

# **DataKeeper Cluster Edition Oracle Cloud Infrastructure Guide**

1 — Last update: 27 October 2023

SIOS TECHNOLOGY CORP.

# Table of Contents

- 1. DataKeeper Cluster Edition Oracle Cloud Infrastructure Guide ..... 3
  - 1.1. Oracle Cloud Infrastructure Overview ..... 4
  - 1.2. Configuration Information ..... 5
    - 1.2.1. OCI Instance Configuration ..... 7
    - 1.2.2. Software Configuration..... 12
    - 1.2.3. OCI Network Configuration ..... 13
  - 1.3. Configuration on OCI..... 14
    - 1.3.1. Creating Security Rules ..... 17
  - 1.4. Configuration for an OCI Instance ..... 19
  - 1.5. Building a DataKeeper Cluster Edition Volume Cluster..... 22
  - 1.6. Creating a SQL Server Cluster on a Failover Cluster..... 27

# 1. DataKeeper Cluster Edition Oracle Cloud Infrastructure Guide

---

This guide walks you through creating the following configurations as examples of using a cluster environment.

- DataKeeper cluster nodes (two nodes cluster join in a domain node)
- Failover Cluster
- SQL Server Cluster

## 1.1. Oracle Cloud Infrastructure Overview

---

Oracle Cloud Infrastructure (OCI) is a set of complementary cloud services that enable you to build and run a wide range of applications and services in a highly available hosted environment provided by Oracle. OCI provides high-performance computing capabilities (such as physical hardware instances) and storage capacity in a flexible overlay virtual network that can be securely accessed from an on-premises network.

For more information, please visit <https://www.oracle.com/cloud/>.

## 1.2. Configuration Information

In this verification, we used two cluster nodes joined in a domain node with the following configuration with DataKeeper for Windows installed.

### Domain node

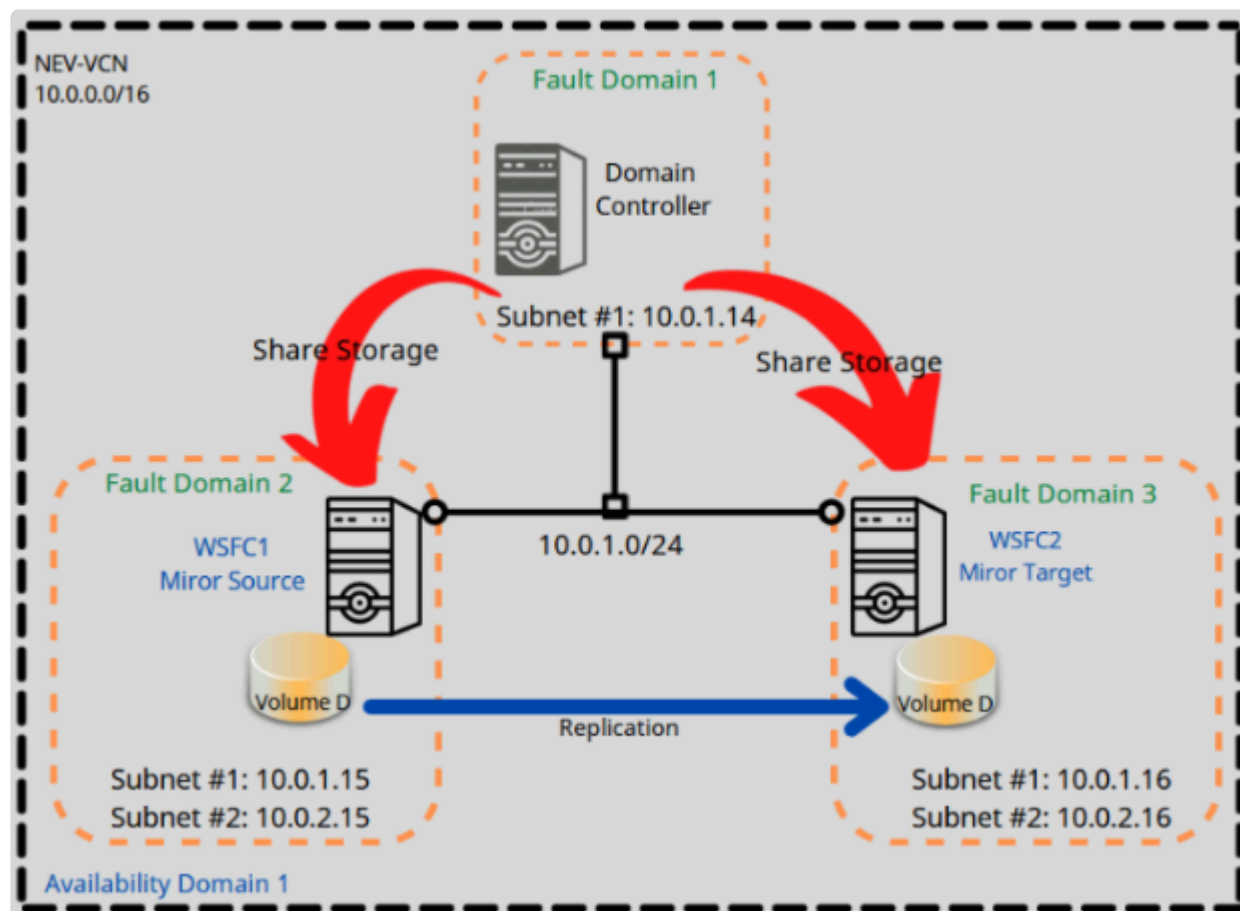
Region	US East
Availability Domain	AD-1
Fault Domain	FD1
Virtual Cloud Network	10.0.0.0/16
Subnet	10.0.1.0/24 (public) 10.0.2.0/24 (private)
Instance	Compute shape: VM.Standard.E4.Flex OS: Windows Server 2019 Standard Additional disks: N/A Network: Global IP address for connection 10.0.1.0/24 (public)
OS	Windows Server 2019 Standard

### Cluster nodes (x2)

Region	US East
Availability Domain	AD-1
Fault Domain	FD2, FD3
Virtual Cloud Network	10.0.0.0/16
Subnet	10.0.1.0/24 (public), 10.0.2.0/24 (private)
Instances	Compute shape: VM.Standard.E4.Flex OS: Windows Server 2019 Standard Additional disks: For Volume D: 50GB (For SQL Server cluster data, replicated by DataKeeper) Network: Global public IP address for remote connection 10.0.1.0/24 (public) 10.0.2.0/24 (private)
OS	Windows Server 2019 Standard

## Verification Environment System Diagram

- Two cluster nodes and a domain node are in different fault domains.
- DataKeeper is used to replicate data between nodes.



## 1.2.1. OCI Instance Configuration

### Domain node

Server name	NODE-AD
Public IP address 1	10.0.1.14/24
CPU	2vCPU 4 processors
Memory	8GB
Disk	System driver 200GB

### Create compute instance

Create an instance to deploy and run applications, or save as a reusable Terraform stack for creating an instance with Resource Manager.

Name

nev-dkce-node01-trang

Create in compartment

siosotechnology (root)

Placement

[Collapse](#)

The [availability domain](#) helps determine which shapes are available.

Availability domain

AD 1  
NqZi:US-ASHBURN-AD-1 ✓

AD 2  
NqZi:US-ASHBURN-AD-2

AD 3  
NqZi:US-ASHBURN-AD-3

[Hide advanced options](#)

Capacity type

☒ On-demand capacity  
Place the instance on a shared host using on-demand capacity.

☐ Preemptible capacity  
Place the instance on a shared host using [preemptible capacity](#). This instance can be reclaimed at any time.

☐ Capacity reservation  
Place the instance on a shared host, and have it count against a [capacity reservation](#).

☐ Dedicated host  
Place the instance on a [dedicated virtual machine host](#).

Fault domain

FAULT-DOMAIN-2


[When should I specify a fault domain?](#)

## Image and shape

[Collapse](#)

A [shape](#) is a template that determines the number of CPUs, amount of memory, and other resources allocated to an instance. The image is the operating system that runs on top of the shape.


### Image



**Windows Server 2019 Standard**  
Image build: 2022.03.08-0

Change image

### Shape



**VM.Standard.E4.Flex**  
Virtual machine, 2 core OCPU, 8 GB memory, 2 Gbps network bandwidth

Change shape

[Show advanced options](#)

## Networking

[Collapse](#)

[Networking](#) is how your instance connects to the internet and other resources in the Console. To make sure you can [connect to your instance](#), assign a public IP address to the instance.

### Primary network

☒ Select existing virtual cloud network ☐ Create new virtual cloud network ☐ Enter subnet OCID

Virtual cloud network in **siostechnology (root)** [\(Change Compartment\)](#)

NEV\_VCN

### Subnet

☒ Select existing subnet ☐ Create new public subnet

Subnet in **siostechnology (root)** [\(Change Compartment\)](#)

Public Subnet-NEV\_VCN (regional)

### Public IP address

☒ Assign a public IPv4 address ☐ Do not assign a public IPv4 address

Assigning a public IP address makes this instance accessible from the internet. If you're not sure whether you need a public IP address, you can always assign one later.

[Hide advanced options](#)

☐ Use network security groups to control traffic

### Private IP address *Optional*

10.0.1.14

### DNS record

☒ Assign a private DNS record ☐ Do not assign a private DNS record

### Hostname *Optional*

NODE-AD

No spaces. Only letters, numbers, and hyphens. 63 characters max.

Fully qualified domain name: NODE-AD sub04080341510.nevvcn.oraclevcn.com

### Launch options

☒ Let Oracle Cloud Infrastructure choose the best networking type

Allow Oracle Cloud Infrastructure to choose the [networking type](#), depending on the instance shape and operating system image.

☐ Paravirtualized networking

For general purpose workloads such as enterprise applications, microservices, and small databases.

☐ Hardware-assisted (SR-IOV) networking

For low-latency workloads such as video streaming, real-time applications, and large or clustered databases.



## Boot volume

A [boot volume](#) is a detachable device that contains the image used to boot the compute instance.

☒ **Specify a custom boot volume size**

[Volume performance](#) varies with volume size. Default boot volume size: 47.0 GB. When you specify a custom boot volume size, service limits apply.

Boot volume size (GB)

200

Integer between 50 GB and 32,768 GB (32 TB). Must be larger than the default boot volume size for the selected image.

☒ **Use in-transit encryption**

[Encrypts data](#) in transit between the instance, the boot volume, and the block volumes.

☐ **Encrypt this volume with a key that you manage**

By default, Oracle manages the keys that encrypt this volume, but you can choose a key from a vault that you have access to if you want greater control over the key's lifecycle and how it's used. [How do I manage my own encryption keys?](#)

## Cluster Node 1

Server name	DKCE-NODE01
Public IP address	Static IP address issued by OCI for connections over the internet.
IP address (public)	10.0.1.15/24
IP address (private)	10.0.2.15/24
CPU	2vCPU 4 processors
Memory	8GB
Disks	System disk 50GB Disk 1 (Volume D) 50GB (used to hold SQL data and replicated by DataKeeper*)

\*The server name is registered as the hostname in the OS. Please do not use “\_” in the hostname.

## Create compute instance

Create an instance to deploy and run applications, or save as a reusable Terraform stack for creating an instance with Resource Manager.

Name

nev-dkce-node01-trang

Create in compartment

siostechnology (root)

### Placement

[Collapse](#)

The [availability domain](#) helps determine which shapes are available.

Availability domain

AD 1

NqZi-US-ASHBURN-AD-1

AD 2

NqZi-US-ASHBURN-AD-2

AD 3

NqZi-US-ASHBURN-AD-3

[Hide advanced options](#)

Capacity type

☒ **On-demand capacity**

Place the instance on a shared host using on-demand capacity.

☐ **Preemptible capacity**

Place the instance on a shared host using [preemptible capacity](#). This instance can be reclaimed at any time.

☐ **Capacity reservation**

Place the instance on a shared host, and have it count against a [capacity reservation](#).

☐ **Dedicated host**

Place the instance on a [dedicated virtual machine host](#).

Fault domain

FAULT-DOMAIN-2

[When should I specify a fault domain?](#)

## Image and shape

[Collapse](#)

A [shape](#) is a template that determines the number of CPUs, amount of memory, and other resources allocated to an instance. The image is the operating system that runs on top of the shape.

### Image



Windows Server 2019 Standard  
Image build: 2022.03.08-0

[Change image](#)

### Shape



VM.Standard.E4.Flex  
Virtual machine, 2 core OCPU, 8 GB memory, 2 Gbps network bandwidth

[Change shape](#)

[Show advanced options](#)

## Networking

[Collapse](#)

[Networking](#) is how your instance connects to the internet and other resources in the Console. To make sure you can [connect to your instance](#), assign a public IP address to the instance.

### Primary network

☒ Select existing virtual cloud network ☐ Create new virtual cloud network ☐ Enter subnet OCID

Virtual cloud network in **siostechnology (root)** [\(Change Compartment\)](#)

NEV\_VCN



### Subnet

☒ Select existing subnet ☐ Create new public subnet

Subnet in **siostechnology (root)** [\(Change Compartment\)](#)

Public Subnet-NEV\_VCN (regional)



### Public IP address

☒ Assign a public IPv4 address ☐ Do not assign a public IPv4 address



Assigning a public IP address makes this instance accessible from the internet. If you're not sure whether you need a public IP address, you can always assign one later.

[Hide advanced options](#)

☐ Use network security groups to control traffic

### Private IP address *Optional*

10.0.1.15

### DNS record

☒ Assign a private DNS record ☐ Do not assign a private DNS record

### Hostname *Optional*

DKCE-NODE01

No spaces. Only letters, numbers, and hyphens. 63 characters max.

Fully qualified domain name: DKCE-NODE01.sub04080341510.nevvcn.oraclevcn.com

### Launch options

☒ Let Oracle Cloud Infrastructure choose the best networking type

Allow Oracle Cloud Infrastructure to choose the [networking type](#), depending on the instance shape and operating system image.

☐ Paravirtualized networking

For general purpose workloads such as enterprise applications, microservices, and small databases.

☐ Hardware-assisted (SR-IOV) networking

For low-latency workloads such as video streaming, real-time applications, and large or clustered databases.

## Boot volume

A [boot volume](#) is a detachable device that contains the image used to boot the compute instance.

☒ **Specify a custom boot volume size**

[Volume performance](#) varies with volume size. Default boot volume size: 47.0 GB. When you specify a custom boot volume size, service limits apply.

Boot volume size (GB)

50

Integer between 50 GB and 32,768 GB (32 TB). Must be larger than the default boot volume size for the selected image.

☒ **Use in-transit encryption**

[Encrypts data](#) in transit between the instance, the boot volume, and the block volumes.

☐ **Encrypt this volume with a key that you manage**

By default, Oracle manages the keys that encrypt this volume, but you can choose a key from a vault that you have access to if you want greater control over the key's lifecycle and how it's used. [How do I manage my own encryption keys?](#)

## Cluster Node 2

Server name	DKCE-NODE02
Public IP address	Static IP address issued by OCI for connections over the internet.
Private IP address (public)	10.0.1.16/24
Memory	8GB
Disks	System disk 50GB Disk 1 (Volume D) 50GB (used to hold SQL data and replicated by DataKeeper*)
CPU	2vCPU 4 processors

\*The server name is registered as the hostname in the OS. Please do not use “\_” in the hostname.

## 1.2.2. Software Configuration

---

In this document, we tested the cluster nodes with the following software configuration.

OS	Windows Server 2019 Standard
DataKeeper	DataKeeper for Windows 8.9.0
SQL Server	SQL Server 2016

## 1.2.3. OCI Network Configuration

---

The following configuration was used for OCI verification. The IP addresses have been granted with public and private subnets assigned to the cluster nodes. With the domain node, the IP address is only associated with a public subnet.

Cluster Nodes	
Virtual Cloud Network	10.0.0.0/16
Public Subnet	10.0.1.0/24
Private Subnet	10.0.2.0/24
Domain Node	
Virtual Cloud Network	10.0.0.0/16
Public Subnet	10.0.1.0/24

The OCI network subnet has a security policy.

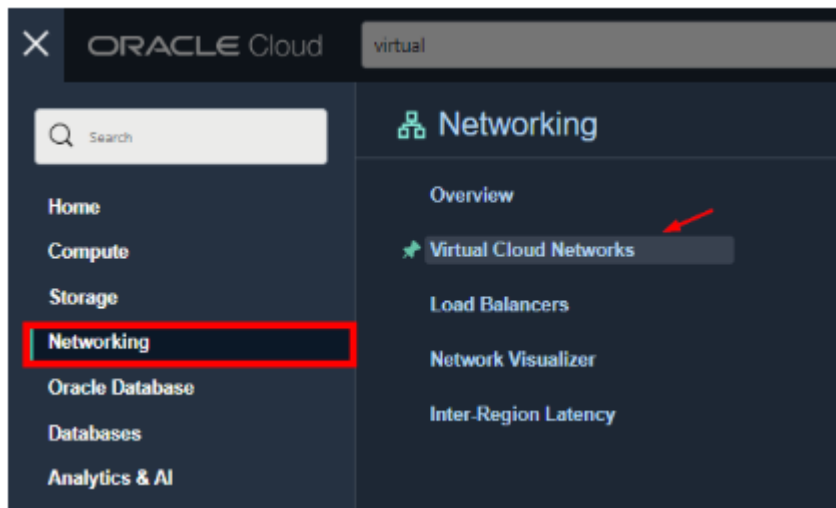
## 1.3. Configuration on OCI

### Creating a VCN Network

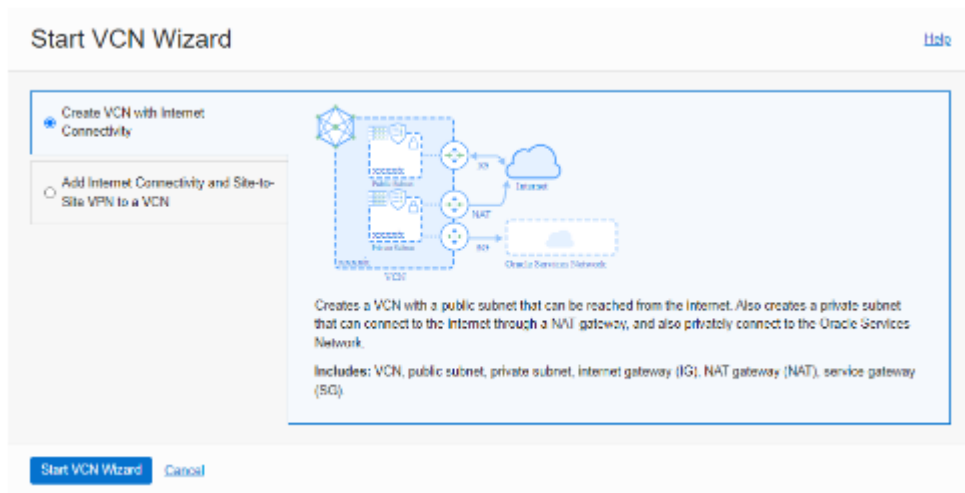
Create the VCN using the following two subnets.

VCN Name	NEV-VCN
Configure VCN and Subnets	
VCN CIDR Block	10.0.0.0/16
Public Subnet CIDR Block	10.0.1.0/24
Private Subnet CIDR Block	10.0.2.0/24
DNS Resolution	Selected

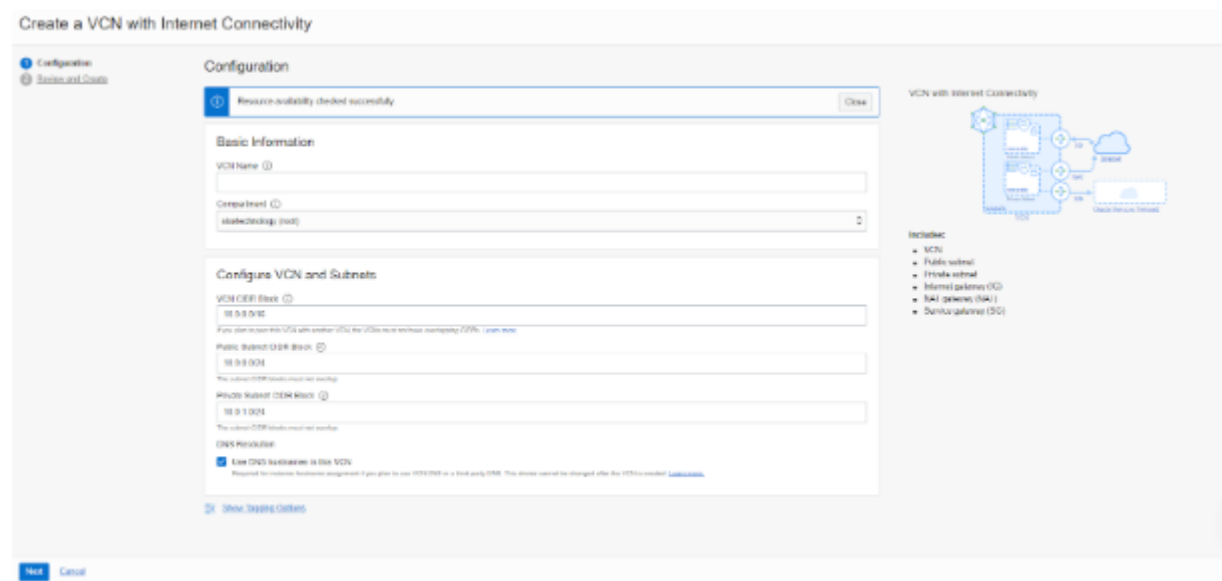
1. Log in to the Oracle Cloud Infrastructure.
2. From the navigation menu, select **Networking** > **Virtual Cloud Networks**.



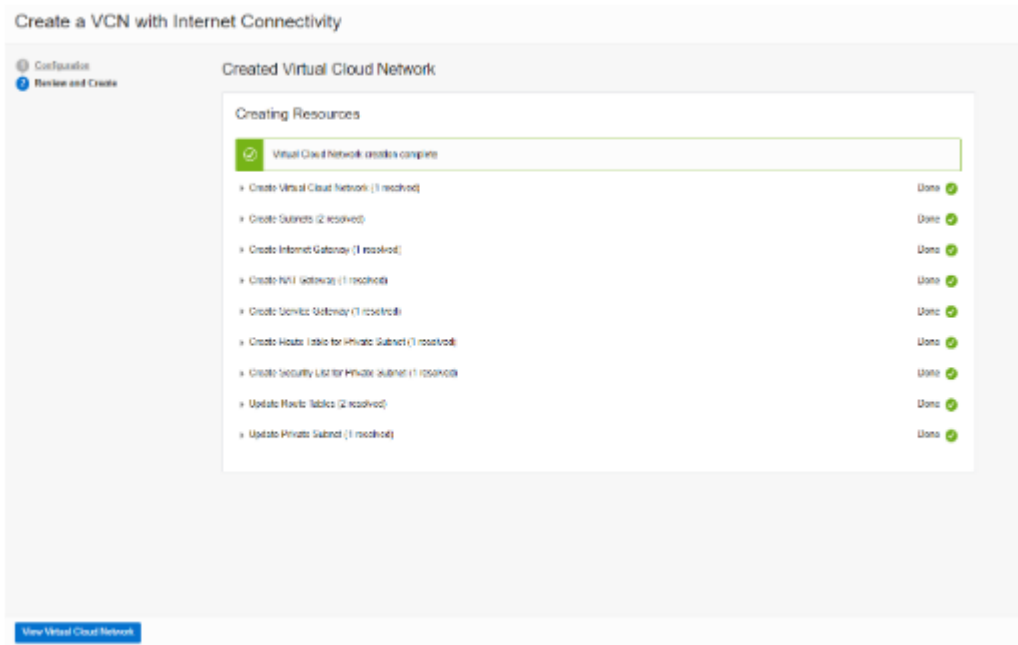
3. Click on **Start VCN Wizard**. Select the **Create VCN with Internet Connectivity** and **Start VCN Wizard**.



4. Enter the VCN name in the **VCN Name** field. In the Configure VCN and Subnets, enter the IP address range for **VCN CIDR Block/Public Subnet CIDR Block/Private Subnet CIDR Block**.



5. Click **Next**.
6. Review and click on **Create**.
7. The new VCN has been created successfully.





## 1.3.1. Creating Security Rules

1. In the **Virtual Cloud Network Details**, scroll down to **Resources** and click on **Security Lists**.

Networking > Virtual Cloud Networks > Virtual Cloud Network Details > Security Lists

**NEV\_VCN**

Move Resource Add Tags Terminate

VCN Information Tags

Compartment: siostechnology (root) OOB: 3f5c3q Show Copy  
 Created: Fri, Apr 8, 2022, 03:44:52 UTC DNS Resolver: NEV\_VCN  
 IPv4 CIDR Block: 10.0.0.0/16 Default Route Table: Default Route Table for NEV\_VCN  
 IPv6 Profile: No Value DNS Domain Name: nevon.oraclecloud.com

Resources

Subnets (2)  
 CIDR Blocks/Prefixes (1)  
 Route Tables (2)  
 Internet Gateways (1)  
 Dynamic Routing Gateways Attachments (3)  
 Network Security Groups (0)

Security Lists in siostechnology (root) Compartment

Create Security List

Name	State	Created
Security List for Private Subnet-NEV_VCN	Available	Fri, Apr 8, 2022, 03:44:54 UTC
Default Security List for NEV_VCN	Available	Fri, Apr 8, 2022, 03:44:52 UTC

Showing 2 items < 1 of 1 >

2. Select the **Default Security Lists for NEV\_VCN > Add Ingress Rules**.

Add rules as shown in the image below:

Default Security List for NEV\_VCN

Instance traffic is controlled by firewall rules on each instance in addition to this Security List

Move Resource Add Tags Terminate

Security List Information Tags

OOB: 3f5c3q Show Copy  
 Created: Fri, Apr 8, 2022, 03:44:52 UTC Compartment: siostechnology (root)

Ingress Rules

Add Ingress Rules Edit Remove

<input type="checkbox"/>	Status	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	Description
<input type="checkbox"/>	No	0.0.0.0/0	TCP	All	22		<input checked="" type="checkbox"/>	TCP traffic for ports: 22 SSH Remote Login Protocol
<input type="checkbox"/>	No	0.0.0.0/0	ICMP			3, 4	<input checked="" type="checkbox"/>	ICMP traffic for: 3, 4 Destination Unreachable - Fragmentation Needed and Don't Fragment was Set
<input type="checkbox"/>	No	10.0.0.0/16	ICMP			3	<input checked="" type="checkbox"/>	ICMP traffic for: 3 Destination Unreachable
<input type="checkbox"/>	No	0.0.0.0/0	TCP	All	3389		<input checked="" type="checkbox"/>	TCP traffic for ports: 3389
<input type="checkbox"/>	No	0.0.0.0/0	SMP				<input checked="" type="checkbox"/>	SMP traffic
<input type="checkbox"/>	No	10.0.1.0/24	TCP	All	All		<input checked="" type="checkbox"/>	TCP traffic for ports: All
<input type="checkbox"/>	No	10.0.1.0/24	UDP	All	All		<input checked="" type="checkbox"/>	UDP traffic for ports: All

0 Selected Showing 7 items < 1 of 1 >

3. Back to Security List and select the **Security List for Private Subnet-NEV\_VCN > Add Ingress Rules**.

Add rules as shown in the image below:

### Security List for Private Subnet-NEV\_VCN

Instance traffic is controlled by firewall rules on each instance in addition to this Security List

[More Resource](#) [Add Tags](#) [Terminate](#)

Security List Information [Tags](#)

OCID: [\\_slgfmq](#) [Show](#) [Copy](#) Compartment: [siosotechnology \(root\)](#)

Created: Fri, Apr 8, 2022, 03:44:54 UTC

### Ingress Rules

[Add Ingress Rules](#) [Edit](#) [Remove](#)

<input type="checkbox"/>	Stateless	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	Description
<input type="checkbox"/>	No	10.0.0.0/16	TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Protocol	
<input type="checkbox"/>	No	0.0.0.0/0	ICMP			3, 4	ICMP traffic for: 3, 4 Destination Unreachable, Fragmentation Needed and Don't Fragment was Set	
<input type="checkbox"/>	No	10.0.0.0/16	ICMP			3	ICMP traffic for: 3 Destination Unreachable	
<input type="checkbox"/>	No	10.0.2.0/24	TCP	All	All		TCP traffic for ports: All	
<input type="checkbox"/>	No	10.0.2.0/24	UDP	All	All		UDP traffic for ports: All	

0 Selected Showing 5 Items

## 1.4. Configuration for an OCI Instance

### GUI Startup and VNC Connection

After creating the instance, run RDP with the public IP using the username and initial password. It will prompt you to change the password.

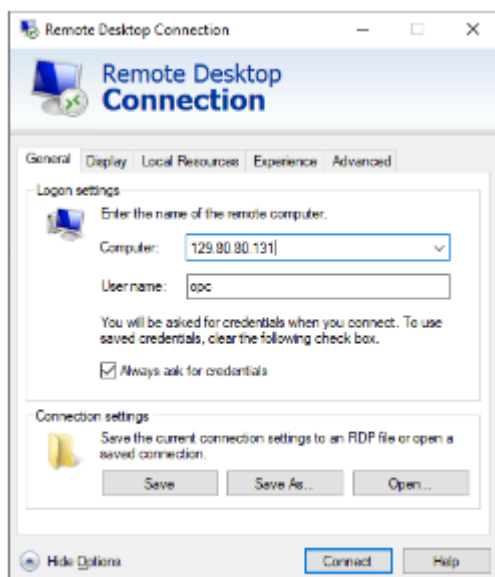
### Instance access

You [connect to a running Windows instance](#) using Remote Desktop. The network that the instance is in must allow Remote Desktop Protocol (RDP) access. Use the instance's initial password to sign in for the first time, and then use the password that you set.

**Public IP address:** 129.80.80.131 [Copy](#)

**Username:** opc

**Initial password:** ..... [Show](#) [Copy](#)



Scroll down to the resource, attached to the second VNICs and block volumes.

- Attached VNICs

Click on **Create VNIC** button, input the second VNIC information.

### VNIC information

Name: Optional

nev-dkce-node01-lrang-vnic2

Select a virtual cloud network in **siostechnology** (root) [\(Change Compartment\)](#)

NEV\_VCN

Network

Normal setup: subnet

The typical choice when adding a VNIC to an instance.

Advanced setup: VLAN

Only for experienced users who have purchased the Oracle Cloud VMware Solution.

Select a subnet in **siostechnology** (root) [\(Change Compartment\)](#)

Private Subnet-NEV\_VCN (regional)

☐ Use network security groups to control traffic (optional) <sup>①</sup>☐ Skip source/destination check <sup>①</sup>

### Primary IP information

Private IP address: Optional

10.0.1.15

Must be within 10.0.2.0 to 10.0.2.255. Must not already be in use.

☐ Assign public IP address (cannot create public IP addresses in a private subnet)

DNS record

☒ Assign a private DNS record ☐ Do not assign a private DNS record

Hostname: Optional

DKCE-NODE01

No spaces. Only letters, numbers, and hyphens. 63 characters max.

Save changes

Cancel

### Attached VNICs

A [virtual network interface card \(VNIC\)](#) lets an instance connect to a virtual cloud network (VCN) and determines how the instance connects with endpoints inside and outside the VCN.

Create VNIC					
Name	Subnet or VLAN <sup>①</sup>	State	FQDN <sup>①</sup>	VLAN tag	MAC address
nev-dkce-node01-lrang (Primary VNIC)	Subnet - <a href="#">Public Subnet-NEV_VCN</a>	Attached	dkce-node01 - <a href="#">Show</a> <a href="#">Copy</a>	549	02:00:17:54:13:AE
nev-dkce-node01-lrang-vnic2	Subnet - <a href="#">Private Subnet-NEV_VCN</a>	Attached	dkce-node01 - <a href="#">Show</a> <a href="#">Copy</a>	3785	02:00:17:02:FE:29

Showing 2 items &lt; 1 of 1 &gt;

- Attached block volumes

Click on **Attached block volumes** and Attach block volume on your instance:

Attached block volume for DataKeeper Replication using Access Read/Write

### Attached block volumes

[Block volumes](#) provide high performance network storage to support a broad range of I/O intensive workloads.

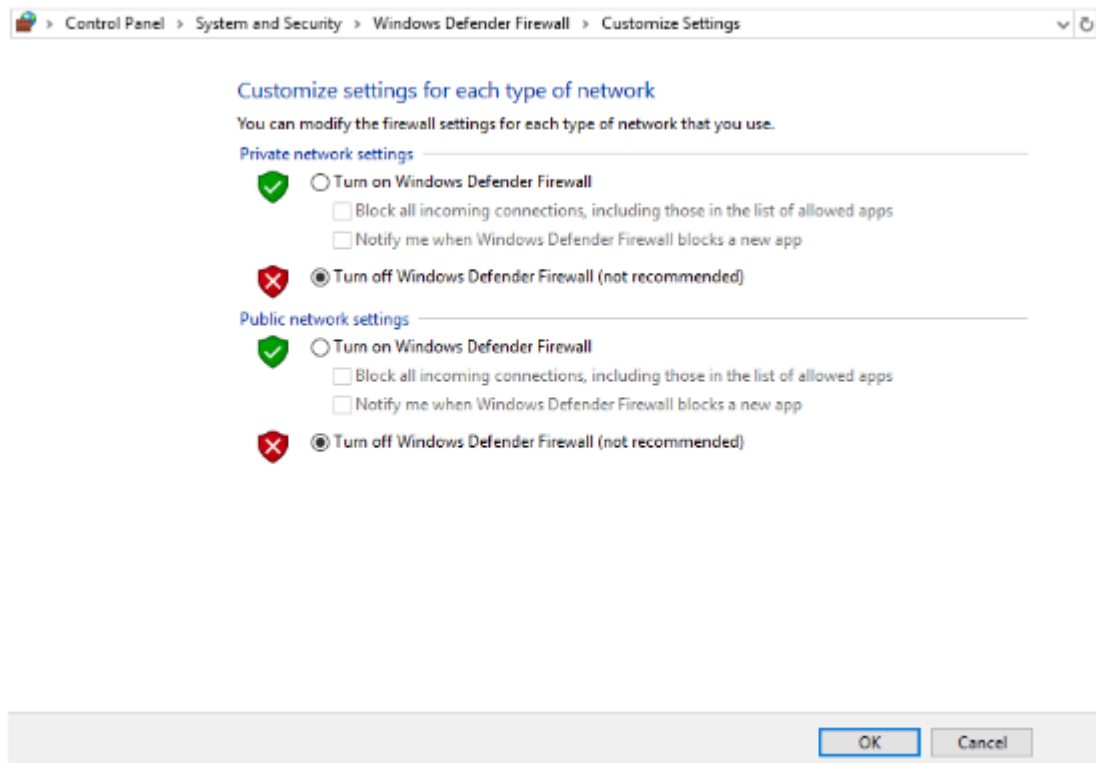
Attach block volume									
Name	State	Volume type	Device path	Type	Access	Size	VFIO	Multipath	Created
NEV_Volume_1	Attached	Block volume	-	paravirtualized	Read/write	50 GB	no	no	Fri, Apr 22, 2022, 09:58:11 UTC

Showing 1 item &lt; 1 of 1 &gt;

## Preparation for Installing DataKeeper Cluster Edition for Windows

- Change the firewall settings.

## Turn off Private/Public Firewall



- Windows Domain Setting

In this document, the cluster nodes are members of a Windows domain, add the cluster nodes (DKCE-NODE01 and DKCE-NODE02) to the domain (SIOS-LKW.local) and log in as the domain administrator (SIOS-LKWAdministrator).

## 1.5. Building a DataKeeper Cluster Edition Volume Cluster

### Creating a DataKeeper Cluster Edition for Windows on OCI Instances

Connect the same size volume to each node. DataKeeper will use this volume. Refer to <https://docs.cloud.oracle.com/en-us/iaas/Content/Block/Tasks/attachingavolume.htm> for information on attaching a volume to an instance.

### Creating the Failover Cluster

Before you create the failover cluster, we strongly recommend that you validate the configuration to make sure that the hardware and hardware settings are compatible with failover clustering. Microsoft supports a cluster solution only if the complete configuration passes all validation tests and if all hardware is certified for the version of Windows Server that the cluster nodes are running.

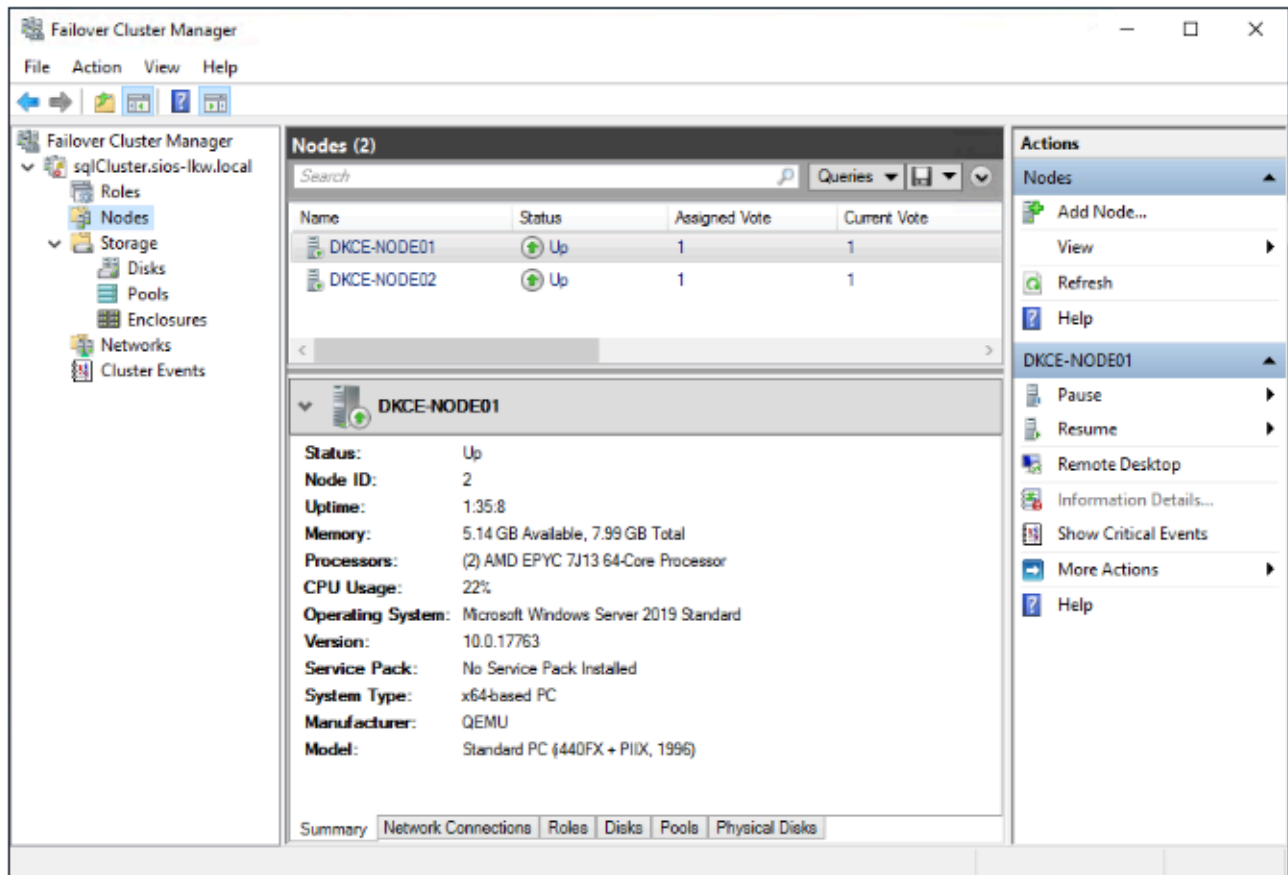
1. Open Failover Cluster Manager from Windows.
2. In the right panel, select Validate Configuration...
3. In the Validate a Configuration Wizard, use the following:

Before You Begin	Default
Select Servers or a Cluster	DKCE-NODE01.sios-lkw.local DKCE-NODE02.sios-lkw.local
Testing Options	Default (Run all tests)
Confirmation	Default
Validating	Check all successes
Summary	Check to "Create the cluster now using the validated nodes..." and Finish

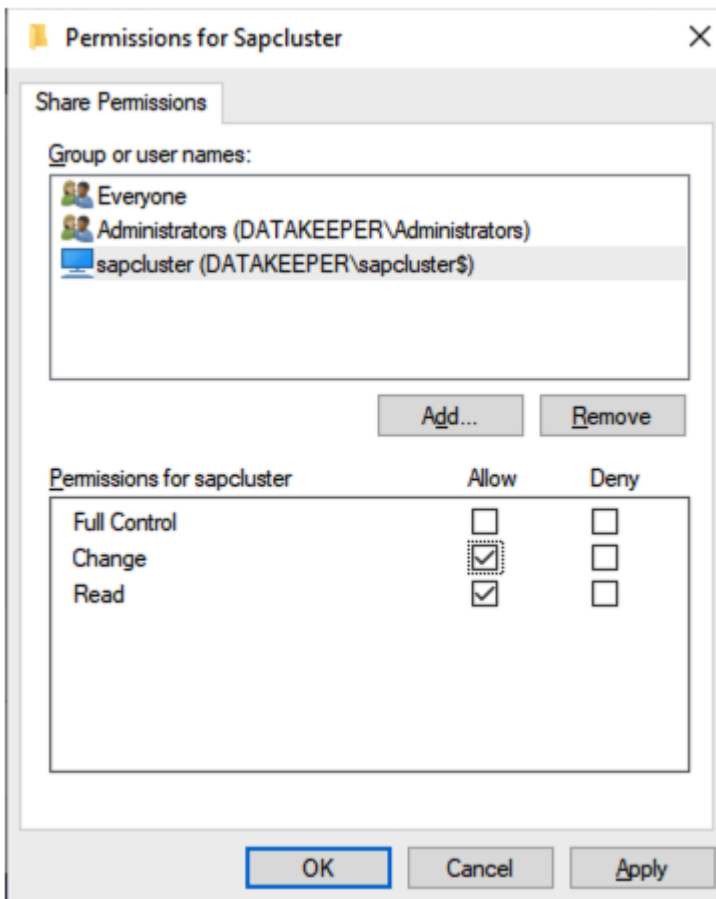
4. In the Create Cluster Wizard, use the following:

Before You Begin	Default
Access Point for Administering the Cluster	Cluster Name: sqlCluster Address: 10.0.1.100
Confirmation	Default
Creating New Cluster	Wait to install
Summary	Finish

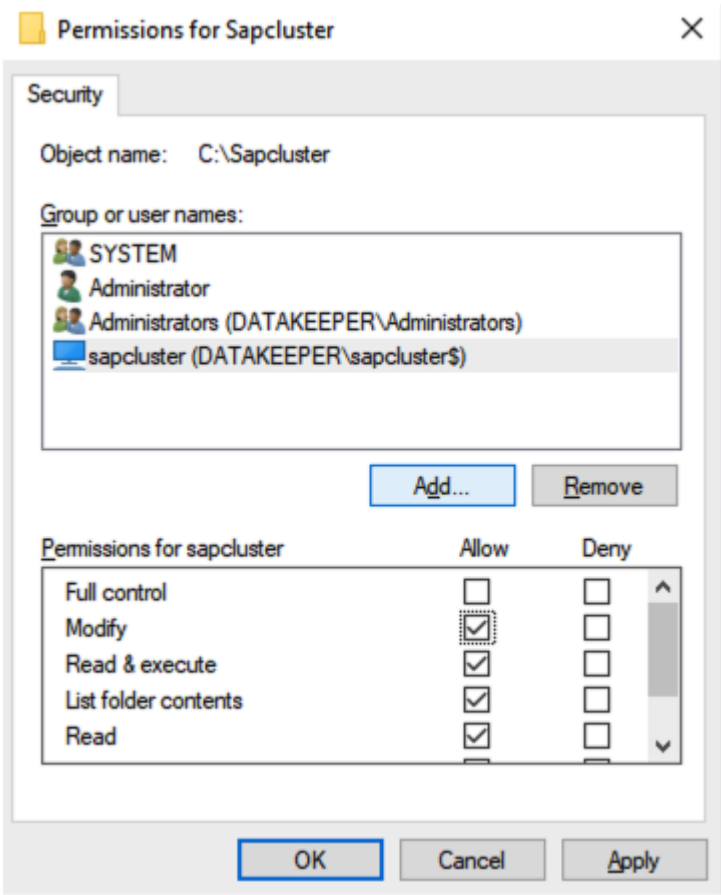
5. The following screen appears when a failover cluster is created.



6. Add the File Share Witness. First, create a folder on another server in a 3rd availability zone. Once you have the folder created, share it and give the Cluster Name Object (CNO). Change permissions at the Share level and Modify permissions at the Security level.







Once the permissions are assigned, run the following PowerShell command to update the cluster quorum to add this file share witness.

Set-ClusterQuorum -FileShareWitness **cluster name**

Installing DataKeeper Cluster Edition

Install DataKeeper Cluster Edition on each of the two OCI instances. For this example, we used DataKeeper Cluster Edition v8.9.0-1543246.

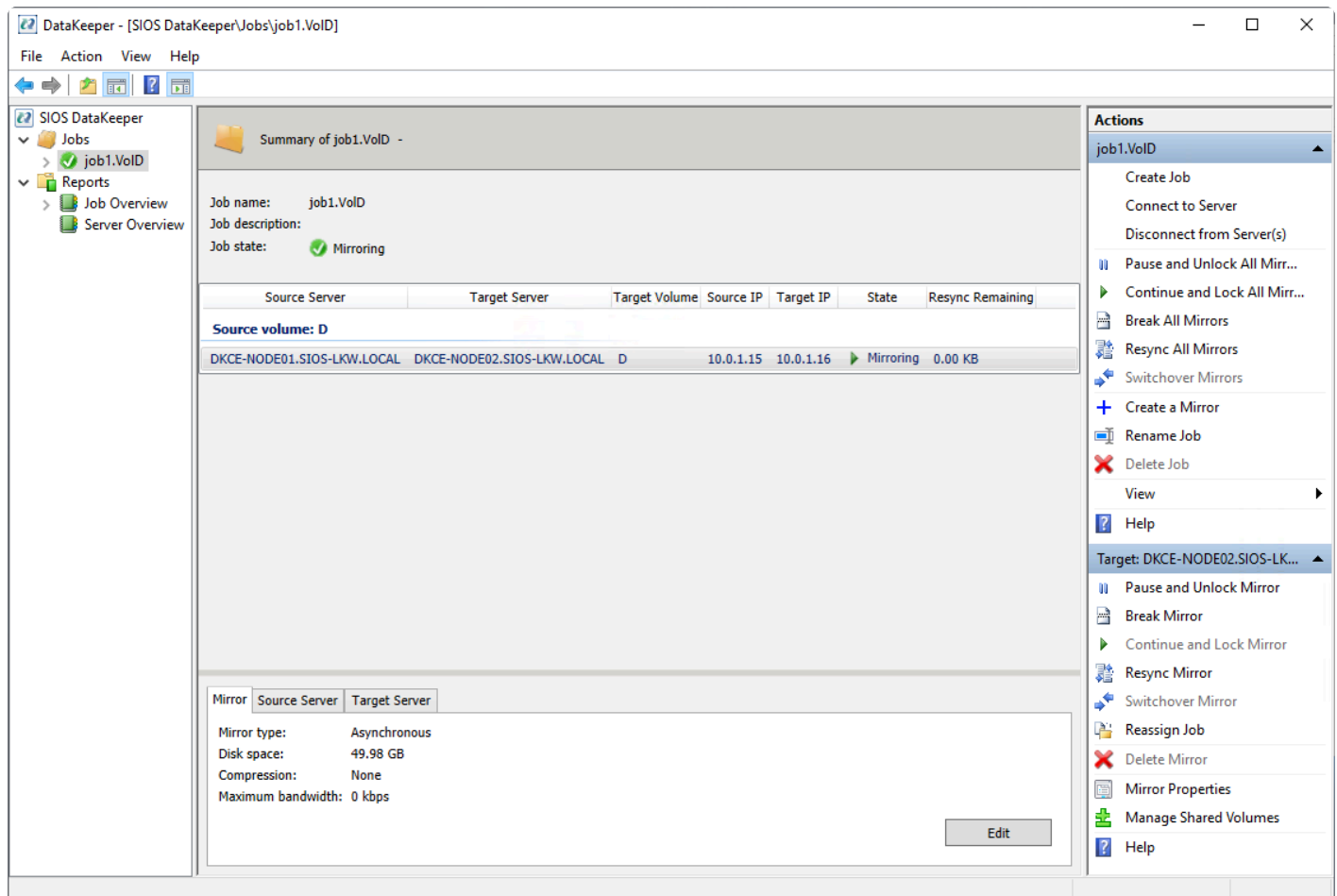
Run DK-8.9.0-Setup.exe file as administrator.

DataKeeper Cluster Edition	
Select feature	Default
Choose Destination Location	C:\Program Files (x86)\SIOS\DataKeeper
System Configuration change prompt	Yes
Service Setup	Domain or Server account (recommended)
DataKeeper Service Logon Account Setup	Password: xxxxxxxxxxxx

	Password Confirm: xxxxxxxxxx
SIOS DataKeeper for Windows	Finish
SIOS License Key Manager	Install License File...
Restart OS	

## Creating a Volume Mirror

- Create a DataKeeper (Replication) resource. DataKeeper specifies a network route between the nodes to be replicated. In order to allow ping over this network route, add a rule to enable ICMP (type 0, 8) communication to the security list of the network you want to use from the OCI management screen.
- Create a new mirror using volume D. Refer to [Creating a Mirror](#).



## 1.6. Creating a SQL Server Cluster on a Failover Cluster

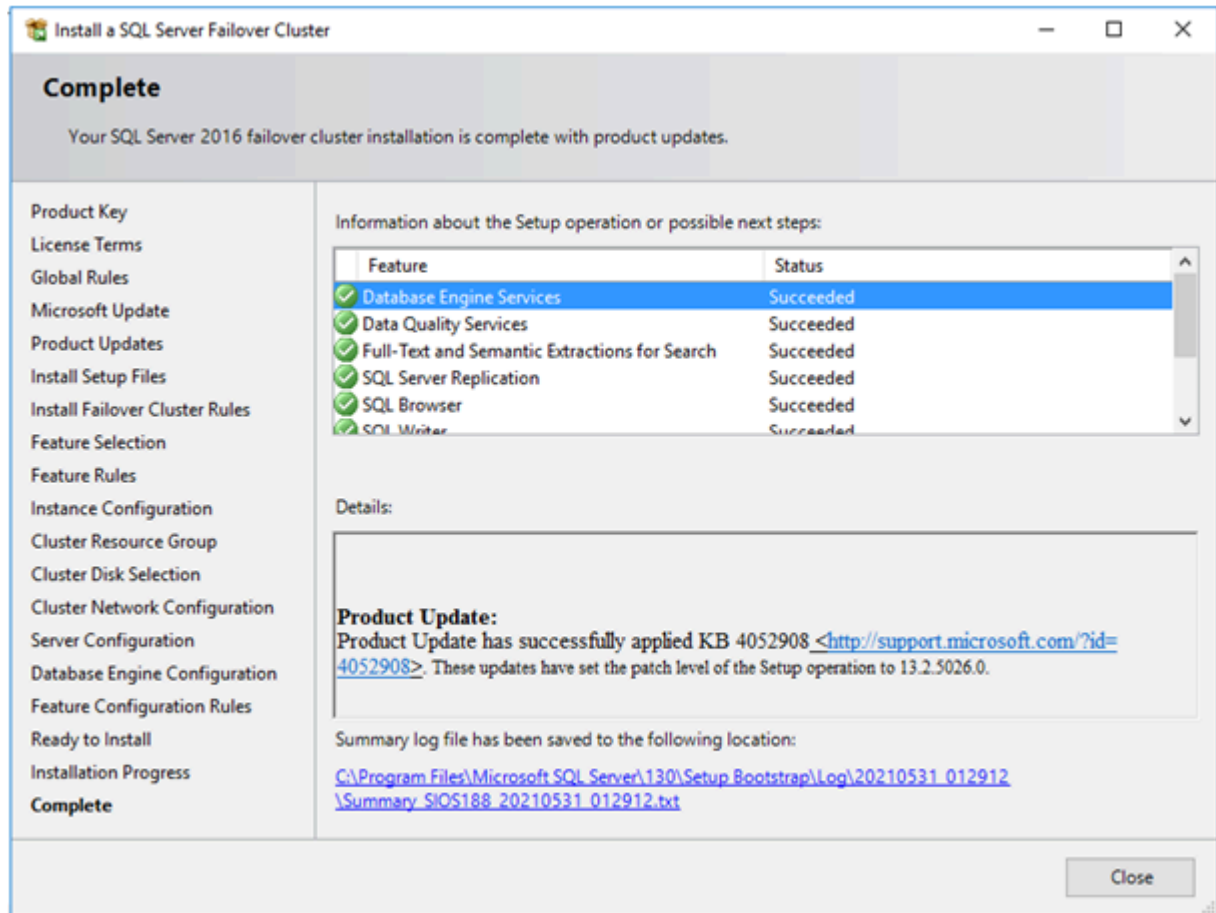
---

### Installing MSSQL Server 2016 on the Source Node

1. Download the SQL Server 2016 (Windows x86-64) installation image from the following site, save it anywhere, and right-click to Mount.

<https://www.microsoft.com/en-us/evalcenter/evaluate-sql-server-2016>

2. After mounting the iso file, double-click on the setup.exe file to open.
3. The **SQL Server Installation Center** screen appears. Select **New SQL Server failover cluster installation**.
4. Complete the following steps:
  - When the **Feature Selection** screen appears, select **Database Engine Service, SQL Server Replication, Full-Text and Semantic Extractions**, and **Data Quality Services**.
  - When the **Instance Configuration** screen appears, input **MSSQLSERVER2016** to fields **SQL Server Network Name**, **Name Instance**, and **Instance ID**.
  - When the **Cluster Network Configuration** screen appears, select the **IPv4** checkbox, and input an available **IP Address** in the Address field.
  - When the **Server Configuration** screen appears, go to the **SQL Server Agent Account Name** field and **click the drop-down**, then **Browse**. Type in **Administrator**, then click the option to **click names**. Return to the **Server Configuration** page. Then, type in the password field and repeat these same steps for SQL Server Database Engine.
  - When the **Database Engine Configuration** screen appears, click **Add Current User** at the bottom of the page.
5. Complete the **Install**.

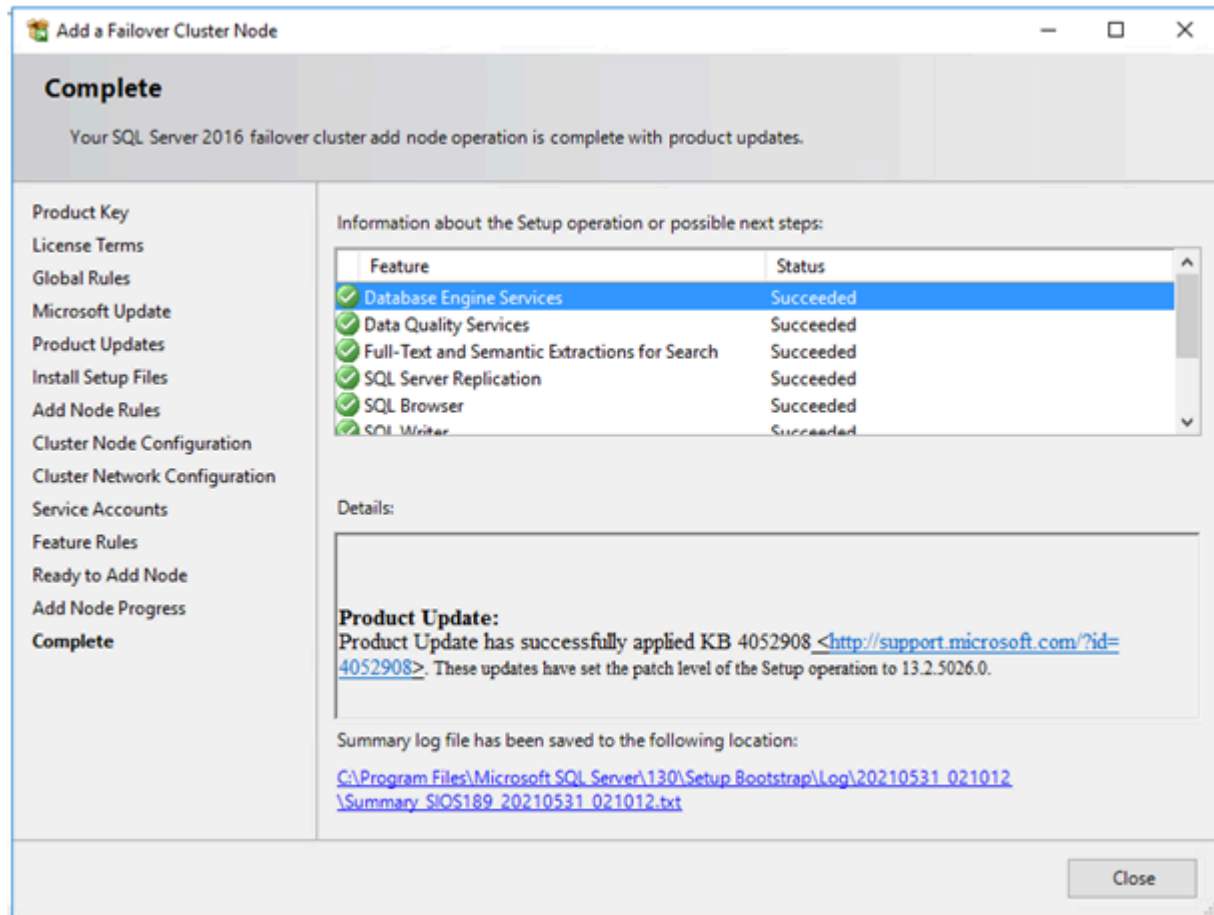


## Installing MSSQL Server 2016 on the Target Node

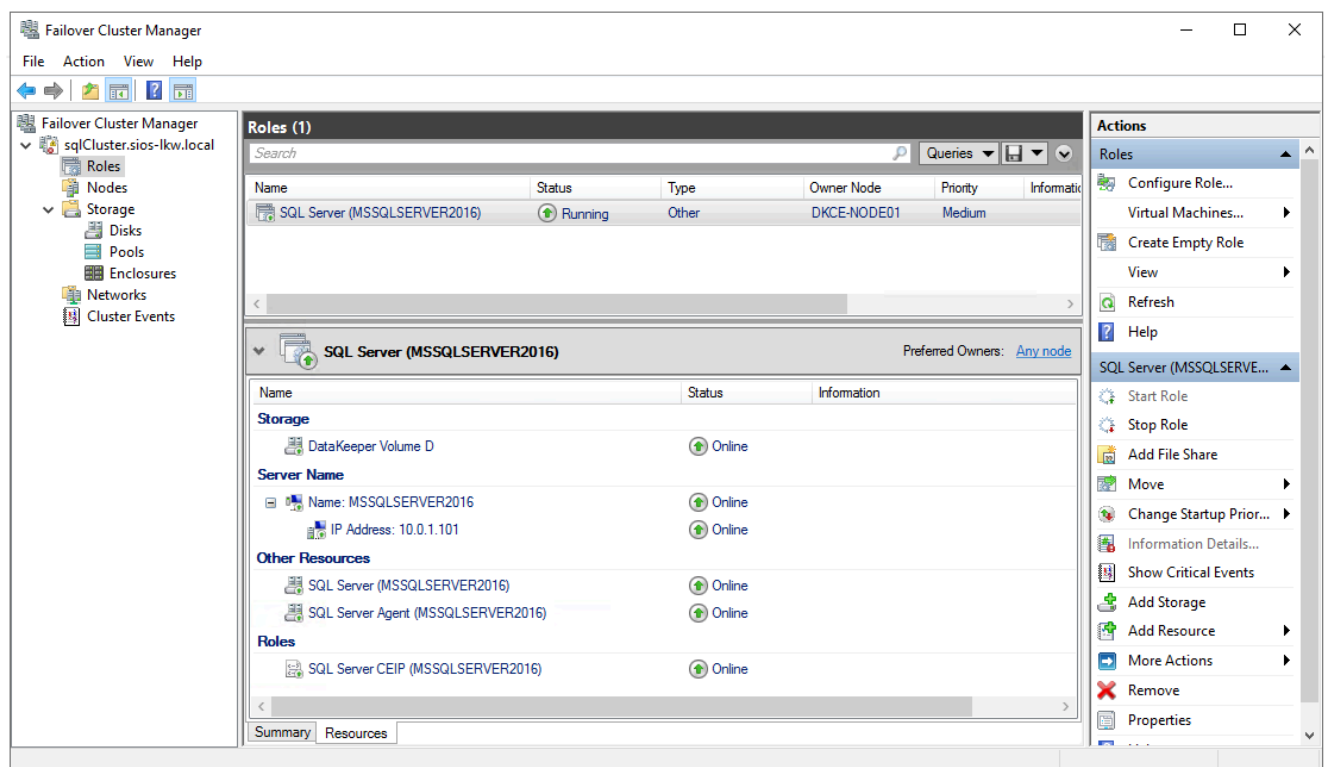
1. Download the SQL Server 2016 (Windows x86-64) installation image from the following site, save it anywhere, and right-click to Mount.

<https://www.microsoft.com/en-us/evalcenter/evaluate-sql-server-2016>

2. After mounting the iso file, double-click on the setup.exe file to open.
3. When the **SQL Server Installation Center** screen appears, select **Add node to a SQL failover cluster**.
4. Complete the following steps:
  - For Service Accounts, input the Password fields as same as the source node.
  - Follow the remaining setup to complete.



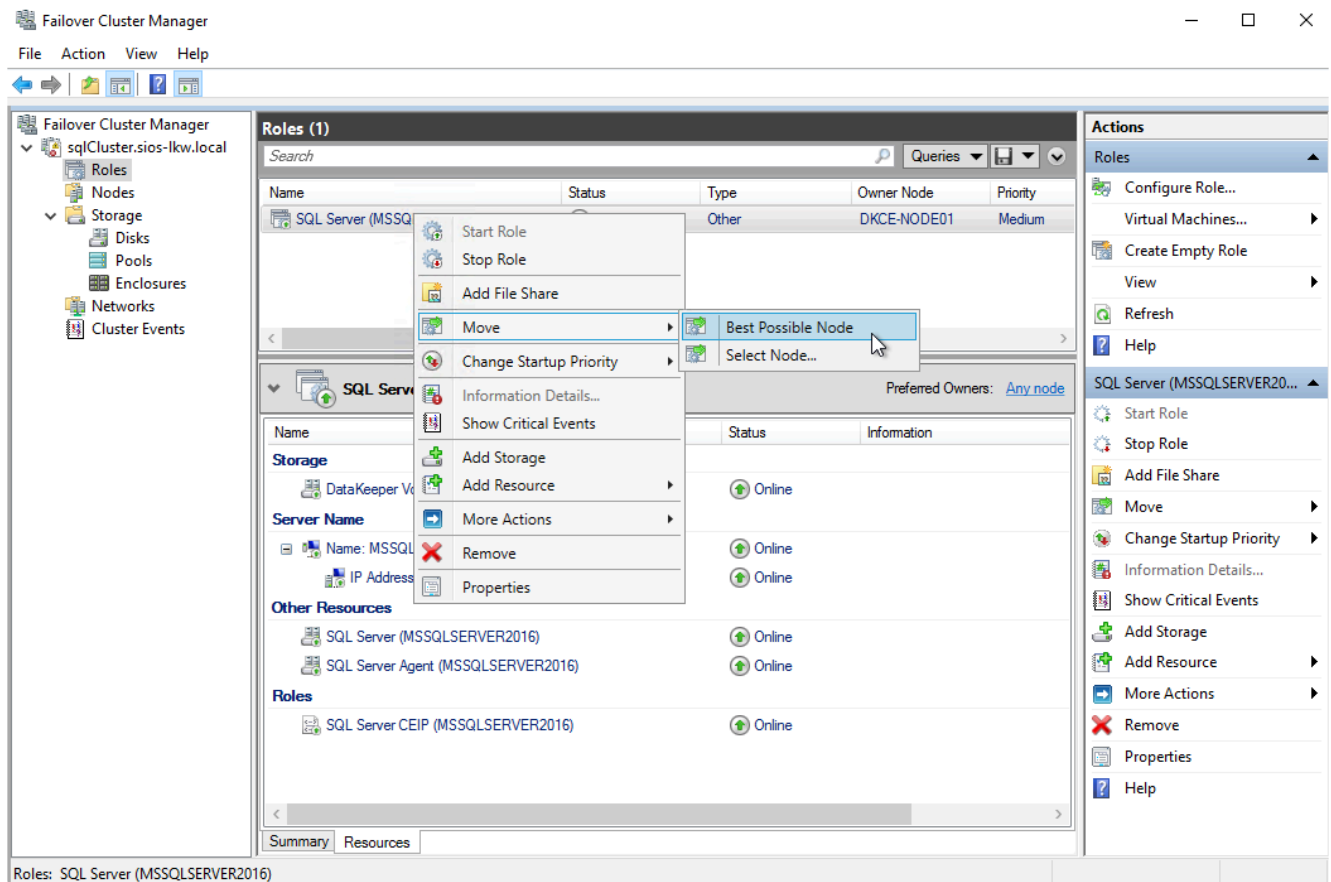
5. The SQL Server Failover cluster has been successfully installed on the Windows Server Failover Cluster.



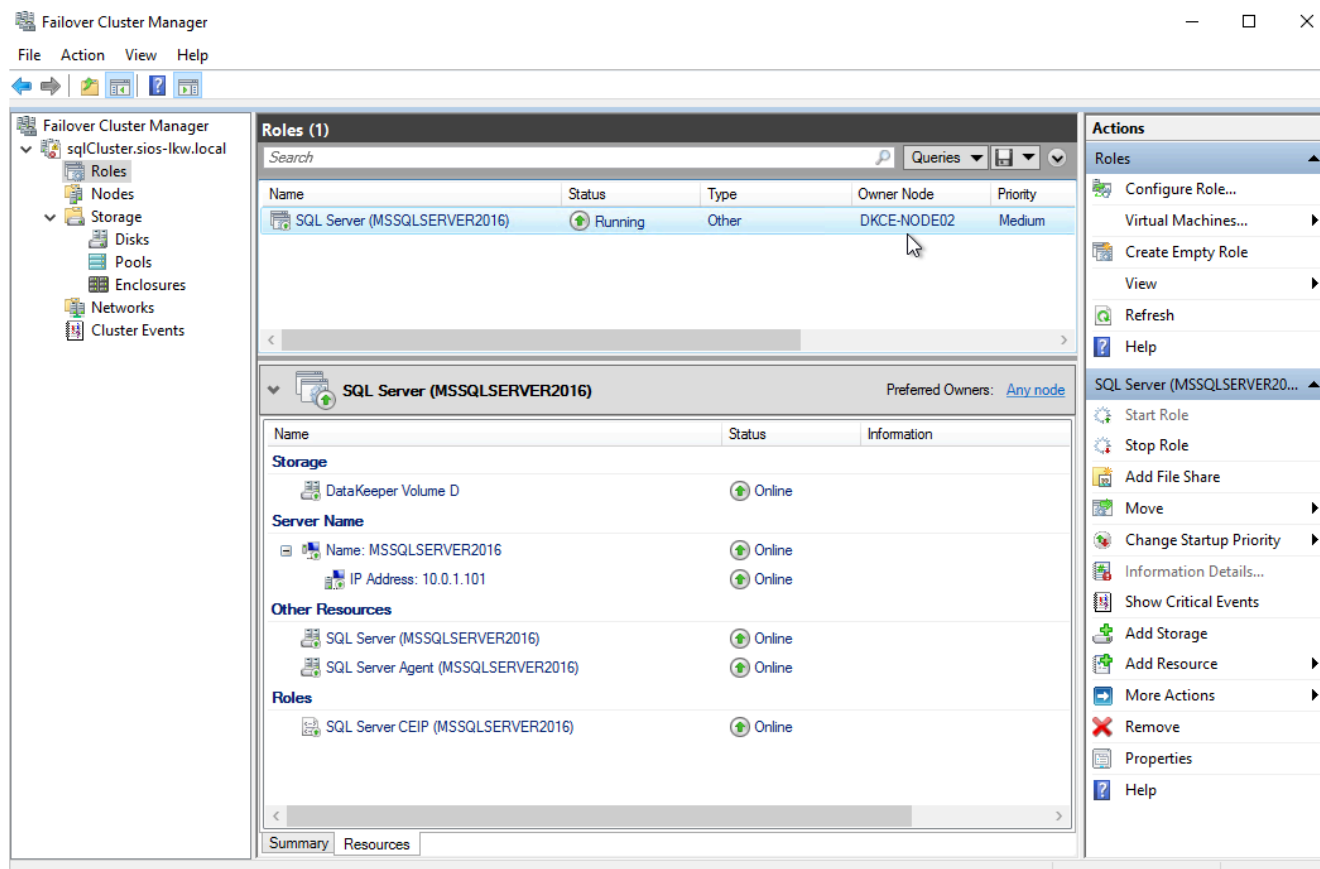
## Check for Fault Tolerance

Performing the switchover from Source Node to Target Node in Windows Server Failover Cluster console:

1. Log in to the Window OS on the Source Node (DKCE-NODE01) as SIOS-LKW\Administrator.
2. Go to Failover Cluster Manager, select **Roles** and right-click on **SQL Server**, then select **Move – Best Possible Node**.



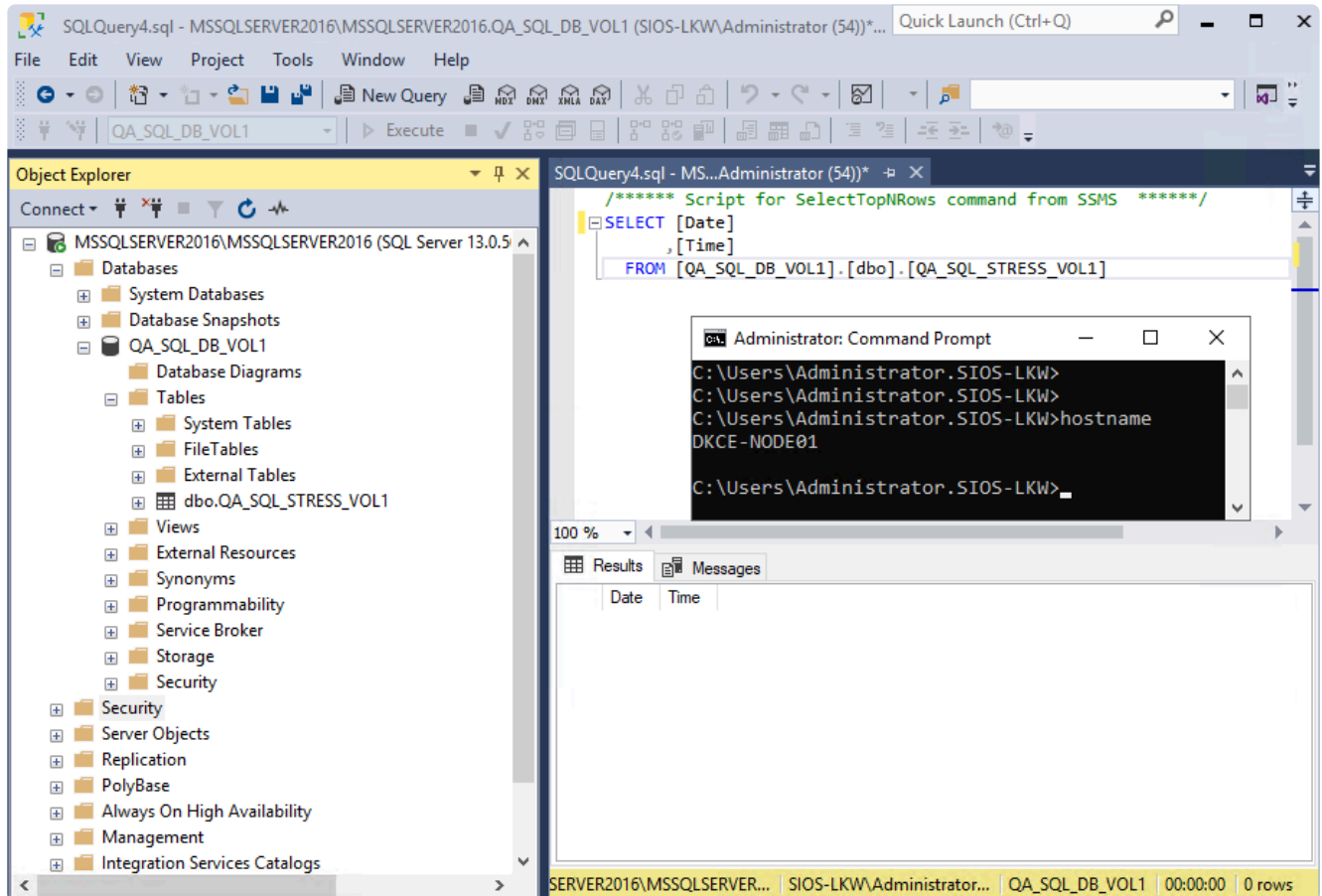
3. Wait until the resource conversion is finished. The SQL Server is running on DKCE-NODE02.



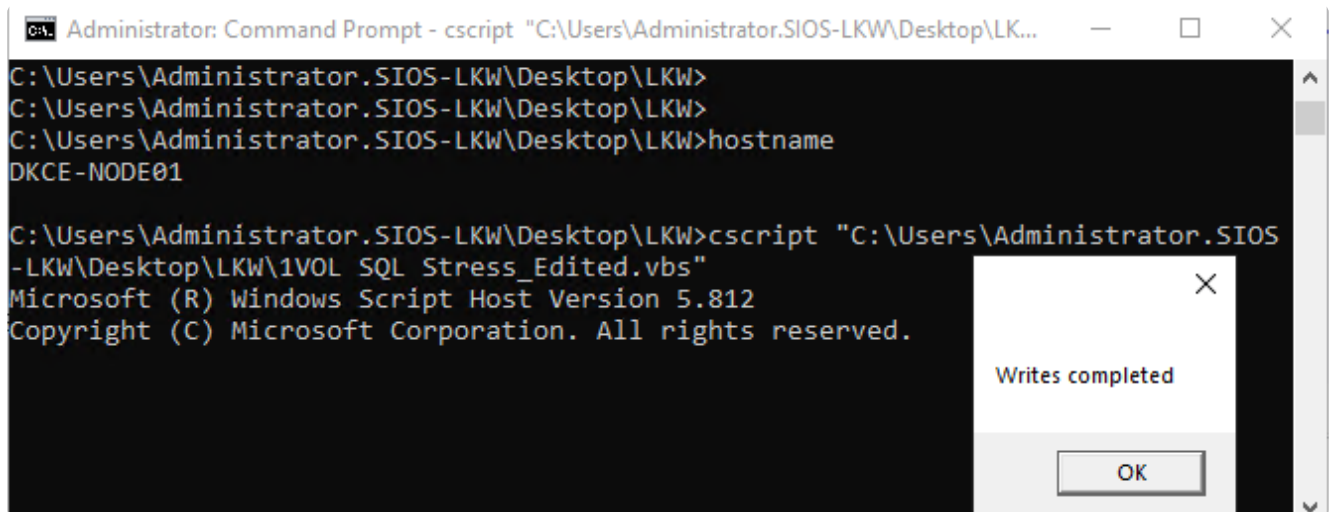
## Connect to the database via SQL Server Management Studio

To connect to the database of SQL Server 2016, follow these steps:

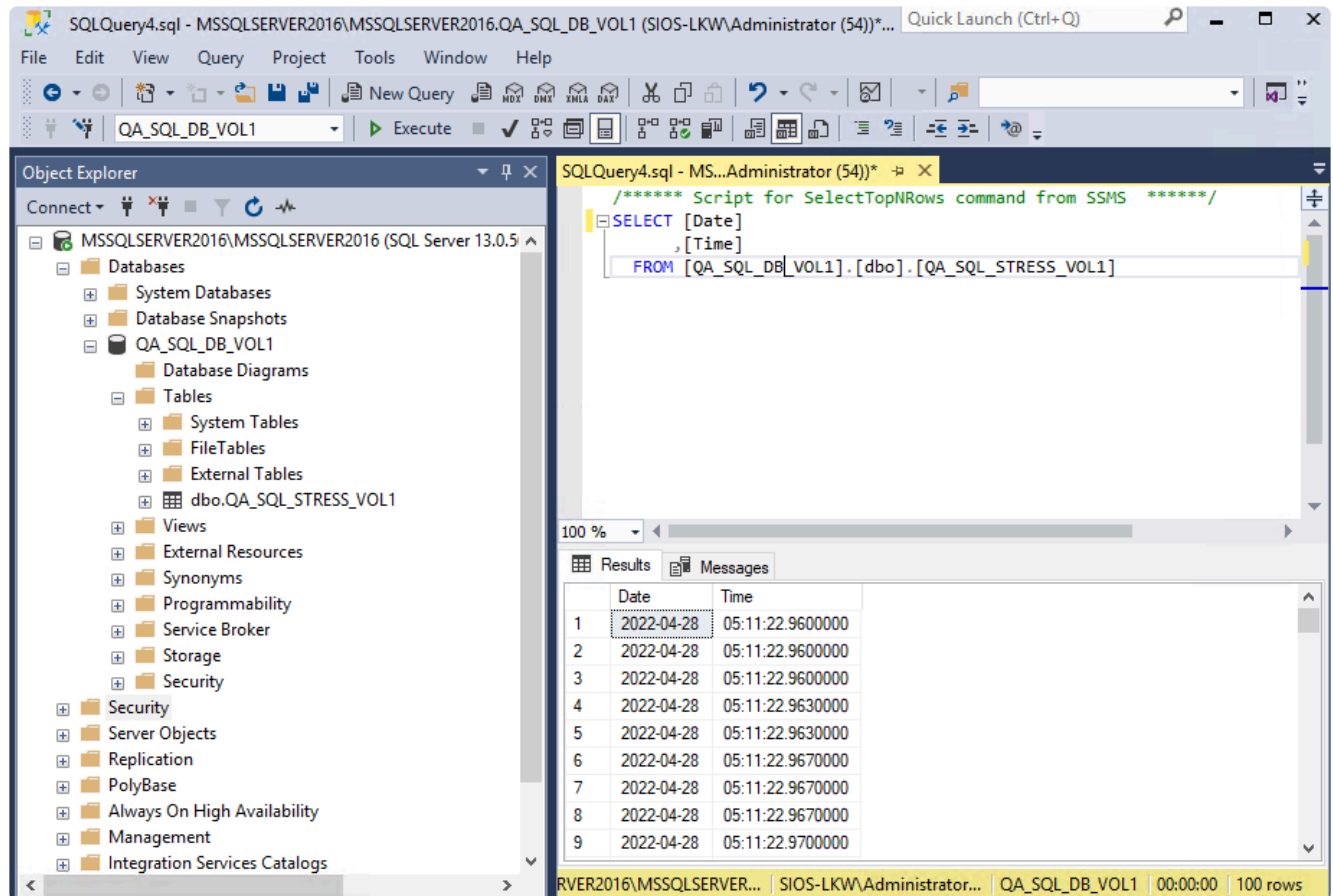
1. Open Microsoft SQL Server Management Studio and connect to the SQL Server 2016 database.



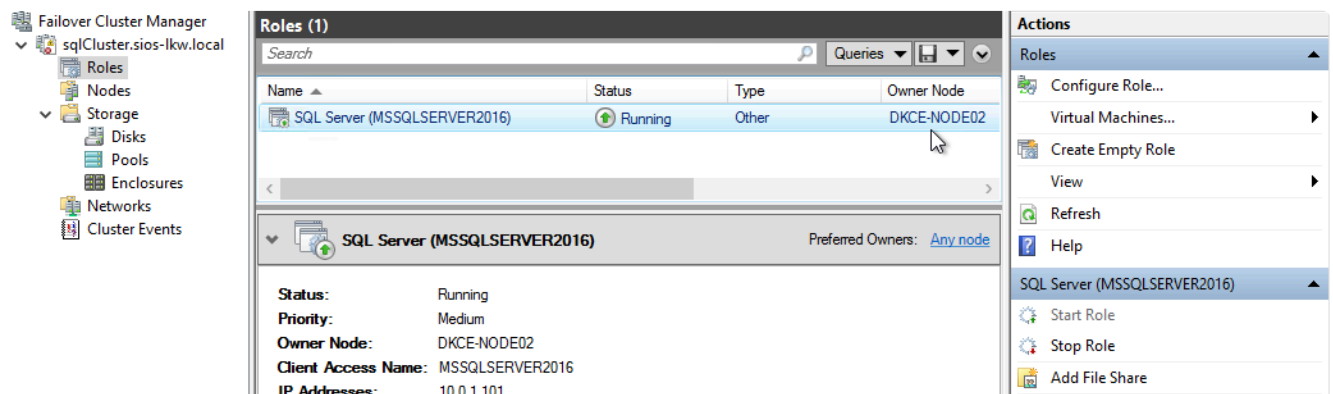
2. Using the script, write constant date\time stamps to the database.







3. Switchover the SQL resource to Target Node then connect to the Database on Target Node.



The screenshot displays the SQL Server Enterprise Manager interface. The Object Explorer on the left shows the database structure for 'MSSQLSERVER2016\MSSQLSERVER2016 (SQL Server 13.0.5015.1)'. The 'QA\_SQL\_DB\_VOL1' database is expanded, showing 'Tables' and 'dbo.QA\_SQL\_STRESS\_VOL1'. The SQL Query Editor on the right shows the following query:

```

/***** Script for SelectTopNRows command from SSMS *****/
SELECT TOP (1000) [Date]
, [Time]
FROM [QA_SQL_DB_VOL1].[dbo].[QA_SQL_STRESS_VOL1]

```

A Command Prompt window is open, showing the command 'hostname' and its output 'DKCE-NODE02'.

The Results pane shows the following data:

	Date	Time
1	2022-04-28	05:11:22.9600000
2	2022-04-28	05:11:22.9600000
3	2022-04-28	05:11:22.9600000
4	2022-04-28	05:11:22.9630000
5	2022-04-28	05:11:22.9630000
6	2022-04-28	05:11:22.9670000
7	2022-04-28	05:11:22.9670000
8	2022-04-28	05:11:22.9670000
9	2022-04-28	05:11:22.9700000

The status bar at the bottom indicates '100 rows'.

- In the SQL Management Studio editor, run the command **select \* from <database table>** to confirm the timestamps have been reflected.