



Crea risorse di database

Workload Factory for NetApp Console

NetApp
October 07, 2026

This PDF was generated from <https://docs.netapp.com/it-it/data-services-workloads/fsx-databases/create-sql-database-server.html> on October 07, 2026. Always check docs.netapp.com for the latest.

Sommario

- Crea risorse di database 1
 - Crea un Microsoft SQL Server in NetApp Workload Factory per database 1
 - Informazioni su questa attività 1
 - Prima di iniziare 2
 - Passaggio 1: Crea un database server 2
 - Passaggio 2: Abilita la connessione remota in Microsoft SQL Server 9
 - Crea un server PostgreSQL in NetApp Workload Factory per database 10
 - Informazioni su questa attività 10
 - Prima di iniziare 10
 - Crea un server PostgreSQL 10
 - Crea un database Microsoft SQL in NetApp Workload Factory for Databases 16
 - Crea un database 17
 - Crea un clone sandbox in NetApp Workload Factory for Databases 18

Crea risorse di database

Crea un Microsoft SQL Server in NetApp Workload Factory per database

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

Informazioni su questa attività

Prima di creare un Microsoft SQL Server con Workload Factory, scopri i tipi di deployment dello storage disponibili per la configurazione dell'host del database, la configurazione di Microsoft Multi-path I/O, il deployment di Active Directory, i dettagli di rete e i requisiti per completare questa operazione.

Dopo l'implementazione, dovrai [abilitare la connessione remota su Microsoft SQL Server](#).

Distribuzioni del file system FSx for ONTAP

Per creare un nuovo Microsoft SQL Server è necessario un file system FSx for ONTAP come backend di storage. Puoi usare un file system FSx for ONTAP esistente o creare un nuovo file system. Se selezioni un file system FSx for ONTAP esistente come backend di storage per il tuo database server, creiamo una nuova storage VM per i workload Microsoft SQL.

I file system FSx for ONTAP hanno due modelli di implementazione di Microsoft SQL Server: *Failover Cluster Instance (FCI)* o *Standalone*. Per il file system FSx for ONTAP vengono create risorse diverse a seconda del modello di implementazione FSx for ONTAP che selezioni.

- **Distribuzione Microsoft SQL con Failover Cluster Instance (FCI):** viene distribuito un file system FSx for NetApp ONTAP Multi-AZ quando per la distribuzione FCI selezioni un nuovo file system FSx for ONTAP. Per una distribuzione FCI, vengono creati volumi e LUN separati per i file di dati, i file di log e i file tempdb. Vengono inoltre creati un volume e un LUN aggiuntivi per il disco di quorum o witness per il cluster Windows.
- **Distribuzione standalone di Microsoft SQL:** quando crei un nuovo Microsoft SQL Server, viene creato un file system Amazon FSx for NetApp ONTAP a zona di disponibilità singola. Inoltre, vengono creati volumi e LUN separati per i file di dati, i file di log e i file tempdb.

Configurazione I/O multi-percorso di Microsoft

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

Per ulteriori informazioni, consulta ["Implementazioni ad alta disponibilità di SQL Server con Amazon FSx for NetApp ONTAP"](#).

Active Directory

Durante la distribuzione di Active Directory (AD) si verificano i seguenti eventi:

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

- 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 Windows vengono assegnate le autorizzazioni per aggiungere computer al dominio.

Gruppi di sicurezza di Active Directory gestiti dall'utente

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

Ripristino delle risorse

Se decidi di eseguire il rollback delle tue risorse Domain Name System (DNS), i record delle risorse in AD e DNS non vengono rimossi automaticamente. Puoi rimuovere i record dal DNS server e da AD come segue.

- Per AD gestito dall'utente, prima ["rimuovi il computer AD"](#). Quindi, connettiti al DNS server da DNS manager e ["eliminare i record di risorsa DNS"](#).
- Per AWS Managed Microsoft AD, ["installare gli strumenti di amministrazione AD"](#). Successivamente, ["rimuovi il computer AD"](#). Infine, connettiti al DNS server da DNS manager e ["eliminare i record di risorsa DNS"](#).

Prima di iniziare

Assicurati di soddisfare i seguenti prerequisiti prima di creare un nuovo host di database.

Credenziali e autorizzazioni

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

Active Directory

Quando ti connetti ad Active Directory, devi disporre dell'accesso amministrativo con le autorizzazioni per eseguire le seguenti operazioni:

- Unisci al dominio
- Crea oggetti computer
- Crea oggetti nell'unità organizzativa (OU) predefinita
- Leggi tutte le proprietà
- Rendi l'utente di dominio un amministratore locale sui nodi AD
- Crea un utente di servizio Microsoft SQL Server in AD, se non esiste già

Passaggio 1: Crea un database server

Per completare questa attività in Workload Factory con le autorizzazioni della modalità *Automate*, puoi utilizzare le modalità di distribuzione *Quick create* o *Advanced create*. Puoi anche utilizzare i seguenti strumenti disponibili in Codebox: REST API, AWS CLI, AWS CloudFormation e Terraform. ["Scopri come usare Codebox per l'automazione"](#).



Quando usi Terraform da Codebox, il codice che copi o scarichi nasconde `fsxadmin` e `vsadmin` password. Dovrai reinserire le password quando esegui il codice. Dovrai includere le seguenti autorizzazioni per l'account utente, oltre alle autorizzazioni della modalità *Automate*:

iam:TagRole e iam:TagInstanceProfile. ["Impara a usare Terraform da Codebox"](#).

Durante la distribuzione, Workload Factory abilita CredSSP per la delega delle credenziali agli script per il provisioning di SQL. Se la delega CredSSP è bloccata per tutti i computer del dominio tramite i criteri di gruppo, la distribuzione non riesce. Al termine della distribuzione, Workload Factory disabilita CredSSP.

Creazione rapida



In *Creazione rapida*, 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.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Database**.
3. Nella panoramica dei database, seleziona **Deploy host** e poi seleziona **Microsoft SQL Server** dal menu.
4. Seleziona **Creazione rapida**.
5. In **AWS settings**, inserisci quanto segue:

- a. **Credenziali AWS:** Seleziona le credenziali AWS con autorizzazioni per l'automazione per distribuire il nuovo host di database.

Le credenziali AWS con autorizzazioni per la *creazione del database host* consentono a Workload Factory di distribuire e gestire il nuovo database host dal tuo account AWS all'interno di Workload Factory.

Le credenziali AWS con autorizzazioni di visualizzazione, pianificazione e analisi consentono a Workload Factory di generare un modello CloudFormation da utilizzare nella console AWS CloudFormation.

Se non disponi di credenziali AWS associate in Workload Factory e vuoi creare il nuovo server in Workload Factory, segui **Option 1** per andare alla pagina Credentials. Aggiungi manualmente le credenziali richieste e le autorizzazioni *database host creation* per i carichi di lavoro database.

Se desideri completare il modulo per creare un nuovo server in Workload Factory in modo da poter scaricare un modello completo di file YAML per la distribuzione in AWS CloudFormation, segui **Opzione 2** per assicurarti di disporre delle autorizzazioni necessarie per creare il nuovo server in AWS CloudFormation. Aggiungi manualmente le credenziali richieste e le autorizzazioni di visualizzazione, pianificazione e analisi per i workload Database.

Facoltativamente, puoi scaricare da Codebox un modello di file YAML parzialmente compilato per creare lo stack al di fuori di Workload Factory senza credenziali o autorizzazioni. Seleziona **CloudFormation** dal menu a tendina in Codebox per scaricare il file YAML.

- b. **Regione & VPC:** Seleziona una regione e una rete VPC.

Assicurati che le sottoreti di deployment siano associate agli endpoint di interfaccia esistenti e che i gruppi di sicurezza consentano l'accesso al protocollo HTTPS (443) per le sottoreti selezionate.

Gli endpoint dell'interfaccia del servizio AWS (SQS, FSx, EC2, CloudWatch, CloudFormation,

SSM) e l'endpoint gateway S3 vengono creati durante la distribuzione se non sono già presenti.

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

Quando utilizzi un DNS cross-VPC, il gruppo di sicurezza per gli endpoint nell'altro VPC in cui risiede il DNS deve consentire la porta 443 alle subnet di distribuzione. In caso contrario, devi fornire un resolver DNS dal VPC locale quando ti connetti a un Active Directory cross-VPC. In un ambiente con più domain controller replicati, se alcuni domain controller non sono raggiungibili dalla subnet, puoi **Reindirizzare a CloudFormation** e inserire `Preferred domain controller` per connetterti ad Active Directory.

- c. **Availability zones:** Seleziona le zone di disponibilità e le subnet in base al modello di implementazione di Failover Cluster Instance (FCI).



Le implementazioni FCI sono supportate solo nelle configurazioni FSx for ONTAP Multiple Availability Zone (MAZ).

- i. Nel campo **Configurazione cluster - Nodo 1**, seleziona la zona di disponibilità primaria per la configurazione MAZ FSx for ONTAP dal menu a discesa **Zona di disponibilità** e una subnet della zona di disponibilità primaria dal menu a discesa **Subnet**.
 - ii. Nel campo **Configurazione cluster - Nodo 2**, seleziona la zona di disponibilità secondaria per la configurazione MAZ FSx for ONTAP dal menu a discesa **Zona di disponibilità** e una sottorete della zona di disponibilità secondaria dal menu a discesa **Sottorete**.
6. In **Application settings**, inserisci un nome utente e una password per le **credenziali del database**.

Per gli account GovCloud, immettere il valore per AWS SSM Parameter ARN nel seguente formato: `{fsx:{ "username": "fsxadmin", "password": "pass" }}`.

Il valore è fornito nel Parameter Store in Dettagli parametro nella console di gestione AWS. Il tipo di parametro AWS SSM deve essere "Secure String" con il nome nel formato `/netapp/wlmdb/<anyname>`. Scopri di più sul recupero dei parametri SSM da ["Documentazione AWS GovCloud"](#).

7. In **Connectivity**, fornisci quanto segue:

a. **Coppia di chiavi:** Seleziona una coppia di chiavi.

b. **Active Directory:**

- i. Nel campo **Nome di dominio**, seleziona o inserisci 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, inserisci un nome nel campo **Search and Add** e fai clic su **Add**.
- ii. Nel campo **indirizzo DNS**, inserisci l'indirizzo IP DNS del dominio. Puoi aggiungere fino a 3 indirizzi IP.

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

- iii. Nel campo **Nome utente**, inserisci il nome utente per il dominio Active Directory.
- iv. Nel campo **Password**, inserisci una password per il dominio di Active Directory.

Per gli account GovCloud, inserisci il valore ARN del parametro AWS SSM per le credenziali di Active Directory nel formato seguente:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Il tipo di parametro AWS SSM deve essere "Secure String" con il nome nel formato `/netapp/wlmdb/<anyname>`. Scopri di più sul recupero dei parametri SSM da ["Documentazione AWS GovCloud"](#).

8. In **Impostazioni infrastruttura**, inserisci quanto segue:

a. **Sistema FSx for ONTAP**: Crea un nuovo file system FSx for ONTAP o usa un file system FSx for ONTAP esistente.

i. **Crea un nuovo FSx per ONTAP**: Inserisci nome utente e password.

Per gli account GovCloud, inserire il valore ARN del parametro AWS SSM per le credenziali FSx for ONTAP nel seguente formato:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Il tipo di parametro AWS SSM deve essere "Secure String" con il nome nel formato `/netapp/wlmdb/<anyname>`. Scopri di più sul recupero dei parametri SSM da ["Documentazione AWS GovCloud"](#).

L'installazione di un nuovo file system FSx per ONTAP potrebbe richiedere 30 minuti o più.

i. **Seleziona un FSx per ONTAP esistente**: Seleziona il nome dell'FSx per ONTAP e inserisci un nome utente e una password per il file system.

Per i file system FSx for ONTAP esistenti, assicurati di quanto segue:

- Il gruppo di routing associato a FSx per ONTAP consente di utilizzare le rotte verso le sottoreti per l'implementazione.
- Il gruppo di sicurezza consente il traffico dalle sottoreti utilizzate per la distribuzione, in particolare sulle porte TCP HTTPS (443) e iSCSI (3260).

b. **Dimensioni dell'unità dati**: Inserisci la capacità dell'unità dati e seleziona l'unità di misura della capacità.

9. Riepilogo:

a. **Anteprima predefinita**: Controlla le configurazioni predefinite impostate da Quick create.

b. **Costo stimato**: Fornisce una stima dei costi che potresti sostenere se distribuissi le risorse mostrate.

10. Fai clic su **Create**.

In alternativa, se vuoi modificare una qualsiasi di queste impostazioni predefinite ora, crea il database server con Advanced create.

Puoi anche selezionare **Salva configurazione** per distribuire l'host più tardi.

Creazione avanzata

Passaggi

1. Accedi al ["NetApp Console"](#).

2. Seleziona il menu , **Carichi di lavoro > Database**.

3. Nella panoramica dei database, seleziona **Deploy host** e poi seleziona **Microsoft SQL Server** dal menu.

4. Seleziona **Creazione avanzata**.

5. Per **Deployment model**, seleziona **Failover Cluster Instance** o **Single instance**.

6. In **AWS settings**, inserisci quanto segue:

- a. **Credenziali AWS:** Seleziona le credenziali AWS con autorizzazioni per l'automazione per distribuire il nuovo host di database.

Le credenziali AWS con autorizzazioni per la *creazione del database host* consentono a Workload Factory di distribuire e gestire il nuovo database host dal tuo account AWS all'interno di Workload Factory.

Le credenziali AWS con autorizzazioni di visualizzazione, pianificazione e analisi consentono a Workload Factory di generare un modello CloudFormation da utilizzare nella console AWS CloudFormation.

Se non disponi di credenziali AWS associate in Workload Factory e vuoi creare il nuovo server in Workload Factory, segui **Option 1** per andare alla pagina Credentials. Aggiungi manualmente le credenziali richieste e le autorizzazioni *database host creation* per i carichi di lavoro database.

Se desideri completare il modulo per creare un nuovo server in Workload Factory in modo da poter scaricare un modello completo di file YAML per la distribuzione in AWS CloudFormation, segui **Opzione 2** per assicurarti di disporre delle autorizzazioni necessarie per creare il nuovo server in AWS CloudFormation. Aggiungi manualmente le credenziali richieste e le autorizzazioni di visualizzazione, pianificazione e analisi per i workload Database.

Facoltativamente, puoi scaricare da Codebox un modello di file YAML parzialmente compilato per creare lo stack al di fuori di Workload Factory senza credenziali o autorizzazioni. Seleziona **CloudFormation** dal menu a tendina in Codebox per scaricare il file YAML.

- b. **Regione & VPC:** Seleziona una regione e una rete VPC.

Assicurati che i gruppi di sicurezza per un endpoint di interfaccia esistente consentano l'accesso tramite protocollo HTTPS (443) alle sottoreti selezionate.

Gli 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` vengono modificati per consentire la risoluzione dell'indirizzo dell'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 implementazione che hai selezionato. Le subnet non devono condividere la stessa tabella di routing per garantire l'alta disponibilità.



Le implementazioni FCI sono supportate solo nelle configurazioni FSx for ONTAP Multiple Availability Zone (MAZ).

- Per le implementazioni a istanza singola:
 - Nel campo **Configurazione cluster - Nodo 1**, seleziona una zona di disponibilità dal menu a tendina **Zona di disponibilità** e una subnet dal menu a tendina **Subnet**.
- Per le implementazioni FCI:
 - Nel campo **Configurazione cluster - Nodo 1**, seleziona la zona di disponibilità primaria per la configurazione MAZ FSx for ONTAP dal menu a discesa **Zona di disponibilità** e una subnet della zona di disponibilità primaria dal menu a discesa **Subnet**.

- Nel campo **Configurazione cluster - Nodo 2**, seleziona la zona di disponibilità secondaria per la configurazione MAZ FSx for ONTAP dal menu a discesa **Zona di disponibilità** e una sottorete della zona di disponibilità secondaria dal menu a discesa **Sottorete**.

d. **Gruppo di sicurezza:** viene creato un gruppo di sicurezza del carico di lavoro per consentire le porte e i protocolli necessari per la comunicazione tra Microsoft SQL e cluster Windows sui nodi. Inoltre, è possibile selezionare uno o più gruppi di sicurezza.

7. In **Impostazioni dell'applicazione**, inserisci quanto segue:

a. In **Tipo di installazione di SQL Server**, seleziona **License included AMI** o **Use custom AMI**.

i. Se selezioni **License included AMI**, fornisci quanto segue:

- A. **Sistema operativo:** Seleziona **Windows server 2016**, **Windows server 2019** o **Windows server 2022**.
- B. **Edizione del database:** Seleziona **SQL Server Standard Edition** o **SQL Server Enterprise Edition**.
- C. **Versione del database:** Seleziona **SQL Server 2016**, **SQL Server 2019** o **SQL Server 2022**.
- D. **SQL Server AMI:** Seleziona una SQL Server AMI dal menu a discesa.

ii. Se selezioni **Use custom AMI**, seleziona un'AMI dal menu a discesa.

b. **Set di regole di confronto di SQL Server:** Seleziona un set di regole di confronto per il server.



Se il set di regole di confronto selezionato non è compatibile con l'installazione, ti consigliamo di selezionare il set di regole di confronto predefinito "SQL_Latin1_General_CP1_CI_AS".

c. **Nome del database:** Inserisci il nome del cluster del database.

d. **Credenziali del database:** immetti un nome utente e una password per un nuovo account di servizio oppure utilizza le credenziali di un account di servizio esistente in Active Directory.

Facoltativo: seleziona **Use managed service account** per l'account di servizio di SQL Server. Usa questa opzione se il tuo ambiente utilizza MSA (Managed Service Account) o Group Managed Service Accounts (gMSA), in cui la gestione delle password è affidata ad Active Directory.

Per gli account GovCloud, immettere il valore per AWS SSM Parameter ARN nel seguente formato: `{fsx:{"username":"fsxadmin","password":"pass"}}`.

Il valore è fornito nel Parameter Store in Dettagli parametro nella console di gestione AWS. Il tipo di parametro AWS SSM deve essere "Secure String" con il nome nel formato `/netapp/wlmdb/<anyname>`. Scopri di più sul recupero dei parametri SSM da ["Documentazione AWS GovCloud"](#).

8. In **Connectivity**, fornisci quanto segue:

a. **Coppia di chiavi:** Seleziona una coppia di chiavi per connetterti in modo sicuro alla tua istanza.

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

i. Nel campo **Nome di dominio**, seleziona o inserisci 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, inserisci un nome nel campo **Search and Add** e fai clic su **Add**.

- ii. Nel campo **indirizzo DNS**, inserisci l'indirizzo IP DNS del dominio. Puoi aggiungere fino a 3 indirizzi IP.

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

- iii. Inserisci il nome utente e la password per il dominio Active Directory.

Per gli account GovCloud, inserisci il valore ARN del parametro AWS SSM per le credenziali di Active Directory nel formato seguente:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Il tipo di parametro AWS SSM deve essere "Secure String" con il nome nel formato `/netapp/wlmdb/<anyname>`. Scopri di più sul recupero dei parametri SSM da ["Documentazione AWS GovCloud"](#).

- iv. **Domain controller preferito**: Facoltativamente, immetti il domain controller preferito da usare per l'adesione ad Active Directory.
- v. **Percorso dell'unità organizzativa preferita**: Facoltativamente, inserisci l'unità organizzativa (OU) preferita in Active Directory a cui unirti.
- vi. **Gruppo Active Directory di destinazione**: Facoltativamente, inserisci il gruppo Active Directory di destinazione a cui aggiungere i computer.

9. In **Impostazioni infrastruttura**, inserisci quanto segue:

- a. **Tipo di istanza DB**: Seleziona il tipo di istanza del database dal menu a tendina.
- b. **Sistema FSx for ONTAP**: Crea un nuovo file system FSx for ONTAP o usa un file system FSx for ONTAP esistente.
 - i. **Crea un nuovo FSx per ONTAP**: Inserisci nome utente e password.

Per gli account GovCloud, immettere il valore ARN del parametro AWS SSM per le credenziali FSx for ONTAP nel seguente formato:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Il tipo di parametro AWS SSM deve essere "Secure String" con il nome nel formato `/netapp/wlmdb/<anyname>`. Scopri di più sul recupero dei parametri SSM da ["Documentazione AWS GovCloud"](#).

L'installazione di un nuovo file system FSx per ONTAP potrebbe richiedere 30 minuti o più.

- ii. **Seleziona un FSx for ONTAP esistente**: Seleziona il nome di FSx for ONTAP dal menu a tendina e immetti un nome utente e una password per il file system.

Per i file system FSx for ONTAP esistenti, assicurati di quanto segue:

- Il gruppo di routing associato a FSx per ONTAP consente di utilizzare le rotte verso le sottoreti per l'implementazione.
 - Il gruppo di sicurezza consente il traffico dalle sottoreti utilizzate per la distribuzione, in particolare sulle porte TCP HTTPS (443) e iSCSI (3260).
- c. **policy di Snapshot**: Attivata per impostazione predefinita. Gli Snapshot vengono acquisiti quotidianamente e hanno un periodo di conservazione di 7 giorni.

Gli snapshot sono assegnati ai volumi creati per i workload SQL.

- d. **Dimensioni dell'unità dati:** Inserisci la capacità dell'unità dati e seleziona l'unità di misura della capacità.
- e. **IOPS allocati:** Seleziona **Automatico** o **Allocato dall'utente**. Se selezioni **Allocato dall'utente**, inserisci il valore IOPS.
- f. **Capacità di throughput:** Seleziona la capacità di throughput dal menu a tendina.

In alcune regioni, puoi selezionare una capacità di throughput di 4 GBps. Per eseguire il provisioning di una capacità di throughput di 4 GBps, il tuo FSx for ONTAP file system deve essere configurato con una capacità minima di storage SSD di 5.120 GiB e 160.000 IOPS SSD.

- g. **Crittografia:** Seleziona una chiave dal tuo account o una chiave da un altro account. Devi inserire l'ARN della chiave di crittografia da un altro account.

Le chiavi di crittografia personalizzate di FSx for ONTAP non sono elencate in base all'applicabilità del servizio. Seleziona una chiave di crittografia FSx appropriata. Le chiavi di crittografia non FSx causeranno un errore durante la creazione del server.

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

- h. **Tag:** Facoltativamente, puoi aggiungere fino a 40 tag.
- i. **Simple Notification Service:** Facoltativamente, puoi abilitare il Simple Notification Service (SNS) per questa configurazione selezionando un topic SNS per Microsoft SQL Server dal menu a discesa.
 - i. Attiva il Simple Notification Service.
 - ii. Seleziona un ARN dal menu a tendina.
- j. **Monitoraggio CloudWatch:** Facoltativamente, puoi abilitare il monitoraggio CloudWatch.

Ti consigliamo di abilitare CloudWatch per il debug in caso di errore. Gli eventi che compaiono nella console AWS CloudFormation sono high-level e non specificano la causa principale. Tutti i log dettagliati vengono salvati nella `C:\cfn\logs` cartella nelle istanze EC2.

In CloudWatch, viene creato un gruppo di log con il nome dello stack. Sotto il gruppo di log appaiono un flusso di log per ogni nodo di convalida e nodo SQL. CloudWatch mostra l'avanzamento dello script e fornisce informazioni per aiutarti a capire se e quando la distribuzione non riesce.

- a. **Ripristino delle risorse:** questa funzionalità non è attualmente supportata.

10. Riepilogo

- a. **Costo stimato:** Fornisce una stima dei costi che potresti sostenere se distribuissi le risorse mostrate.

11. Fai clic su **Create** per distribuire il nuovo database host.

In alternativa, puoi salvare la configurazione.

Passaggio 2: Abilita la connessione remota in Microsoft SQL Server

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

Passaggi

1. Usa l'identità del computer per NTLM facendo riferimento a ["Sicurezza di rete: Consenti al sistema locale di utilizzare l'identità del computer per NTLM"](#) nella documentazione Microsoft.
2. Verifica la configurazione dinamica delle porte facendo riferimento a ["Si è verificato un errore relativo alla rete o specifico dell'istanza durante la creazione di una connessione a SQL Server"](#) nella documentazione Microsoft.
3. Consenti l'indirizzo IP o la subnet del client richiesti nel gruppo di sicurezza.

Cosa c'è dopo

Ora puoi ["crea un database in Workload Factory for Databases"](#).

Crea un server PostgreSQL in NetApp Workload Factory per database

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

Informazioni su questa attività

Prima di creare un server PostgreSQL da Workload Factory, scopri i tipi di deployment dello storage disponibili per la configurazione dell'host del database, le modalità operative di Workload Factory e i requisiti necessari per completare questa operazione.

Distribuzioni del file system FSx for ONTAP

Per creare un nuovo server PostgreSQL, ti serve un file system FSx for ONTAP come backend di storage. Puoi usare un file system FSx for ONTAP esistente oppure crearne uno nuovo. Se selezioni un file system FSx for ONTAP esistente come backend di storage del tuo database server, creiamo una nuova storage VM per i carichi di lavoro PostgreSQL.

I file system FSx for ONTAP hanno due modelli di distribuzione del server PostgreSQL: *High Availability (HA)* o *single instance*. A seconda del modello di distribuzione FSx for ONTAP che selezioni, vengono create risorse diverse per il file system FSx for ONTAP.

- **Implementazione ad alta disponibilità (HA):** viene implementato un file system FSx for NetApp ONTAP Multi-AZ quando selezioni un nuovo file system FSx for ONTAP per l'implementazione HA. Per un'implementazione HA, vengono creati volumi e LUN separati per i file di dati, log e tempdb. Vengono creati un volume e un LUN aggiuntivi per il disco di quorum o witness per il cluster Windows. L'implementazione HA configura la replica in streaming tra i server PostgreSQL primario e secondario.
- **Implementazione a istanza singola:** quando viene creato un nuovo server PostgreSQL, viene creato un file system FSx for ONTAP a zona di disponibilità singola. Inoltre, vengono creati volumi e LUN separati per i file di dati, di log e tempdb.

Prima di iniziare

Devi avere ["concedere i permessi per la creazione dell'host del database"](#) nel tuo account AWS per creare un nuovo host di database in workload factory.

Crea un server PostgreSQL

Per completare questa attività in workload factory con le autorizzazioni della modalità *Automate*, puoi usare le

modalità di distribuzione *Quick create* o *Advanced create*. Puoi anche usare i seguenti strumenti disponibili in Codebox: REST API, AWS CLI, AWS CloudFormation e Terraform. ["Scopri come usare Codebox per l'automazione"](#).



Quando usi Terraform da Codebox, il codice che copi o scarichi nasconde `fsxadmin` e `vsadmin` password. Dovrai reinserire le password quando esegui il codice. Dovrai includere le seguenti autorizzazioni per l'account utente oltre alle autorizzazioni della modalità *Automate*: `iam:TagRole` e `iam:TagInstanceProfile`. ["Impara a usare 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.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Database**.
3. Dalla sezione Panoramica dei database, seleziona **Distribuisci host** e quindi **Server PostgreSQL** dal menu.
4. Seleziona **Creazione rapida**.
5. In **Landing zone**, inserisci quanto segue:

- a. **Credenziali AWS:** Seleziona le credenziali AWS con autorizzazioni per l'automazione per distribuire il nuovo host di database.

Le credenziali AWS con autorizzazioni per la *creazione del database host* consentono a Workload Factory di distribuire e gestire il nuovo database host dal tuo account AWS all'interno di Workload Factory.

Le credenziali AWS con autorizzazioni di visualizzazione, pianificazione e analisi consentono a Workload Factory di generare un modello CloudFormation da utilizzare nella console AWS CloudFormation.

Se non disponi di credenziali AWS associate in Workload Factory e vuoi creare il nuovo server in Workload Factory, segui **Option 1** per andare alla pagina Credentials. Aggiungi manualmente le credenziali richieste e le autorizzazioni *database host creation* per i carichi di lavoro database.

Se desideri completare il modulo per creare un nuovo server in Workload Factory in modo da poter scaricare un modello completo di file YAML per la distribuzione in AWS CloudFormation, segui **Opzione 2** per assicurarti di disporre delle autorizzazioni necessarie per creare il nuovo server in AWS CloudFormation. Aggiungi manualmente le credenziali richieste e le autorizzazioni di visualizzazione, pianificazione e analisi per i workload Database.

Facoltativamente, puoi scaricare da Codebox un modello di file YAML parzialmente compilato per creare lo stack al di fuori di Workload Factory senza credenziali o autorizzazioni. Seleziona **CloudFormation** dal menu a tendina in Codebox per scaricare il file YAML.

- b. **Regione & VPC:** Seleziona una regione e una rete VPC.

Assicurati che i gruppi di sicurezza per un endpoint di interfaccia esistente consentano l'accesso tramite protocollo HTTPS (443) alle sottoreti selezionate.

Gli endpoint dell'interfaccia del servizio AWS (SQS, FSx, EC2, CloudWatch, CloudFormation, SSM) e l'endpoint gateway S3 vengono creati durante la distribuzione se non sono già presenti.

Gli attributi DNS VPC `EnableDnsSupport` e `EnableDnsHostnames` vengono 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 sottoreti.



Le implementazioni HA sono supportate solo nelle configurazioni FSx for ONTAP con Multiple Availability Zone (MAZ).

Per garantire l'alta disponibilità, le sottoreti non dovrebbero condividere la stessa tabella di routing.

- i. Nel campo **Configurazione cluster - Nodo 1**, seleziona la zona di disponibilità primaria per la configurazione MAZ FSx for ONTAP dal menu a discesa **Zona di disponibilità** e una subnet della zona di disponibilità primaria dal menu a discesa **Subnet**.
 - ii. Nel campo **Configurazione cluster - Nodo 2**, seleziona la zona di disponibilità secondaria per la configurazione MAZ FSx for ONTAP dal menu a discesa **Zona di disponibilità** e una sottorete della zona di disponibilità secondaria dal menu a discesa **Sottorete**.
6. In **Application settings**, inserisci un nome utente e una password per le **credenziali del database**.
7. Nella sezione **Connettività**, seleziona una coppia di chiavi per connetterti in modo sicuro alla tua istanza.
8. In **Impostazioni infrastruttura**, inserisci quanto segue:
- a. **Sistema FSx for ONTAP:** Crea un nuovo file system FSx for ONTAP o usa un file system FSx for ONTAP esistente.
 - i. **Crea un nuovo FSx per ONTAP:** Inserisci nome utente e password.

Per gli account GovCloud, inserire il valore ARN del parametro AWS SSM per le credenziali FSx for ONTAP nel seguente formato:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Il tipo di parametro AWS SSM deve essere "Secure String" con il nome nel formato `/netapp/wlmdb/<anyname>`. Scopri di più sul recupero dei parametri SSM da "[Documentazione AWS GovCloud](#)".

L'installazione di un nuovo file system FSx per ONTAP potrebbe richiedere 30 minuti o più.

- i. **Seleziona un FSx for ONTAP esistente:** Seleziona il nome di FSx for ONTAP dal menu a tendina e immetti un nome utente e una password per il file system.

Per i file system FSx for ONTAP esistenti, assicurati di quanto segue:

- Il gruppo di routing associato a FSx per ONTAP consente di utilizzare le rotte verso le sottoreti per l'implementazione.
- Il gruppo di sicurezza consente il traffico dalle sottoreti utilizzate per la distribuzione, in particolare sulle porte TCP HTTPS (443) e iSCSI (3260).

- b. **Dimensioni dell'unità dati:** Inserisci la capacità dell'unità dati e seleziona l'unità di misura della capacità.

9. Riepilogo:

- a. **Anteprima predefinita:** Controlla le configurazioni predefinite impostate da Quick create.

- b. **Costo stimato:** Fornisce una stima dei costi che potresti sostenere se distribuissi le risorse mostrate.

10. Fai clic su **Create**.

In alternativa, se vuoi modificare una qualsiasi di queste impostazioni predefinite ora, crea il database server con Advanced create.

Puoi anche selezionare **Salva configurazione** per distribuire l'host più tardi.

Creazione avanzata

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Database**.
3. Dalla sezione Panoramica dei database, seleziona **Distribuisci host** e quindi **Server PostgreSQL** dal menu.
4. Seleziona **Creazione avanzata**.
5. In **Modello di distribuzione**, seleziona **Istanza standalone** o **Alta disponibilità (HA)**.
6. In **Landing zone**, inserisci quanto segue:

- a. **Credenziali AWS:** Seleziona le credenziali AWS con autorizzazioni per l'automazione per distribuire il nuovo host di database.

Le credenziali AWS con autorizzazioni per la *creazione del database host* consentono a Workload Factory di distribuire e gestire il nuovo database host dal tuo account AWS all'interno di Workload Factory.

Le credenziali AWS con autorizzazioni di visualizzazione, pianificazione e analisi consentono a Workload Factory di generare un modello CloudFormation da utilizzare nella console AWS CloudFormation.

Se non disponi di credenziali AWS associate in Workload Factory e vuoi creare il nuovo server in Workload Factory, segui **Option 1** per andare alla pagina Credentials. Aggiungi manualmente le credenziali richieste e le autorizzazioni *database host creation* per i carichi di lavoro database.

Se desideri completare il modulo per creare un nuovo server in Workload Factory in modo da poter scaricare un modello completo di file YAML per la distribuzione in AWS CloudFormation, segui **Opzione 2** per assicurarti di disporre delle autorizzazioni necessarie per creare il nuovo server in AWS CloudFormation. Aggiungi manualmente le credenziali richieste e le autorizzazioni di visualizzazione, pianificazione e analisi per i workload Database.

Facoltativamente, puoi scaricare da Codebox un modello di file YAML parzialmente compilato per creare lo stack al di fuori di Workload Factory senza credenziali o autorizzazioni. Seleziona **CloudFormation** dal menu a tendina in Codebox per scaricare il file YAML.

- b. **Regione & VPC:** Seleziona una regione e una rete VPC.

Assicurati che i gruppi di sicurezza per un endpoint di interfaccia esistente consentano l'accesso tramite protocollo HTTPS (443) alle sottoreti selezionate.

Gli 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` vengono modificati per consentire la risoluzione dell'indirizzo dell'endpoint se non sono già impostati su `true`.

- c. **Zone di disponibilità:** Seleziona le zone di disponibilità e le sottoreti.

Per implementazioni a istanza singola

Nel campo **Configurazione cluster - Nodo 1**, seleziona una zona di disponibilità dal menu a discesa **Zona di disponibilità** e una subnet dal menu a discesa **Subnet**.

Per implementazioni HA

- i. Nel campo **Configurazione cluster - Nodo 1**, seleziona la zona di disponibilità primaria per la configurazione MAZ FSx for ONTAP dal menu a discesa **Zona di disponibilità** e una subnet della zona di disponibilità primaria dal menu a discesa **Subnet**.
 - ii. Nel campo **Configurazione cluster - Nodo 2**, seleziona la zona di disponibilità secondaria per la configurazione MAZ FSx for ONTAP dal menu a discesa **Zona di disponibilità** e una sottorete della zona di disponibilità secondaria dal menu a discesa **Sottorete**.
- d. **Gruppo di sicurezza:** viene creato un gruppo di sicurezza del carico di lavoro per consentire le porte e i protocolli necessari per PostgreSQL. Inoltre, è possibile selezionare uno o più gruppi di sicurezza.
7. In **Impostazioni dell'applicazione**, inserisci quanto segue:
- a. Seleziona il **sistema operativo** dal menu a tendina.
 - b. Seleziona la **versione di PostgreSQL** dal menu a tendina.
 - c. **Nome del database server:** Inserisci il nome del cluster del database.
 - d. **Credenziali del database:** immetti un nome utente e una password per un nuovo account di servizio oppure utilizza le credenziali di un account di servizio esistente in Active Directory.

Per gli account GovCloud, inserisci il valore ARN del parametro AWS SSM per le credenziali nel seguente formato: `{fsx:{"username":"fsxadmin","password":"pass"}}`. Il tipo di parametro AWS SSM deve essere "Secure String" con il nome nel formato `/netapp/wlmdb/<anyname>`. Scopri di più sul recupero dei parametri SSM da ["Documentazione AWS GovCloud"](#).

8. Nella sezione **Connettività**, seleziona una coppia di chiavi per connetterti in modo sicuro alla tua istanza.

9. In **Impostazioni infrastruttura**, inserisci quanto segue:

- a. **Tipo di istanza DB:** Seleziona il tipo di istanza del database dal menu a tendina.
- b. **Sistema FSx for ONTAP:** Crea un nuovo file system FSx for ONTAP o usa un file system FSx for ONTAP esistente.
 - i. **Crea un nuovo FSx per ONTAP:** Inserisci nome utente e password.

Per gli account GovCloud, immettere il valore ARN del parametro AWS SSM per le credenziali FSx for ONTAP nel seguente formato:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Il tipo di parametro AWS SSM deve essere "Secure String" con il nome nel formato `/netapp/wlmdb/<anyname>`. Scopri di più sul recupero dei parametri SSM da ["Documentazione AWS GovCloud"](#).

L'installazione di un nuovo file system FSx per ONTAP potrebbe richiedere 30 minuti o più.

- ii. **Seleziona un FSx for ONTAP esistente:** Seleziona il nome di FSx for ONTAP dal menu a tendina e immetti un nome utente e una password per il file system.

Per i file system FSx for ONTAP esistenti, assicurati di quanto segue:

- Il gruppo di routing associato a FSx per ONTAP consente di utilizzare le rotte verso le sottoreti per l'implementazione.
- Il gruppo di sicurezza consente il traffico dalle sottoreti utilizzate per la distribuzione, in particolare sulle porte TCP HTTPS (443) e iSCSI (3260).

- c. **policy di Snapshot:** Attivata per impostazione predefinita. Gli Snapshot vengono acquisiti quotidianamente e hanno un periodo di conservazione di 7 giorni.

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

- d. **Dimensioni dell'unità dati:** Inserisci la capacità dell'unità dati e seleziona l'unità di misura della capacità.

- e. **IOPS allocati:** Seleziona **Automatico** o **Allocato dall'utente**. Se selezioni **Allocato dall'utente**, inserisci il valore IOPS.

- f. **Capacità di throughput:** Seleziona la capacità di throughput dal menu a tendina.

In alcune regioni, puoi selezionare una capacità di throughput di 4 GBps. Per eseguire il provisioning di una capacità di throughput di 4 GBps, il tuo FSx for ONTAP file system deve essere configurato con una capacità minima di storage SSD di 5.120 GiB e 160.000 IOPS SSD.

- g. **Crittografia:** Seleziona una chiave dal tuo account o una chiave da un altro account. Devi inserire l'ARN della chiave di crittografia da un altro account.

Le chiavi di crittografia personalizzate di FSx for ONTAP non sono elencate in base all'applicabilità del servizio. Seleziona una chiave di crittografia FSx appropriata. Le chiavi di crittografia non FSx causeranno un errore durante la creazione del server.

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

- h. **Tag:** Facoltativamente, puoi aggiungere fino a 40 tag.

- i. **Servizio di notifica semplice:** Facoltativamente, è possibile abilitare il Servizio di notifica semplice (SNS) per questa configurazione selezionando un argomento SNS per PostgreSQL dal menu a tendina.

i. Attiva il Simple Notification Service.

ii. Seleziona un ARN dal menu a tendina.

- j. **Monitoraggio CloudWatch:** Facoltativamente, puoi abilitare il monitoraggio CloudWatch.

Ti consigliamo di abilitare CloudWatch per il debug in caso di errore. Gli eventi che compaiono nella console AWS CloudFormation sono high-level e non specificano la causa principale. Tutti i log dettagliati vengono salvati nella `C:\cfn\logs` cartella nelle istanze EC2.

In CloudWatch, viene creato un gruppo di log con il nome dello stack. Sotto il gruppo di log appaiono un flusso di log per ogni nodo di convalida e nodo SQL. CloudWatch mostra l'avanzamento dello script e fornisce informazioni per aiutarti a capire se e quando la distribuzione non riesce.

- a. **Ripristino delle risorse:** questa funzionalità non è attualmente supportata.

10. Riepilogo

a. **Costo stimato:** Fornisce una stima dei costi che potresti sostenere se distribuissi le risorse mostrate.

11. Fai clic su **Create** per distribuire il nuovo database host.

In alternativa, puoi salvare la configurazione.

Cosa c'è dopo

Puoi configurare manualmente utenti, accesso remoto e database sul server PostgreSQL distribuito.

Crea un database Microsoft SQL in NetApp Workload Factory for Databases

La creazione di un nuovo database Microsoft SQL ti consente di gestire la risorsa all'interno di NetApp Workload Factory for Databases.

Informazioni su questa attività

Al momento della creazione del database, nel file system FSx for ONTAP vengono creati due nuovi volumi costituiti da LUN indipendenti per ospitare i file di dati e i file di log del database. I file del database nel nuovo database sono con thin provisioning e consumano solo pochi MB della dimensione totale allocata per il nuovo database.

Se vuoi separare lo storage per il database, puoi farlo usando un *punto di montaggio virtuale*. Il punto di montaggio virtuale ti consente di consolidare i database su alcune unità comuni sull'host.

La creazione di un database in workload factory richiede le autorizzazioni di visualizzazione, pianificazione e analisi. In alternativa, puoi copiare o scaricare un modello di codice parzialmente completato per completare l'operazione al di fuori di workload factory. "[Scopri le autorizzazioni di Workload Factory](#)" per decidere quale modalità vuoi utilizzare.



I server Microsoft SQL che utilizzano il protocollo SMB non supportano la creazione di database.

Prima di iniziare

Completa i seguenti prerequisiti prima di creare un nuovo database.

- **Credenziali e autorizzazioni:** Devi avere "[Credenziali dell'account AWS e autorizzazioni per operations and remediation](#)" per creare un nuovo database in Workload Factory.

In alternativa, puoi usare Codebox per copiare un modello, così puoi distribuire un database al di fuori di workload factory usando l'API REST. "[Scopri di più sull'automazione di Codebox](#)".

- **Host Windows:** Devi avere un numero sufficiente di lettere di unità disponibili in Microsoft SQL Server per creare nuove unità per il nuovo database se usi la modalità *Quick create*.
- **Microsoft SQL Server:** Devi disporre di un Microsoft SQL Server gestito in workload factory for Databases per ospitare il nuovo database.
- **AWS Systems Manager:** Assicurati che il NT Authority\SYSTEM privilegio utente sia abilitato nell'host Microsoft SQL tramite AWS Systems Manager.

Crea un database

In Workload Factory, per completare questa attività, puoi utilizzare le modalità di distribuzione *Creazione rapida* o *Creazione avanzata*.

Creazione rapida

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Database**.
3. Dal menu Database, seleziona **Inventario**.
4. Nell'inventario, seleziona **Microsoft SQL Server** come tipo di motore del database.
5. Seleziona un database server con un'istanza gestita di SQL Server in cui creare il database.
6. Fai clic sul menu Azioni dell'istanza gestita e quindi seleziona **Crea database utente**.
7. Nella pagina Crea database utenti, nella sezione Informazioni sul database, inserisci le seguenti informazioni:
 - a. **Nome del database**: Inserisci il nome del database.
 - b. **Regole di confronto**: Seleziona una regola di confronto per il database. In Microsoft SQL Server è selezionata la regola di confronto predefinita `SQL_Latin1_General_CP1_CI_AS`.
8. In Impostazioni file, fornisci quanto segue:
 - a. **Modalità impostazioni file**: Seleziona **Creazione rapida**.
 - b. **Nomi e percorsi dei file**:
 - **Nome del file di dati**: Inserisci il nome del file di dati.
 - **Nome del file di log**: Inserisci il nome del file di log.
 - c. **Dimensioni dei file**: Inserisci la dimensione dei dati e la dimensione del file di log per il database.
9. Fai clic su **Create**.

In alternativa, se vuoi modificare ora una di queste impostazioni predefinite, cambia **Modalità impostazioni file** in **Creazione avanzata**.

Creazione avanzata

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Database**.
3. Dal menu Database, seleziona **Inventario**.
4. Nell'inventario, seleziona **Microsoft SQL Server** come tipo di motore del database.
5. Seleziona un database server con un'istanza gestita di SQL Server in cui creare il database.
6. Fai clic sul menu Azioni dell'istanza gestita e quindi seleziona **Crea database utente**.
7. Seleziona **Crea database utente**.
8. Nella pagina Crea database utenti, nella sezione Informazioni sul database, inserisci le seguenti informazioni:

- a. **Nome del database:** Inserisci il nome del database.
 - b. **Regole di confronto:** Seleziona le regole di confronto per il database. Su Microsoft SQL Server è selezionata l'impostazione predefinita delle regole di confronto "SQL_Latin1_General_CP1_CI_AS".
9. In Impostazioni file, fornisci quanto segue:
 - a. **Modalità impostazioni file:** Seleziona **Creazione avanzata**.
 - b. **Nomi e percorsi dei file:**
 - i. **File di dati:** Seleziona una lettera di unità e inserisci il nome del file di dati.

Se vuoi, fai clic sulla casella **Punto di montaggio virtuale**.
 - ii. **File di log:** Seleziona una lettera di unità e inserisci il nome del file di log.

Se vuoi, fai clic sulla casella **Punto di montaggio virtuale**.
 - c. **Dimensioni dei file:** Inserisci la dimensione dei dati e la dimensione del file di log per il database.
10. Fai clic su **Create**.

Se hai creato l'host del database, puoi controllare lo stato di avanzamento del processo nella scheda **Monitoraggio processi**.

Crea un clone sandbox in NetApp Workload Factory for Databases

La creazione di un clone sandbox di un database in NetApp Workload Factory for Databases ti consente di utilizzare il clone per sviluppo, test, integrazione, analisi, formazione, QA e altro ancora, senza modificare il database di origine.

Informazioni su questa attività

Un clone sandbox viene creato dallo snapshot più recente nel database di origine. Può essere clonato nello stesso Microsoft SQL Server del database di origine oppure in un altro Microsoft SQL Server, purché condividano lo stesso file system FSx for ONTAP.

Prima di iniziare

Assicurati di aver completato i seguenti prerequisiti prima di creare un clone sandbox.

- **Credenziali e autorizzazioni:** Devi avere ["Credenziali dell'account AWS e autorizzazioni per operations and remediation"](#) per creare un clone sandbox in Workload Factory.

In alternativa, puoi utilizzare Codebox per copiare un modello parzialmente completato o creare un modello completo in modo da poter creare il clone sandbox al di fuori di Workload Factory utilizzando l'API REST ["Scopri di più sull'automazione di Codebox"](#).

- **Microsoft SQL Server:** Devi disporre di un Microsoft SQL Server gestito in Workload Factory for Databases per ospitare il nuovo clone sandbox.
- **AWS Systems Manager:** Assicurati che il NT Authority\SYSTEM privilegio utente sia abilitato nell'host Microsoft SQL tramite AWS Systems Manager.
- **Database di origine:** Hai bisogno di un database di origine disponibile per la clonazione.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Database**.
3. In Databases, seleziona la scheda **Sandboxes**.
4. Nella scheda Sandboxes, seleziona **Crea nuova sandbox**.
5. Nella pagina Crea nuova sandbox, alla voce Origine del database, inserisci le seguenti informazioni:
 - a. **Host del database di origine**: Seleziona l'host del database di origine.
 - b. **Istanza del database di origine**: Seleziona l'istanza del database di origine.
 - c. **Database di origine**: Seleziona il database di origine da clonare.
6. In Destinazione database, fornisci quanto segue:
 - a. **Host del database di destinazione**: Seleziona un host del database di destinazione per il clone sandbox che si trova nella stessa VPC e ha lo stesso FSx for ONTAP file system dell'host di origine.
 - b. **Istanza del database di destinazione**: seleziona l'istanza del database di destinazione per il clone sandbox.
 - c. **Database di destinazione**: Inserisci un nome per il clone della sandbox.
7. **Montaggio**: Quando cloni un database SQL che contiene più file di dati e/o file di log, Workload Factory clona tutti i file sotto la lettera di unità assegnata automaticamente o definita.

Seleziona una delle seguenti opzioni:

- a. **Assegnazione automatica del punto di montaggio**
- b. **Definisci il percorso del punto di montaggio**

Fornisci le seguenti informazioni per definire il percorso del punto di montaggio:

- Inserisci la lettera dell'unità per il percorso del file di dati.
- Inserisci la lettera dell'unità per il percorso del file di log.

8. **Definisci tag**: Seleziona un tag per definire il clone della sandbox.
9. Fai clic su **Create**.

Per verificare lo stato di avanzamento del lavoro, vai alla scheda **Monitoraggio del lavoro**.

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.