Creare un nuovo server di database

Database workloads

NetApp
January 05, 2026

Sommario

Creare un nuovo server di database

Creare un server Microsoft SQL in Workload Factory per i database

Per creare un nuovo Microsoft SQL Server o un host di database in Workload Factory for Databases è necessario un'implementazione del file system FSx for ONTAP e risorse per Active Directory.

A proposito di questa attività

Prima di creare un Microsoft SQL Server da Workload Factory, informati sui tipi di distribuzione dell'archiviazione disponibili per la configurazione dell'host del database, sulla configurazione Microsoft Multi-path I/O, sulla distribuzione di Active Directory, sui dettagli di rete e sui requisiti per completare questa operazione.

Dopo la distribuzione, sarà necessario Attivare la connessione remota su Microsoft SQL Server.

FSX per implementazioni di file system ONTAP

La creazione di un nuovo Microsoft SQL Server richiede un file system FSX per ONTAP come backend dello storage. Puoi usare un file system FSX for ONTAP esistente o creare un nuovo file system. Se selezioni un file system FSX per ONTAP esistente come back-end dello storage del database server, creiamo una nuova macchina virtuale di storage per i carichi di lavoro Microsoft SQL.

I file system FSX per ONTAP hanno due modelli di distribuzione di Microsoft SQL Server: *Istanza cluster di failover (FCI)* o *standalone*. Vengono create risorse diverse per il file system FSX per ONTAP in base al modello di distribuzione di FSX per ONTAP selezionato.

- **Istanza cluster di failover (FCI) distribuzione Microsoft SQL**: Viene distribuito un file system FSX per NetApp ONTAP con più zone di disponibilità quando viene selezionato un nuovo file system FSX per ONTAP per la distribuzione FCI. Volumi e LUN separati vengono creati per i file di dati, log e tempdb per un'implementazione FCI. Vengono creati un volume e un LUN aggiuntivi per Quorum o disco di controllo per il cluster Windows.
- **Distribuzione autonoma di Microsoft SQL**: Quando viene creato un nuovo Microsoft SQL Server, viene creato un file system FSX per ONTAP con un'unica zona di disponibilità. Inoltre, vengono creati volumi e LUN separati per i file di dati, log e tempdb.

Configurazione i/o Microsoft Multi-path

Entrambi i modelli di distribuzione di Microsoft SQL Server richiedono la creazione di LUN tramite il protocollo di archiviazione iSCSI. Workload Factory configura Microsoft Multi-path I/O (MPIO) come parte della configurazione di LUN per SQL Server su FSx per ONTAP. MPIO è configurato in base alle best practice di AWS e NetApp .

Per ulteriori informazioni, fare riferimento a "Distribuzioni di SQL Server ad alta disponibilità tramite Amazon FSx for NetApp ONTAP" .

Active Directory

Durante la distribuzione di Active Directory (ad) si verifica quanto segue:

- Se non si fornisce un account di servizio SQL esistente, viene creato un nuovo account di servizio Microsoft SQL nel dominio.

- Il cluster Windows, i nomi host dei nodi e il nome FCI di Microsoft SQL vengono aggiunti come computer gestiti all'account del servizio Microsoft SQL.
- Alla voce del cluster di Windows vengono assegnate autorizzazioni per aggiungere computer al dominio.

Gruppi di protezione Active Directory gestiti dagli utenti

Se si seleziona "Active Directory gestita dall'utente" durante la distribuzione di Microsoft SQL Server in Workload Factory, è necessario fornire un gruppo di sicurezza che consenta il traffico tra le istanze EC2 e il servizio directory per la distribuzione. Workload Factory non associa automaticamente il gruppo di sicurezza per Active Directory gestito dall'utente come fa per AWS Managed Microsoft AD.

Rollback delle risorse

Se si decide di ripristinare le risorse DNS (Domain Name System), i record di risorse in ad e DNS non vengono rimossi automaticamente. È possibile rimuovere i record dal server DNS e da ad nel modo seguente.

- Per ad gestito dall'utente, prima "Rimuovere il computer ad". Quindi, connettersi al server DNS da Gestione DNS e "Eliminare i record di risorse DNS".
- Per AWS Managed Microsoft ad, "Installare gli strumenti di amministrazione di ad". Successivamente, "Rimuovere il computer ad". Infine, connettersi al server DNS dal gestore DNS e da "Eliminare i record di risorse DNS".

Prima di iniziare

Prima di creare un nuovo host di database, accertarsi di disporre dei seguenti prerequisiti.

Credenziali e autorizzazioni

Devi "concedere i permessi di creazione dell'host del database" nel tuo account AWS per creare un nuovo host di database in Workload Factory.

Active Directory

Quando ci si connette ad Active Directory, è necessario disporre dell'accesso amministrativo con autorizzazioni per effettuare le seguenti operazioni:

- Accedere al dominio
- Creare oggetti computer
- Creare oggetti nell'unità organizzativa predefinita
- Leggi tutte le proprietà
- Rendere l'utente di dominio un amministratore locale sui nodi ad
- Creare un utente del servizio Microsoft SQL Server nell'ad, se non esiste già

Passaggio 1: Creare un server di database

È possibile utilizzare le modalità di distribuzione *Creazione rapida* o *Creazione avanzata* per completare questa attività in Workload Factory con le autorizzazioni della modalità *Automatizza*. Puoi anche utilizzare i seguenti strumenti disponibili in Codebox: REST API, AWS CLI, AWS CloudFormation e Terraform. "Scopri come utilizzare Codebox per l'automazione" .

Quando si utilizza Terraform da Codebox, il codice che si copia o si scarica nasconde `fsxadmin` e `vsadmin` password. Sarà necessario immettere nuovamente le password quando si esegue il codice. È necessario includere le seguenti autorizzazioni per l'account utente oltre alle autorizzazioni in modalità *automatizza*: `iam:TagRole` E `iam:TagInstanceProfile`. "Scopri come utilizzare Terraform da Codebox".

Durante la distribuzione, Workload Factory abilita CredSSP per la delega delle credenziali agli script per il provisioning di SQL. Quando la delega CredSSP è bloccata per tutti i computer del dominio con i criteri di gruppo, la distribuzione fallisce. Dopo la distribuzione, Workload Factory disabilita CredSSP.

Creazione rapida

In *Quick create*, FCI è il modello di distribuzione predefinito, Windows 2016 è la versione predefinita di Windows e SQL 2019 Standard Edition è la versione predefinita di SQL.

Fasi

1. Accedere utilizzando uno dei "esperienze di console".
2. Nel riquadro Database, seleziona **Distribuisci host** e poi seleziona **Microsoft SQL Server** dal menu.
3. Selezionare **creazione rapida**.
4. In **Impostazioni AWS**, fornire quanto segue:
   a. **Credenziali AWS**: Selezionare le credenziali AWS con autorizzazioni automatiche per implementare il nuovo host del database.

      Le credenziali AWS con autorizzazioni di lettura/scrittura consentono a Workload Factory di distribuire e gestire il nuovo host del database dal tuo account AWS all'interno di Workload Factory.

      Le credenziali AWS con autorizzazioni di *sola lettura* consentono a Workload Factory di generare un modello CloudFormation da utilizzare nella console AWS CloudFormation.

      Se non hai credenziali AWS associate a Workload Factory e vuoi creare il nuovo server in Workload Factory, segui l'**Opzione 1** per andare alla pagina Credenziali. Aggiungere manualmente le credenziali e le autorizzazioni richieste per la modalità *lettura/scrittura* per i carichi di lavoro del database.

      Se desideri compilare il modulo di creazione di un nuovo server in Workload Factory per poter scaricare un modello di file YAML completo per la distribuzione in AWS CloudFormation, segui l'**Opzione 2** per assicurarti di disporre delle autorizzazioni necessarie per creare il nuovo server in AWS CloudFormation. Aggiungere manualmente le credenziali e le autorizzazioni richieste per la modalità *read* per i carichi di lavoro del database.

      Facoltativamente, puoi scaricare un modello di file YAML parzialmente completato da Codebox per creare lo stack al di fuori di Workload Factory senza credenziali o autorizzazioni. Selezionare **CloudFormation** dal menu a discesa nella Codebox per scaricare il file YAML.

   b. **Regione e VPC**: Selezionare una regione e una rete VPC.

      Assicurarsi che le subnet di distribuzione siano associate agli endpoint dell'interfaccia esistenti e che i gruppi di sicurezza consentano l'accesso al protocollo HTTPS (443) alle subnet selezionate.

      Endpoint dell'interfaccia del servizio AWS (SQS, FSX, EC2, CloudWatch, CloudFormation, SSM) e l'endpoint del gateway S3 vengono creati durante la distribuzione se non vengono trovati.

      Gli attributi DNS VPC `EnableDnsSupport` e `EnableDnsHostnames` sono stati modificati per abilitare la risoluzione degli indirizzi degli endpoint se non sono già impostati su `true`.

      Quando si utilizza un DNS cross-VPC, il gruppo di sicurezza per gli endpoint sull'altra VPC in cui risiede il DNS dovrebbe consentire la porta 443 per le subnet di distribuzione. In caso contrario, è necessario fornire un resolver DNS dalla VPC locale quando ci si unisce a un Active Directory cross-VPC. In un ambiente con più controller di dominio replicati, se alcuni controller di dominio non sono raggiungibili dalla subnet, è possibile **reindirizzare a CloudFormation** e immettere `Preferred domain controller` per connettersi ad Active Directory.

c. **Zone di disponibilità**: Selezionare zone di disponibilità e subnet in base al modello di distribuzione istanza cluster failover (FCI).

> Le implementazioni FCI sono supportate solo nelle configurazioni FSX for ONTAP con più zone di disponibilità (MAZ).

i. Nel campo **Configurazione cluster - nodo 1**, selezionare l'area di disponibilità primaria per la configurazione MAZ FSX per ONTAP dal menu a discesa **zona di disponibilità** e una subnet dall'area di disponibilità primaria dal menu a discesa **sottorete**.

ii. Nel campo **Configurazione cluster - nodo 2**, selezionare l'area di disponibilità secondaria per la configurazione MAZ FSX per ONTAP dal menu a discesa **zona di disponibilità** e una subnet dall'area di disponibilità secondaria dal menu a discesa **sottorete**.

5. In **Impostazioni applicazione**, immettere un nome utente e una password per **credenziali database**.
6. In **connettività**, fornire quanto segue:
   a. **Coppia di chiavi**: Selezionare una coppia di chiavi.
   b. **Active Directory**:
      i. Nel campo **Nome dominio**, selezionare o immettere un nome per il dominio.
         A. Per le Active Directory gestite da AWS, i nomi di dominio vengono visualizzati nel menu a discesa.
         B. Per un Active Directory gestito dall'utente, immettere un nome nel campo **Cerca e Aggiungi** e fare clic su **Aggiungi**.
      ii. Nel campo **indirizzo DNS**, immettere l'indirizzo IP DNS per il dominio. È possibile aggiungere fino a 3 indirizzi IP.

      Per le Active Directory gestite da AWS, gli indirizzi IP DNS vengono visualizzati nel menu a discesa.

      iii. Nel campo **Nome utente**, immettere il nome utente per il dominio Active Directory.
      iv. Nel campo **Password**, immettere una password per il dominio Active Directory.
7. In **Impostazioni infrastruttura**, fornire quanto segue:
   a. **FSX per ONTAP system**: Creare un nuovo file system FSX per ONTAP o utilizzare un file system FSX per ONTAP esistente.
      i. **Crea nuovo file FSX per ONTAP**: Inserisci nome utente e password.

      Un nuovo file system FSX per ONTAP può aggiungere 30 minuti o più di tempo di installazione.

      ii. **Selezionare un file FSX esistente per ONTAP**: Selezionare FSX per nome ONTAP dal menu a discesa e immettere un nome utente e una password per il file system.

      Per i file system FSX for ONTAP esistenti, verificare quanto segue:

      - Il gruppo di routing collegato a FSX per ONTAP consente di utilizzare i percorsi verso le sottoreti per la distribuzione.
      - Il gruppo di protezione consente il traffico proveniente dalle subnet utilizzate per la distribuzione, in particolare dalle porte TCP HTTPS (443) e iSCSI (3260).
   b. **Dimensione unità dati**: Immettere la capacità dell'unità dati e selezionare l'unità di capacità.

8. Riepilogo:
    a. **Anteprima predefinita**: Esaminare le configurazioni predefinite impostate da creazione rapida.
    b. **Costo stimato**: Fornisce una stima degli addebiti che potrebbero essere sostenuti se sono state distribuite le risorse visualizzate.
9. Fare clic su **Create** (Crea).

    In alternativa, se si desidera modificare subito una di queste impostazioni predefinite, creare il server database con creazione avanzata.

    È inoltre possibile selezionare **Salva configurazione** per distribuire l'host in un secondo momento.

Creazione avanzata

Fasi

1. Accedi utilizzando uno dei"esperienze di console" . Nel riquadro Database, seleziona **Distribuisci host** e poi seleziona **Microsoft SQL Server** dal menu.
2. Selezionare **creazione avanzata**.
3. Per **modello di distribuzione**, selezionare **istanza cluster di failover** o **istanza singola**.
4. In **Impostazioni AWS**, fornire quanto segue:
    a. **Credenziali AWS**: Selezionare le credenziali AWS con autorizzazioni automatiche per implementare il nuovo host del database.

        Le credenziali AWS con autorizzazioni di lettura/scrittura consentono a Workload Factory di distribuire e gestire il nuovo host del database dal tuo account AWS all'interno di Workload Factory.

        Le credenziali AWS con autorizzazioni di *sola lettura* consentono a Workload Factory di generare un modello CloudFormation da utilizzare nella console AWS CloudFormation.

        Se non hai credenziali AWS associate a Workload Factory e vuoi creare il nuovo server in Workload Factory, segui l'**Opzione 1** per andare alla pagina Credenziali. Aggiungere manualmente le credenziali e le autorizzazioni richieste per la modalità *lettura/scrittura* per i carichi di lavoro del database.

        Se desideri compilare il modulo di creazione di un nuovo server in Workload Factory per poter scaricare un modello di file YAML completo per la distribuzione in AWS CloudFormation, segui l'**Opzione 2** per assicurarti di disporre delle autorizzazioni necessarie per creare il nuovo server in AWS CloudFormation. Aggiungere manualmente le credenziali e le autorizzazioni richieste per la modalità di sola lettura per i carichi di lavoro del database.

        Facoltativamente, puoi scaricare un modello di file YAML parzialmente completato da Codebox per creare lo stack al di fuori di Workload Factory senza credenziali o autorizzazioni. Selezionare **CloudFormation** dal menu a discesa nella Codebox per scaricare il file YAML.

    b. **Regione e VPC**: Selezionare una regione e una rete VPC.

        Garantire che i gruppi di protezione per un endpoint dell'interfaccia esistente consentano l'accesso al protocollo HTTPS (443) alle subnet selezionate.

        Endpoint dell'interfaccia del servizio AWS (SQS, FSX, EC2, CloudWatch, Cloud Formation, SSM) e l'endpoint del gateway S3 vengono creati durante la distribuzione se non vengono trovati.

Gli attributi DNS del VPC `EnableDnsSupport` e `EnableDnsHostnames` sono stati modificati per abilitare la risoluzione degli indirizzi degli endpoint se non sono già impostati su `true`.

c. **Zone di disponibilità**: seleziona le zone di disponibilità e le subnet in base al modello di distribuzione selezionato. Per garantire un'elevata disponibilità, le subnet non devono condividere la stessa tabella di routing.

> Le implementazioni FCI sono supportate solo nelle configurazioni FSX for ONTAP con più zone di disponibilità (MAZ).

- Per distribuzioni a istanza singola:
  - Nel campo **Configurazione cluster - nodo 1**, selezionare una zona di disponibilità dal menu a discesa **zona di disponibilità** e una sottorete dal menu a discesa **sottorete**.
- Per le distribuzioni FCI:
  - Nel campo **Configurazione cluster - nodo 1**, selezionare l'area di disponibilità primaria per la configurazione MAZ FSX per ONTAP dal menu a discesa **zona di disponibilità** e una subnet dall'area di disponibilità primaria dal menu a discesa **sottorete**.
  - Nel campo **Configurazione cluster - nodo 2**, selezionare l'area di disponibilità secondaria per la configurazione MAZ FSX per ONTAP dal menu a discesa **zona di disponibilità** e una subnet dall'area di disponibilità secondaria dal menu a discesa **sottorete**.

d. **Gruppo di protezione**: Selezionare un gruppo di protezione esistente o creare un nuovo gruppo di protezione. Tre gruppi di protezione vengono collegati ai nodi SQL (istanze EC2) durante la distribuzione del nuovo server.

i. Viene creato un gruppo di protezione del carico di lavoro per consentire le porte e i protocolli necessari per la comunicazione dei cluster Microsoft SQL e Windows sui nodi.

ii. Nel caso di Active Directory gestito da AWS, il gruppo di protezione collegato al servizio directory viene aggiunto automaticamente ai nodi Microsoft SQL per consentire la comunicazione con Active Directory.

iii. Per un file system FSX for ONTAP esistente, il gruppo di sicurezza ad esso associato viene aggiunto automaticamente ai nodi SQL, consentendo così la comunicazione con il file system. Quando viene creato un nuovo sistema FSX per ONTAP, viene creato un nuovo gruppo di protezione per il file system FSX per ONTAP e lo stesso gruppo di protezione viene collegato anche ai nodi SQL.

Per un Active Directory gestito dall'utente, assicurarsi che il gruppo di protezione configurato sull'istanza ad consenta il traffico dalle subnet utilizzate per la distribuzione. Il gruppo di protezione deve consentire la comunicazione con i controller di dominio Active Directory dalle subnet in cui sono configurate le istanze EC2 per Microsoft SQL.

5. In **Impostazioni applicazione**, fornire quanto segue:

a. In **tipo di installazione di SQL Server**, selezionare **licenza inclusa AMI** o **utilizza AMI personalizzato**.

i. Se si seleziona **licenza inclusa AMI**, specificare quanto segue:

A. **Sistema operativo**: Selezionare **Windows server 2016**, **Windows server 2019** o **Windows server 2022**.

B. **Database Edition**: Selezionare **SQL Server Standard Edition** o **SQL Server Enterprise Edition**.

C. **Versione database**: Selezionare **SQL Server 2016**, **SQL Server 2019** o **SQL Server 2022**.

D. **SQL Server AMI**: Selezionare un'interfaccia AMI di SQL Server dal menu a discesa.

ii. Se si seleziona **Usa AMI personalizzato**, selezionare un AMI dal menu a discesa.

b. **Regole di confronto di SQL Server**: Selezionare un set di regole di confronto per il server.

> Se il gruppo di regole di confronto selezionato non è compatibile per l'installazione, si consiglia di selezionare la regole di confronto predefinita "SQL_Latin1_General_CP1_ci_AS".

c. **Nome database**: Immettere il nome del cluster di database.

d. **Credenziali database**: Immettere un nome utente e una password per un nuovo account di servizio o utilizzare le credenziali di account di servizio esistenti in Active Directory.

Facoltativo: selezionare **Utilizza account di servizio gestito** per l'account di servizio di SQL Server. Utilizzare questa opzione se l'ambiente utilizza MSA (Managed Service Account) o Group Managed Service Account (gMSA) in cui la gestione delle password è affidata ad Active Directory.

6. In **connettività**, fornire quanto segue:

a. **Coppia di chiavi**: Selezionare una coppia di chiavi per connettersi in modo sicuro all'istanza.

b. **Active Directory**: Fornire i seguenti dettagli di Active Directory:

i. Nel campo **Nome dominio**, selezionare o immettere un nome per il dominio.

A. Per le Active Directory gestite da AWS, i nomi di dominio vengono visualizzati nel menu a discesa.

B. Per un Active Directory gestito dall'utente, immettere un nome nel campo **Cerca e Aggiungi** e fare clic su **Aggiungi**.

ii. Nel campo **indirizzo DNS**, immettere l'indirizzo IP DNS per il dominio. È possibile aggiungere fino a 3 indirizzi IP.

Per le Active Directory gestite da AWS, gli indirizzi IP DNS vengono visualizzati nel menu a discesa.

iii. Nel campo **Nome utente**, immettere il nome utente per il dominio Active Directory.

iv. Nel campo **Password**, immettere una password per il dominio Active Directory.

v. **Controller di dominio preferito**: facoltativamente, immettere il controller di dominio preferito da utilizzare per l'aggiunta di Active Directory.

vi. **Percorso dell'unità organizzativa preferita**: facoltativamente, immettere l'unità organizzativa (OU) preferita in Active Directory a cui unirsi.

vii. **Gruppo Active Directory di destinazione**: facoltativamente, immettere il gruppo Active Directory di destinazione a cui aggiungere i computer.

7. In **Impostazioni infrastruttura**, fornire quanto segue:

a. **DB Instance type**: Selezionare il tipo di istanza del database dal menu a discesa.

b. **FSX per ONTAP system**: Creare un nuovo file system FSX per ONTAP o utilizzare un file system FSX per ONTAP esistente.

i. **Crea nuovo file FSX per ONTAP**: Inserisci nome utente e password.

Un nuovo file system FSX per ONTAP può aggiungere 30 minuti o più di tempo di installazione.

ii. **Selezionare un file FSX esistente per ONTAP**: Selezionare FSX per nome ONTAP dal menu a discesa e immettere un nome utente e una password per il file system.

Per i file system FSX for ONTAP esistenti, verificare quanto segue:

- Il gruppo di routing collegato a FSX per ONTAP consente di utilizzare i percorsi verso le sottoreti per la distribuzione.
- Il gruppo di protezione consente il traffico proveniente dalle subnet utilizzate per la distribuzione, in particolare dalle porte TCP HTTPS (443) e iSCSI (3260).

c. **Snapshot policy**: Attivato per impostazione predefinita. Le snapshot vengono acquisite giornalmente e hanno un periodo di conservazione di 7 giorni.

Le snapshot vengono assegnate ai volumi creati per i carichi di lavoro SQL.

d. **Dimensione unità dati**: Immettere la capacità dell'unità dati e selezionare l'unità di capacità.

e. **IOPS forniti**: Selezionare **automatico** o **fornito dall'utente**. Se si seleziona **provisioning utente**, immettere il valore IOPS.

f. **Capacità di throughput**: Selezionare la capacità di throughput dal menu a discesa.

In alcune regioni, è possibile selezionare una capacità di 4 Gbps di throughput. Per fornire una capacità di throughput di 4 Gbps, il file system FSX per ONTAP deve essere configurato con un minimo di 5.120 GiB di capacità di storage SSD e 160.000 IOPS SSD.

g. **Crittografia**: Selezionare una chiave dal proprio account o una chiave da un altro account. È necessario immettere la chiave di crittografia ARN da un altro account.

Le chiavi di crittografia personalizzate di FSX per ONTAP non sono elencate in base all'applicabilità del servizio. Selezionare una chiave di crittografia FSX appropriata. Le chiavi di crittografia non FSX causeranno un errore nella creazione del server.

Le chiavi gestite da AWS vengono filtrate in base all'applicabilità del servizio.

h. **Tags**: Opzionalmente, è possibile aggiungere fino a 40 tag.

i. **Simple Notification Service**: In alternativa, è possibile attivare Simple Notification Service (SNS) per questa configurazione selezionando un argomento SNS per Microsoft SQL Server dal menu a discesa.

i. Attivare il servizio di notifica semplice.

ii. Selezionare un ARN dal menu a discesa.

j. **Monitoraggio di CloudWatch**: Facoltativamente, è possibile attivare il monitoraggio di CloudWatch.

Si consiglia di abilitare CloudWatch per il debug in caso di errore. Gli eventi visualizzati nella console AWS CloudFormation sono di alto livello e non specificano la causa principale. Tutti i registri dettagliati vengono salvati nella `C:\cfn\logs` cartella nelle istanze EC2.

In CloudWatch, viene creato un gruppo di log con il nome dello stack. Un flusso di log per ogni nodo di convalida e nodo SQL viene visualizzato sotto il gruppo di log. CloudWatch mostra lo stato di avanzamento degli script e fornisce informazioni che aiutano a capire se e quando la distribuzione

non riesce.

a. **Rollback delle risorse**: Questa funzione non è attualmente supportata.

8. Riepilogo
   a. **Costo stimato**: Fornisce una stima degli addebiti che potrebbero essere sostenuti se sono state distribuite le risorse visualizzate.
9. Fare clic su **Crea** per distribuire il nuovo host del database.

   In alternativa, è possibile salvare la configurazione.

Passaggio 2: Abilitare la connessione remota su Microsoft SQL Server

Dopo la distribuzione del server, Workload Factory non abilita la connessione remota su Microsoft SQL Server. Per abilitare la connessione remota, completare i seguenti passaggi.

Fasi

1. Utilizzare l'identità del computer per NTLM facendo riferimento a "Protezione della rete: Consente al sistema locale di utilizzare l'identità del computer per NTLM" nella documentazione Microsoft.
2. Verificare la configurazione dinamica della porta facendo riferimento a "Si è verificato un errore relativo alla rete o specifico dell'istanza durante la connessione a SQL Server" nella documentazione Microsoft.
3. Consentire l'IP o la subnet client richiesti nel gruppo di protezione.

Cosa succederà

Ora puoi"creare un database in Workload Factory per i database" .

Creare un server PostgreSQL in NetApp Workload Factory

Per creare un nuovo server PostgreSQL o un host di database in NetApp Workload Factory for Databases è necessario un'implementazione del file system FSx for ONTAP e risorse per Active Directory.

A proposito di questa attività

Prima di creare un server PostgreSQL da Workload Factory, informati sui tipi di distribuzione dello storage disponibili per la configurazione dell'host del database, sulle modalità operative di Workload Factory e sui requisiti per completare questa operazione.

FSX per implementazioni di file system ONTAP

La creazione di un nuovo server PostgreSQL richiede un file system FSX per ONTAP come backend dello storage. Puoi usare un file system FSX for ONTAP esistente o creare un nuovo file system. Se selezioni un file system FSX per ONTAP esistente come back-end dello storage del database server, creiamo una nuova macchina virtuale di storage per i workload PostgreSQL.

+ I file system FSx per ONTAP hanno due modelli di distribuzione del server PostgreSQL: *Alta disponibilità (HA)* o *singola istanza*. A seconda del modello di distribuzione FSx for ONTAP selezionato, vengono create risorse diverse per il file system FSx for ONTAP .

- **Distribuzione ad alta disponibilità (ha)**: Viene implementato un file system FSX per NetApp ONTAP con più zone di disponibilità quando viene selezionato un nuovo file system FSX per ONTAP per la

distribuzione ha. Volumi e LUN separati vengono creati per i file di dati, log e tempdb per un'implementazione HA. Vengono creati un volume e un LUN aggiuntivi per Quorum o disco di controllo per il cluster Windows. L'installazione HA configura la replica Streaming tra i server PostgreSQL primario e secondario.

- **Distribuzione a istanza singola**: Quando viene creato un nuovo server PostgreSQL, viene creato un file system FSX per ONTAP. Inoltre, vengono creati volumi e LUN separati per i file di dati, log e tempdb.

Prima di iniziare

Devi avere "concedere i permessi di creazione dell'host del database" nel tuo account AWS per creare un nuovo host del database in Workload Factory.

Creare un server PostgreSQL

È possibile utilizzare le modalità di distribuzione *creazione rapida* o *creazione avanzata* per completare questa attività in fabbrica dei carichi di lavoro con autorizzazioni *automatizza*. Puoi anche utilizzare i seguenti tool disponibili in Codebox: API REST, interfaccia a riga di comando di AWS, AWS CloudFormation e Terraform. "Scopri come utilizzare Codebox per l'automazione".

> Quando si utilizza Terraform da Codebox, il codice che si copia o si scarica nasconde `fsxadmin` e `vsadmin` password. Sarà necessario immettere nuovamente le password quando si esegue il codice. È necessario includere le seguenti autorizzazioni per l'account utente oltre alle autorizzazioni in modalità *automatizza*: `iam:TagRole` E `iam:TagInstanceProfile`. "Scopri come utilizzare Terraform da Codebox".

Creazione rapida

In *Quick create*, HA è il modello di distribuzione predefinito, Windows 2016 è la versione predefinita di Windows e SQL 2019 Standard Edition è la versione predefinita di SQL.

Fasi

1. Accedere utilizzando uno dei "esperienze di console".
2. Nel riquadro Database, seleziona **Distribuisci host** e poi seleziona **PostgreSQL Server** dal menu.
3. Selezionare **creazione rapida**.
4. In **zona di atterraggio**, specificare quanto segue:
   a. **Credenziali AWS**: Selezionare le credenziali AWS con autorizzazioni automatiche per implementare il nuovo host del database.

      Le credenziali AWS con autorizzazioni di lettura/scrittura consentono a Workload Factory di distribuire e gestire il nuovo host del database dal tuo account AWS all'interno di Workload Factory.

      Le credenziali AWS con autorizzazioni di *sola lettura* consentono a Workload Factory di generare un modello CloudFormation da utilizzare nella console AWS CloudFormation.

      Se non disponi delle credenziali AWS associate alla fabbrica dei carichi di lavoro e desideri creare il nuovo server nella fabbrica dei carichi di lavoro, segui **opzione 1** per andare alla pagina credenziali. Aggiungere manualmente le credenziali e le autorizzazioni richieste per la modalità *lettura/scrittura* per i carichi di lavoro del database.

      Se si desidera completare il modulo di creazione di un nuovo server in fabbrica del carico di lavoro in modo da poter scaricare un modello di file YAML completo per la distribuzione in AWS CloudFormation, seguire **opzione 2** per assicurarsi di disporre delle autorizzazioni necessarie per creare il nuovo server in AWS CloudFormation. Aggiungere manualmente le credenziali e le autorizzazioni richieste per la modalità di *sola lettura* per i carichi di lavoro del database.

      In alternativa, è possibile scaricare un modello di file YAML parzialmente completato dalla Codebox per creare lo stack al di fuori della fabbrica del carico di lavoro senza credenziali o autorizzazioni. Selezionare **CloudFormation** dal menu a discesa nel Codebox per scaricare il file YAML.

   b. **Regione e VPC**: Selezionare una regione e una rete VPC.

      Garantire che i gruppi di protezione per un endpoint dell'interfaccia esistente consentano l'accesso al protocollo HTTPS (443) alle subnet selezionate.

      Endpoint dell'interfaccia del servizio AWS (SQS, FSX, EC2, CloudWatch, CloudFormation, SSM) e l'endpoint del gateway S3 vengono creati durante la distribuzione se non vengono trovati.

      Gli attributi DNS VPC `EnableDnsSupport` e `EnableDnsHostnames` sono stati modificati per abilitare la risoluzione degli indirizzi degli endpoint se non sono già impostati su `true`.

   c. **Zone di disponibilità**: Selezionare zone di disponibilità e subnet.

      Le implementazioni HA sono supportate solo nelle configurazioni FSX for ONTAP con più zone di disponibilità (MAZ).

Le sottoreti non devono condividere la stessa tabella di routing per la disponibilità elevata.

i. Nel campo **Configurazione cluster - nodo 1**, selezionare l'area di disponibilità primaria per la configurazione MAZ FSX per ONTAP dal menu a discesa **zona di disponibilità** e una subnet dall'area di disponibilità primaria dal menu a discesa **sottorete**.

ii. Nel campo **Configurazione cluster - nodo 2**, selezionare l'area di disponibilità secondaria per la configurazione MAZ FSX per ONTAP dal menu a discesa **zona di disponibilità** e una subnet dall'area di disponibilità secondaria dal menu a discesa **sottorete**.

5. In **Impostazioni applicazione**, immettere un nome utente e una password per **credenziali database**.
6. In **connettività**, selezionare una coppia di chiavi per connettersi in modo sicuro all'istanza.
7. In **Impostazioni infrastruttura**, fornire quanto segue:
   a. **FSX per ONTAP system**: Creare un nuovo file system FSX per ONTAP o utilizzare un file system FSX per ONTAP esistente.
      i. **Crea nuovo file FSX per ONTAP**: Inserisci nome utente e password.

      Un nuovo file system FSX per ONTAP può aggiungere 30 minuti o più di tempo di installazione.

      ii. **Selezionare un file FSX esistente per ONTAP**: Selezionare FSX per nome ONTAP dal menu a discesa e immettere un nome utente e una password per il file system.

      Per i file system FSX for ONTAP esistenti, verificare quanto segue:

      - Il gruppo di routing collegato a FSX per ONTAP consente di utilizzare i percorsi verso le sottoreti per la distribuzione.
      - Il gruppo di protezione consente il traffico proveniente dalle subnet utilizzate per la distribuzione, in particolare dalle porte TCP HTTPS (443) e iSCSI (3260).

   b. **Dimensione unità dati**: Immettere la capacità dell'unità dati e selezionare l'unità di capacità.
8. Riepilogo:
   a. **Anteprima predefinita**: Esaminare le configurazioni predefinite impostate da creazione rapida.
   b. **Costo stimato**: Fornisce una stima degli addebiti che potrebbero essere sostenuti se sono state distribuite le risorse visualizzate.
9. Fare clic su **Create** (Crea).

   In alternativa, se si desidera modificare subito una di queste impostazioni predefinite, creare il server database con creazione avanzata.

   È inoltre possibile selezionare **Salva configurazione** per distribuire l'host in un secondo momento.

Creazione avanzata

Fasi

1. Accedere utilizzando uno dei "esperienze di console".
2. Nel riquadro Database, seleziona **Distribuisci host** e poi seleziona **PostgreSQL Server** dal menu.
3. Selezionare **creazione avanzata**.
4. In **modello di distribuzione**, selezionare **istanza standalone** o **alta disponibilità (ha)**.
5. In **zona di atterraggio**, specificare quanto segue:

a. **Credenziali AWS**: Selezionare le credenziali AWS con autorizzazioni automatiche per implementare il nuovo host del database.

   Le credenziali AWS con autorizzazioni *automatizza* consentono al workload di implementare e gestire in fabbrica il nuovo host del database dal tuo account AWS all'interno di una fabbrica di carichi di lavoro.

   Le credenziali AWS con autorizzazioni di *sola lettura* consentono a Workload Factory di generare un modello CloudFormation da utilizzare nella console AWS CloudFormation.

   Se non disponi delle credenziali AWS associate alla fabbrica dei carichi di lavoro e desideri creare il nuovo server nella fabbrica dei carichi di lavoro, segui **opzione 1** per andare alla pagina credenziali. Aggiungere manualmente le credenziali e le autorizzazioni richieste per la modalità *lettura/scrittura* per i carichi di lavoro del database.

   Se si desidera completare il modulo di creazione di un nuovo server in fabbrica del carico di lavoro in modo da poter scaricare un modello di file YAML completo per la distribuzione in AWS CloudFormation, seguire **opzione 2** per assicurarsi di disporre delle autorizzazioni necessarie per creare il nuovo server in AWS CloudFormation. Aggiungere manualmente le credenziali e le autorizzazioni richieste per la modalità di *sola lettura* per i carichi di lavoro del database.

   In alternativa, è possibile scaricare un modello di file YAML parzialmente completato dalla Codebox per creare lo stack al di fuori della fabbrica del carico di lavoro senza credenziali o autorizzazioni. Selezionare **CloudFormation** dal menu a discesa nel Codebox per scaricare il file YAML.

b. **Regione e VPC**: Selezionare una regione e una rete VPC.

   Garantire che i gruppi di protezione per un endpoint dell'interfaccia esistente consentano l'accesso al protocollo HTTPS (443) alle subnet selezionate.

   Endpoint dell'interfaccia del servizio AWS (SQS, FSX, EC2, CloudWatch, Cloud Formation, SSM) e l'endpoint del gateway S3 vengono creati durante la distribuzione se non vengono trovati.

   Gli attributi DNS del VPC `EnableDnsSupport` e `EnableDnsHostnames` sono stati modificati per abilitare la risoluzione degli indirizzi degli endpoint se non sono già impostati su `true`.

c. **Zone di disponibilità**: Selezionare zone di disponibilità e subnet.

   Per distribuzioni di istanze singole

   Nel campo **Configurazione cluster - nodo 1**, selezionare una zona di disponibilità dal menu a discesa **zona di disponibilità** e una sottorete dal menu a discesa **sottorete**.

   Per distribuzioni HA

   i. Nel campo **Configurazione cluster - nodo 1**, selezionare l'area di disponibilità primaria per la configurazione MAZ FSX per ONTAP dal menu a discesa **zona di disponibilità** e una subnet dall'area di disponibilità primaria dal menu a discesa **sottorete**.

   ii. Nel campo **Configurazione cluster - nodo 2**, selezionare l'area di disponibilità secondaria per la configurazione MAZ FSX per ONTAP dal menu a discesa **zona di disponibilità** e una subnet dall'area di disponibilità secondaria dal menu a discesa **sottorete**.

d. **Gruppo di protezione**: Selezionare un gruppo di protezione esistente o creare un nuovo gruppo di protezione.

Due gruppi di protezione vengono collegati ai nodi SQL (istanze EC2) durante la distribuzione del nuovo server.

i. Viene creato un gruppo di protezione del carico di lavoro per consentire porte e protocolli richiesti per PostgreSQL.

ii. Per un nuovo file system FSX per ONTAP, viene creato un nuovo gruppo di protezione che viene allegato al nodo SQL. Per un file system FSX for ONTAP esistente, il gruppo di sicurezza ad esso associato viene aggiunto automaticamente al nodo PostgreSQL che consente la comunicazione con il file system.

6. In **Impostazioni applicazione**, fornire quanto segue:
   a. Selezionare **sistema operativo** dal menu a discesa.
   b. Selezionare **PostgreSQL versione** dal menu a discesa.
   c. **Nome server database**: Immettere il nome del cluster di database.
   d. **Credenziali database**: Immettere un nome utente e una password per un nuovo account di servizio o utilizzare le credenziali di account di servizio esistenti in Active Directory.
7. In **connettività**, selezionare una coppia di chiavi per connettersi in modo sicuro all'istanza.
8. In **Impostazioni infrastruttura**, fornire quanto segue:
   a. **DB Instance type**: Selezionare il tipo di istanza del database dal menu a discesa.
   b. **FSX per ONTAP system**: Creare un nuovo file system FSX per ONTAP o utilizzare un file system FSX per ONTAP esistente.
      i. **Crea nuovo file FSX per ONTAP**: Inserisci nome utente e password.

      Un nuovo file system FSX per ONTAP può aggiungere 30 minuti o più di tempo di installazione.

      ii. **Selezionare un file FSX esistente per ONTAP**: Selezionare FSX per nome ONTAP dal menu a discesa e immettere un nome utente e una password per il file system.

      Per i file system FSX for ONTAP esistenti, verificare quanto segue:

      - Il gruppo di routing collegato a FSX per ONTAP consente di utilizzare i percorsi verso le sottoreti per la distribuzione.
      - Il gruppo di protezione consente il traffico proveniente dalle subnet utilizzate per la distribuzione, in particolare dalle porte TCP HTTPS (443) e iSCSI (3260).

   c. **Snapshot policy**: Attivato per impostazione predefinita. Le snapshot vengono acquisite giornalmente e hanno un periodo di conservazione di 7 giorni.

      Gli snapshot vengono assegnati ai volumi creati per i carichi di lavoro PostgreSQL.

   d. **Dimensione unità dati**: Immettere la capacità dell'unità dati e selezionare l'unità di capacità.
   e. **IOPS forniti**: Selezionare **automatico** o **fornito dall'utente**. Se si seleziona **provisioning utente**, immettere il valore IOPS.
   f. **Capacità di throughput**: Selezionare la capacità di throughput dal menu a discesa.

      In alcune regioni, è possibile selezionare una capacità di 4 Gbps di throughput. Per fornire una capacità di throughput di 4 Gbps, il file system FSX per ONTAP deve essere configurato con un minimo di 5.120 GiB di capacità di storage SSD e 160.000 IOPS SSD.

g. **Crittografia**: Selezionare una chiave dal proprio account o una chiave da un altro account. È necessario immettere la chiave di crittografia ARN da un altro account.

   Le chiavi di crittografia personalizzate di FSX per ONTAP non sono elencate in base all'applicabilità del servizio. Selezionare una chiave di crittografia FSX appropriata. Le chiavi di crittografia non FSX causeranno un errore nella creazione del server.

   Le chiavi gestite da AWS vengono filtrate in base all'applicabilità del servizio.

h. **Tags**: Opzionalmente, è possibile aggiungere fino a 40 tag.

i. **Simple Notification Service**: In alternativa, è possibile attivare Simple Notification Service (SNS) per questa configurazione selezionando un argomento SNS per Microsoft SQL Server dal menu a discesa.

   i. Attivare il servizio di notifica semplice.

   ii. Selezionare un ARN dal menu a discesa.

j. **Monitoraggio di CloudWatch**: Facoltativamente, è possibile attivare il monitoraggio di CloudWatch.

   Si consiglia di abilitare CloudWatch per il debug in caso di errore. Gli eventi visualizzati nella console AWS CloudFormation sono di alto livello e non specificano la causa principale. Tutti i registri dettagliati vengono salvati nella `C:\cfn\logs` cartella nelle istanze EC2.

In CloudWatch, viene creato un gruppo di log con il nome dello stack. Un flusso di log per ogni nodo di convalida e nodo SQL viene visualizzato sotto il gruppo di log. CloudWatch mostra lo stato di avanzamento degli script e fornisce informazioni che aiutano a capire se e quando la distribuzione non riesce.

a. **Rollback delle risorse**: Questa funzione non è attualmente supportata.

9. Riepilogo

   a. **Costo stimato**: Fornisce una stima degli addebiti che potrebbero essere sostenuti se sono state distribuite le risorse visualizzate.

10. Fare clic su **Crea** per distribuire il nuovo host del database.

    In alternativa, è possibile salvare la configurazione.

Cosa succederà

È possibile configurare manualmente gli utenti, l'accesso remoto e i database sul server PostgreSQL distribuito.

Informazioni sul copyright

Informazioni sul marchio commerciale