le cas contraire, vous devez fournir un résolveur DNS du VPC local lors de la connexion à un Active Directory inter-VPC. Dans un environnement de contrôleurs de domaine répliqués multiples, si certains contrôleurs de domaine ne sont pas accessibles depuis le sous-réseau, vous pouvez effectuer une redirection vers CloudFormation et saisir `Preferred domain controller` pour se 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 ici ne sont pris en charge que sur plusieurs zones de disponibilité (MAZ) FSX pour les configurations ONTAP.

i. Dans le champ **Configuration du cluster - nœud 1**, sélectionnez la zone de disponibilité principale de la configuration MAZ FSX pour ONTAP dans le menu déroulant **zone de disponibilité** et un sous-réseau dans 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 pour ONTAP dans le menu déroulant **zone de disponibilité** et un sous-réseau dans la zone de disponibilité secondaire dans le menu déroulant **sous-réseau**.

5. Sous **Paramètres de l'application**, entrez un nom d'utilisateur et un mot de passe pour **informations d'identification de la base de données**.
6. Sous **connectivité**, fournissez les informations suivantes :
   a. **Paire de clés** : sélectionnez une paire de clés.
   b. **Active Directory** :
      i. Dans le champ **Nom de domaine**, sélectionnez ou entrez un nom pour le domaine.
         A. Pour les Active Directory gérés par AWS, les noms de domaine apparaissent dans le menu déroulant.
         B. Pour un Active Directory géré par l'utilisateur, entrez un nom dans le champ **Rechercher et Ajouter**, puis cliquez sur **Ajouter**.
      ii. Dans le champ **DNS address**, entrez l'adresse IP DNS du domaine. Vous pouvez ajouter jusqu'à 3 adresses IP.

      Pour les répertoires actifs gérés par AWS, les adresses IP DNS apparaissent dans le menu déroulant.

      iii. Dans le champ **Nom d'utilisateur**, entrez le nom d'utilisateur du domaine Active Directory.
      iv. Dans le champ **Mot de passe**, entrez un mot de passe pour le domaine Active Directory.
7. Sous **Paramètres d'infrastructure**, fournissez les informations suivantes :
   a. **FSX pour système ONTAP** : créez un nouveau système de fichiers FSX pour ONTAP ou utilisez un système de fichiers FSX pour ONTAP existant.
      i. **Créer une nouvelle FSX pour ONTAP** : entrez le nom d'utilisateur et le mot de passe.

      Un nouveau système de fichiers FSX pour ONTAP peut ajouter 30 minutes ou plus de temps d'installation.

ii. **Sélectionnez une FSX pour ONTAP** existante : sélectionnez le nom de FSX pour ONTAP dans le menu déroulant et entrez un nom d'utilisateur et un mot de passe pour le système de fichiers.

Pour les systèmes de fichiers FSX for ONTAP existants, vérifiez les points suivants :

- Le groupe de routage rattaché à FSX pour ONTAP permet d'utiliser les routes vers les sous-réseaux pour le déploiement.
- Le groupe de sécurité autorise le trafic à partir des sous-réseaux utilisés pour le déploiement, en particulier les ports TCP HTTPS (443) et iSCSI (3260).

b. **Taille du lecteur de données** : entrez la capacité du lecteur de données et sélectionnez l'unité de capacité.

8. Résumé :
   a. **Prévisualisation par défaut** : consultez les configurations par défaut définies par création rapide.
   b. **Coût estimé** : fournit une estimation des frais que vous pourriez engager si vous avez déployé les ressources indiquées.
9. Cliquez sur **Créer**.

Sinon, si vous souhaitez modifier l'un de ces paramètres par défaut 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 en utilisant l'un des"expériences de la console" . Dans la mosaïque Bases de données, sélectionnez **Déployer l'hôte**, puis sélectionnez **Microsoft SQL Server** dans le menu.
2. Sélectionnez **création avancée**.
3. Pour **modèle de déploiement**, sélectionnez **instance de cluster de basculement** ou **instance unique**.
4. Sous **paramètres AWS**, fournissez les informations suivantes :
   a. **Informations d'identification AWS** : sélectionnez les informations d'identification AWS avec des autorisations d'automatisation pour déployer le nouvel hôte de base de données.

   Les informations d'identification AWS avec des autorisations de lecture/écriture permettent à Workload Factory de déployer et de gérer le nouvel hôte de base de données à partir de votre compte AWS dans Workload Factory.

   Les informations d'identification AWS avec des autorisations en lecture seule permettent à Workload Factory de générer un modèle CloudFormation que vous pouvez utiliser dans la console AWS CloudFormation.

   Si vous n'avez pas d'informations d'identification AWS associées à Workload Factory et que vous souhaitez créer le nouveau serveur dans Workload Factory, suivez l'**Option 1** pour accéder à la page Informations d'identification. Ajoutez manuellement les informations d'identification et les autorisations requises pour le mode *lecture/écriture* 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 pouvoir 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 et les autorisations requises pour le mode *lecture seule* pour les charges de travail de base de données.

En option, vous pouvez télécharger un modèle de fichier YAML partiellement complété à partir de Codebox pour créer la pile en dehors de Workload Factory sans aucune information d'identification ni autorisation. Sélectionnez **CloudFormation** dans la liste déroulante de la boîte de code 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 noeud final d'interface existant autorisent l'accès au protocole HTTPS (443) aux sous-réseaux sélectionnés.

   Terminaux de l'interface de services AWS (SQS, FSX, EC2, CloudWatch, formation du cloud, SSM) et le noeud final de la passerelle S3 sont créés lors du déploiement s'ils sont introuvables.

   Les attributs DNS VPC `EnableDnsSupport` et `EnableDnsHostnames` sont modifiés pour activer la résolution de l'adresse du point de terminaison si ce n'est pas déjà fait 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 une haute disponibilité.

   Les déploiements ici ne sont pris en charge que sur plusieurs zones de disponibilité (MAZ) FSX pour les configurations ONTAP.

   - Pour les déploiements d'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 de la configuration MAZ FSX pour ONTAP dans le menu déroulant **zone de disponibilité** et un sous-réseau dans 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 pour ONTAP dans le menu déroulant **zone de disponibilité** et un sous-réseau dans la zone de disponibilité secondaire dans le menu déroulant **sous-réseau**.

d. **Groupe de sécurité** : sélectionnez un groupe de sécurité existant ou créez un nouveau groupe de sécurité. Trois groupes de sécurité sont rattachés aux nœuds SQL (instances EC2) lors du déploiement du nouveau serveur.

   i. Un groupe de sécurité de la charge de travail est créé pour autoriser les ports et les protocoles requis pour les communications de cluster Microsoft SQL et Windows sur les nœuds.

   ii. Dans le cas d'Active Directory géré par AWS, le groupe de sécurité rattaché au service d'annuaire est automatiquement ajouté aux nœuds Microsoft SQL pour permettre la

communication avec Active Directory.

iii. Pour un système de fichiers FSX for ONTAP existant, le groupe de sécurité qui lui est associé est automatiquement ajouté aux nœuds SQL qui permettent la communication avec le système de fichiers. Lorsqu'un nouveau système FSX pour ONTAP est créé, un nouveau groupe de sécurité est créé pour le système de fichiers FSX pour ONTAP et le même groupe de sécurité est également rattaché aux nœuds SQL.

Pour un Active Directory géré par l'utilisateur, assurez-vous que le groupe de sécurité configuré sur l'instance AD autorise le trafic à partir des sous-réseaux utilisés pour le déploiement. Le groupe de sécurité doit permettre la communication avec les contrôleurs de domaine Active Directory à partir des sous-réseaux où les instances EC2 pour Microsoft SQL sont configurées.

5. Sous **Paramètres de l'application**, fournissez les informations suivantes :
   a. Sous **SQL Server install type**, sélectionnez **License Incomed ami** ou **Use custom ami**.
      i. Si vous sélectionnez **Licence avec ami**, fournissez les informations suivantes :
         A. **Système d'exploitation** : sélectionnez **Windows Server 2016**, **Windows Server 2019** ou **Windows Server 2022**.
         B. **Édition de la 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. **Ami SQL Server** : sélectionnez une ami SQL Server dans le menu déroulant.
      ii. Si vous sélectionnez **utiliser ami personnalisé**, sélectionnez un ami dans le menu déroulant.
   b. **Classement SQL Server** : sélectionnez un jeu de classement 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** : entrez le nom du cluster de base de données.
   d. **Informations d'identification de la base de données** : saisissez un nom d'utilisateur et un mot de passe pour un nouveau compte de service ou utilisez les informations d'identification de compte de service existantes dans Active Directory.

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

6. Sous **connectivité**, fournissez les informations suivantes :
   a. **Paire de clés** : sélectionnez une paire de clés pour vous connecter en toute sécurité à votre instance.
   b. **Active Directory** : fournissez les détails Active Directory suivants :
      i. Dans le champ **Nom de domaine**, sélectionnez ou entrez un nom pour le domaine.
         A. Pour les Active Directory gérés par AWS, les noms de domaine apparaissent dans le menu déroulant.

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

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

Pour les répertoires actifs gérés par AWS, les adresses IP DNS apparaissent dans le menu déroulant.

iii. Dans le champ **Nom d'utilisateur**, entrez le nom d'utilisateur du domaine Active Directory.

iv. Dans le champ **Mot de passe**, entrez un mot de passe pour le domaine Active Directory.

v. **Contrôleur de domaine préféré** : Vous pouvez saisir le contrôleur de domaine préféré auquel Active Directory devra se joindre.

vi. **Chemin d'accès à l'unité organisationnelle préférée** : Vous pouvez également saisir l'unité organisationnelle (UO) préférée dans Active Directory à rejoindre.

vii. **Groupe Active Directory cible** : Vous pouvez éventuellement saisir le groupe Active Directory cible auquel ajouter les ordinateurs.

7. Sous **Paramètres d'infrastructure**, fournissez les informations suivantes :

a. **Type d'instance DB** : sélectionnez le type d'instance de base de données dans le menu déroulant.

b. **FSX pour système ONTAP** : créez un nouveau système de fichiers FSX pour ONTAP ou utilisez un système de fichiers FSX pour ONTAP existant.

i. **Créer une nouvelle FSX pour ONTAP** : entrez le nom d'utilisateur et le mot de passe.

Un nouveau système de fichiers FSX pour ONTAP peut ajouter 30 minutes ou plus de temps d'installation.

ii. **Sélectionnez une FSX pour ONTAP** existante : sélectionnez le nom de FSX pour ONTAP dans le menu déroulant et entrez un nom d'utilisateur et un mot de passe pour le système de fichiers.

Pour les systèmes de fichiers FSX for ONTAP existants, vérifiez les points suivants :

- Le groupe de routage rattaché à FSX pour ONTAP permet d'utiliser les routes vers les sous-réseaux pour le déploiement.
- Le groupe de sécurité autorise le trafic à partir des sous-réseaux utilisés pour le déploiement, en particulier les ports TCP HTTPS (443) et iSCSI (3260).

c. **Règle Snapshot** : activée par défaut. Les snapshots sont pris tous les jours et disposent d'une période de conservation de 7 jours.

Les snapshots sont attribués aux volumes créés pour les charges de travail SQL.

d. **Taille du lecteur de données** : entrez la capacité du lecteur de données et sélectionnez l'unité de capacité.

e. **IOPS approvisionnées** : sélectionnez **automatique** ou **utilisateur-provisionné**. Si vous sélectionnez **utilisateur-provisionné**, entrez la valeur d'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 Gbit/s. Pour

provisionner une capacité de débit de 4 Gbit/s, votre système de fichiers FSX for ONTAP doit être configuré avec une capacité de stockage SSD d'au moins 5,120 Gio et 160,000 IOPS SSD.

g. **Cryptage** : sélectionnez une clé de votre compte ou une clé d'un autre compte. Vous devez entrer la clé de cryptage ARN d'un autre compte.

   Les clés de chiffrement personnalisées FSX pour 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 entraînent un échec de la création du serveur.

   Les clés gérées par AWS sont filtrées en fonction de l'applicabilité du service.

h. **Tags**: Vous pouvez éventuellement ajouter jusqu'à 40 tags.

i. **Simple notification Service** : vous pouvez éventuellement activer le service SNS (simple notification Service) pour cette configuration en sélectionnant une rubrique SNS pour Microsoft SQL Server dans le menu déroulant.

   i. Activez le service de notification simple.

   ii. Sélectionnez un ARN dans le menu déroulant.

j. **Surveillance de CloudWatch** : vous pouvez éventuellement activer la surveillance de CloudWatch.

   Nous vous recommandons d'activer CloudWatch pour le débogage en cas de défaillance. Les événements qui apparaissent dans la console AWS CloudFormation sont de haut niveau et ne spécifient 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 noeud de validation et noeud 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. **Annulation de ressources** : cette fonction n'est pas prise en charge actuellement.

8. Récapitulatif

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

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

   Vous pouvez également enregistrer la configuration.

Étape 2 : activez 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 du port dynamique en vous reportant à la section "Une erreur liée au réseau ou spécifique à une instance s'est produite lors de l'établissement d'une connexion à SQL Server" de la

documentation Microsoft.

3. Autorisez l'adresse IP ou le sous-réseau du client requis dans le groupe de sécurité.

Et la suite

Maintenant vous pouvez"créer une base de données dans Workload Factory pour les bases de données" .

Créer un serveur PostgreSQL dans NetApp Workload Factory

La création d'un nouveau serveur PostgreSQL ou d'un hôte de base de données dans NetApp Workload Factory for Databases nécessite un déploiement de système de fichiers FSx pour ONTAP et des ressources pour Active Directory.

Description de la tâche

Avant de créer un serveur PostgreSQL à partir de Workload Factory, découvrez les types de déploiement de stockage disponibles pour la configuration de l'hôte de base de données, les modes de fonctionnement de Workload Factory et les exigences pour effectuer cette opération.

FSX pour les déploiements de systèmes de fichiers ONTAP

La création d'un nouveau serveur PostgreSQL requiert un système de fichiers FSX pour ONTAP en tant que système back-end de stockage. Vous pouvez utiliser un système de fichiers FSX pour ONTAP existant ou créer un nouveau système de fichiers. Si vous sélectionnez un système de fichiers FSX pour ONTAP existant comme back-end de stockage du serveur de base de données, nous créons une nouvelle VM de stockage pour les charges de travail PostgreSQL.

+ Les systèmes de fichiers FSx pour ONTAP ont deux modèles de déploiement de serveur PostgreSQL : *Haute disponibilité (HA)* ou *instance unique*. Différentes ressources sont créées pour le système de fichiers FSx for ONTAP en fonction du modèle de déploiement FSx for ONTAP que vous sélectionnez.

- **Déploiement haute disponibilité (HA)** : un système de fichiers FSX pour NetApp ONTAP à plusieurs zones de disponibilité est déployé lorsqu'un nouveau système de fichiers FSX pour ONTAP est sélectionné pour le déploiement haute disponibilité. Des volumes et des LUN distincts sont créés pour les fichiers de données, de journaux et de tempdb pour un déploiement HA. Un volume et une LUN supplémentaires sont créés pour quorum ou disque témoin pour le cluster Windows. Le déploiement HAUTE DISPONIBILITÉ configure la réplication de flux entre les serveurs PostgreSQL principaux et secondaires.
- **Déploiement d'une instance unique** : un système de fichiers FSX pour ONTAP à zone de disponibilité unique est créé lors de la création d'un nouveau serveur PostgreSQL. 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 avoir "accorder les permissions 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.

Créez un serveur PostgreSQL

Vous pouvez utiliser les modes de déploiement *Quick CREATE* ou *Advanced CREATE* pour effectuer cette tâche en usine avec des autorisations de mode *automate*. Vous pouvez également utiliser les outils suivants disponibles dans la Codebox : l'API REST, la CLI AWS, AWS CloudFormation et Terraform. "Découvrez comment utiliser Codebox pour l'automatisation".

Lorsque vous utilisez Terraform à partir de Codebox, le code que vous copiez ou téléchargez se cache `fsxadmin` et `vsadmin` passe. Vous devrez saisir à nouveau les mots de passe lorsque vous exécuterez le code. Vous devrez inclure les autorisations suivantes pour le compte d'utilisateur en plus des autorisations *automate* mode : `iam:TagRole` et `iam:TagInstanceProfile`. "Découvrez comment utiliser Terraform à partir de Codebox".

Création rapide

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

Étapes

1. Connectez-vous à l'aide de l'un des "expériences de la console".
2. Dans la mosaïque Bases de données, sélectionnez **Déployer l'hôte**, puis sélectionnez **Serveur PostgreSQL** dans le menu.
3. Sélectionnez **création rapide**.
4. Sous **zone d'atterrissage**, fournissez les informations suivantes :
   a. **Informations d'identification AWS** : sélectionnez les informations d'identification AWS avec des autorisations d'automatisation pour déployer le nouvel hôte de base de données.

      Les informations d'identification AWS avec des autorisations de lecture/écriture permettent à Workload Factory de déployer et de gérer le nouvel hôte de base de données à partir de votre compte AWS dans Workload Factory.

      Les informations d'identification AWS avec des autorisations en lecture seule permettent à Workload Factory de générer un modèle CloudFormation que vous pouvez utiliser dans la console AWS CloudFormation.

      Si vous ne disposez pas d'informations d'identification AWS associées à l'usine de la charge de travail et que vous souhaitez créer le nouveau serveur en usine de la charge de travail, suivez **option 1** pour accéder à la page informations d'identification. Ajoutez manuellement les informations d'identification et les autorisations requises pour le mode *lecture/écriture* pour les charges de travail de base de données.

      Si vous souhaitez remplir le formulaire Créer un nouveau serveur en usine de charges de travail afin de télécharger un modèle de fichier YAML complet pour le déploiement dans AWS CloudFormation, suivez **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 et les autorisations requises pour le mode *lecture seule* pour les charges de travail de base de données.

      Vous pouvez également télécharger un modèle de fichier YAML partiellement rempli à partir de la Codebox pour créer la pile en dehors de l'usine de la charge de travail sans informations d'identification ni autorisations. Sélectionnez **CloudFormation** dans la liste déroulante de la zone de code 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 noeud final d'interface existant autorisent l'accès au protocole HTTPS (443) aux sous-réseaux sélectionnés.

      Terminaux de l'interface de services AWS (SQS, FSX, EC2, CloudWatch, CloudFormation, SSM) et le noeud final de la passerelle S3 sont créés pendant le déploiement s'ils sont introuvables.

      Les attributs DNS VPC `EnableDnsSupport` et `EnableDnsHostnames` sont modifiés pour activer la résolution de l'adresse du terminal s'ils ne sont pas déjà définis sur `true`.

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

> Les déploiements HAUTE DISPONIBILITÉ ne sont pris en charge que dans plusieurs configurations FSX pour ONTAP avec plusieurs zones de disponibilité (MAZ).

Les sous-réseaux ne doivent pas partager la même table de routage pour la haute disponibilité.

i. Dans le champ **Configuration du cluster - nœud 1**, sélectionnez la zone de disponibilité principale de la configuration MAZ FSX pour ONTAP dans le menu déroulant **zone de disponibilité** et un sous-réseau dans 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 pour ONTAP dans le menu déroulant **zone de disponibilité** et un sous-réseau dans la zone de disponibilité secondaire dans le menu déroulant **sous-réseau**.

5. Sous **Paramètres de l'application**, entrez un nom d'utilisateur et un mot de passe pour **informations d'identification de la base de données**.
6. Sous **connectivité**, sélectionnez une paire de clés pour vous connecter en toute sécurité à votre instance.
7. Sous **Paramètres d'infrastructure**, fournissez les informations suivantes :
   a. **FSX pour système ONTAP** : créez un nouveau système de fichiers FSX pour ONTAP ou utilisez un système de fichiers FSX pour ONTAP existant.
      i. **Créer une nouvelle FSX pour ONTAP** : entrez le nom d'utilisateur et le mot de passe.

      Un nouveau système de fichiers FSX pour ONTAP peut ajouter 30 minutes ou plus de temps d'installation.

      ii. **Sélectionnez une FSX pour ONTAP** existante : sélectionnez le nom de FSX pour ONTAP dans le menu déroulant et entrez un nom d'utilisateur et un mot de passe pour le système de fichiers.

      Pour les systèmes de fichiers FSX for ONTAP existants, vérifiez les points suivants :

      - Le groupe de routage rattaché à FSX pour ONTAP permet d'utiliser les routes vers les sous-réseaux pour le déploiement.
      - Le groupe de sécurité autorise le trafic à partir des sous-réseaux utilisés pour le déploiement, en particulier les ports TCP HTTPS (443) et iSCSI (3260).

   b. **Taille du lecteur de données** : entrez la capacité du lecteur de données et sélectionnez l'unité de capacité.
8. Résumé :
   a. **Prévisualisation par défaut** : consultez les configurations par défaut définies par création rapide.
   b. **Coût estimé** : fournit une estimation des frais que vous pourriez engager si vous avez déployé les ressources indiquées.
9. Cliquez sur **Créer**.

Sinon, si vous souhaitez modifier l'un de ces paramètres par défaut 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 à l'aide de l'un des "expériences de la console".
2. Dans la mosaïque Bases de données, sélectionnez **Déployer l'hôte**, puis sélectionnez **Serveur PostgreSQL** dans le menu.
3. Sélectionnez **création avancée**.
4. Sous **modèle de déploiement**, sélectionnez **instance autonome** ou **haute disponibilité (HA)**.
5. Sous **zone d'atterrissage**, fournissez les informations suivantes :
   a. **Informations d'identification AWS** : sélectionnez les informations d'identification AWS avec des autorisations d'automatisation pour déployer le nouvel hôte de base de données.

      Les identifiants AWS avec autorisations *automatiser* permettent à la charge de travail de déployer et de gérer en usine le nouvel hôte de base de données à partir de votre compte AWS dans l'usine de la charge de travail.

      Les informations d'identification AWS avec des autorisations en lecture seule permettent à Workload Factory de générer un modèle CloudFormation que vous pouvez utiliser dans la console AWS CloudFormation.

      Si vous ne disposez pas d'informations d'identification AWS associées à l'usine de la charge de travail et que vous souhaitez créer le nouveau serveur en usine de la charge de travail, suivez **option 1** pour accéder à la page informations d'identification. Ajoutez manuellement les informations d'identification et les autorisations requises pour le mode *lecture/écriture* pour les charges de travail de base de données.

      Si vous souhaitez remplir le formulaire Créer un nouveau serveur en usine de charges de travail afin de télécharger un modèle de fichier YAML complet pour le déploiement dans AWS CloudFormation, suivez **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 et les autorisations requises pour le mode *lecture seule* pour les charges de travail de base de données.

      Vous pouvez également télécharger un modèle de fichier YAML partiellement rempli à partir de la Codebox pour créer la pile en dehors de l'usine de la charge de travail sans informations d'identification ni autorisations. Sélectionnez **CloudFormation** dans la liste déroulante de la zone de code 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 noeud final d'interface existant autorisent l'accès au protocole HTTPS (443) aux sous-réseaux sélectionnés.

      Terminaux de l'interface de services AWS (SQS, FSX, EC2, CloudWatch, formation du cloud, SSM) et le noeud final de la passerelle S3 sont créés lors du déploiement s'ils sont introuvables.

      Les attributs DNS VPC `EnableDnsSupport` et `EnableDnsHostnames` sont modifiés pour activer la résolution de l'adresse du point de terminaison si ce n'est pas déjà fait 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 **zone de disponibilité** et un sous-réseau dans le menu déroulant **sous-réseau**.

Pour les déploiements HA

i. Dans le champ **Configuration du cluster - nœud 1**, sélectionnez la zone de disponibilité principale de la configuration MAZ FSX pour ONTAP dans le menu déroulant **zone de disponibilité** et un sous-réseau dans 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 pour ONTAP dans le menu déroulant **zone de disponibilité** et un sous-réseau dans la zone de disponibilité secondaire dans le menu déroulant **sous-réseau**.

d. **Groupe de sécurité** : sélectionnez un groupe de sécurité existant ou créez un nouveau groupe de sécurité.

Deux groupes de sécurité sont rattachés aux nœuds SQL (instances EC2) lors du déploiement du nouveau serveur.

i. Un groupe de sécurité des charges de travail est créé pour autoriser les ports et les protocoles requis pour PostgreSQL.

ii. Pour un nouveau système de fichiers FSX for ONTAP, un nouveau groupe de sécurité est créé et rattaché au nœud SQL. Pour un système de fichiers FSX for ONTAP existant, le groupe de sécurité qui lui est associé est automatiquement ajouté au nœud PostgreSQL, ce qui permet la communication avec le système de fichiers.

6. Sous **Paramètres de l'application**, fournissez les informations suivantes :
   a. Sélectionnez **système d'exploitation** dans le menu déroulant.
   b. Sélectionnez **PostgreSQL version** dans le menu déroulant.
   c. **Nom du serveur de base de données** : entrez le nom du cluster de base de données.
   d. **Informations d'identification de la base de données** : saisissez un nom d'utilisateur et un mot de passe pour un nouveau compte de service ou utilisez les informations d'identification de compte de service existantes dans Active Directory.
7. Sous **connectivité**, sélectionnez une paire de clés pour vous connecter en toute sécurité à votre instance.
8. Sous **Paramètres d'infrastructure**, fournissez les informations suivantes :
   a. **Type d'instance DB** : sélectionnez le type d'instance de base de données dans le menu déroulant.
   b. **FSX pour système ONTAP** : créez un nouveau système de fichiers FSX pour ONTAP ou utilisez un système de fichiers FSX pour ONTAP existant.
      i. **Créer une nouvelle FSX pour ONTAP** : entrez le nom d'utilisateur et le mot de passe.

      Un nouveau système de fichiers FSX pour ONTAP peut ajouter 30 minutes ou plus de temps d'installation.

      ii. **Sélectionnez une FSX pour ONTAP** existante : sélectionnez le nom de FSX pour ONTAP

dans le menu déroulant et entrez un nom d'utilisateur et un mot de passe pour le système de fichiers.

Pour les systèmes de fichiers FSX for ONTAP existants, vérifiez les points suivants :

- Le groupe de routage rattaché à FSX pour ONTAP permet d'utiliser les routes vers les sous-réseaux pour le déploiement.
- Le groupe de sécurité autorise le trafic à partir des sous-réseaux utilisés pour le déploiement, en particulier les ports TCP HTTPS (443) et iSCSI (3260).

c. **Règle Snapshot** : activée par défaut. Les snapshots sont pris tous les jours et disposent d'une période de conservation de 7 jours.

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

d. **Taille du lecteur de données** : entrez la capacité du lecteur de données et sélectionnez l'unité de capacité.

e. **IOPS approvisionnées** : sélectionnez **automatique** ou **utilisateur-provisionné**. Si vous sélectionnez **utilisateur-provisionné**, entrez la valeur d'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 Gbit/s. Pour provisionner une capacité de débit de 4 Gbit/s, votre système de fichiers FSX for ONTAP doit être configuré avec une capacité de stockage SSD d'au moins 5,120 Gio et 160,000 IOPS SSD.

g. **Cryptage** : sélectionnez une clé de votre compte ou une clé d'un autre compte. Vous devez entrer la clé de cryptage ARN d'un autre compte.

Les clés de chiffrement personnalisées FSX pour 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 entraînent un échec de la création du serveur.

Les clés gérées par AWS sont filtrées en fonction de l'applicabilité du service.

h. **Tags**: Vous pouvez éventuellement ajouter jusqu'à 40 tags.

i. **Simple notification Service** : vous pouvez éventuellement activer le service SNS (simple notification Service) pour cette configuration en sélectionnant une rubrique SNS pour Microsoft SQL Server dans le menu déroulant.

   i. Activez le service de notification simple.

   ii. Sélectionnez un ARN dans le menu déroulant.

j. **Surveillance de CloudWatch** : vous pouvez éventuellement activer la surveillance de CloudWatch.

Nous vous recommandons d'activer CloudWatch pour le débogage en cas de défaillance. Les événements qui apparaissent dans la console AWS CloudFormation sont de haut niveau et ne spécifient 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 noeud de validation et noeud 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. **Annulation de ressources** : cette fonction n’est pas prise en charge actuellement.

9. Récapitulatif
   a. **Coût estimé** : fournit une estimation des frais que vous pourriez engager si vous avez déployé les ressources indiquées.
10. Cliquez sur **Créer** pour déployer le nouvel hôte de base de données.

    Vous pouvez également enregistrer la configuration.

Et la suite

Vous pouvez configurer manuellement les utilisateurs, l’accès à distance et les bases de données sur le serveur PostgreSQL déployé.