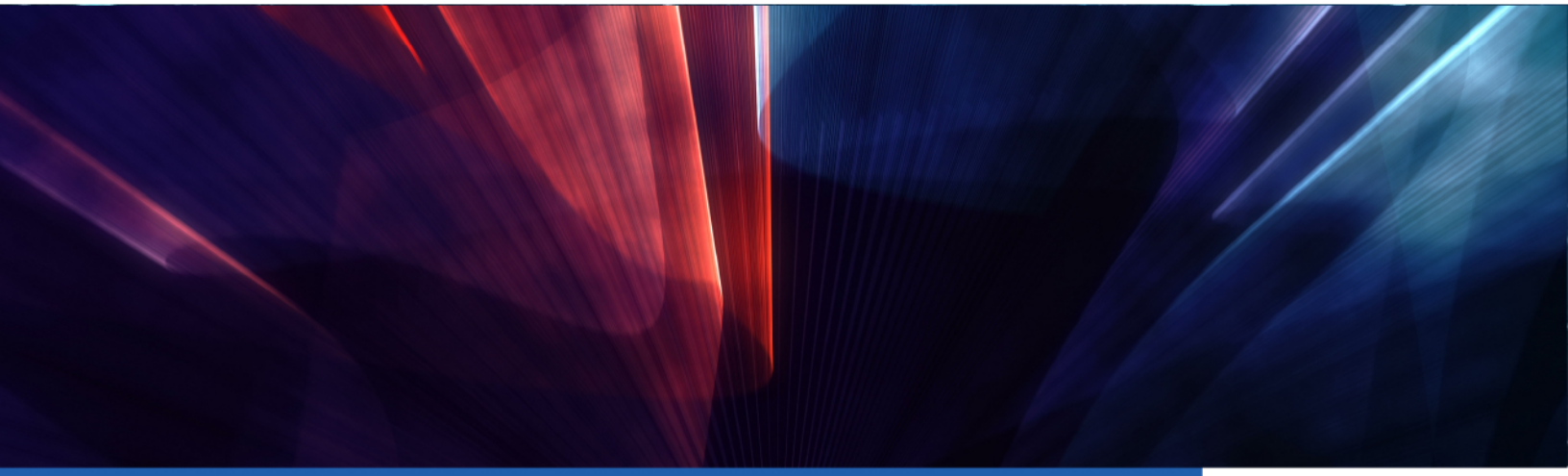
SIOS

Step by Step: SQL Server 2019 FCI in OCI



us.sios.com

Introduction

If you are deploying business-critical applications in Oracle Cloud Infrastructure (OCI), it's crucial to understand and leverage the availability SLA (Service Level Agreement) provided by OCI for optimal uptime and reliability. OCI's SLA varies based on the deployment strategy you choose:

Deployment across Availability Domains: OCI offers a 99.99% availability SLA when you deploy two or more Virtual Machines (VMs) across different Availability Domains within the same OCI region.

Deployment across Fault Domains: If you deploy VMs across Fault Domains, OCI provides a 99.95% availability SLA. It is important to note that not every OCI region has multiple Availability Domains, so in some regions, deployments across Fault Domains will be your only option.

Single VM Deployment: For deployments involving a single VM, the SLA stands at 99.9%.

This framework means that OCI guarantees a certain level of external connectivity based on how you deploy your VMs:

It's important to note that the SLA covers the availability of the VM itself, not the applications or services running on it. To ensure application availability, additional measures such as application monitoring, recovery planning, data replication, and transactional replication (for databases like SQL Server) are necessary. Strategies might include load balancing, clustering, or data replication to manage application availability effectively.

To meet the criteria for the 99.99% availability SLA in OCI, it's essential to deploy your VMs across multiple Availability Domains. This post will guide you on designing your OCI infrastructure to facilitate SQL Server Failover Cluster Instances that span Availability Domains, ensuring maximum uptime and reliability for your critical business applications.

Create the VCN and Subnets

In this guide, I assume you have some familiarity with Oracle Cloud Infrastructure (OCI) and a basic understanding of networking concepts. I will illustrate common configuration tasks with descriptions, and where necessary, provide additional guidance to navigate some of the common challenges encountered in OCI networking.

Starting with a well-thought-out network plan is crucial. This document won't cover the intricacies of cloud network planning, so the following example should be considered just one of many possibilities. Your network configurations may vary significantly. However, an important consideration is to plan for the use of at least three Availability Domains, allocating one for each cluster node and another for the file share witness. The important thing required for clustering is that each Availability Domain MUST be in a different subnet.

Although we are not covering configurations that span Fault Domains instead of Availability Domains, the same applies to clusters that span Fault Domains - all nodes must reside in different subnets.

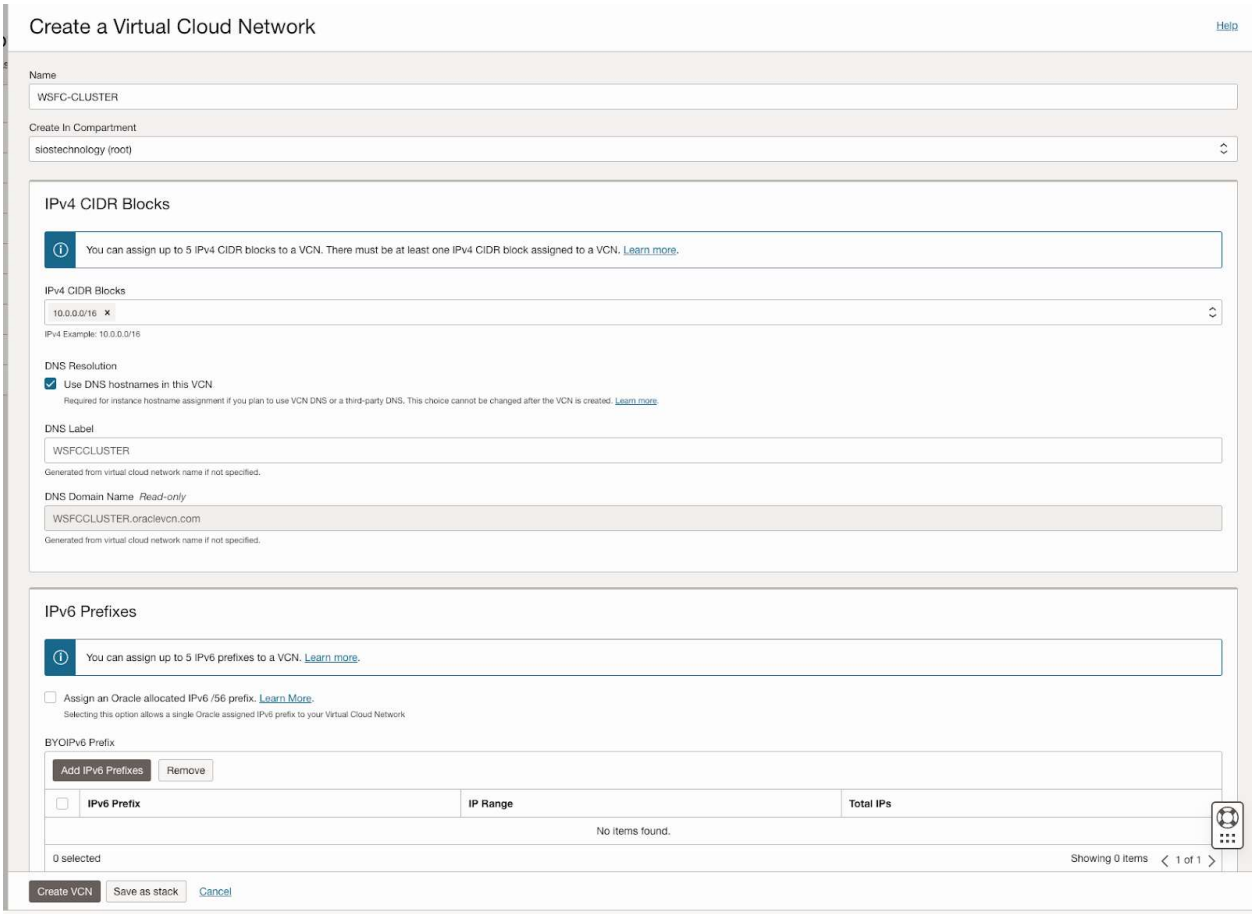
In our scenario, we will set up three subnets across three different Availability Domains within a single Virtual Cloud Network (VCN) in OCI.

VCN: 10.0.0.0/16

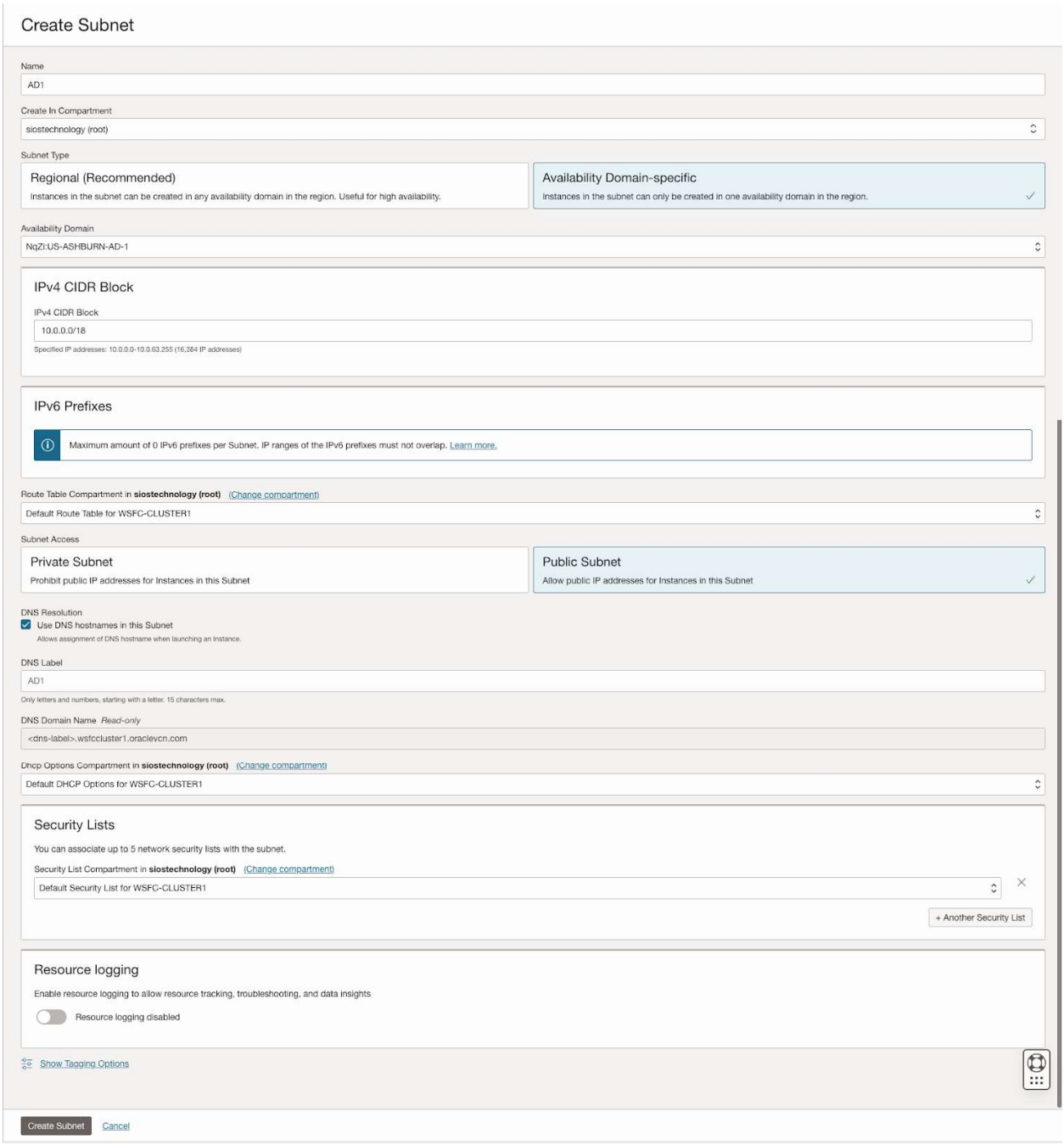
- AD1: 10.0.0.0/18
- AD2: 10.0.64.0/18
- AD3: 10.0.128.0/18

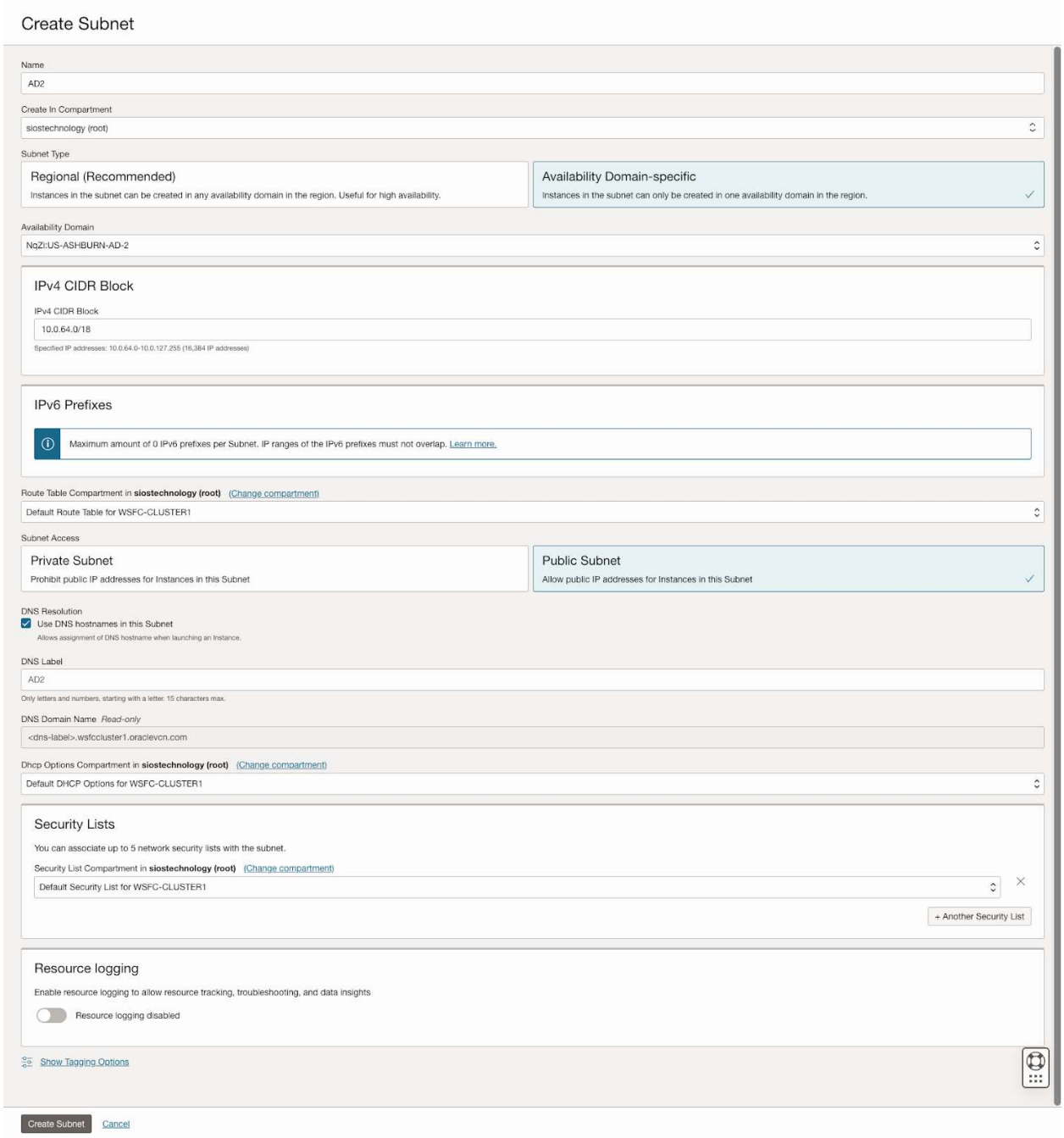
OCI's user interface can change, but at the time of writing, the process for creating a new VCN and three subnets is straightforward in the OCI console. The specifics can be found in OCI's documentation or through its user interface, which guides you through the necessary steps for VCN and subnet creation.

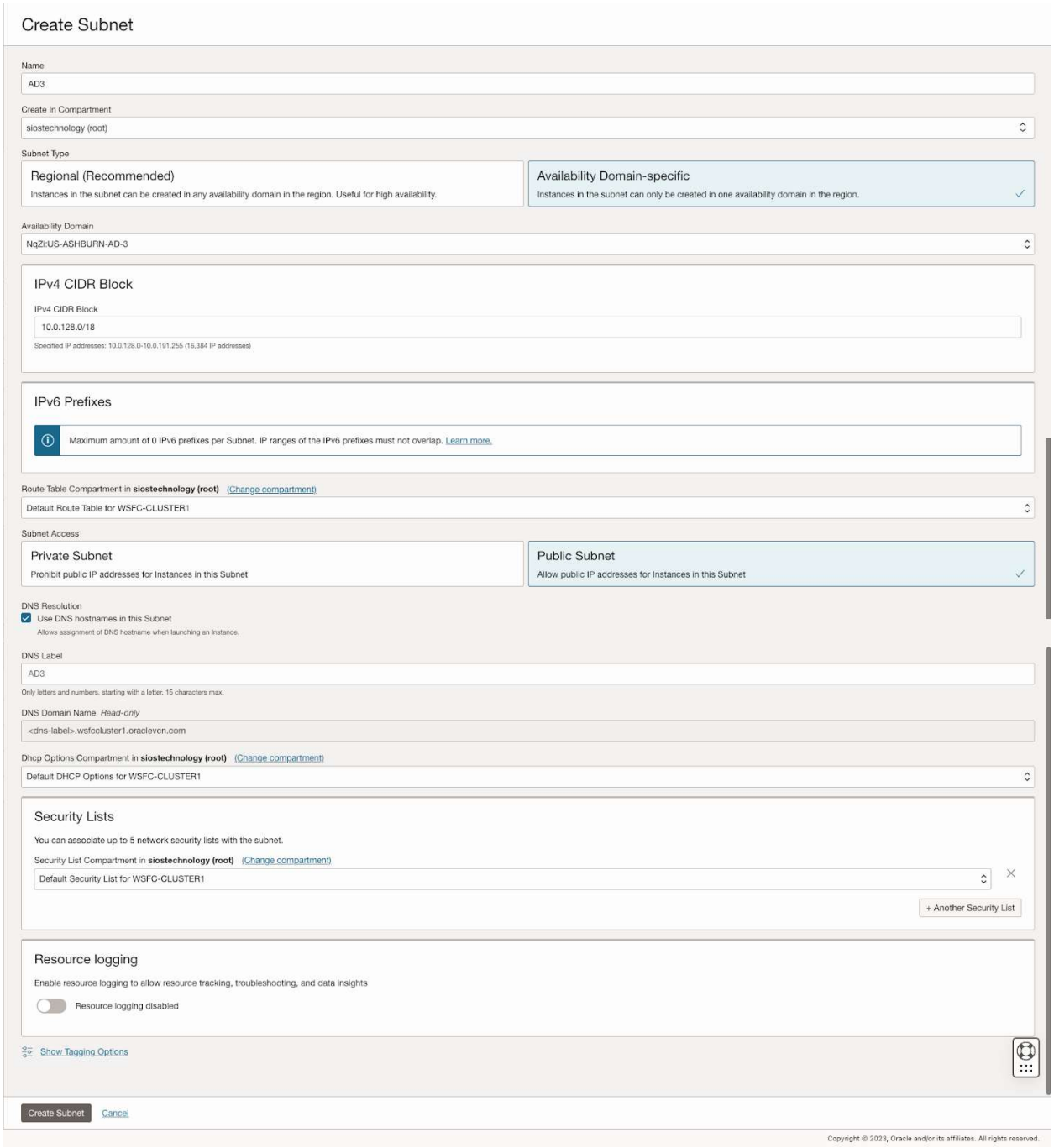
Create the VCN



Create three subnets in the VCN

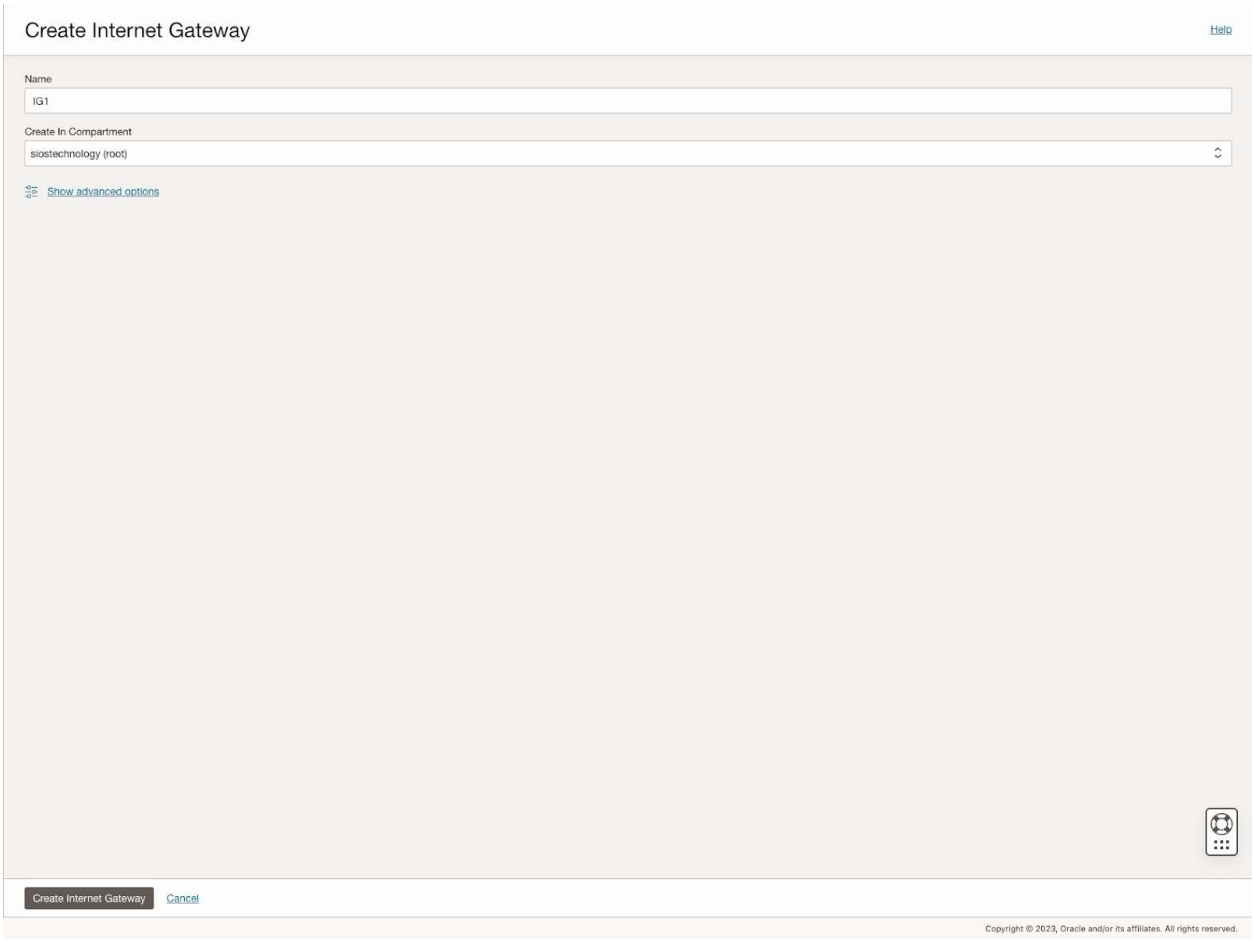



Create Subnet
Name
AD2
Create In Compartment
siostechnology (root)
Subnet Type
Regional (Recommended)
Instances in the subnet can be created in any availability domain in the region. Useful for high availability.
Availability Domain-specific
Instances in the subnet can only be created in one availability domain in the region.
Availability Domain
NqZI:US-ASHBURN-AD-2
IPv4 CIDR Block
IPv4 CIDR Block
10.0.64.0/18
Specified IP addresses: 10.0.64.0-10.0.127.255 (16,384 IP addresses)
IPv6 Prefixes
Maximum amount of 0 IPv6 prefixes per Subnet. IP ranges of the IPv6 prefixes must not overlap. Learn more.
Route Table Compartment in siostechnology (root) (Change compartment)
Default Route Table for WSFC-CLUSTER1
Subnet Access
Private Subnet
Prohibit public IP addresses for Instances in this Subnet
Public Subnet
Allow public IP addresses for Instances in this Subnet
DNS Resolution
Use DNS hostnames in this Subnet
Allows assignment of DNS hostname when launching an Instance.
DNS Label
AD2
Only letters and numbers, starting with a letter. 15 characters max.
DNS Domain Name Read-only
<dns-label>.wsfccluster1.oraclevcn.com
Dhcp Options Compartment in siostechnology (root) (Change compartment)
Default DHCP Options for WSFC-CLUSTER1
Security Lists
You can associate up to 5 network security lists with the subnet.
Security List Compartment in siostechnology (root) (Change compartment)
Default Security List for WSFC-CLUSTER1
+ Another Security List
Resource logging
Enable resource logging to allow resource tracking, troubleshooting, and data insights
Resource logging disabled
Show Tagging Options
Create Subnet
Cancel

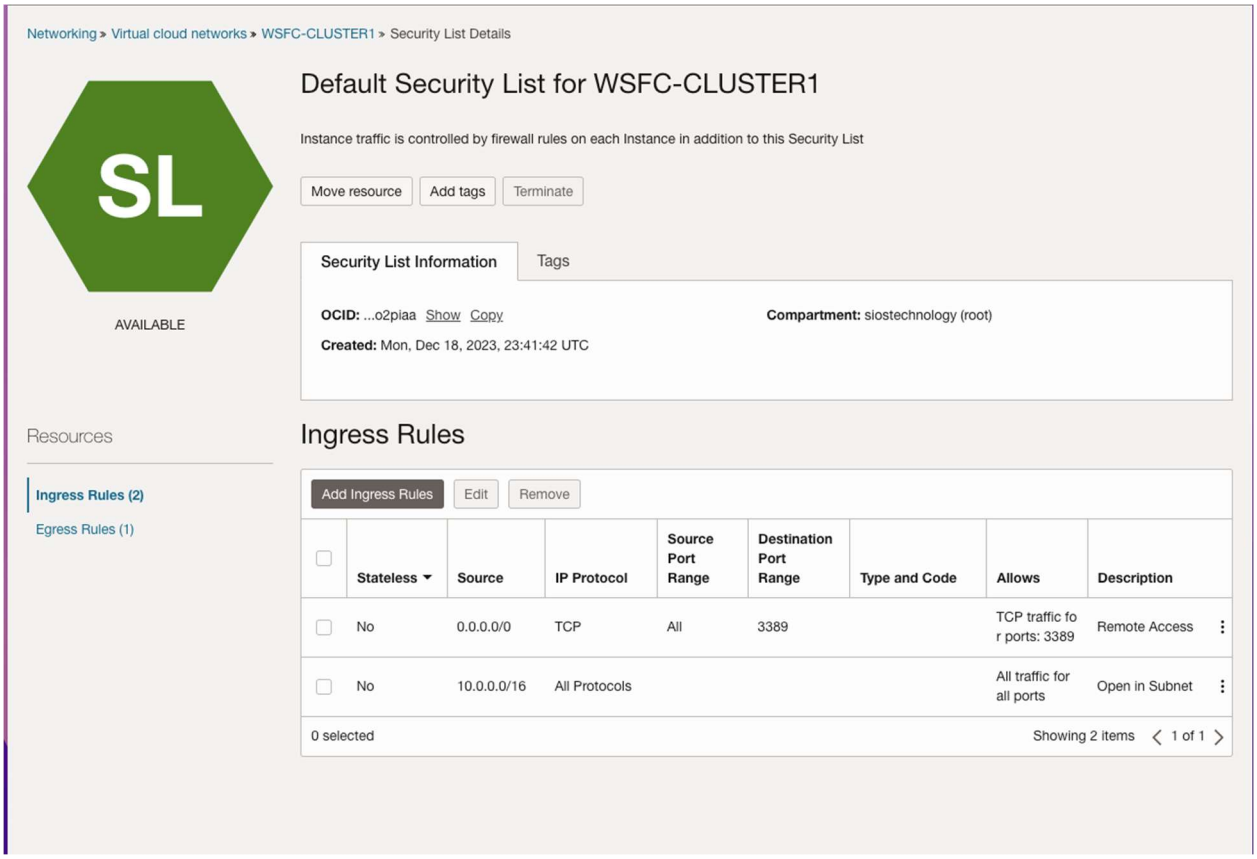

Create Subnet
Name
AD3
Create In Compartment
siostechnology (root)
Subnet Type
Regional (Recommended)
Instances in the subnet can be created in any availability domain in the region. Useful for high availability.
Availability Domain-specific
Instances in the subnet can only be created in one availability domain in the region.
Availability Domain
NqZI:US-ASHBURN-AD-3
IPv4 CIDR Block
IPv4 CIDR Block
10.0.128.0/18
Specified IP addresses: 10.0.128.0-10.0.191.255 (16,384 IP addresses)
IPv6 Prefixes
Maximum amount of 0 IPv6 prefixes per Subnet. IP ranges of the IPv6 prefixes must not overlap. Learn more.
Route Table Compartment in siostechnology (root) (Change compartment)
Default Route Table for WSFC-CLUSTER1
Subnet Access
Private Subnet
Prohibit public IP addresses for Instances in this Subnet
Public Subnet
Allow public IP addresses for Instances in this Subnet
DNS Resolution
Use DNS hostnames in this Subnet
Allows assignment of DNS hostname when launching an Instance.
DNS Label
AD3
Only letters and numbers, starting with a letter. 15 characters max.
DNS Domain Name Read-only
<dns-label>.wsfccluster1.oraclevcn.com
Dhcp Options Compartment in siostechnology (root) (Change compartment)
Default DHCP Options for WSFC-CLUSTER1
Security Lists
You can associate up to 5 network security lists with the subnet.
Security List Compartment in siostechnology (root) (Change compartment)
Default Security List for WSFC-CLUSTER1
+ Another Security List
Resource logging
Enable resource logging to allow resource tracking, troubleshooting, and data insights
Resource logging disabled
Show Tagging Options
Create Subnet
Cancel
Copyright © 2023, Oracle and/or its affiliates. All rights reserved.

Create the Internet gateway

The internet gateway is how our instances will gain access to the internet. In your network you may not want your instances to be able to access the internet, but for this example we will enable it and add it to our default route table.

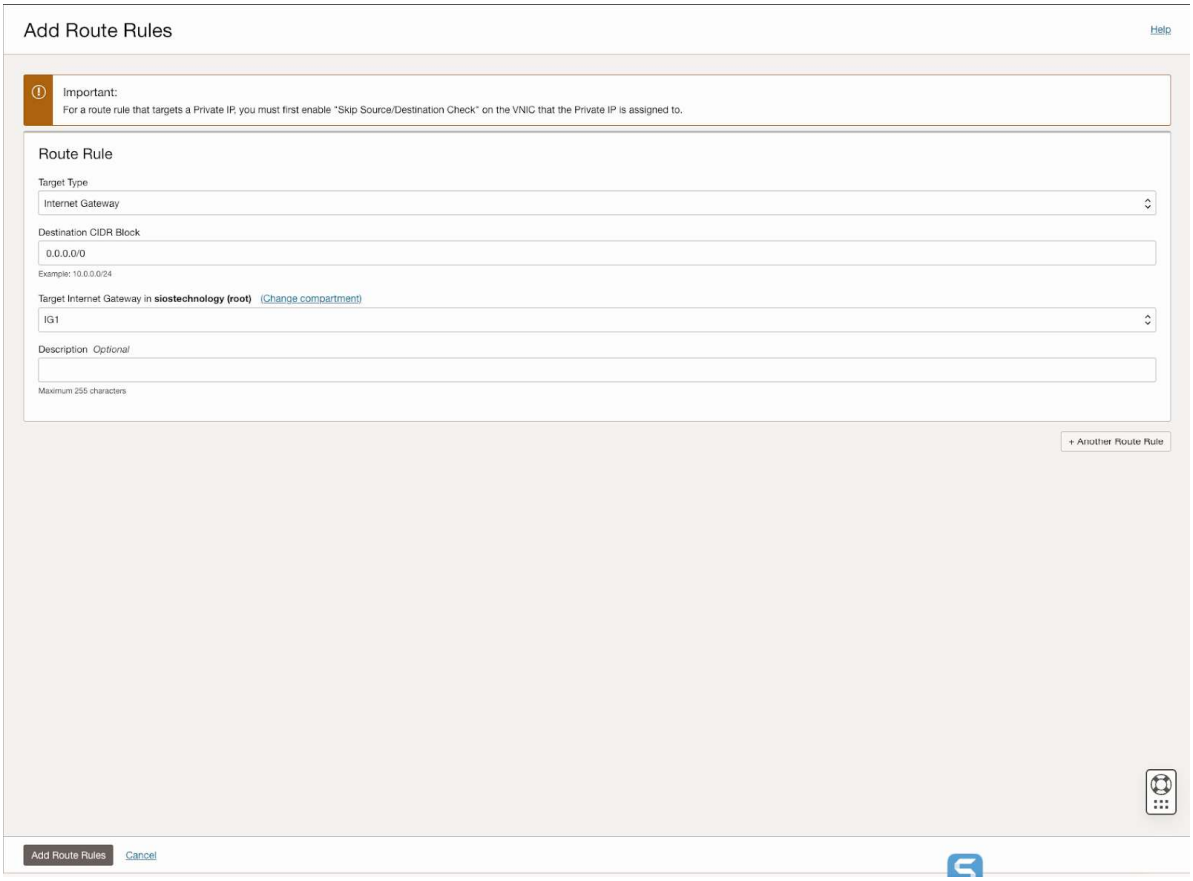


Edit the Default Security List

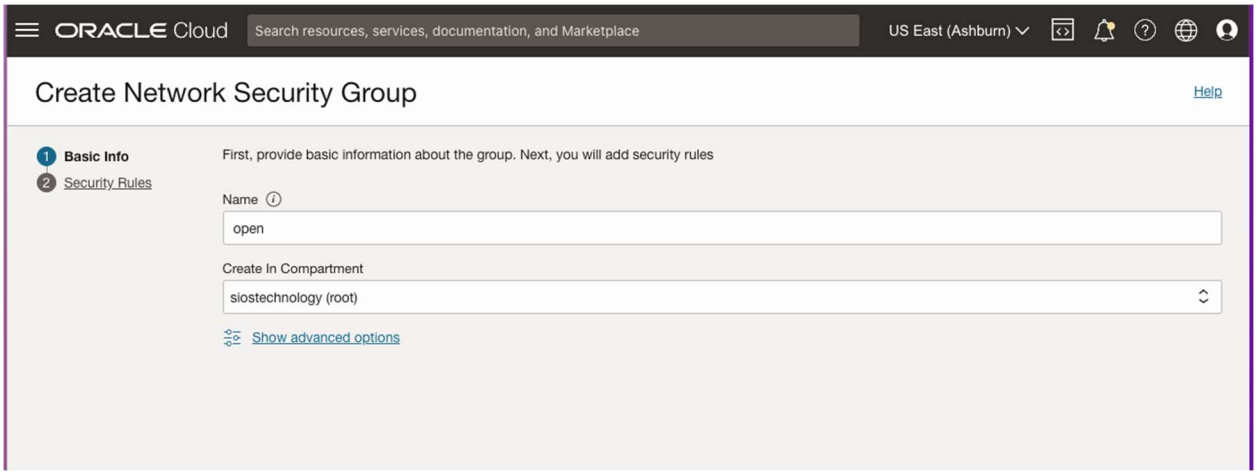


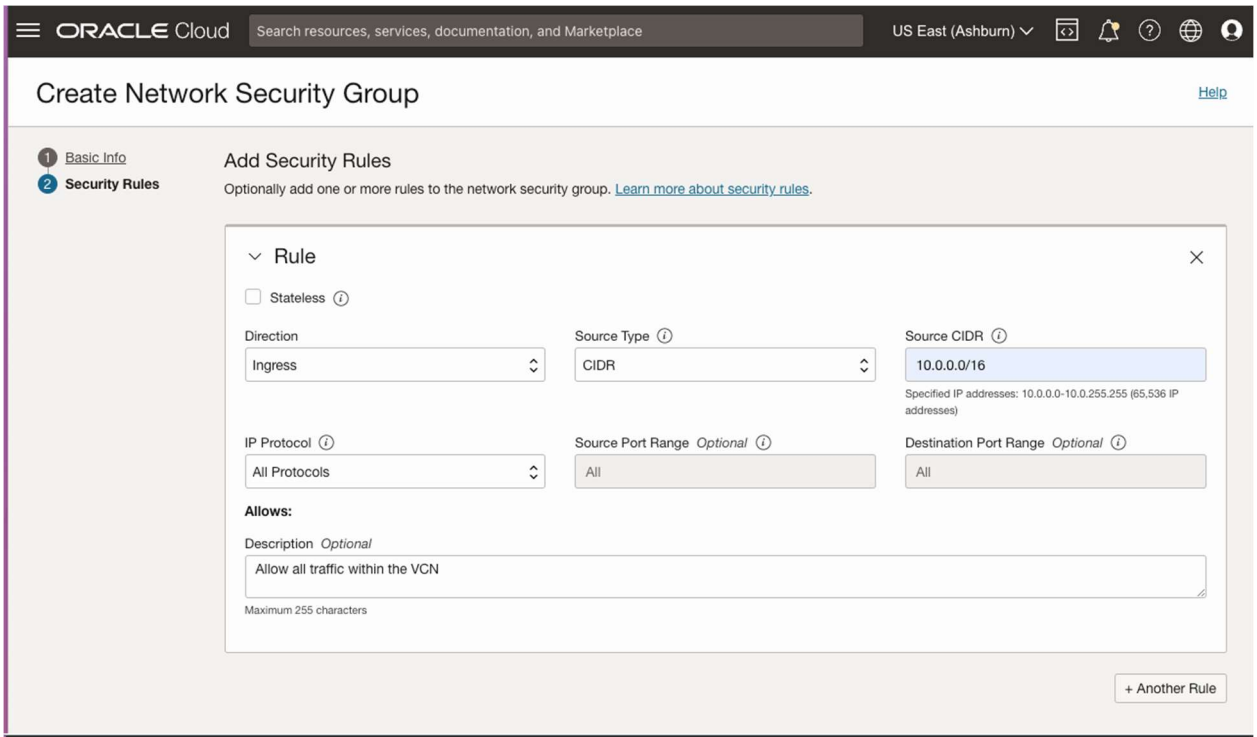
Edit the route table

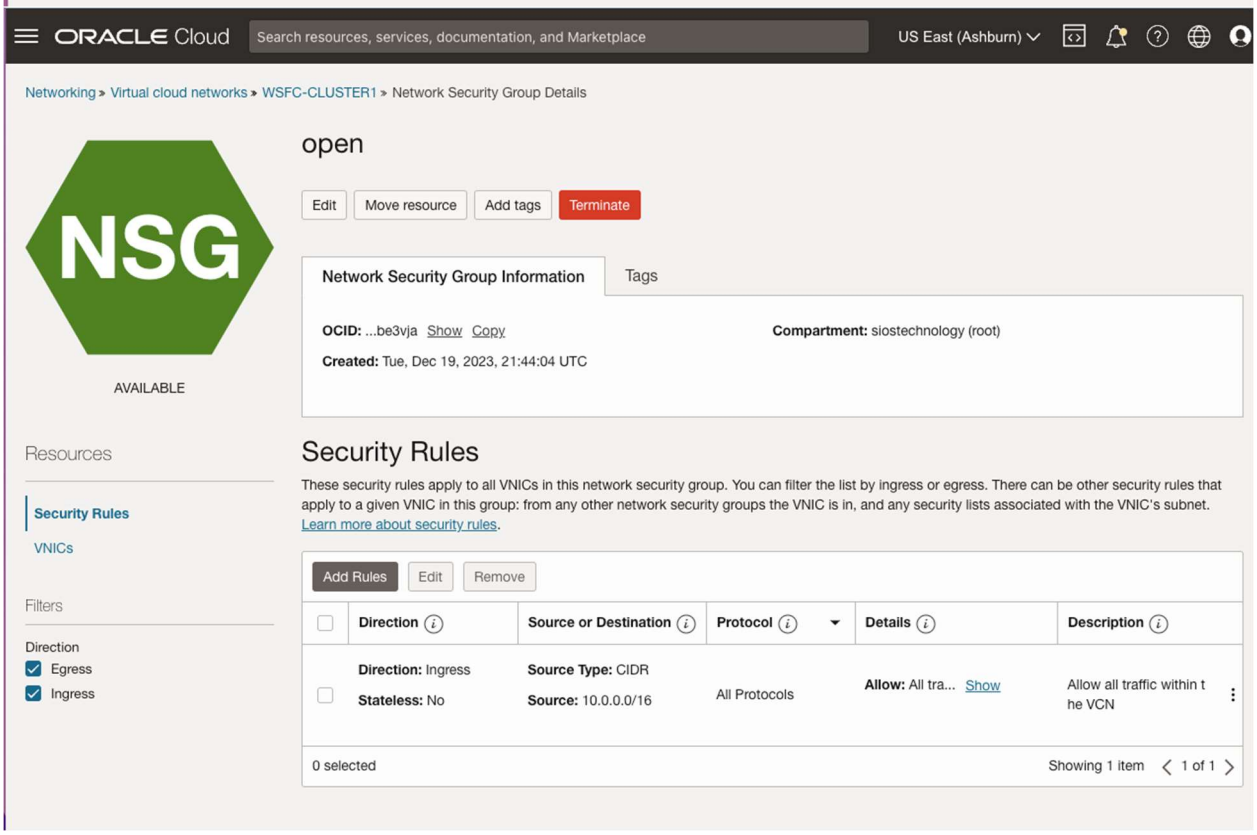
Edit the route table so that all traffic destined for outside the VCN is routed through the internet gateway.



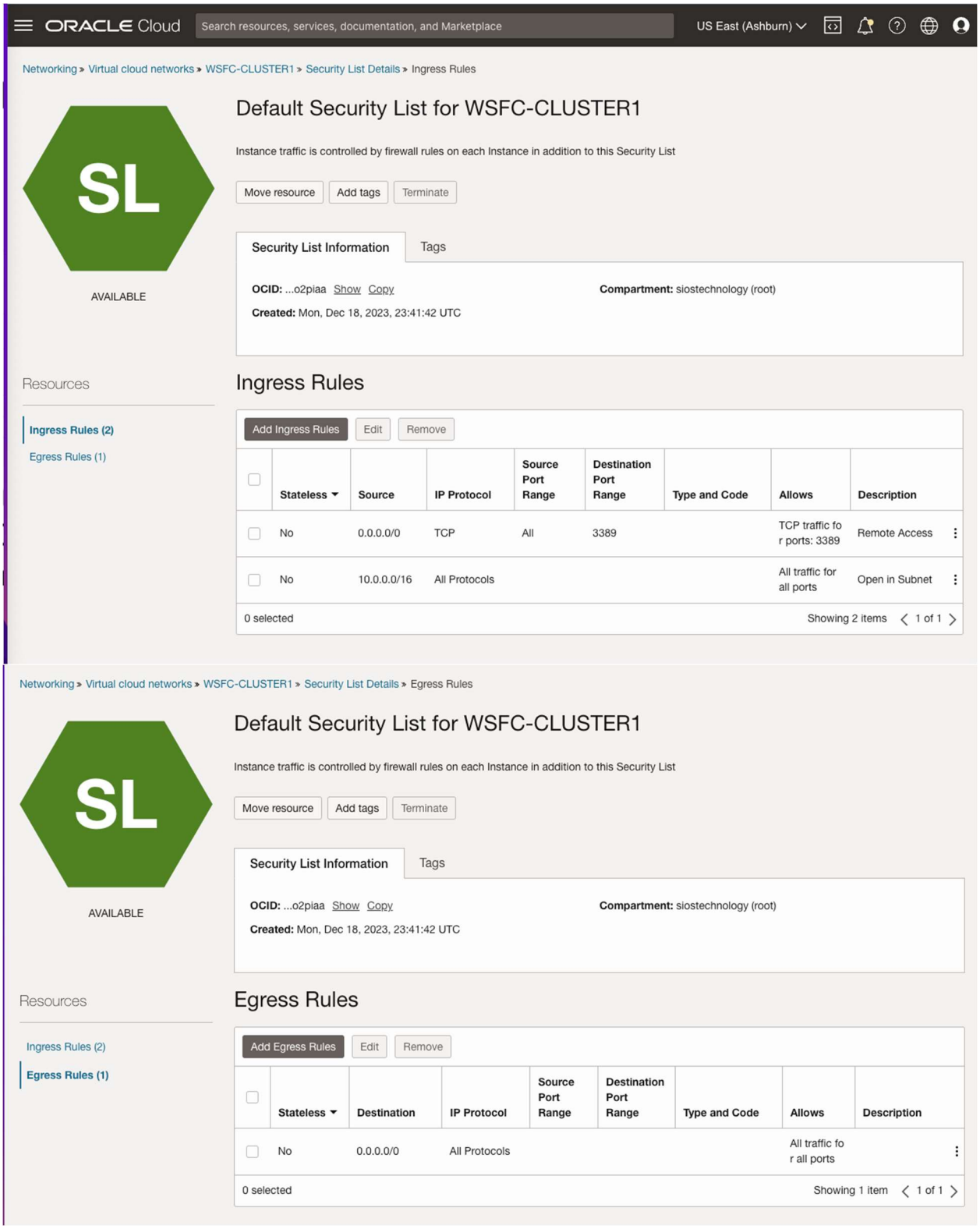
Create Network Security Group




ORACLE Cloud
Search resources, services, documentation, and Marketplace
US East (Ashburn)
Create Network Security Group
Help
1 Basic Info
2 Security Rules
Add Security Rules
Optionally add one or more rules to the network security group. Learn more about security rules.
Rule
Stateless
Direction
Ingress
Source Type
CIDR
Source CIDR
10.0.0.0/16
Specified IP addresses: 10.0.0.0-10.0.255.255 (65,536 IP addresses)
IP Protocol
All Protocols
Source Port Range Optional
All
Destination Port Range Optional
All
Allows:
Description Optional
Allow all traffic within the VCN
Maximum 255 characters
+ Another Rule


ORACLE Cloud
Search resources, services, documentation, and Marketplace
US East (Ashburn)
Networking > Virtual cloud networks > WSFC-CLUSTER1 > Network Security Group Details
NSG
AVAILABLE
open
Edit
Move resource
Add tags
Terminate
Network Security Group Information
Tags
OCID: ...be3vja Show Copy
Compartment: siostechnology (root)
Created: Tue, Dec 19, 2023, 21:44:04 UTC
Resources
Security Rules
VNICs
Filters
Direction
Egress
Ingress
Security Rules
These security rules apply to all VNICs in this network security group. You can filter the list by ingress or egress. There can be other security rules that apply to a given VNIC in this group: from any other network security groups the VNIC is in, and any security lists associated with the VNIC's subnet.
Learn more about security rules.
Add Rules
Edit
Remove
Direction
Source or Destination
Protocol
Details
Description
Direction: Ingress
Stateless: No
Source Type: CIDR
Source: 10.0.0.0/16
All Protocols
Allow: All tra... Show
Allow all traffic within the VCN
0 selected
Showing 1 item
1 of 1

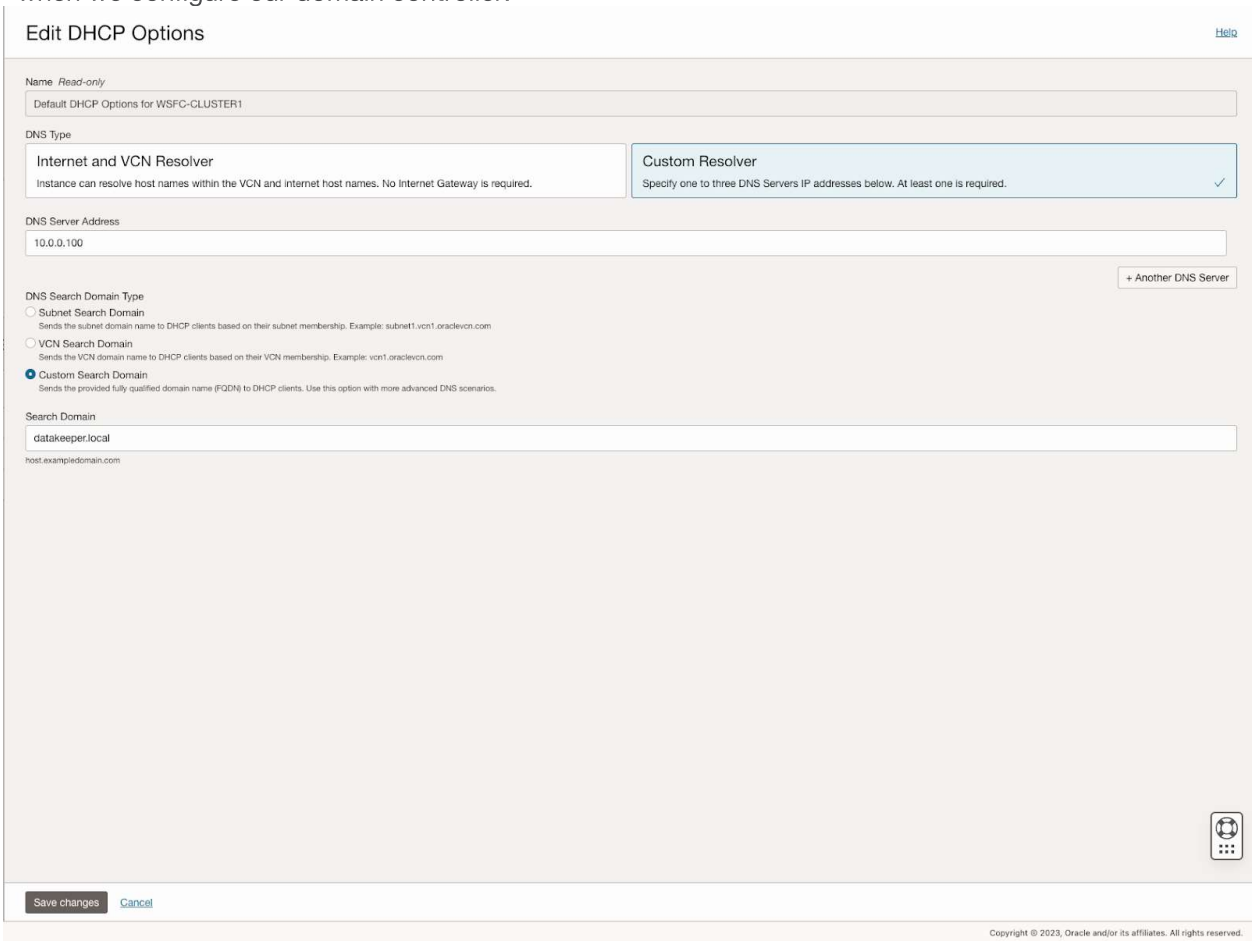
Edit the security list



These settings allow unfettered access across availability domains, and allows RDP access from anywhere. You may consider limiting which IP addresses can RDP to your instances or even setting up a “jump VM” used exclusively for RDP access from the public network.

Edit DHCP options

For active directory to work correctly, you must set the DC1 as the primary DNS server in the DHCP options as shown below. In this case, we set it to 10.0.0.100, which is the static IP of the domain controller we are configuring. You should also add your domain to the custom search domain. In this case, we will use the domain called datakeeper.local, which we will build later when we configure our domain controller.



Provision the VMs

Now that the VCN is configured, it is time to start provisioning the VMs. In this example we are going to use Windows Server 2022 and SQL Server 2019. However, the steps described in this article are almost identical across all versions of Windows Server and SQL Server, so you shouldn't have any issues regardless of which version of Windows or SQL Server you plan to use.

Before you begin, it is once again important to start with a plan. In this case you will want to plan your server names, IP addresses and their availability zone placement. As mentioned earlier, each cluster node and the file share witness must each reside in a different availability zone.

In the example configuration, we will deploy active-directory in an instance (DC1) that will also act as a file share witness.

AD1 - DC1 (10.0.0.100)

AD2 - SQL1 - (10.0.64.100, 10.0.64.101, 10.0.64.102)

AD3 - SQL2 - (10.0.128.100, 10.0.128.101, 10.0.128.102)

You may have noticed that each of the cluster nodes (SQL1, SQL2) have three IP addresses.

The first address is the private IP address of the instance. The other two IP addresses will be added as secondary addresses on each instance. These IP addresses account for the core cluster IP address and the virtual IP address associated with the SQL Server FCI network name resource.

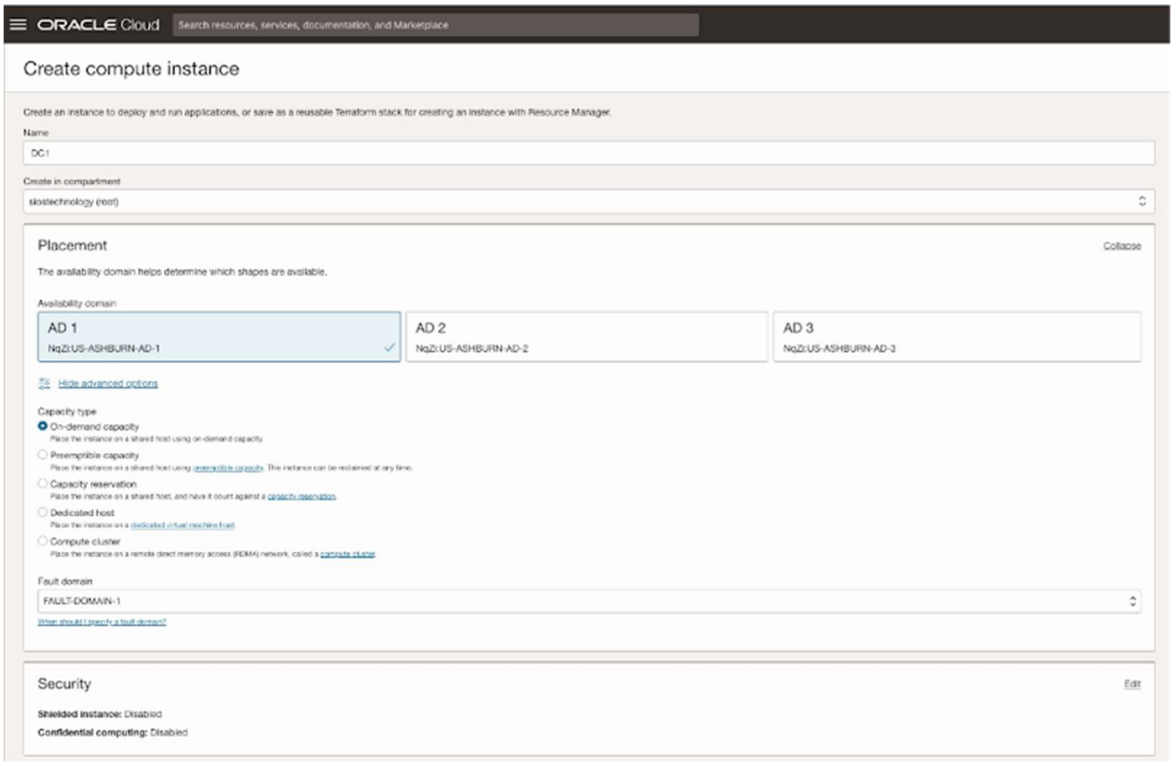
When we provision the cluster nodes we will use the base Windows Server 2022 images with no SQL Server software included. Instead we will download the SQL Server installation media and use a perpetual SQL Server license instead of the “pay-as-you-go” licensing available on the Marketplace.

The following sections illustrate the process of provisioning the three VMs used in this example.

Provision DC1 in FD1

When choosing an instance type you must size it properly for the workload. This is similar to what you would do if you were sizing a physical server to use on-premises, but the difference is that you can adjust the size easily if you over-provision, or under-provision the first time, or if your workload increases or decreases over time.

When specifying the instance details, make sure you choose the right VCN and the subnet for proper placement. On this first screen you also specify the static IP you want to associate with this instance.



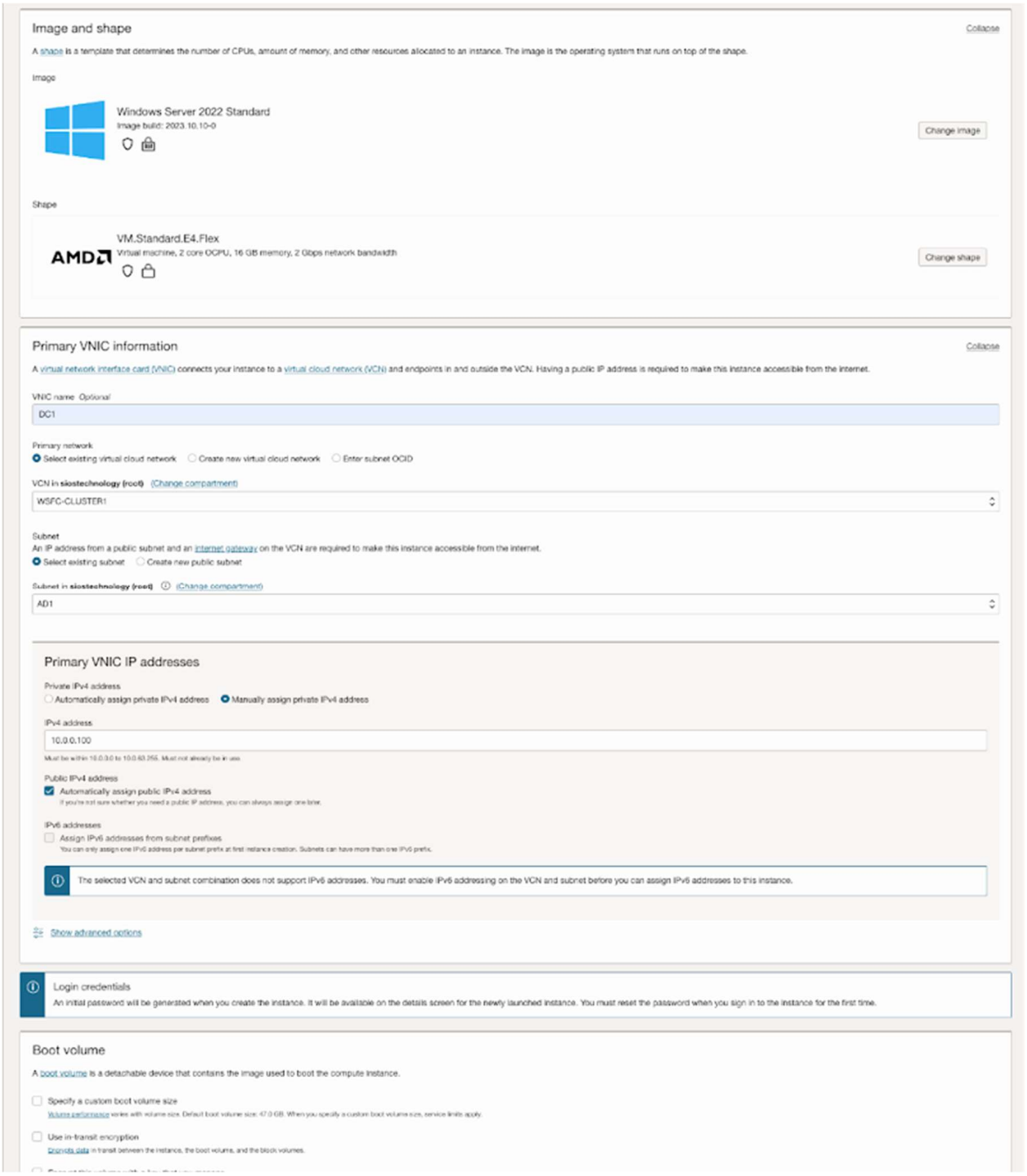
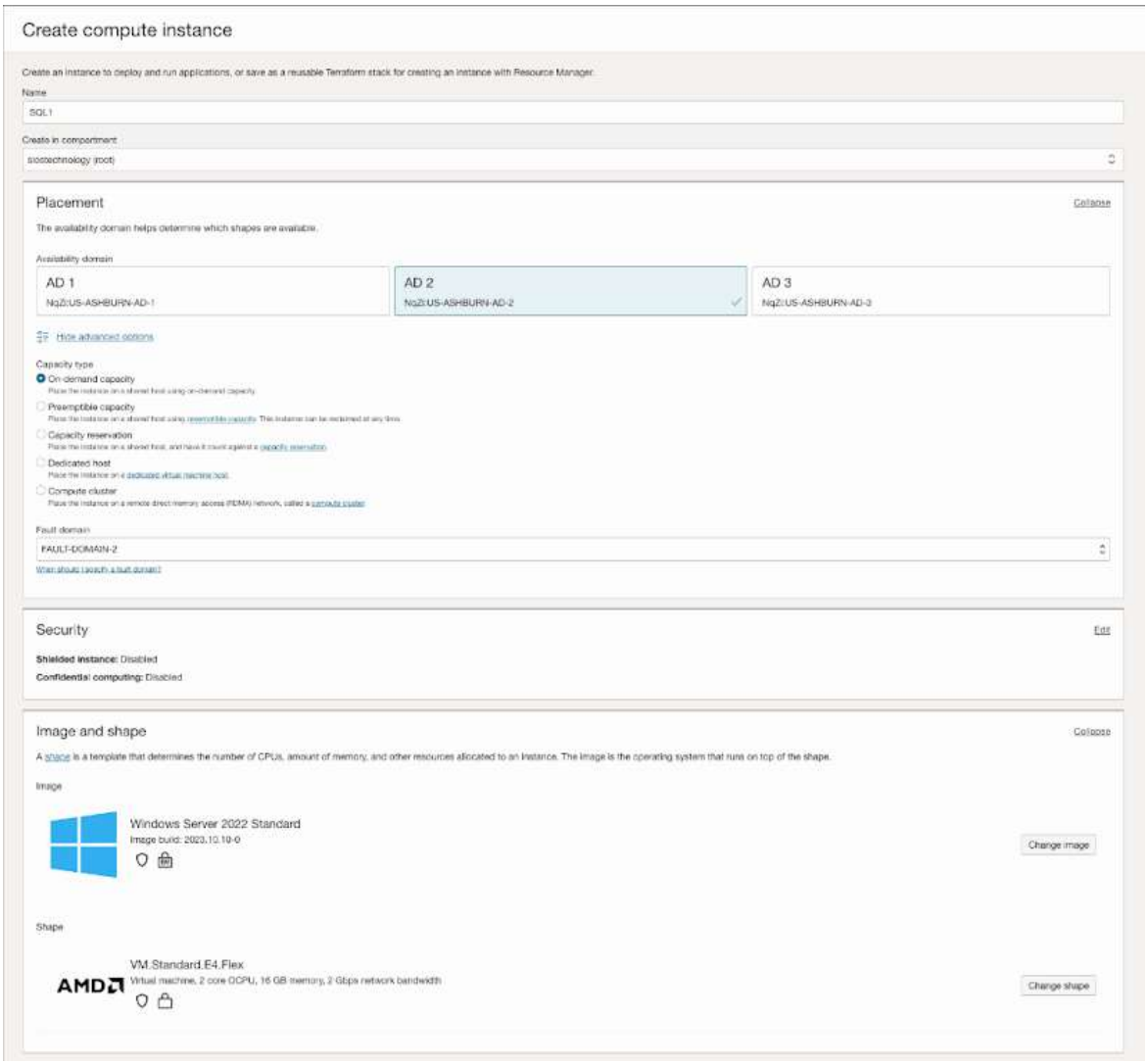
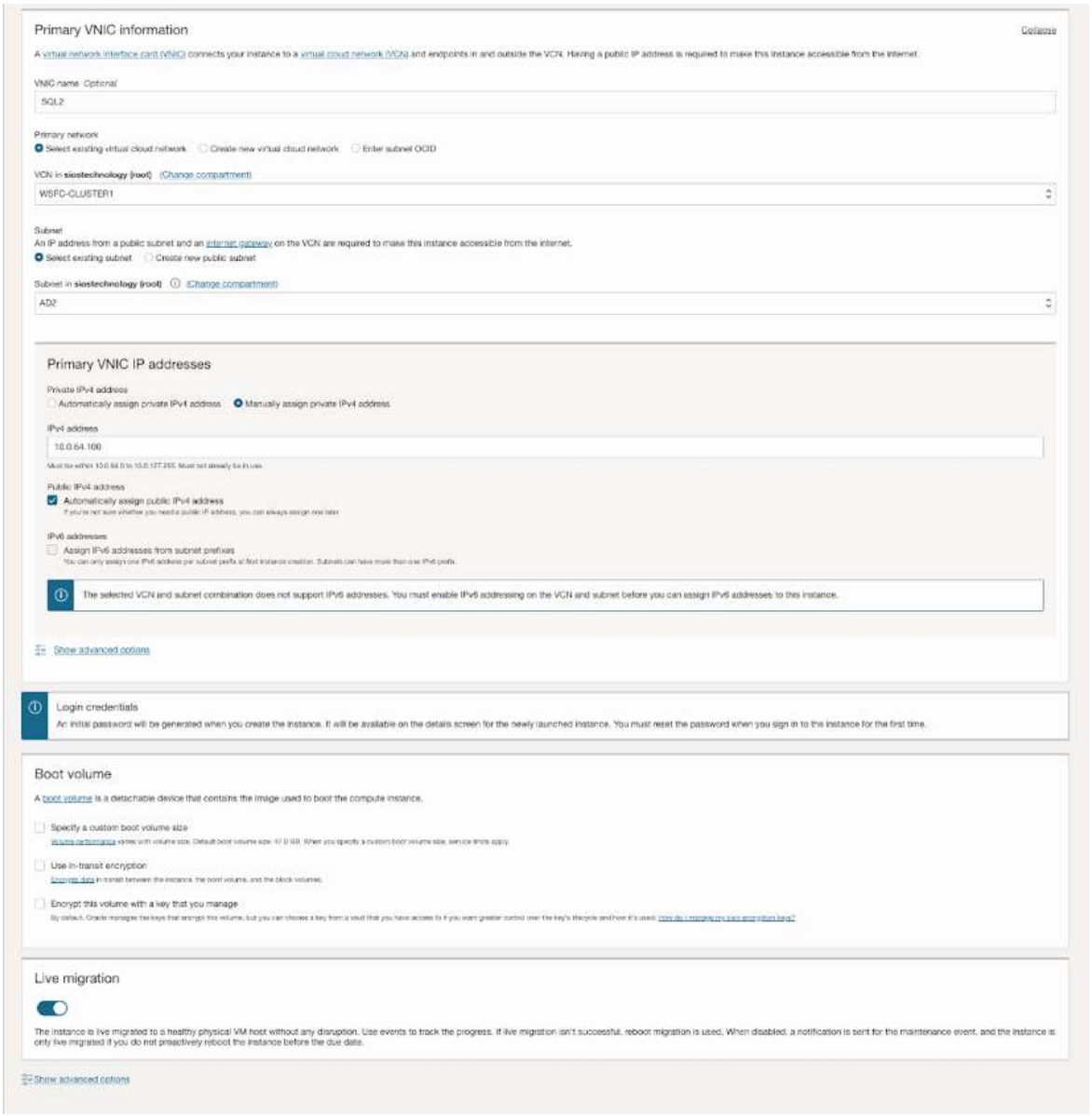


Image and shape
Collapse
A shape is a template that determines the number of CPUs, amount of memory, and other resources allocated to an instance. The image is the operating system that runs on top of the shape.
Image
Windows Server 2022 Standard
Image build: 2023.10.10-0
Change image
Shape
VM.Standard.E4.Flex
Virtual machine, 2 core OCPU, 16 GB memory, 2 Gbps network bandwidth
Change shape
Primary VNIC information
Collapse
A virtual network interface card (VNIC) connects your instance to a virtual cloud network (VCN) and endpoints in and outside the VCN. Having a public IP address is required to make this instance accessible from the internet.
VNIC name Optional
DC1
Primary network
Select existing virtual cloud network
Create new virtual cloud network
Enter subnet OCID
VCN in siostechnology (root) (Change compartment)
WSFC-CLUSTER1
Subnet
An IP address from a public subnet and an internet gateway on the VCN are required to make this instance accessible from the internet.
Select existing subnet
Create new public subnet
Subnet in siostechnology (root) (Change compartment)
AD1
Primary VNIC IP addresses
Private IPv4 address
Automatically assign private IPv4 address
Manually assign private IPv4 address
IPv4 address
10.0.0.100
Public IPv4 address
Automatically assign public IPv4 address
IPv6 addresses
Assign IPv6 addresses from subnet prefixes
The selected VCN and subnet combination does not support IPv6 addresses. You must enable IPv6 addressing on the VCN and subnet before you can assign IPv6 addresses to this instance.
Show advanced options
Login credentials
An initial password will be generated when you create the instance. It will be available on the details screen for the newly launched instance. You must reset the password when you sign in to the instance for the first time.
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
Use in-transit encryption

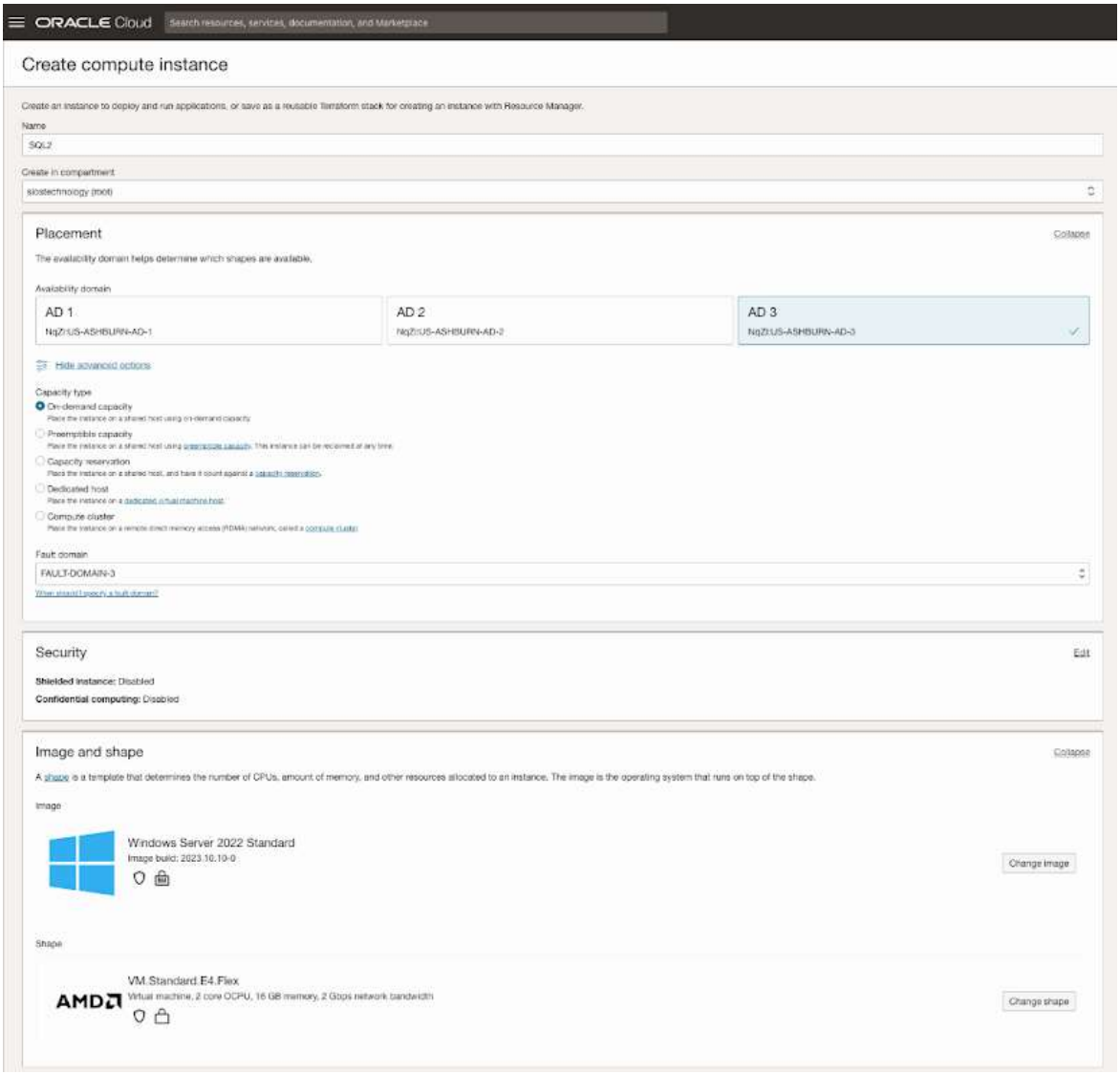
Provision SQL1 in FD2

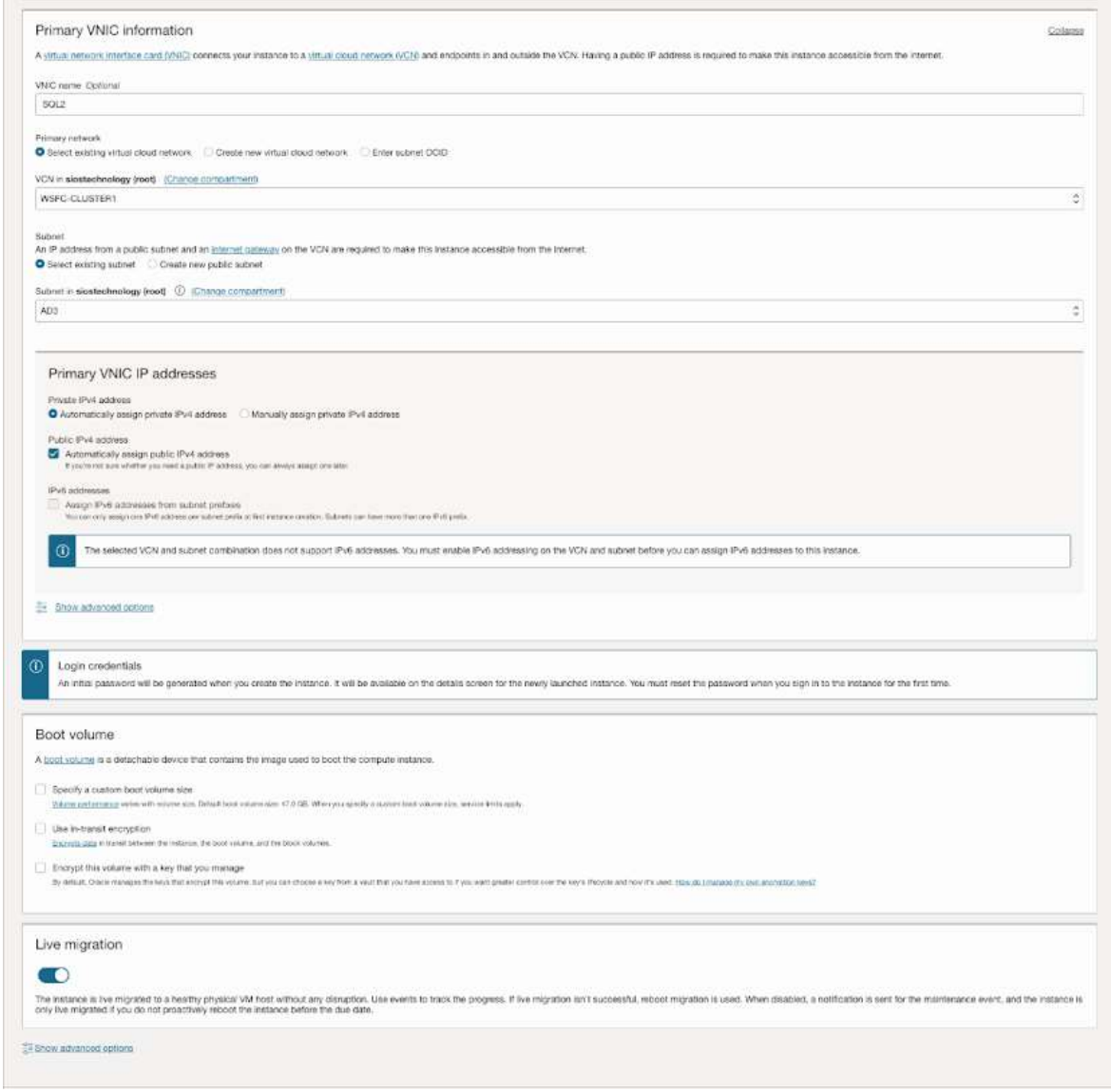
As discussed earlier, this example uses the base install of Windows Server 2022. SQL Server 2019 will be downloaded later and used for the SQL Server FCI installation.




Primary VNIC information
Collapse
A virtual network interface card (VNIC) connects your instance to a virtual cloud network (VCN) and endpoints in and outside the VCN. Having a public IP address is required to make this instance accessible from the internet.
VNIC name Optional
SQL2
Primary network
Select existing virtual cloud network
Create new virtual cloud network
Enter subnet OCID
VCN in siostechnology (root) (Change compartment)
WSFC-CLUSTER1
Subnet
An IP address from a public subnet and an internet gateway on the VCN are required to make this instance accessible from the internet.
Select existing subnet
Create new public subnet
Subnet in siostechnology (root) (Change compartment)
AD2
Primary VNIC IP addresses
Private IPv4 address
Automatically assign private IPv4 address
Manually assign private IPv4 address
IPv4 address
10.0.64.100
Public IPv4 address
Automatically assign public IPv4 address
IPv6 addresses
Assign IPv6 addresses from subnet prefixes
The selected VCN and subnet combination does not support IPv6 addresses. You must enable IPv6 addressing on the VCN and subnet before you can assign IPv6 addresses to this instance.
Show advanced options
Login credentials
An initial password will be generated when you create the instance. It will be available on the details screen for the newly launched instance. You must reset the password when you sign in to the instance for the first time.
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
Use in-transit encryption
Encrypt this volume with a key that you manage
Live migration
The instance is live migrated to a healthy physical VM host without any disruption. Use events to track the progress. If live migration isn't successful, reboot migration is used. When disabled, a notification is sent for the maintenance event, and the instance is only live migrated if you do not proactively reboot the instance before the due date.
Show advanced options

Provision SQL2 in FD3





Adding Additional Volumes

Each server in the cluster requires at least one additional volume. These volumes are crucial for the storage needs of the SQL Server FCI and are replicated by SIOS DataKeeper.

Multiple Volumes

You can add multiple volumes to separate your data, logs, and backups.

Storage Types: Various storage types are available to suit different requirements.

Attachment Methods

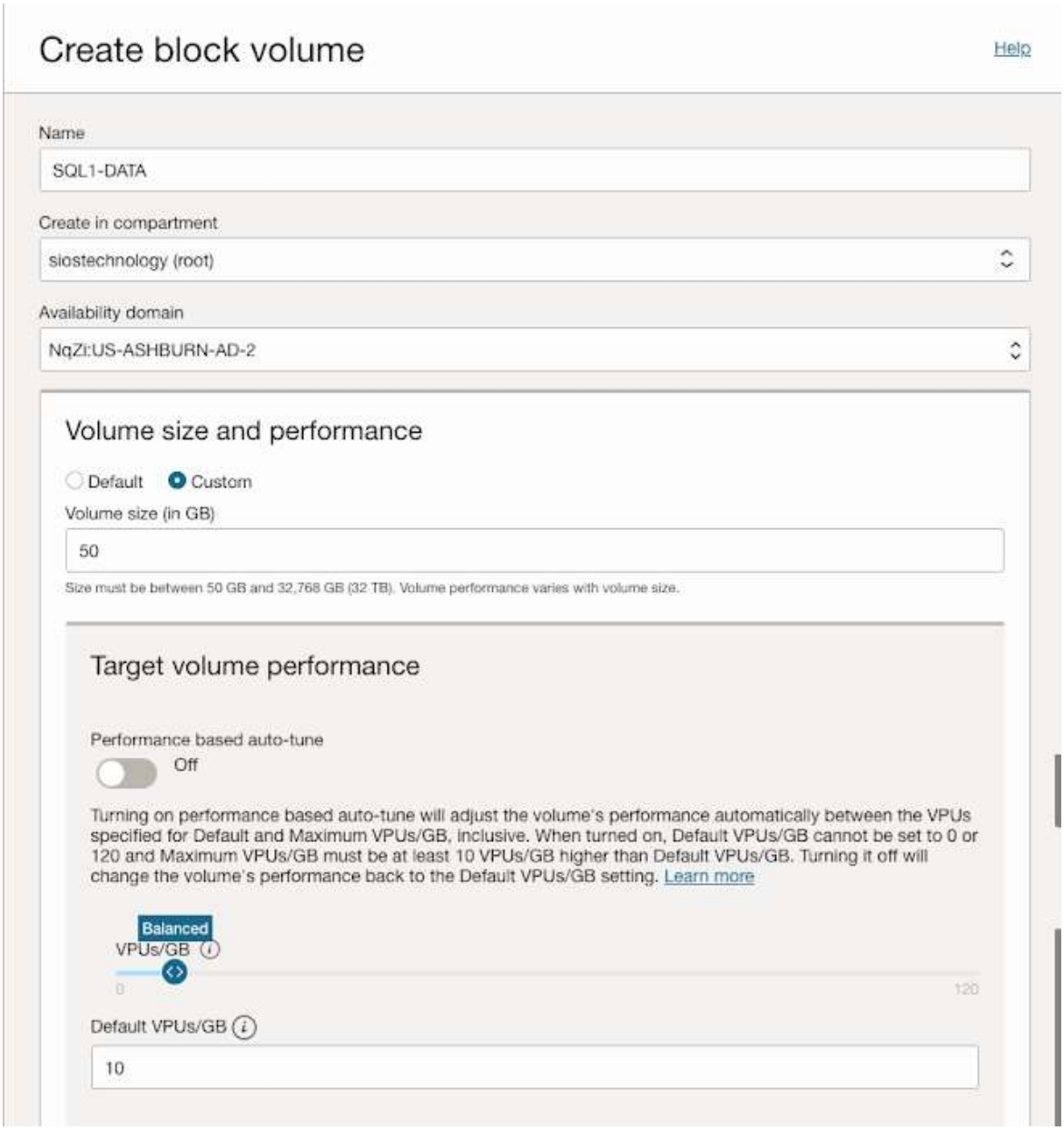
There are multiple ways to attach storage to your servers.

Example Configuration

Below, we have included screen captures demonstrating one of the many possible storage configurations. This serves as a practical example to aid in understanding the setup process. This process should be completed on SQL1 and SQL2.

Create Block Volumes

First, create the block volumes in the right Availability domain for SQL1 and SQL2.



IOPS: 3,000 IOPS

Throughput: 24 MB/s

Balanced choice for most workloads including those that perform random I/O such as boot disks. Learn more
Actual performance depends on the attached instance's shape. Select the appropriate instance shape to optimize performance. Learn more
See Oracle Storage Cloud Pricing for Volume Performance Units (VPUs) cost details.

Detached volume auto-tune

On

Turning on detached volume auto-tune will change the volume's performance automatically to Lower Cost when it is detached. When reattached, its performance is automatically adjusted to the previous setting. Learn more

Backup policies

Select backup policy in **siostechnology (root)** (Change compartment)

No Backup Policy Selected

Cross region replication

Enables asynchronous cross region volume replication. Learn more

ON OFF

Encryption

Encrypt using Oracle-managed keys
Leaves all encryption-related matters to Oracle.

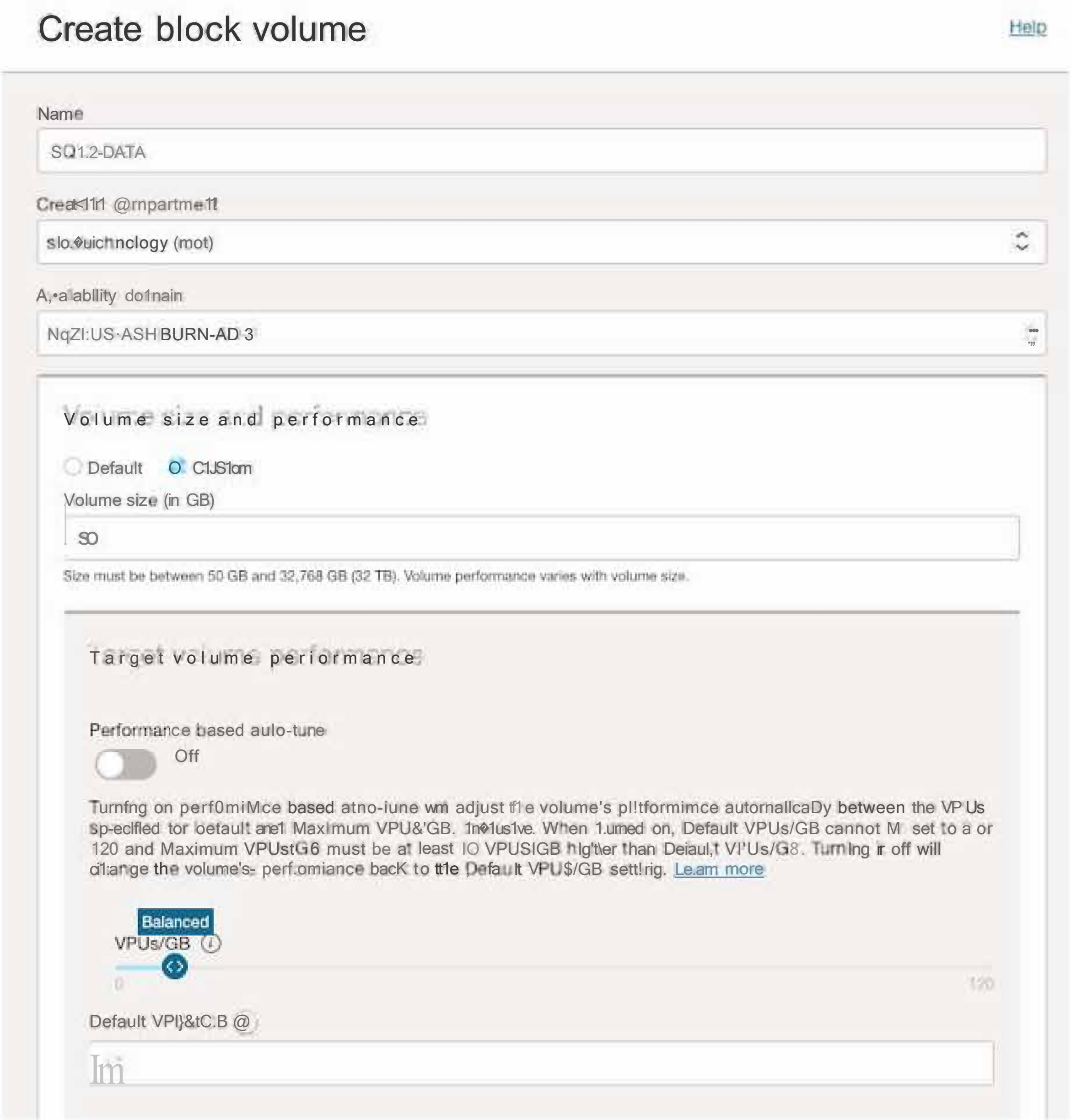
Encrypt using customer-managed keys
Requires you to have access to a valid Key Management key.

Show Tagging Options

View detail page after this block volume is created

Create Block Volume | Save as stack | Cancel

Copyright © 2023, Oracle and/or its affiliates. All rights reserved.


Create block volume
Help
Name
SQL2-DATA
Create in compartment
sios-technology (root)
Availability domain
NqZI:US-ASHBURN-AD-3
Volume size and performance
Default
Custom
Volume size (in GB)
50
Size must be between 50 GB and 32,768 GB (32 TB). Volume performance varies with volume size.
Target volume performance
Performance based auto-tune
Off
Turning on performance based auto-tune will adjust the volume's performance automatically between the VPUs specified for Default and Maximum VPUs/GB, inclusive. When turned on, Default VPUs/GB cannot be set to 0 or 120 and Maximum VPUs/GB must be at least 10 VPUs/GB higher than Default VPUs/GB. Turning it off will change the volume's performance back to the Default VPUs/GB setting. Learn more
Balanced
VPUs/GB
0
120
Default VPUs/GB

IOPS: 3,000 IOPS

Throughput: 24 MB/s

Balanced choice for most workloads including those that perform random I/O such as boot disks. Learn more
Actual performance depends on the attached instance's shape. Select the appropriate instance shape to optimize performance. Learn more
See Oracle Storage Cloud Pricing for Volume Performance Units (VPUs) cost details.

Detached volume auto-tune

On

Turning on detached volume auto-tune will change the volume's performance automatically to Lower Cost when it is detached. When reattached, its performance is automatically adjusted to the previous setting. Learn more

Backup policies

Select backup policy in **siostechnology (root)** (Change compartment)

No Backup Policy Selected

Cross region replication

Enables asynchronous cross region volume replication. Learn more

ON OFF

Encryption

Encrypt using Oracle-managed keys
Leaves all encryption-related matters to Oracle.

Encrypt using customer-managed keys
Requires you to have access to a valid Key Management key.

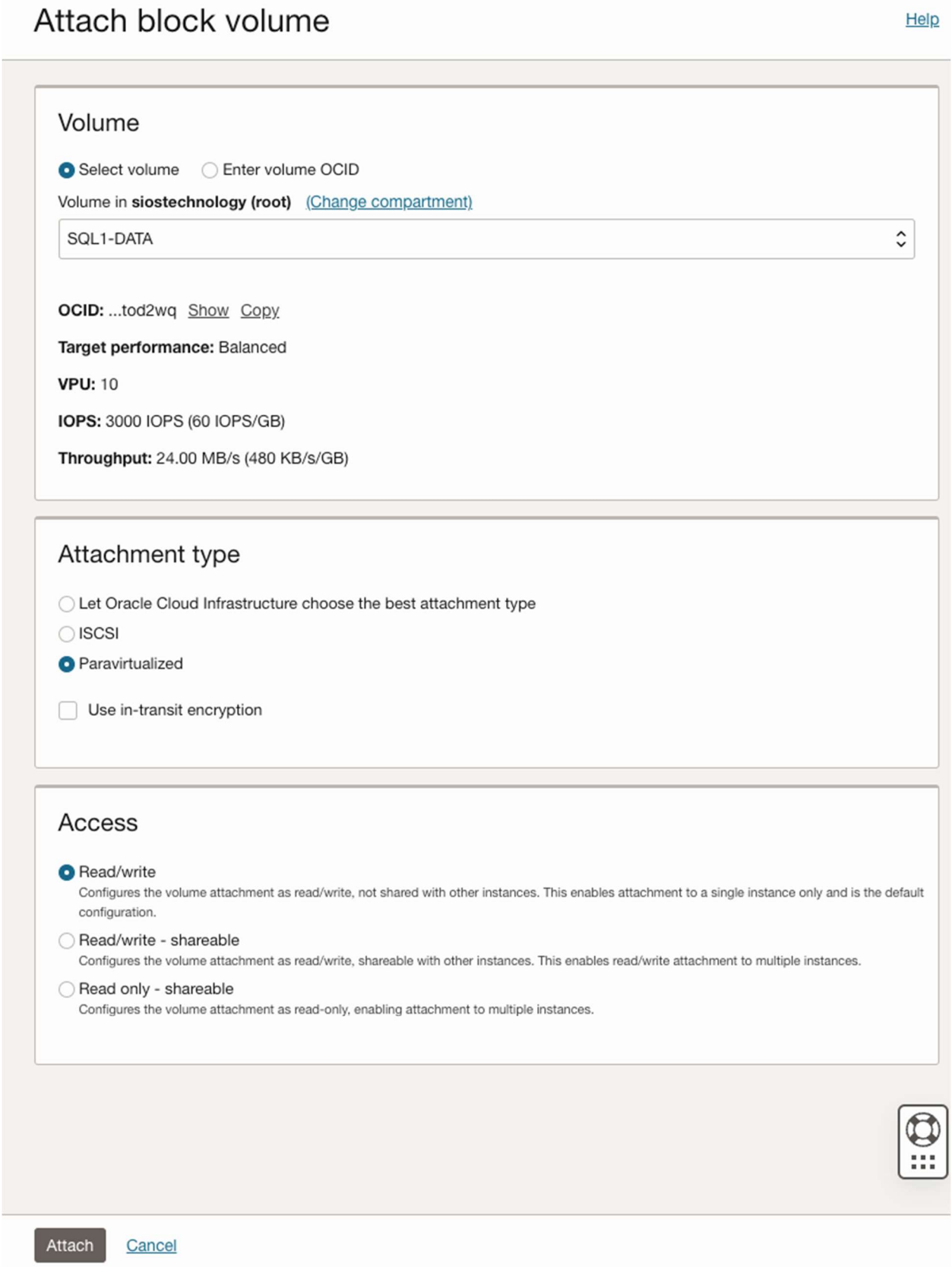
Show Tagging Options

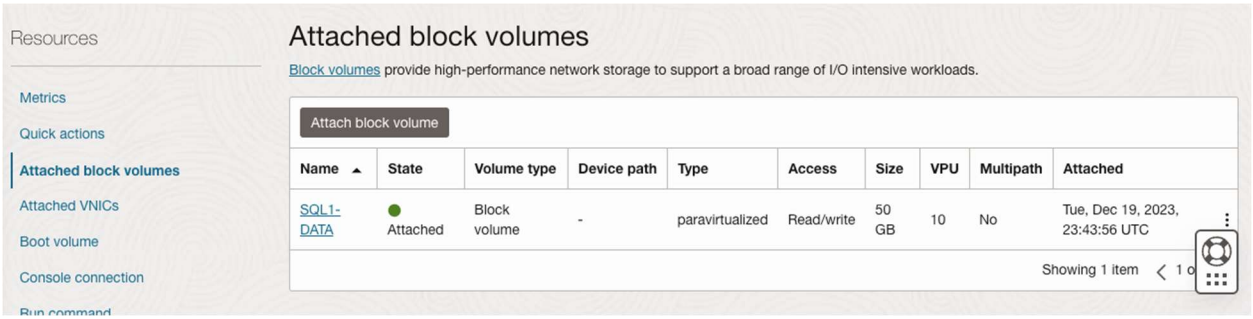
View detail page after this block volume is created

Create Block Volume | Save as stack | Cancel

Attach Volumes

Now that the volumes have been created, you must attach them to the instances.




Resources
Metrics
Quick actions
Attached block volumes
Attached VNICs
Boot volume
Console connection
Run command
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
VPU
Multipath
Attached
SQL1-DATA
Attached
Block volume
-
paravirtualized
Read/write
50 GB
10
No
Tue, Dec 19, 2023, 23:43:56 UTC
Showing 1 item

Attach block volume

Help

Volume

(•) Select volume ( ) Enter volume OCID

Volume in **siostechnology (root)** (Change compartment)

SQL2-DATA

OCID: ...vqfnpa Show Copy

Target performance: Balanced

VPU: 10

IOPS: 3000 IOPS (60 IOPS/GB)

Throughput: 24.00 MB/s (480 KB/s/GB)

Attachment type

( ) Let Oracle Cloud Infrastructure choose the best attachment type

( ) ISCSI

(•) Paravirtualized

[ ] Use in-transit encryption

Access

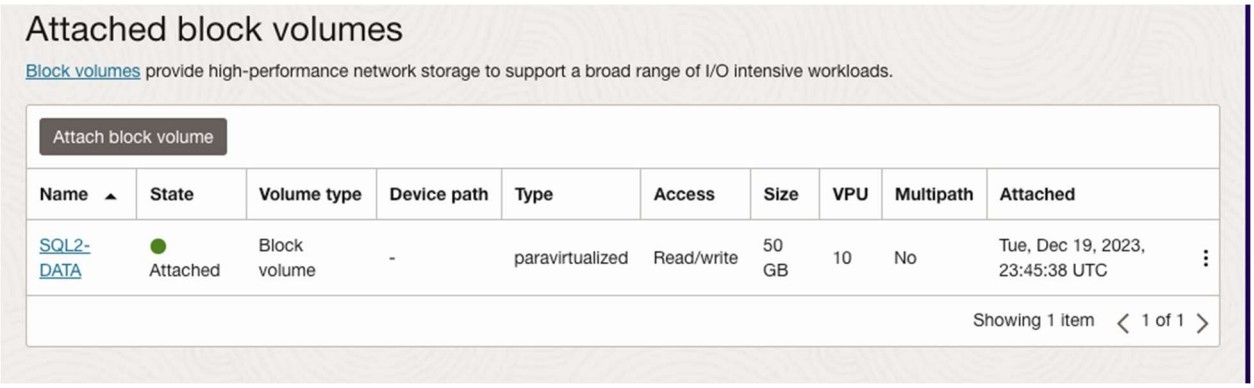
(•) Read/write
Configures the volume attachment as read/write, not shared with other instances. This enables attachment to a single instance only and is the default configuration.

( ) Read/write - shareable
Configures the volume attachment as read/write, shareable with other instances. This enables read/write attachment to multiple instances.

( ) Read only - shareable
Configures the volume attachment as read-only, enabling attachment to multiple instances.

Attach Cancel

Copyright © 2023, Oracle and/or its affiliates. All rights reserved.



Key Points to Remember

The setup is flexible. You can configure one or more volumes based on your specific needs.

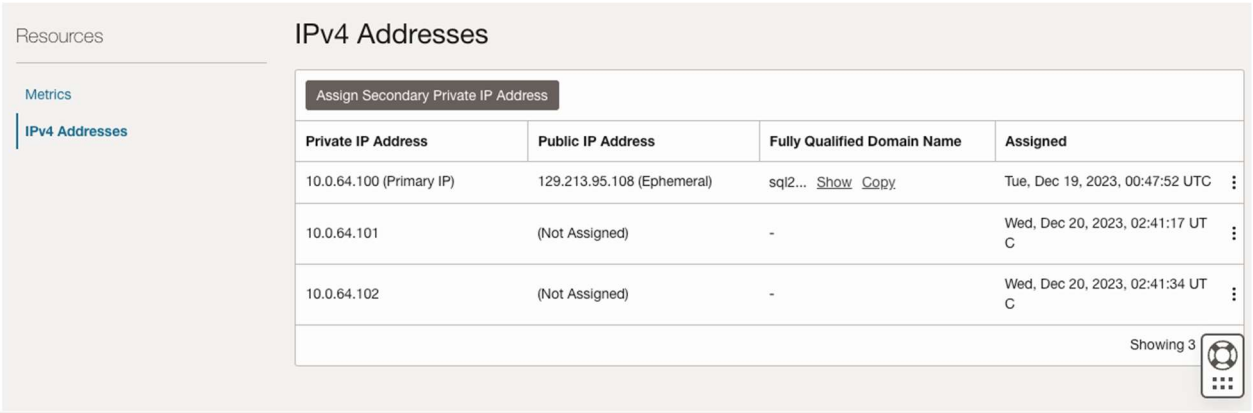
Consider different storage types and attachment methods available for your configuration.

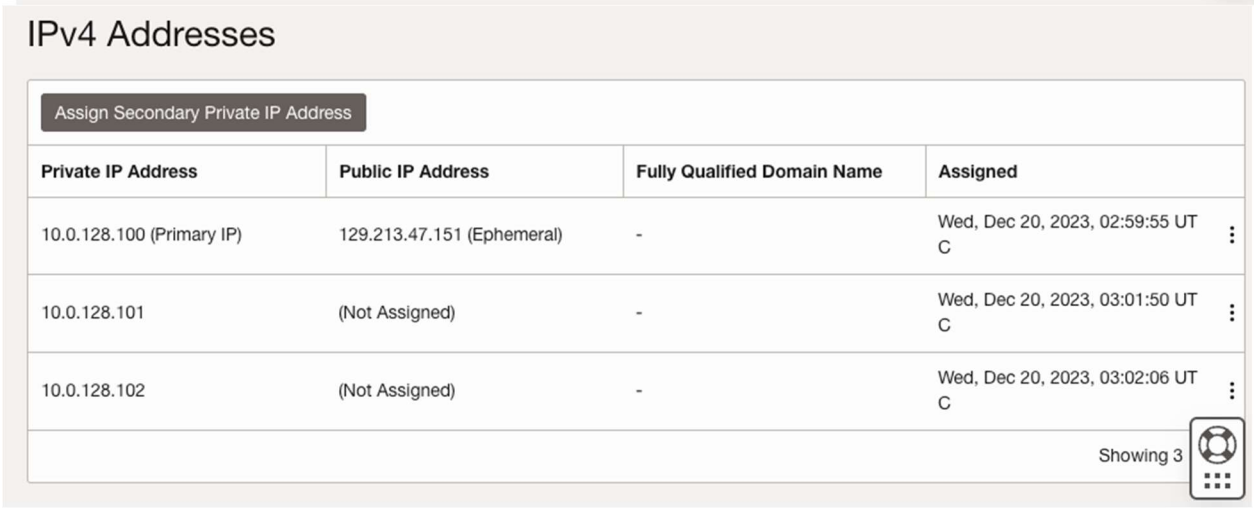
Add the Secondary IP Addresses

In order for Windows Server Failover Clustering to work properly in OCI, you have to add the cluster IP address as secondary address on the virtual network interface (VNIC) attached to SQL1 and SQL1. As you recall, we discussed using the following IP addresses on each of our cluster nodes.

	SQL1	SQL2
Primary Address	10.0.64.100	10.0.128.100
Cluster IP 1 (core cluster resource)	***10.0.64.101***	***10.0.128.101***
Cluster IP 2 (SQL Server Cluster IP)	***10.0.64.102***	***10.0.128.102***

On both SQL1 and SQL2, edit the attached VNIC to add the secondary addresses.

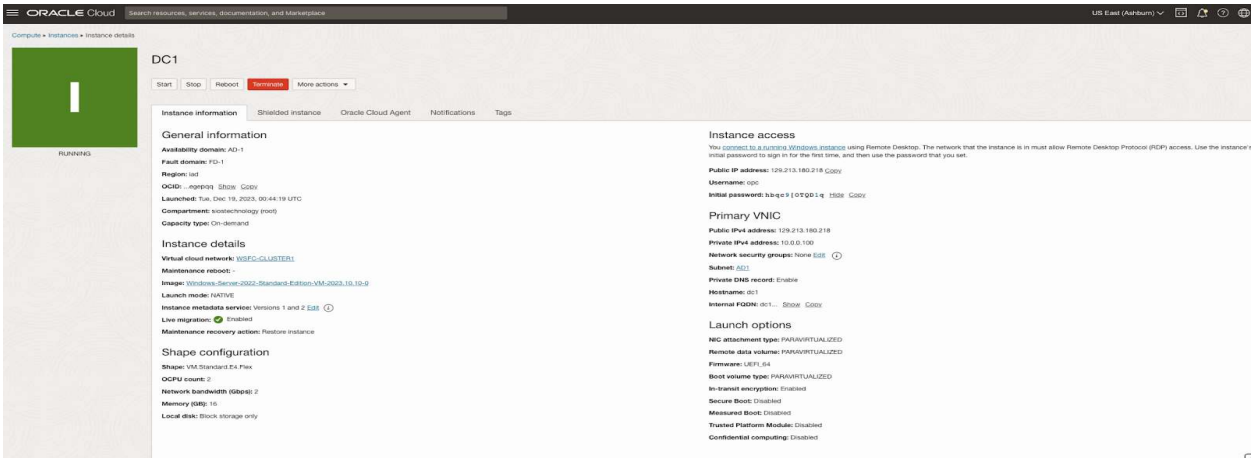




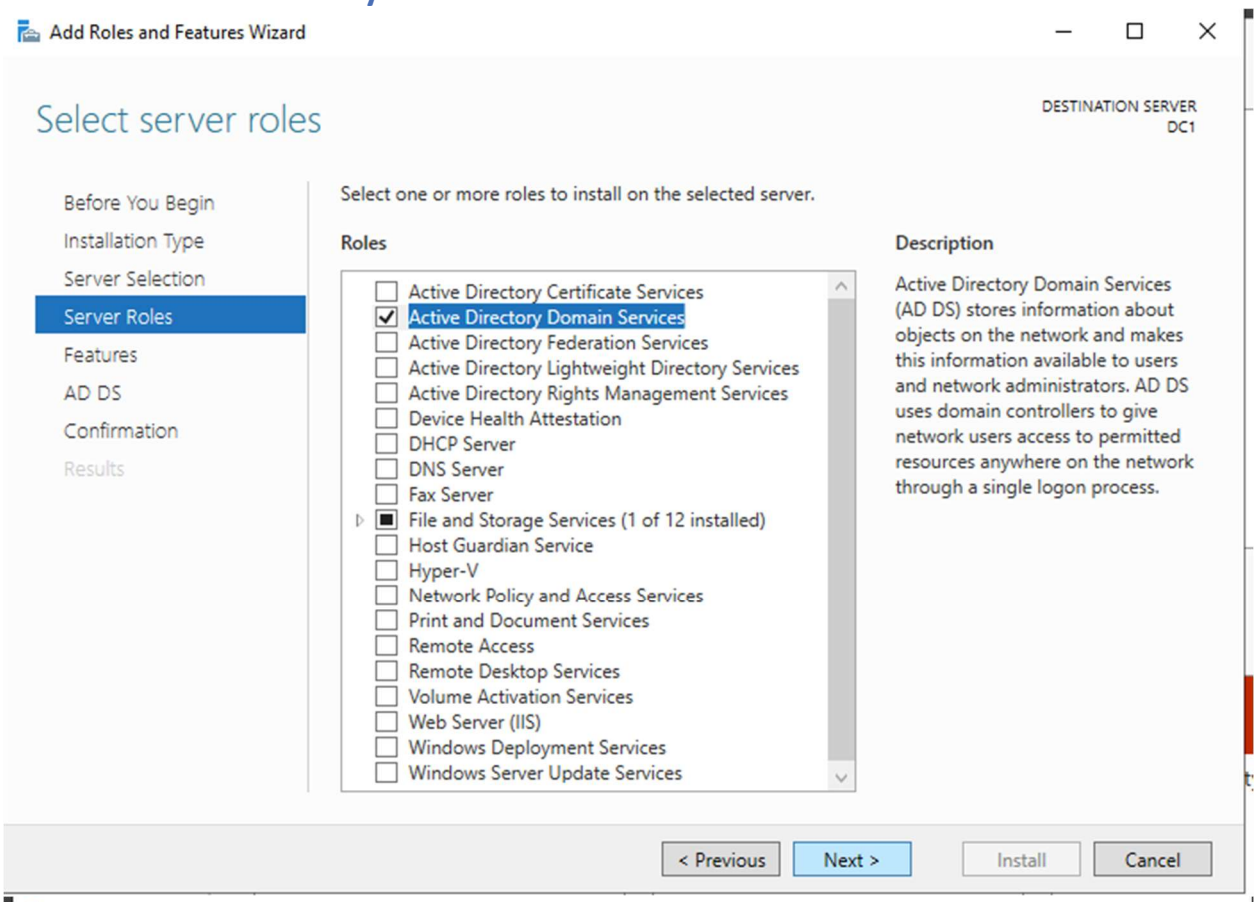
Create the Domain

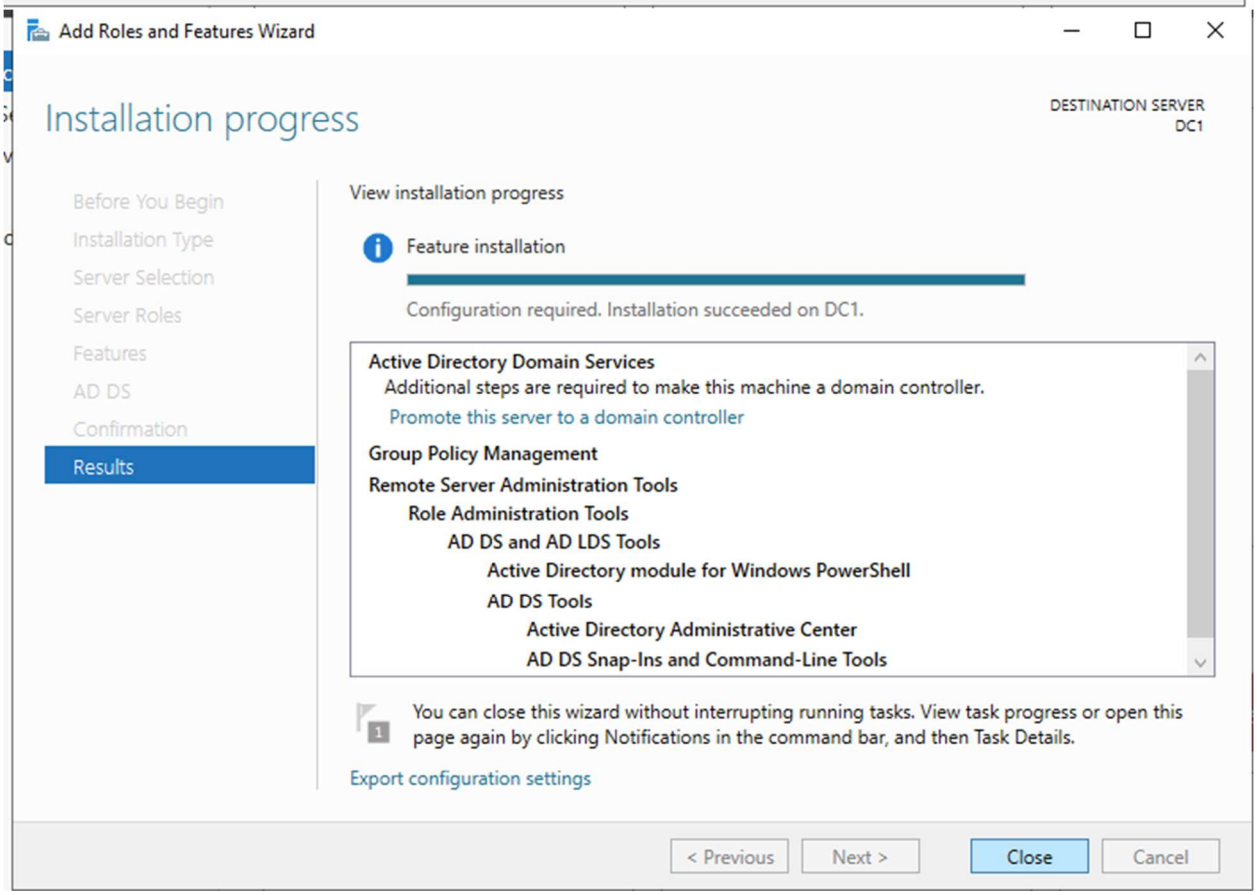
For resilience, you should provision multiple AD controllers across different availability zones, but for the purposes of this guide, we are just going to provision one AD controller. Follow the screenshots below to configure AD on DC1.

Log on using the credentials listed in the Instance Details section. You will be prompted to reset your password.



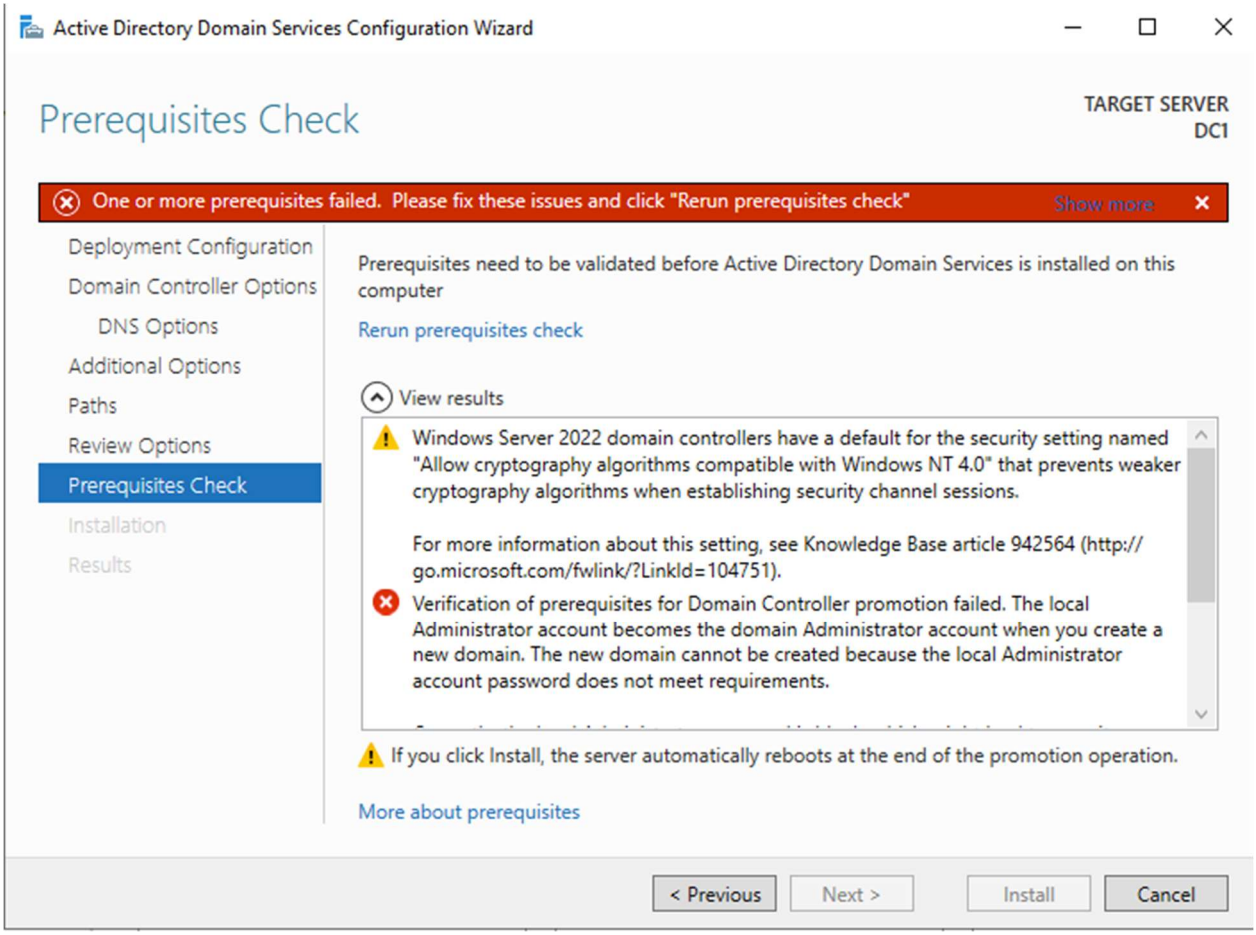
Enable Active Directory Domain Services



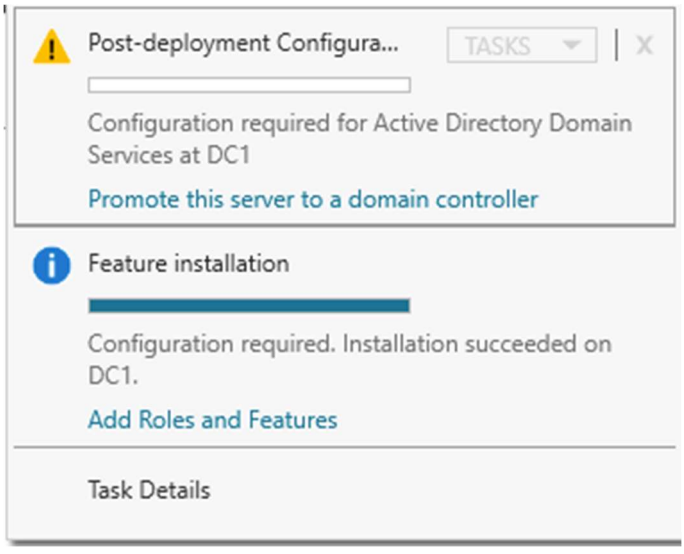


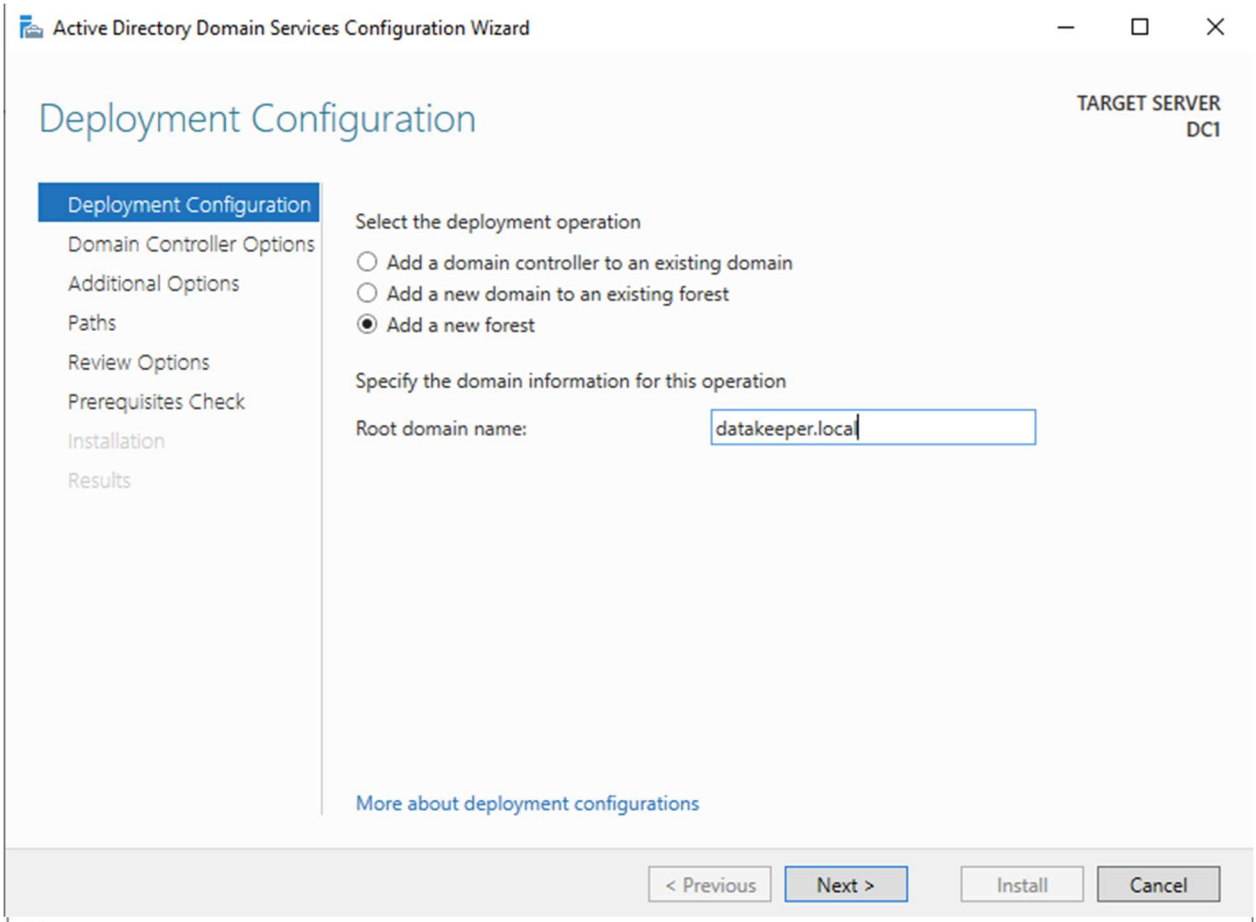
Promote Server to Domain Controller

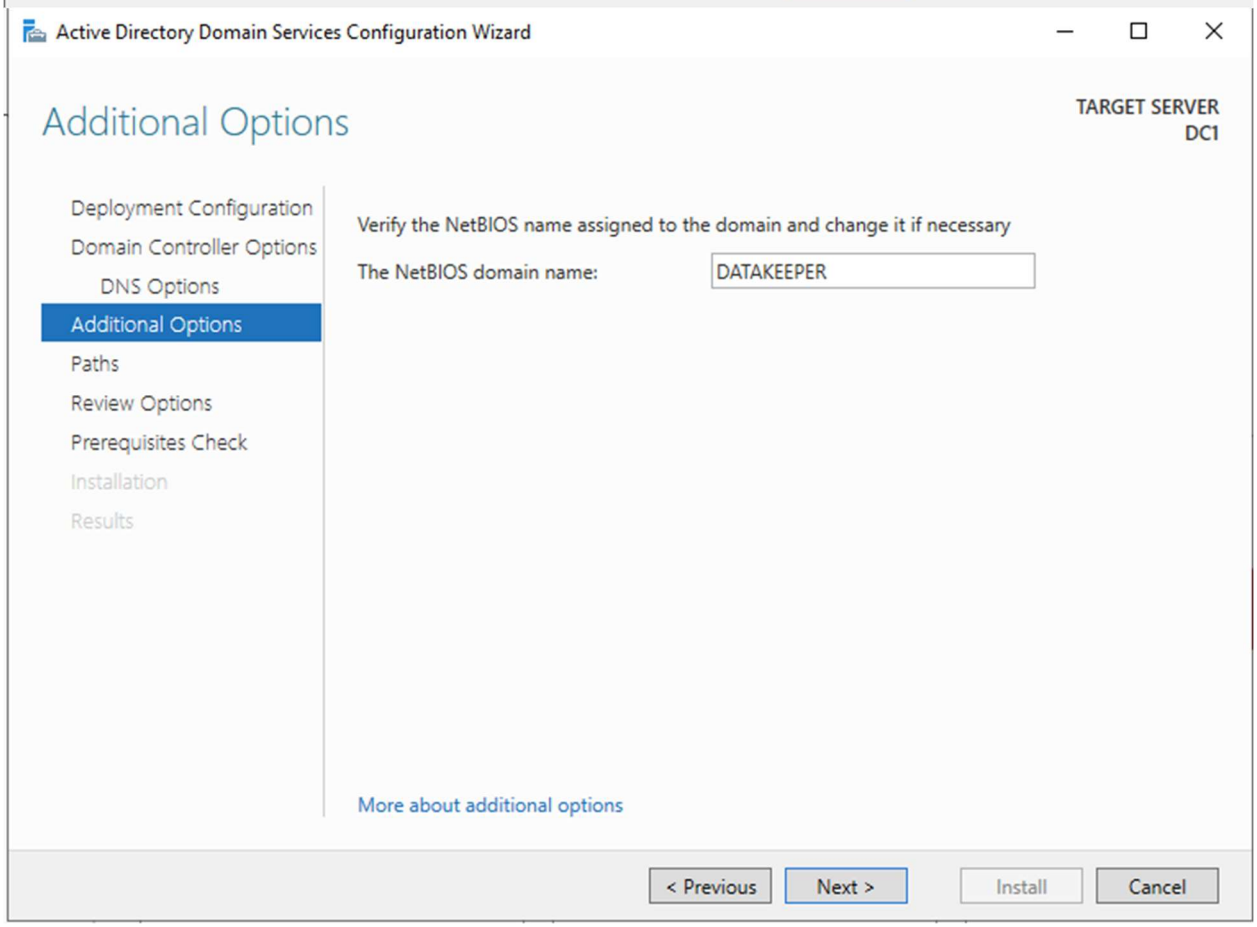
Before you begin this process, enable the local Administrator account on the server and set the password. If you don't, you will receive this message when you try to promote the domain controller.

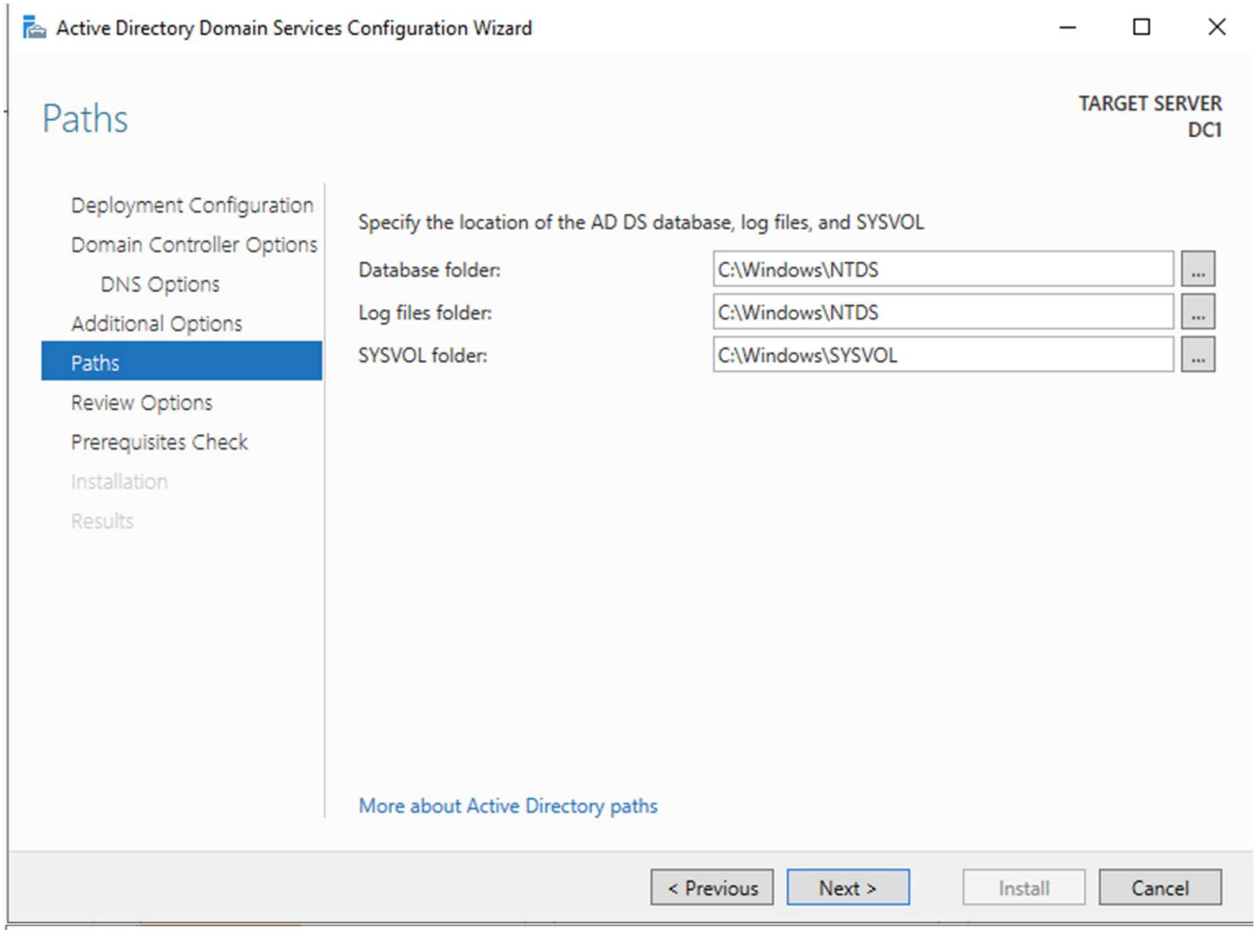


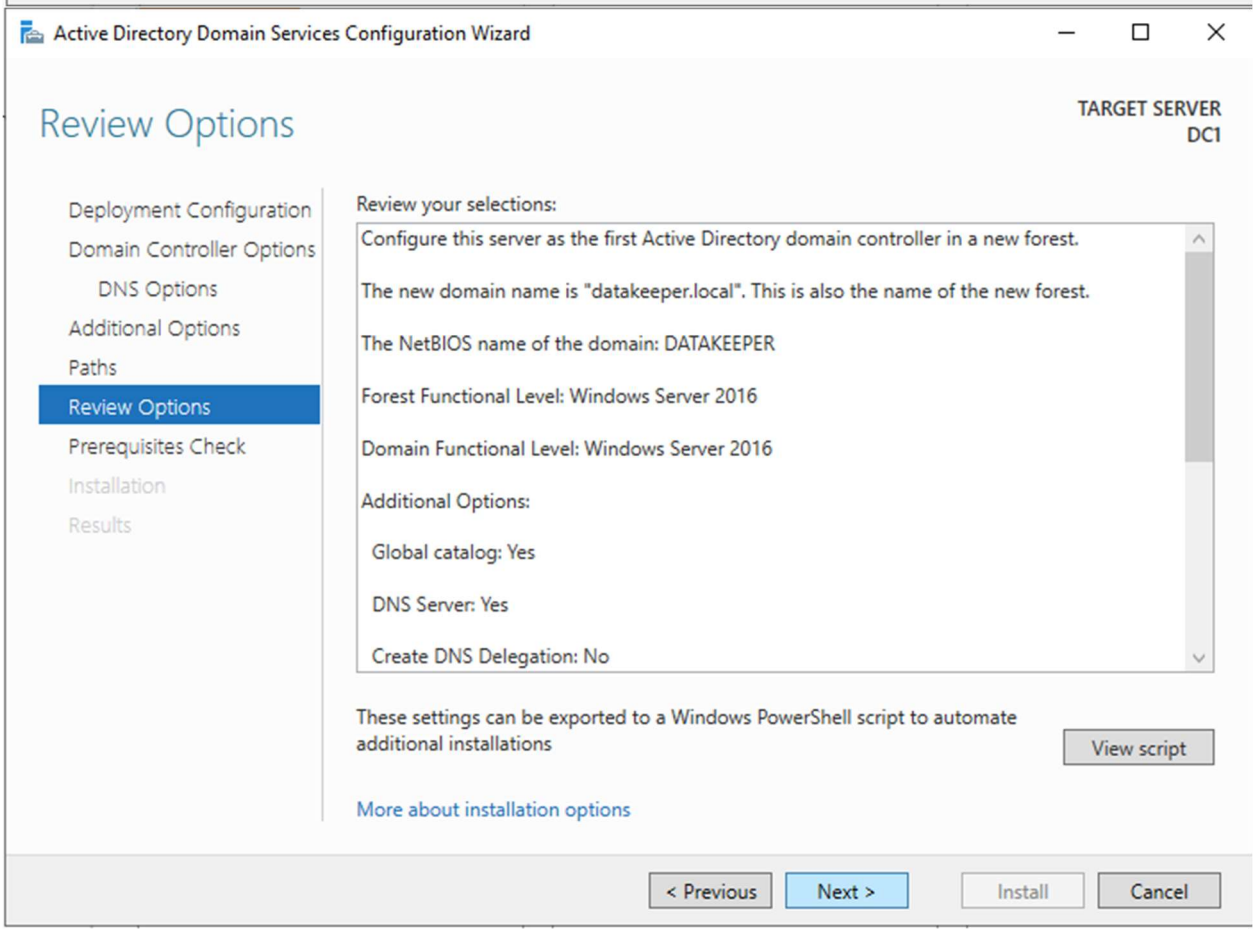
Once you have the Administrator account enabled and the password set, proceed with the Post-Deployment Configuration

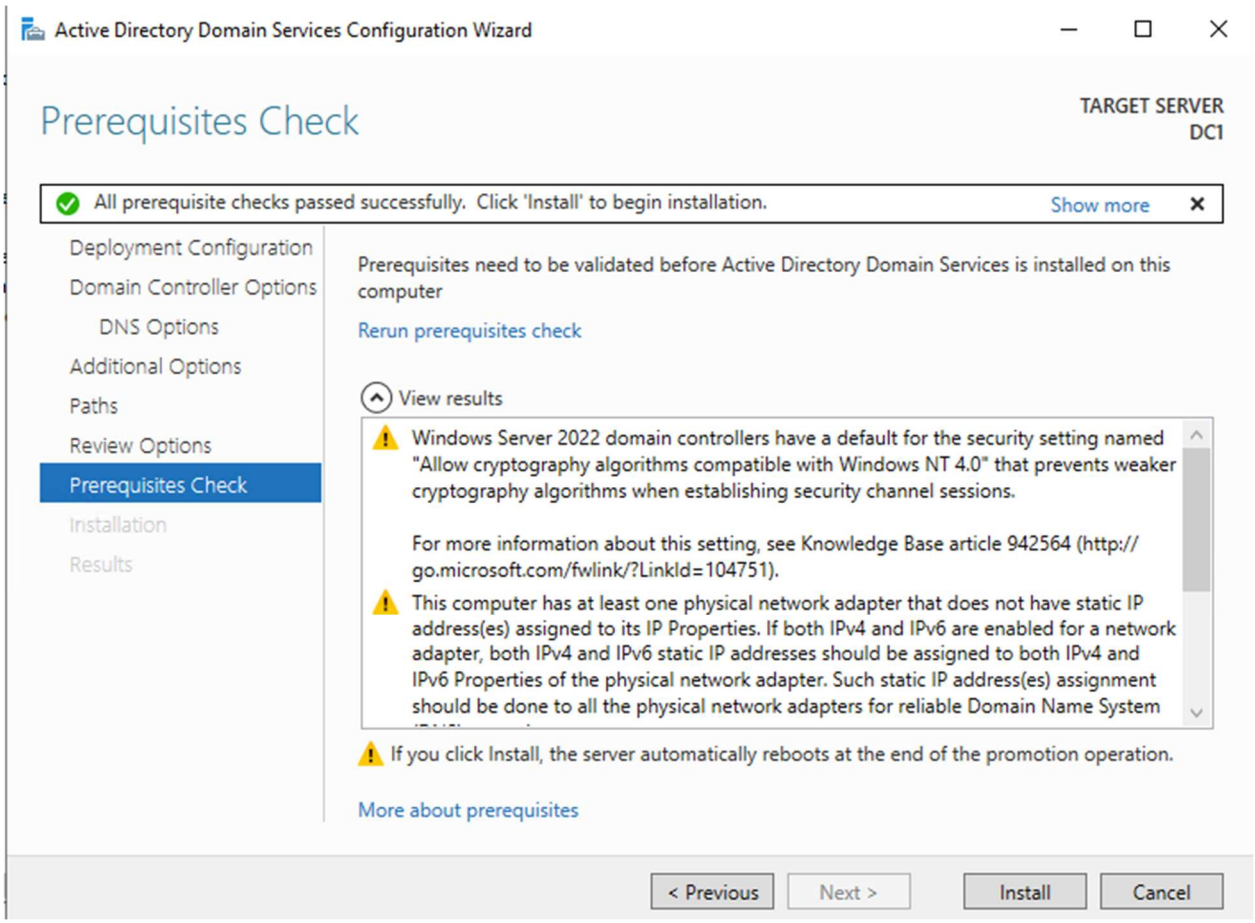



Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
DC1
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select the deployment operation
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
Specify the domain information for this operation
Root domain name:
datakeeper.local
More about deployment configurations
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Additional Options
TARGET SERVER
DC1
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Verify the NetBIOS name assigned to the domain and change it if necessary
The NetBIOS domain name:
DATAKEEPER
More about additional options
< Previous
Next >
Install
Cancel

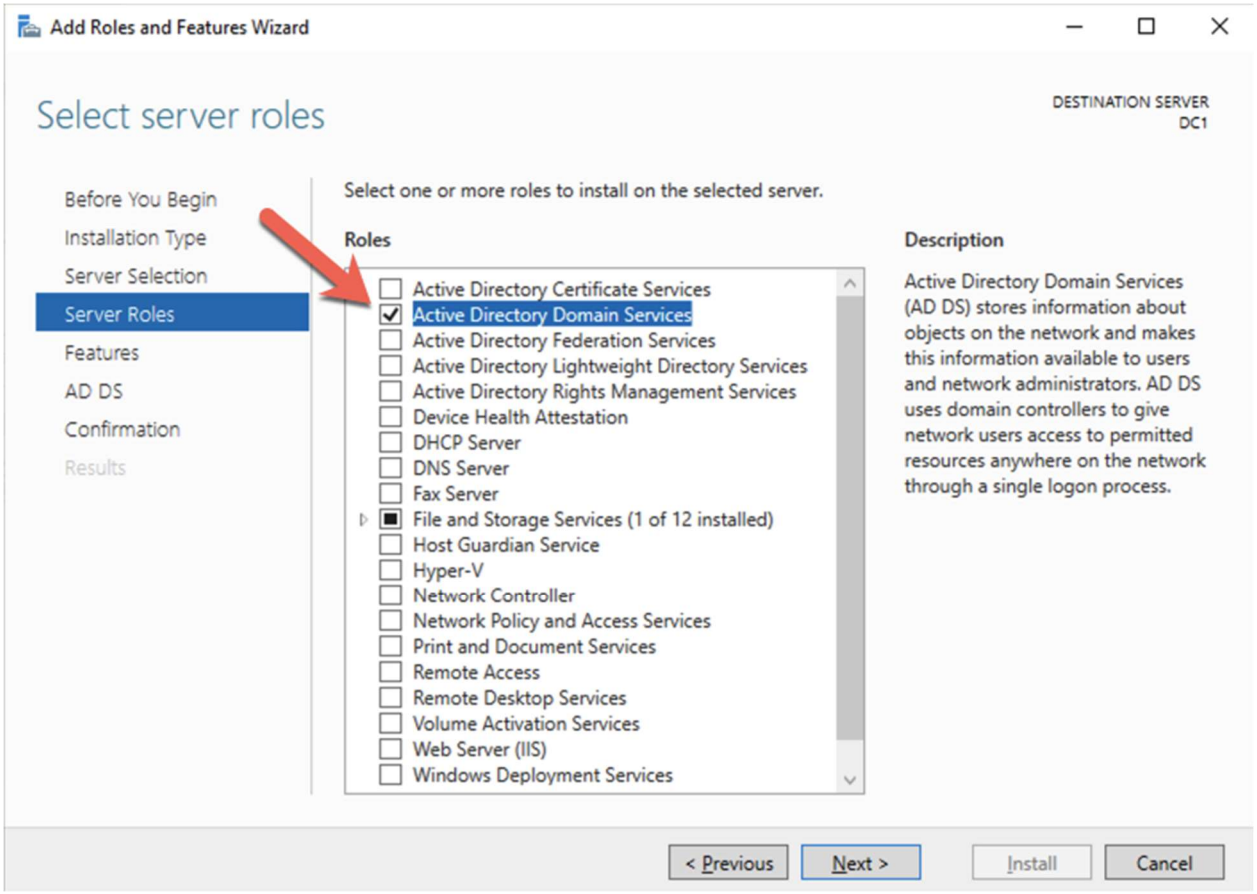

Active Directory Domain Services Configuration Wizard
Paths
TARGET SERVER
DC1
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify the location of the AD DS database, log files, and SYSVOL
Database folder:
C:\Windows\NTDS
Log files folder:
C:\Windows\NTDS
SYSVOL folder:
C:\Windows\SYSVOL
More about Active Directory paths
< Previous
Next >
Install
Cancel

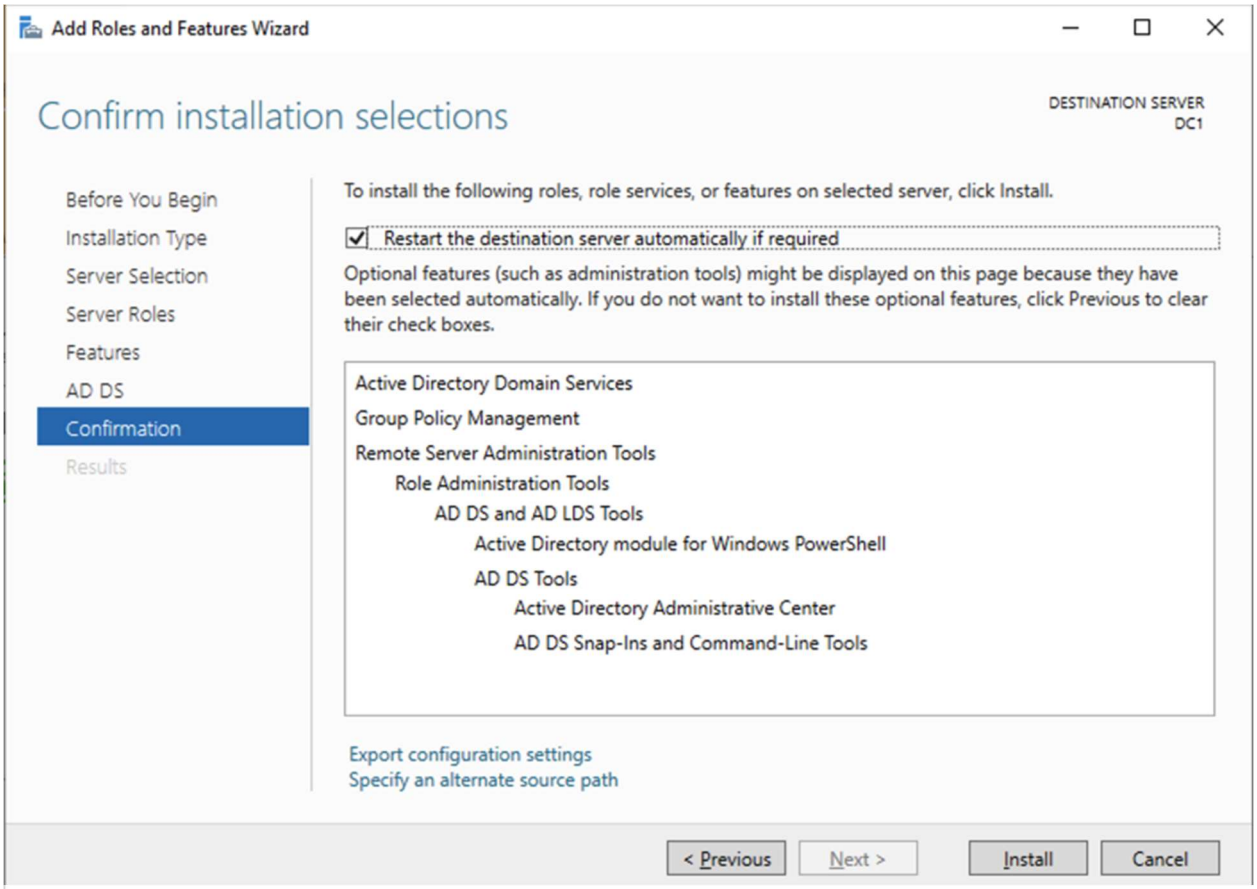

Active Directory Domain Services Configuration Wizard
Review Options
TARGET SERVER
DC1
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Review your selections:
Configure this server as the first Active Directory domain controller in a new forest.
The new domain name is "datakeeper.local". This is also the name of the new forest.
The NetBIOS name of the domain: DATAKEEPER
Forest Functional Level: Windows Server 2016
Domain Functional Level: Windows Server 2016
Additional Options:
Global catalog: Yes
DNS Server: Yes
Create DNS Delegation: No
These settings can be exported to a Windows PowerShell script to automate additional installations
View script
More about installation options
< Previous
Next >
Install
Cancel

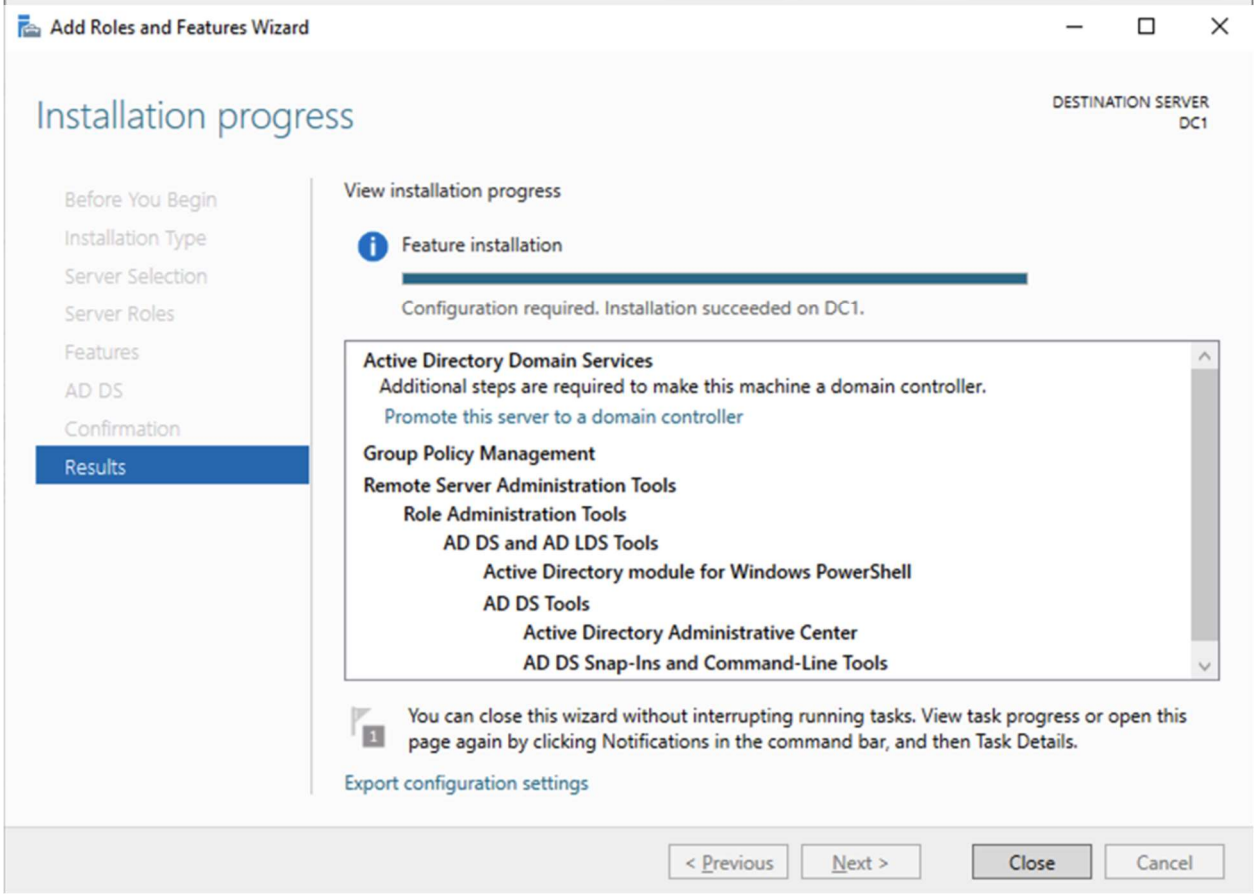

Active Directory Domain Services Configuration Wizard
Prerequisites Check
TARGET SERVER
DC1
All prerequisite checks passed successfully. Click 'Install' to begin installation.
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Prerequisites need to be validated before Active Directory Domain Services is installed on this computer
Rerun prerequisites check
View results
Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System
If you click Install, the server automatically reboots at the end of the promotion operation.
More about prerequisites
< Previous
Next >
Install
Cancel

Before enabling Active Directory Domain Services, you must enable the local Administrator account and log on with that account.

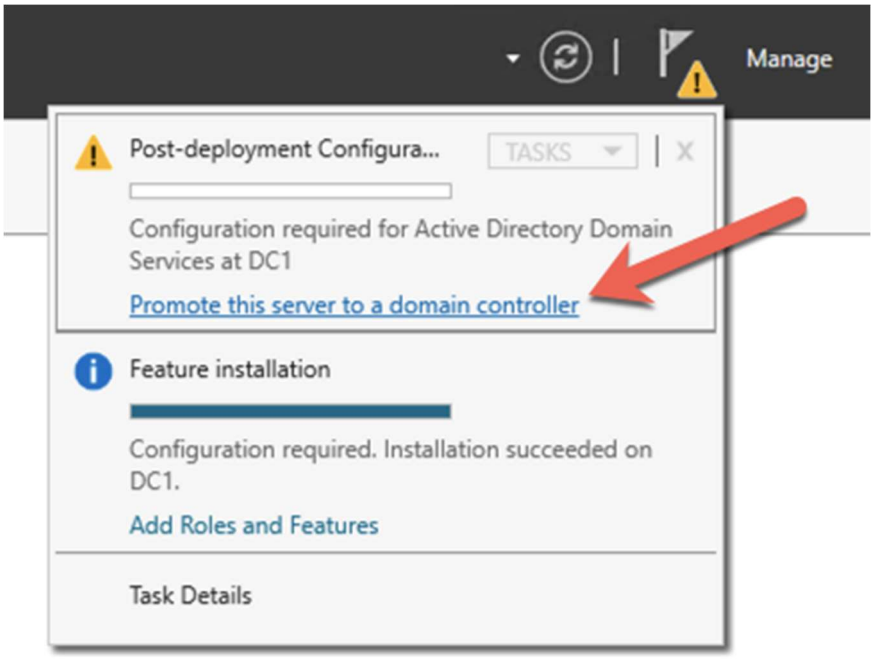
Using your favorite RDP program, connect to DC1 using the public IP address associated with the instance. Add the Active Directory Domain Services role.



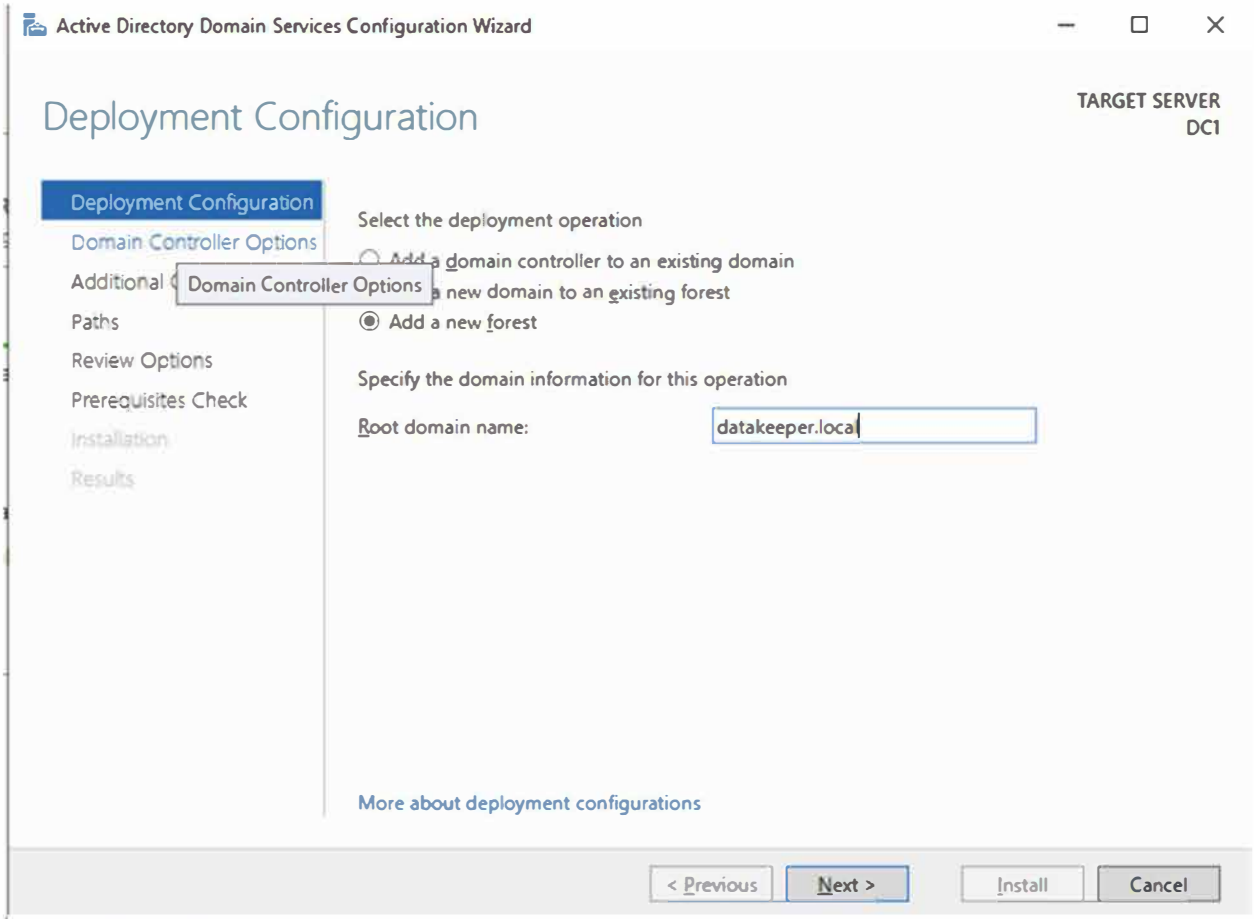

Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
DC1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

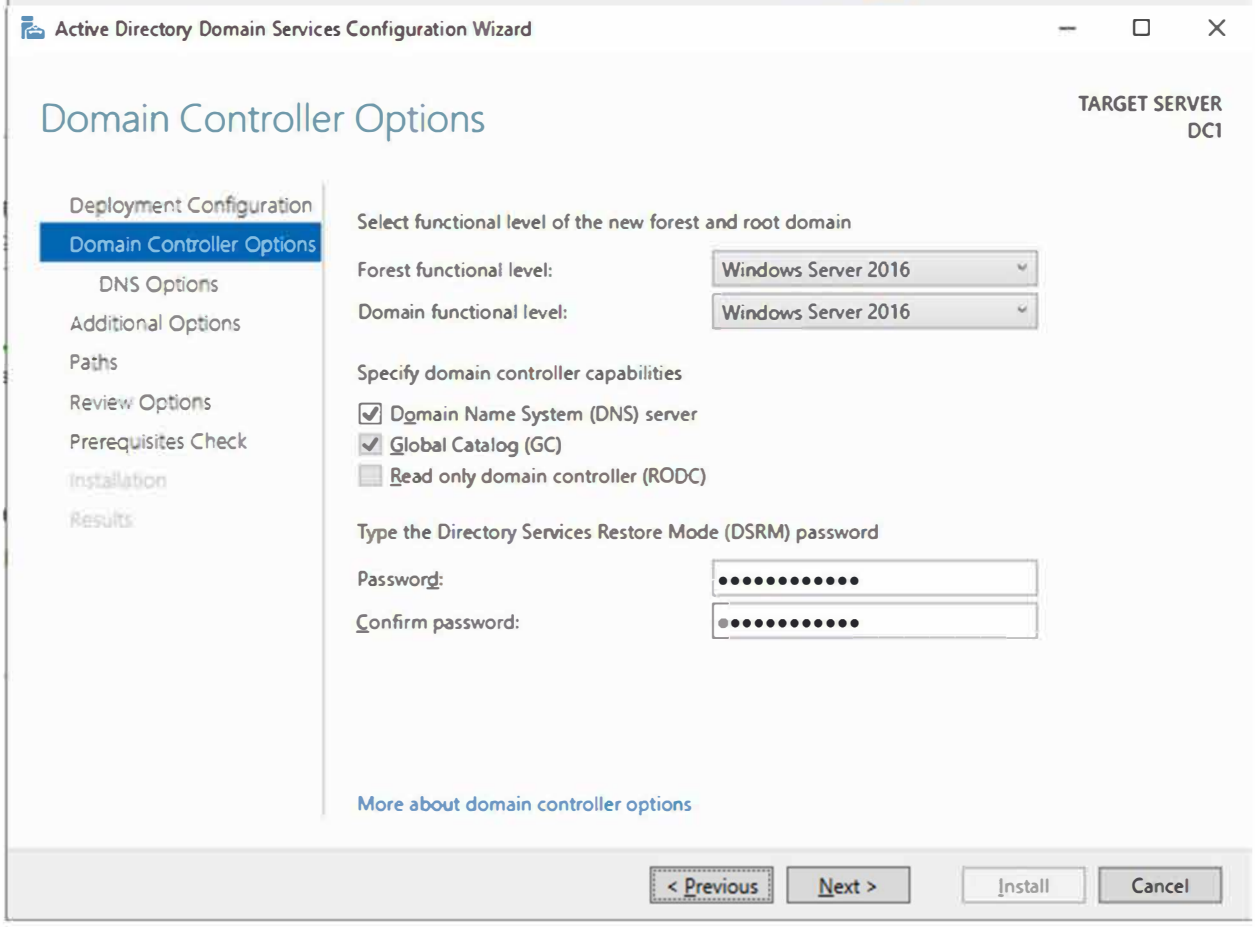

Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
DC1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
View installation progress
Feature installation
Configuration required. Installation succeeded on DC1.
Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel

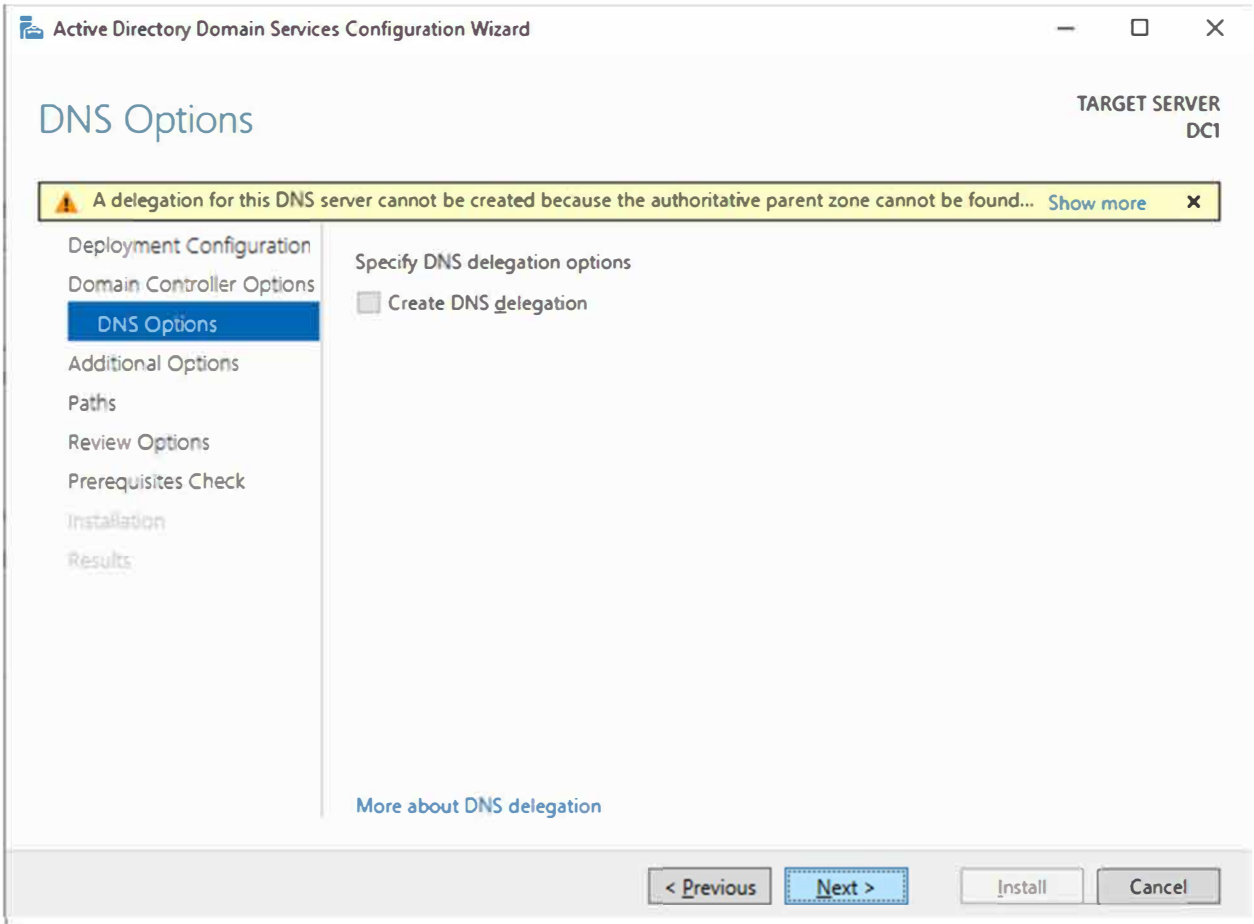
After the installation completes, promote this server to a domain controller.

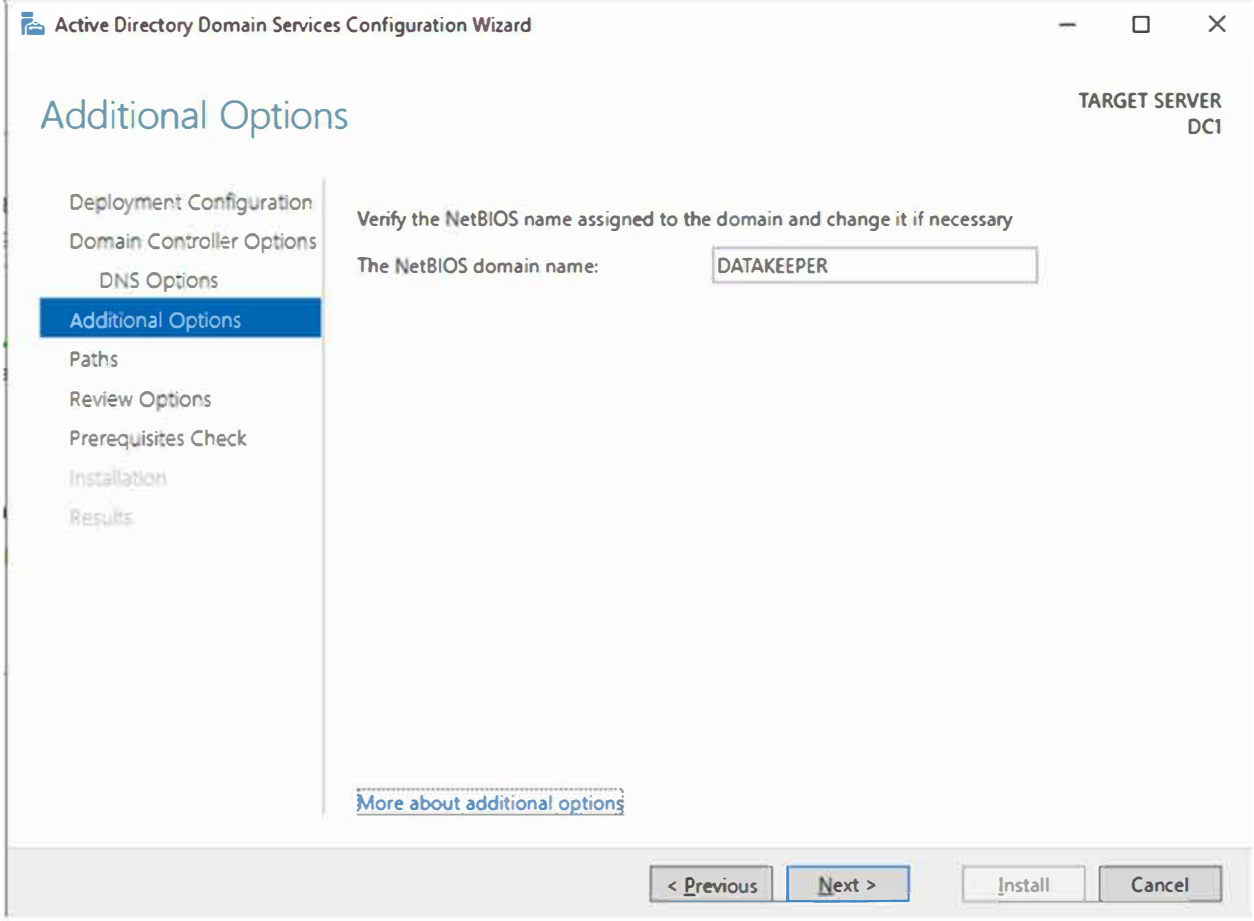


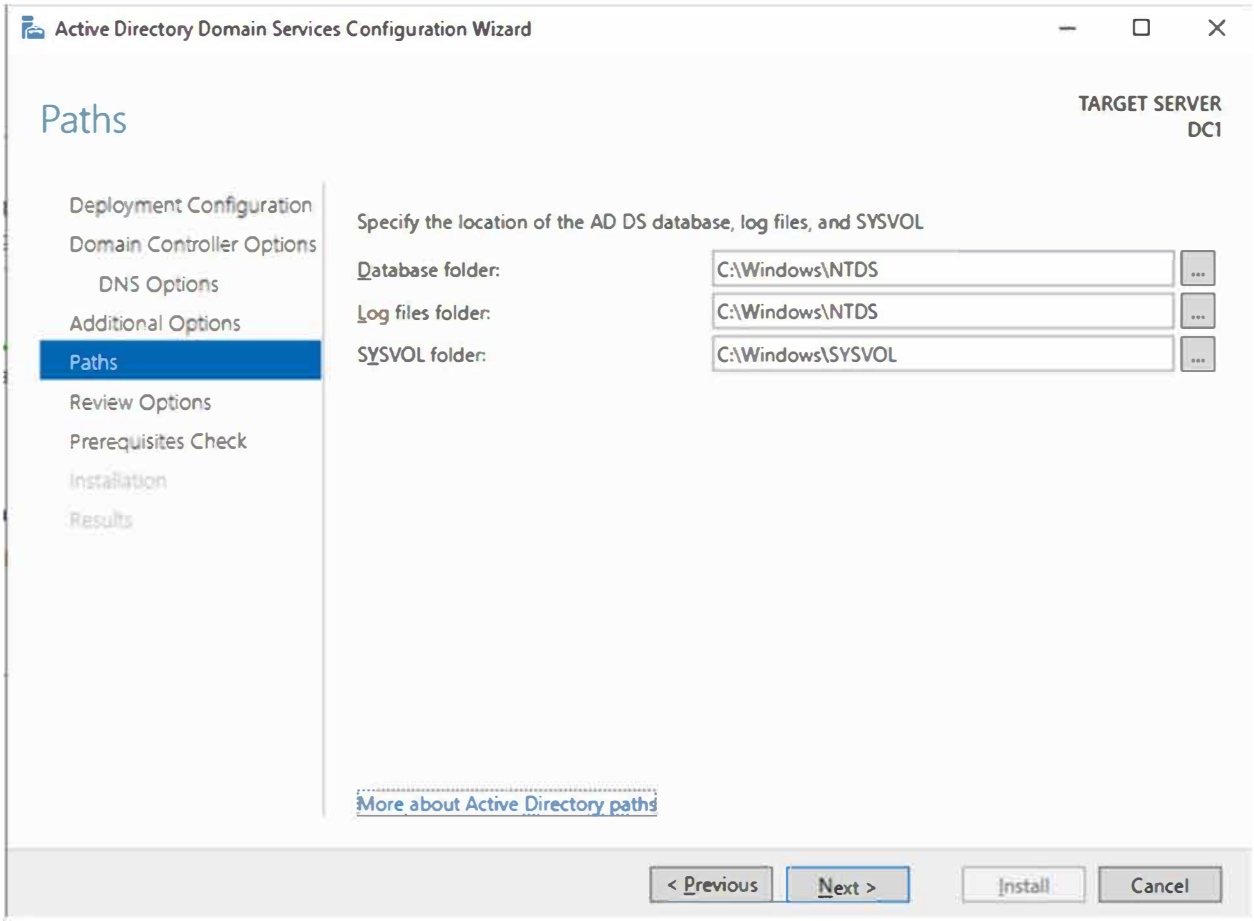
For our purposes we are going to create a new domain.

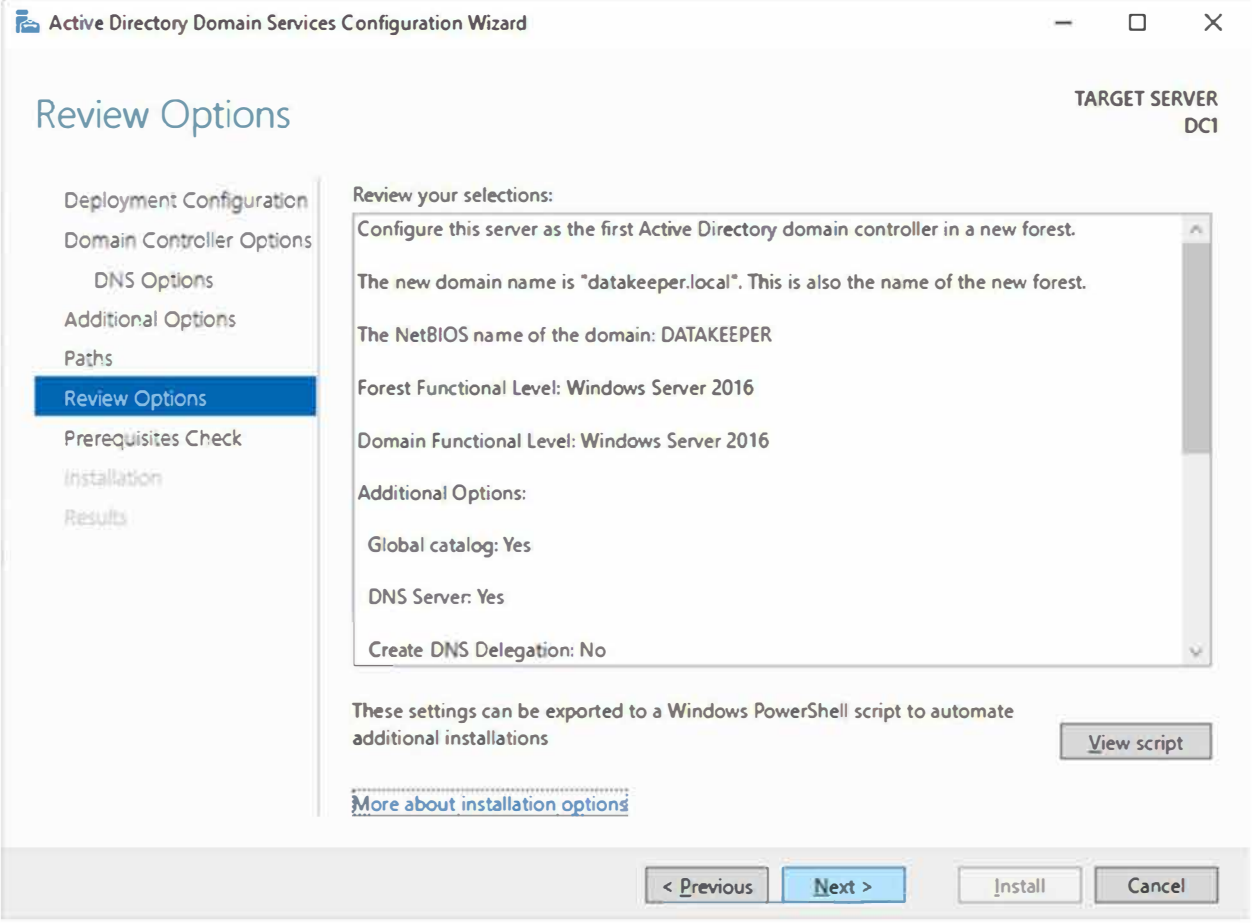

Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
DC1
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Domain Controller Options
Select the deployment operation
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
Specify the domain information for this operation
Root domain name:
datakeeper.local
More about deployment configurations
< Previous
Next >
Install
Cancel

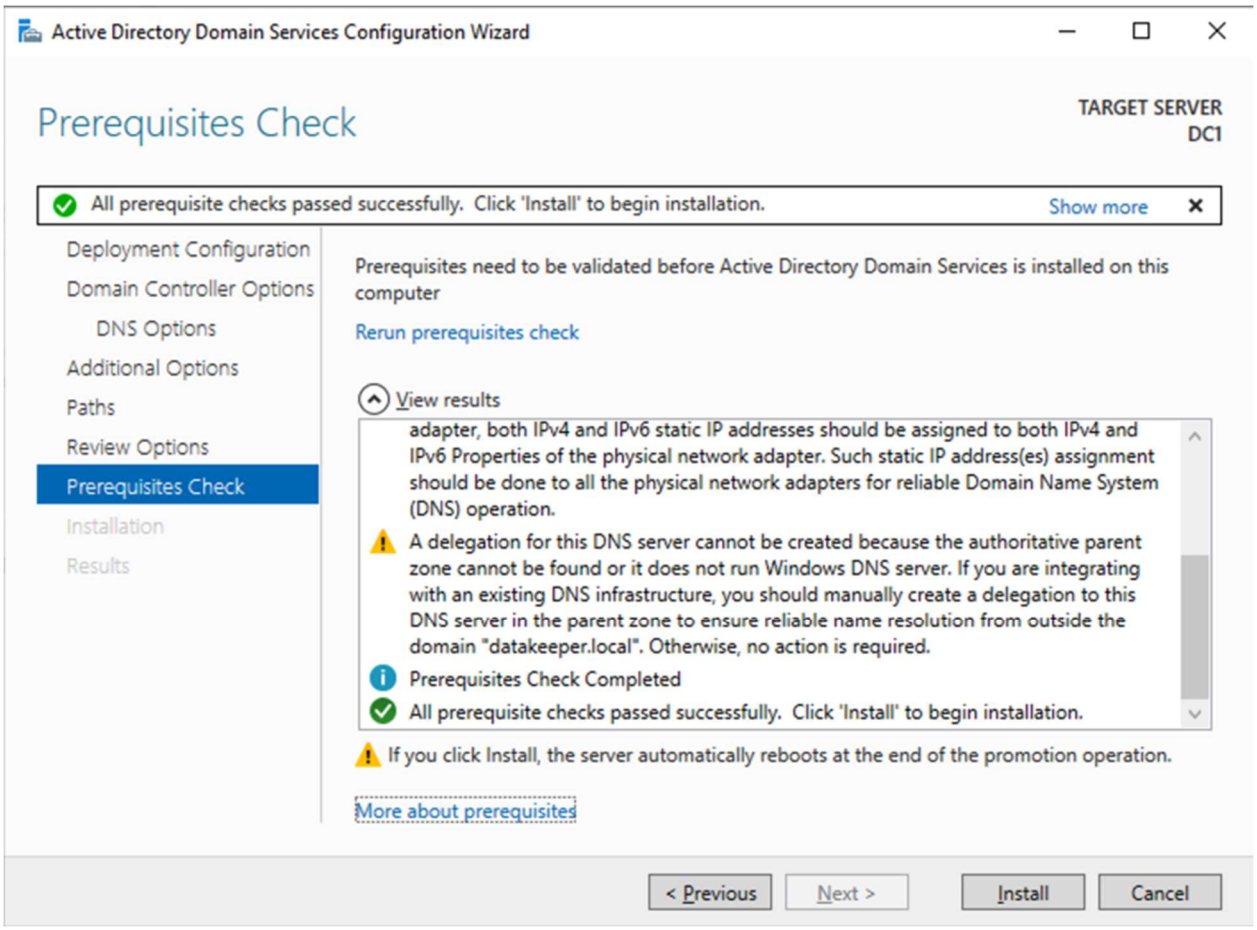

Active Directory Domain Services Configuration Wizard
Domain Controller Options
TARGET SERVER
DC1
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select functional level of the new forest and root domain
Forest functional level:
Windows Server 2016
Domain functional level:
Windows Server 2016
Specify domain controller capabilities
Domain Name System (DNS) server
Global Catalog (GC)
Read only domain controller (RODC)
Type the Directory Services Restore Mode (DSRM) password
Password:
Confirm password:
More about domain controller options
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
DNS Options
TARGET SERVER
DC1
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found...
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify DNS delegation options
Create DNS delegation
More about DNS delegation
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Additional Options
TARGET SERVER
DC1
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Verify the NetBIOS name assigned to the domain and change it if necessary
The NetBIOS domain name:
DATAKEEPER
More about additional options
< Previous
Next >
Install
Cancel

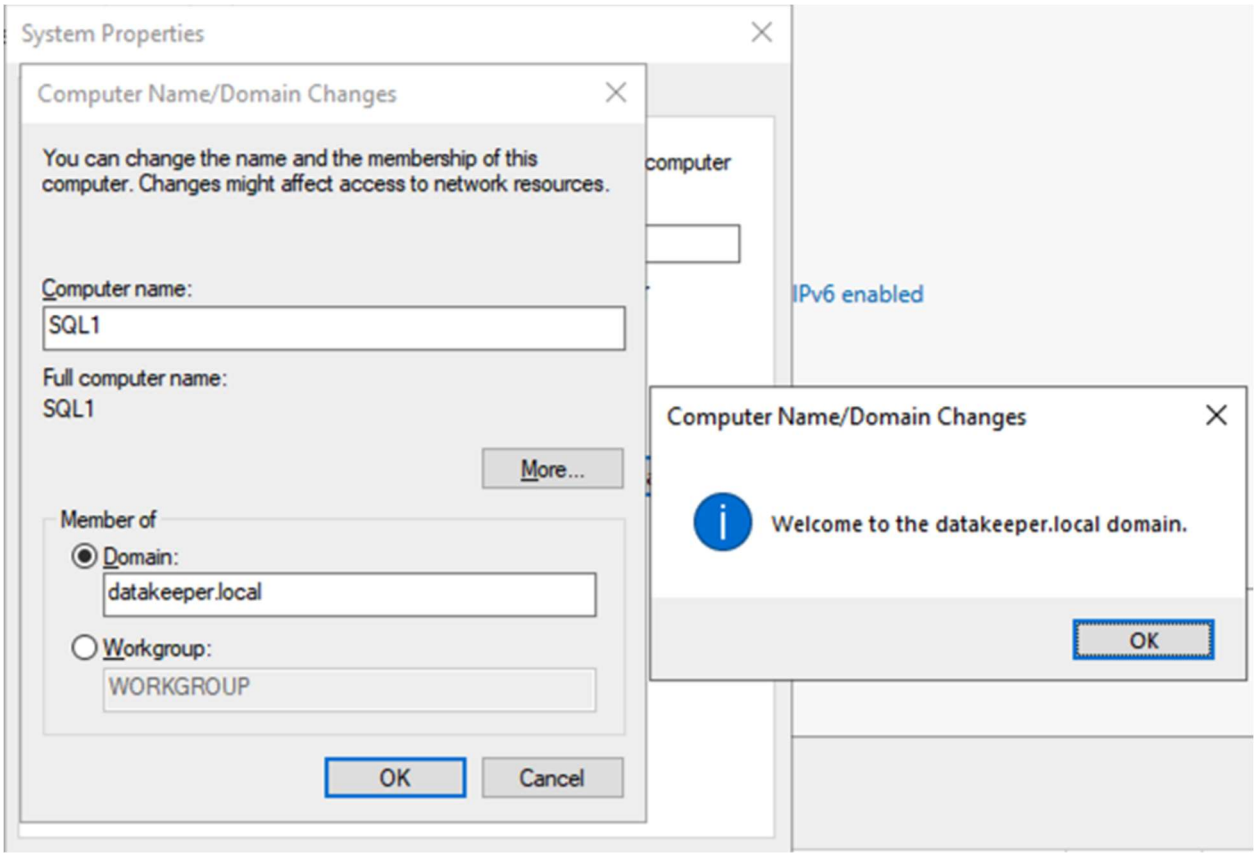

Active Directory Domain Services Configuration Wizard
Paths
TARGET SERVER
DC1
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify the location of the AD DS database, log files, and SYSVOL
Database folder:
C:\Windows\NTDS
Log files folder:
C:\Windows\NTDS
SYSVOL folder:
C:\Windows\SYSVOL
More about Active Directory paths
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Review Options
TARGET SERVER
DC1
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Review your selections:
Configure this server as the first Active Directory domain controller in a new forest.
The new domain name is "datakeeper.local". This is also the name of the new forest.
The NetBIOS name of the domain: DATAKEEPER
Forest Functional Level: Windows Server 2016
Domain Functional Level: Windows Server 2016
Additional Options:
Global catalog: Yes
DNS Server: Yes
Create DNS Delegation: No
These settings can be exported to a Windows PowerShell script to automate additional installations
View script
More about installation options
< Previous
Next >
Install
Cancel



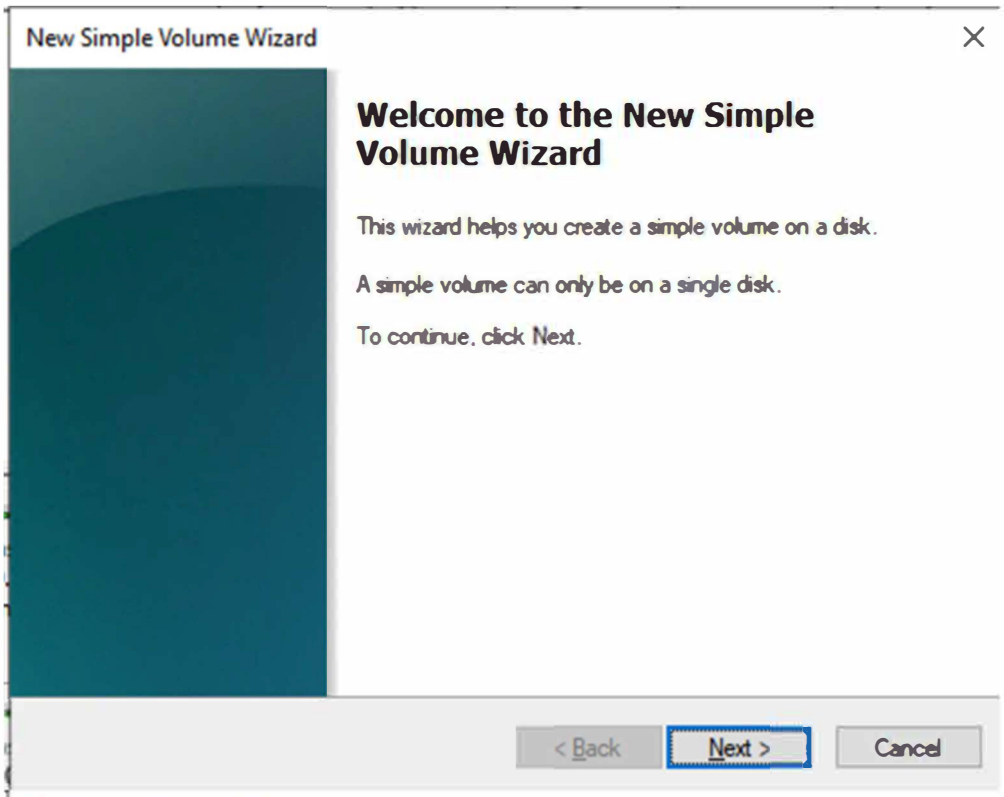
Reboot DC1 and move on to the next section.

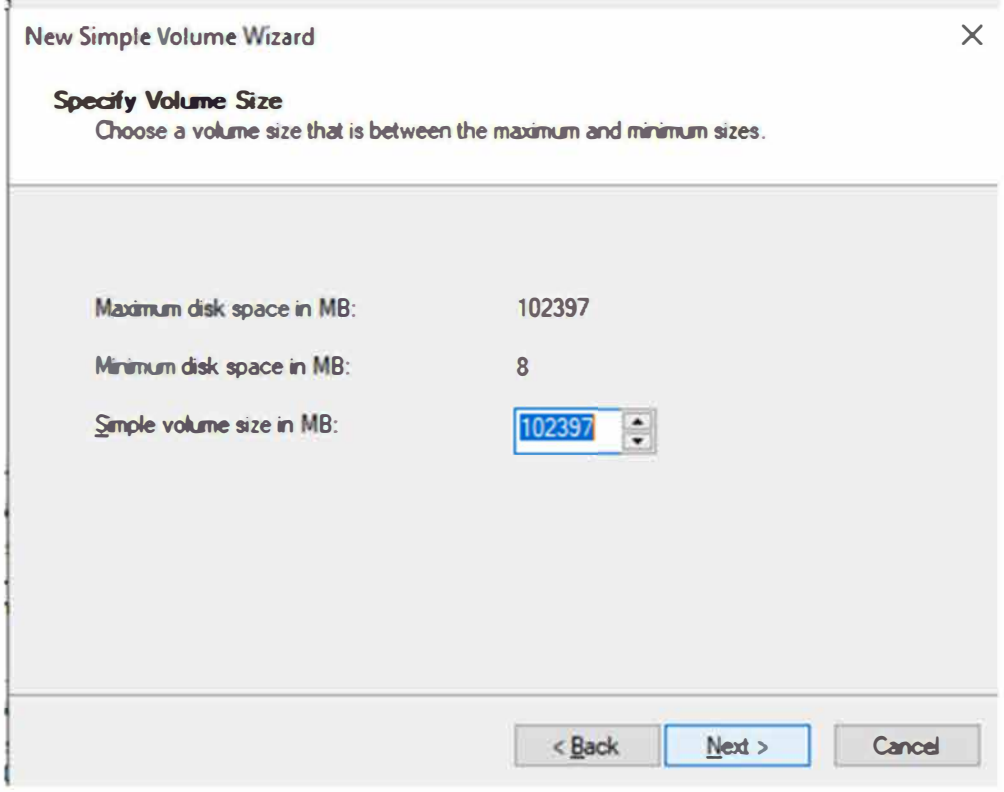
Join SQL1 and SQL2 to the Domain

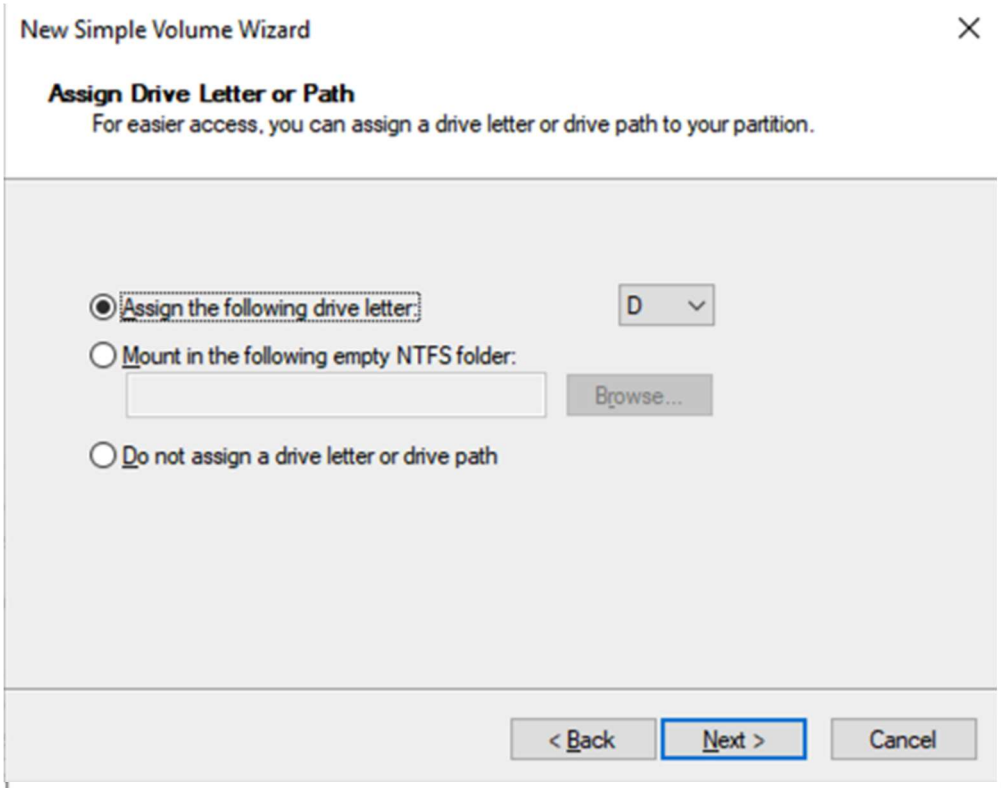


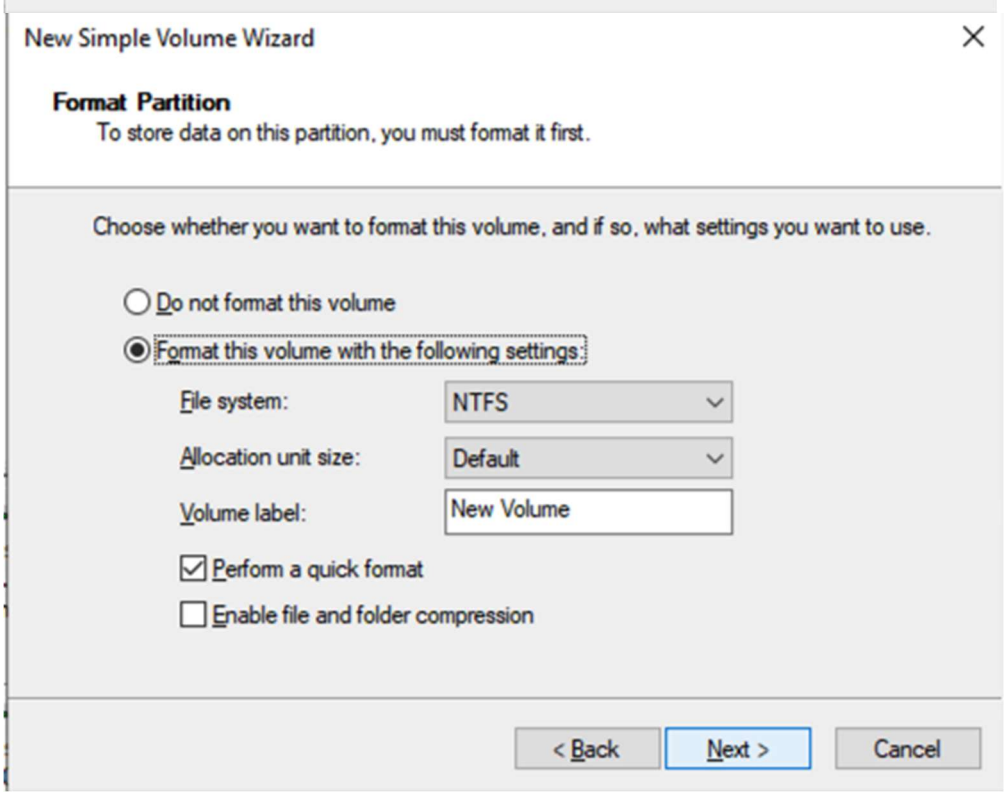
Prepare the Storage

Once SQL1 and SQL2 are added to the domain, connect to the instances with the Domain Admin account you created to complete the rest of the configuration steps. The first thing you need to do is to attach and format the EBS volumes that we added to SQL1 and SQL2 as shown below.


New Simple Volume Wizard
Welcome to the New Simple Volume Wizard
This wizard helps you create a simple volume on a disk.
A simple volume can only be on a single disk.
To continue, click Next.
< Back
Next >
Cancel


New Simple Volume Wizard
Specify Volume Size
Choose a volume size that is between the maximum and minimum sizes.
Maximum disk space in MB:
102397
Minimum disk space in MB:
8
Simple volume size in MB:
102397
< Back
Next >
Cancel


New Simple Volume Wizard
Assign Drive Letter or Path
For easier access, you can assign a drive letter or drive path to your partition.
Assign the following drive letter:
D
Mount in the following empty NTFS folder:
Browse...
Do not assign a drive letter or drive path
< Back
Next >
Cancel


New Simple Volume Wizard
Format Partition
To store data on this partition, you must format it first.
Choose whether you want to format this volume, and if so, what settings you want to use.
Do not format this volume
Format this volume with the following settings:
File system:
NTFS
Allocation unit size:
Default
Volume label:
New Volume
Perform a quick format
Enable file and folder compression
< Back
Next >
Cancel

Configure Failover Clustering Feature

Enable the Failover Clustering feature on both SQL1 and SQL2.

Run this PowerShell command on SQL1 and SQL2

```
Install-WindowsFeature -Name Failover-Clustering -
IncludeManagementTools
```

Validate your Cluster

Run this PowerShell command from SQL1 or SQL2

```
Test-Cluster -Node sql1,sql2
```

Depending upon the version of Windows Server you are using, you will see some warnings about Network and possibly storage. The network warning will likely tell you that each cluster node is accessible via a single interface. Earlier versions of Windows will warn you about the lack of shared storage.

You can ignore both of those errors as they are expected in a cluster hosted on OCI. As long as you have received no Errors, you can proceed with the next section. If you receive any errors, fix them, then run validation again and continue on to the next section.

Create the Cluster

Next, you will create the cluster. In the example below, you will notice I use the two IP addresses we planned to use, 10.0.64.101 and 10.0.128.101. You can run this Powershell from either cluster node.

```
New-Cluster -Name cluster1 -Node sql1,sql2 -
StaticAddress 10.0.64.101, 10.0.128.101
```

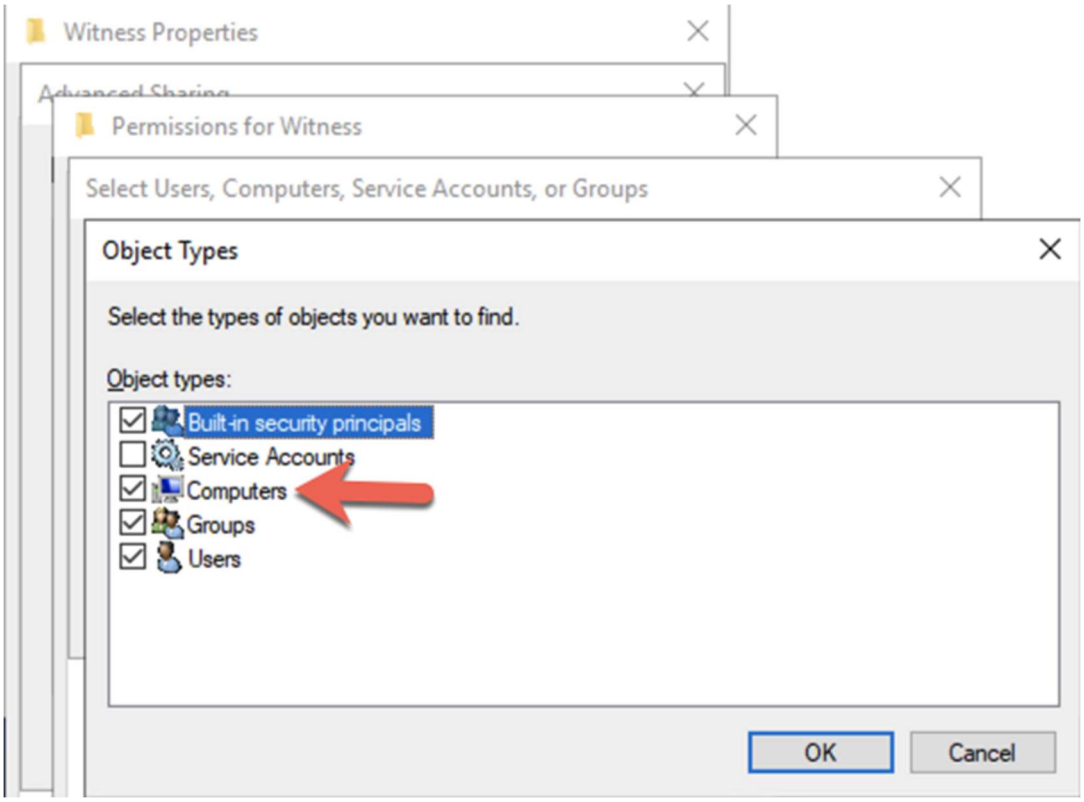
Please Note: do NOT try to create the cluster via the WSFC GUI. You will find that because the instances are using DHCP, the GUI will not give you the option to assign IP addresses for the cluster and instead will hand out duplicate IP addresses.

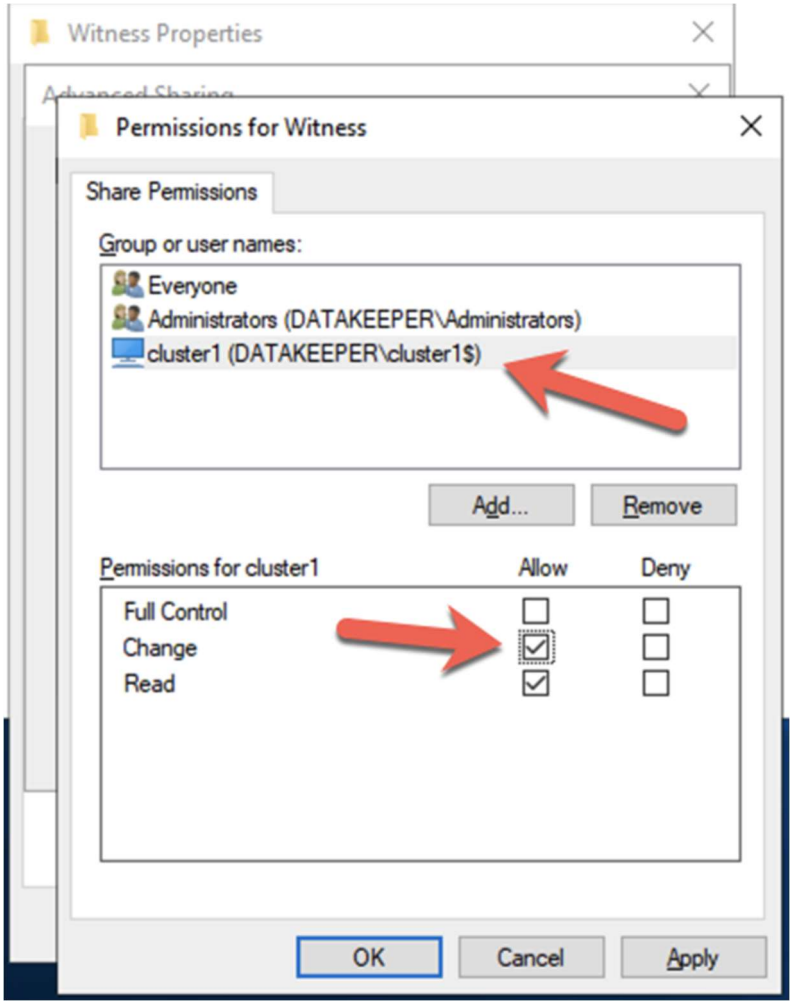
Add the File Share Witness

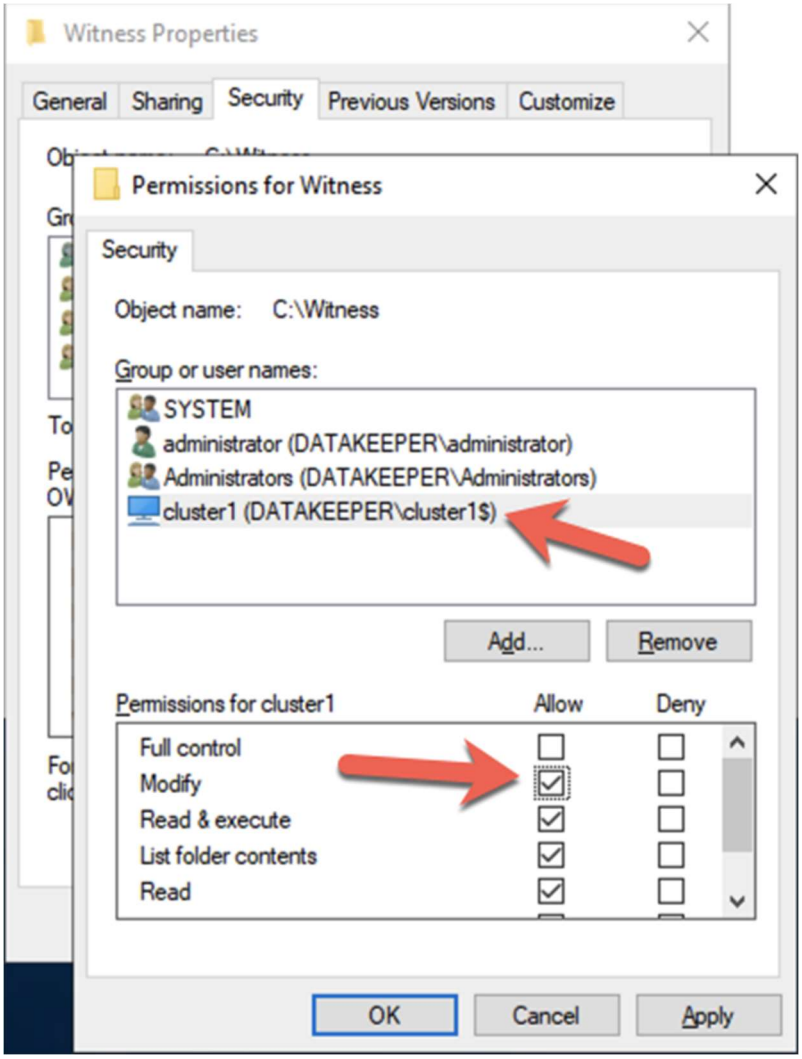
To maintain the cluster quorum, you need to add a witness. In OCI, the type of witness you will want to use is a File Share Witness. The file share witness must reside on a server that resides in a different Fault Domain than the two cluster nodes.

In the example below, the file share witness will be created on DC1, which resides in FD1.

On DC1, create a file share and assign the cluster name object (CNO) read-write permissions on the folder. Add permissions for the CNO on both the Share and Security tab of a folder that you created, In the example below I created a folder called “Witness”.



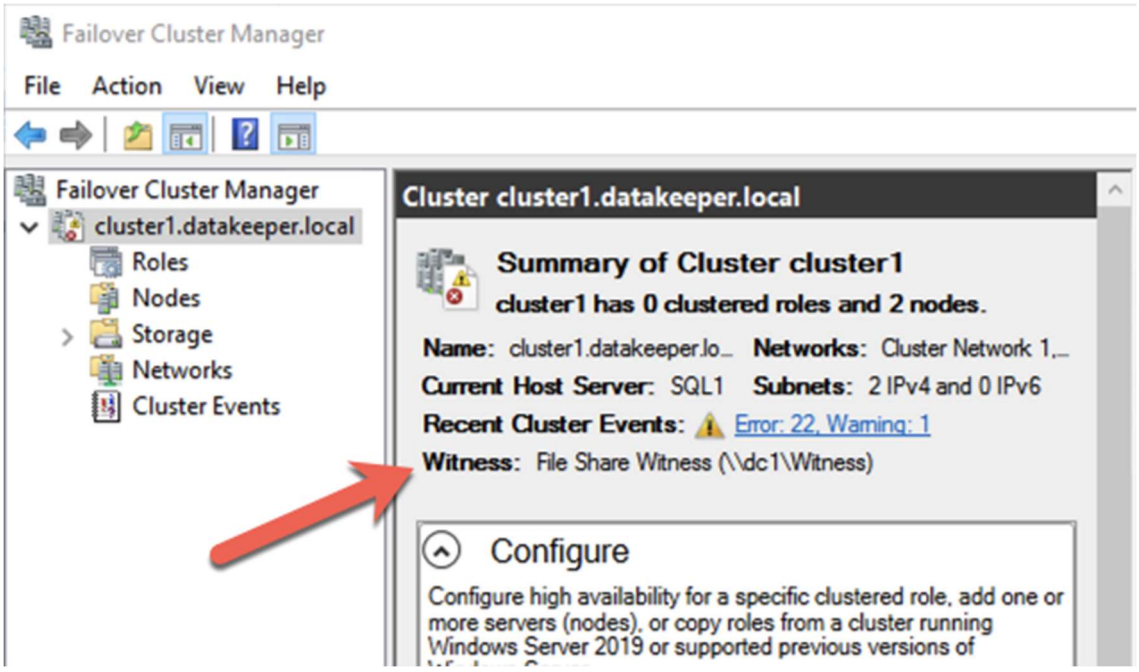

Witness Properties
Permissions for Witness
Share Permissions
Group or user names:
Everyone
Administrators (DATAKEEPER\Administrators)
cluster1 (DATAKEEPER\cluster1$)
Add...
Remove
Permissions for cluster1
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply



Once the folder has been created and the appropriate permissions have been assigned to the CNO, run the following PowerShell command on SQL1 or SQL2.

```
Set-ClusterQuorum -Cluster cluster1 -
FileShareWitness \\dc1\Witness
```

Your cluster should now look like the following when you launch the Failover Cluster Manager on SQL1 or SQL2.



Creating the SQL Server FCI

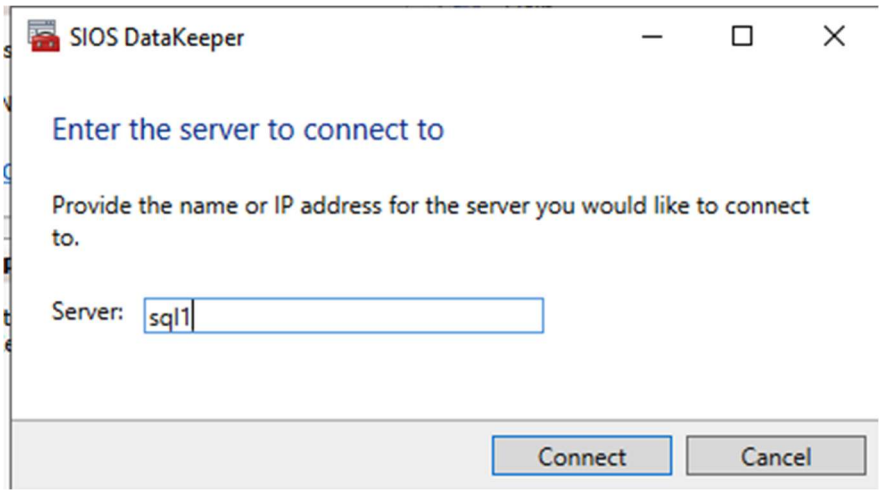
Install DataKeeper Cluster Edition

Before you can move on with the next steps, you will need to install DataKeeper Cluster Edition on both SQL1 and SQL2. Download the setup executable and run the DataKeeper setup on both nodes. Refer to the SIOS documentation for specific guidance on the installation.

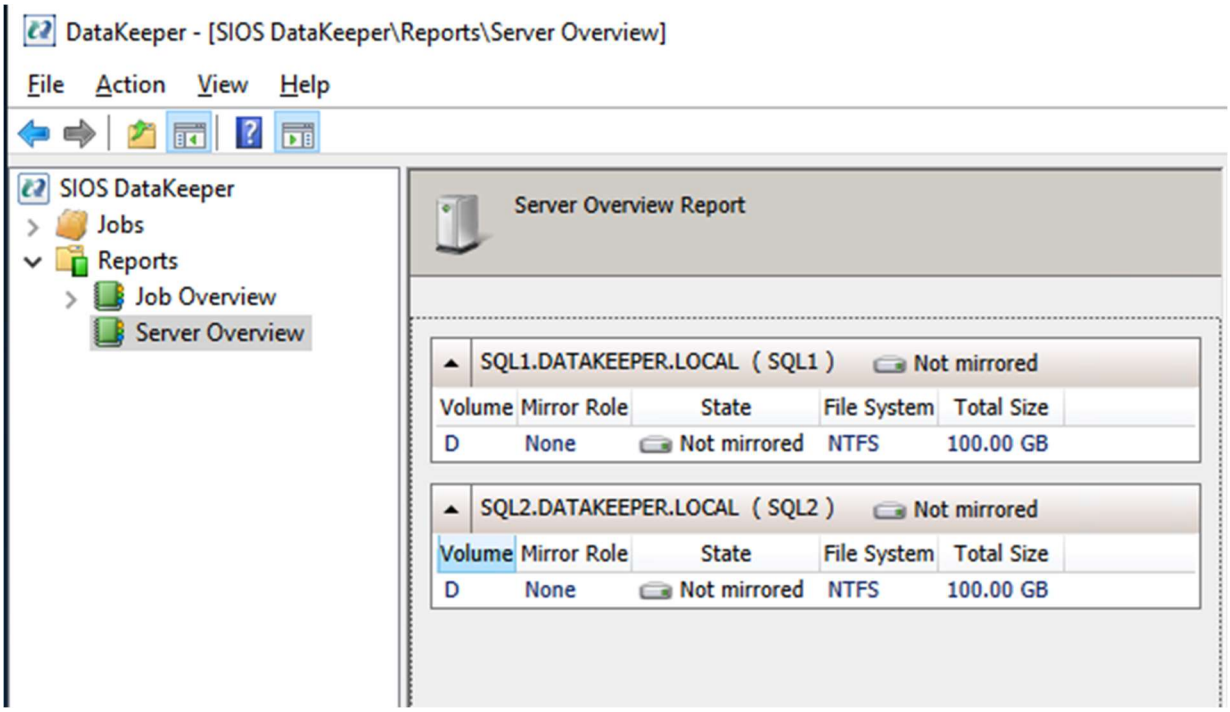
Create the DataKeeper Volume Resource

Launch the DataKeeper UI on either of the cluster nodes and create your DataKeeper Volume Resource as shown below.

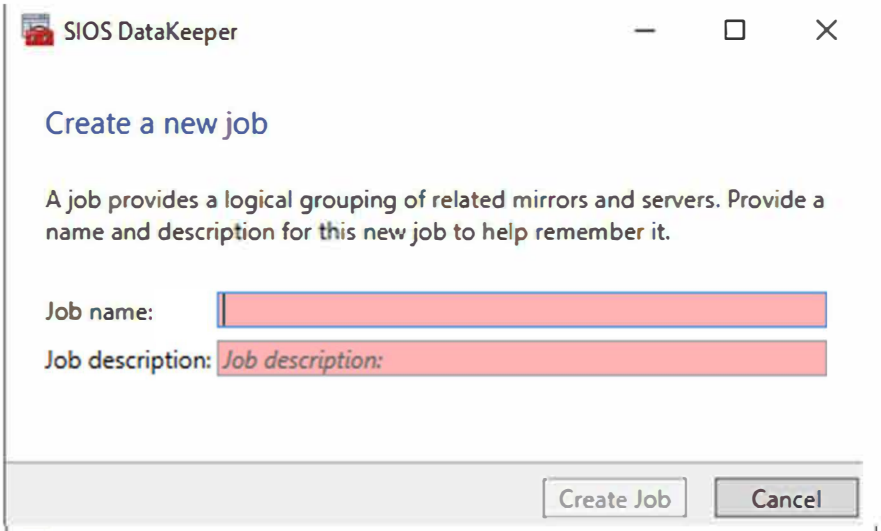
Connect to both servers, first SQL1 and then SQL2

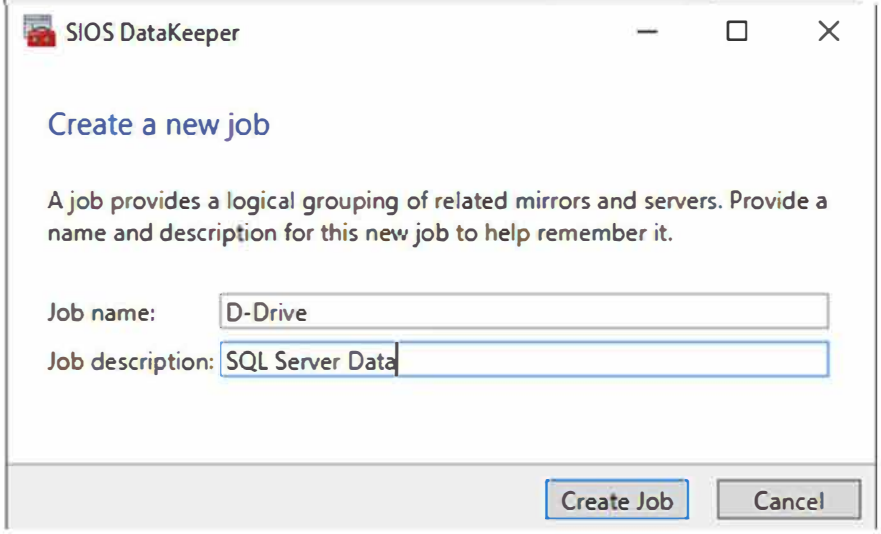


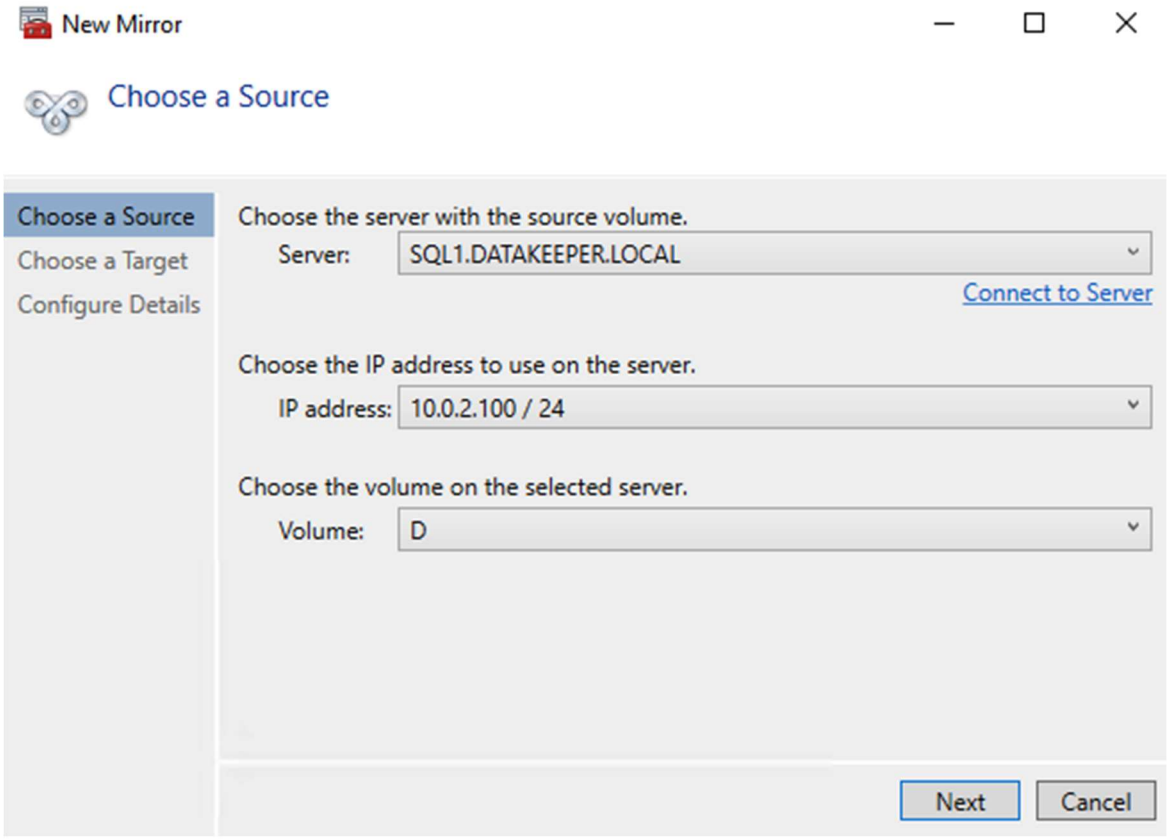
If you have connected to both servers and the storage is configured properly, the Server Overview Report should look something like this.

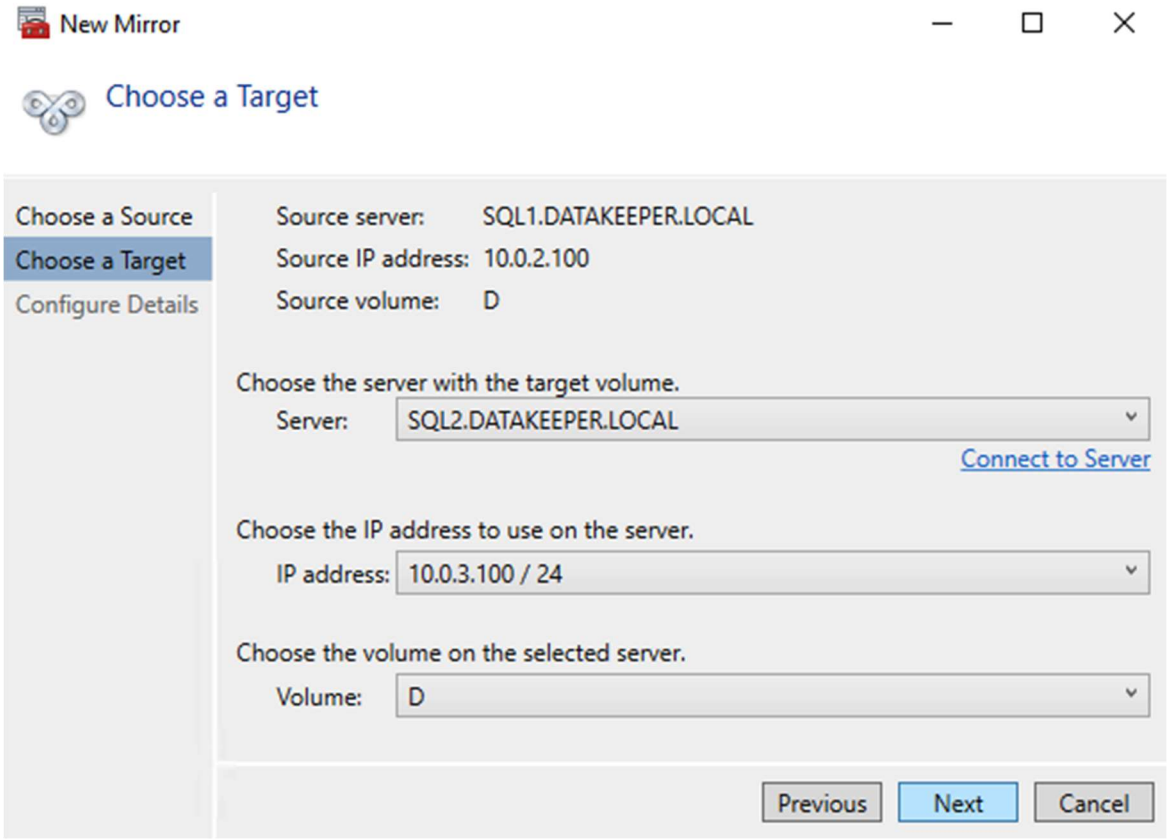


Click Create Job to start the Job Creation Wizard

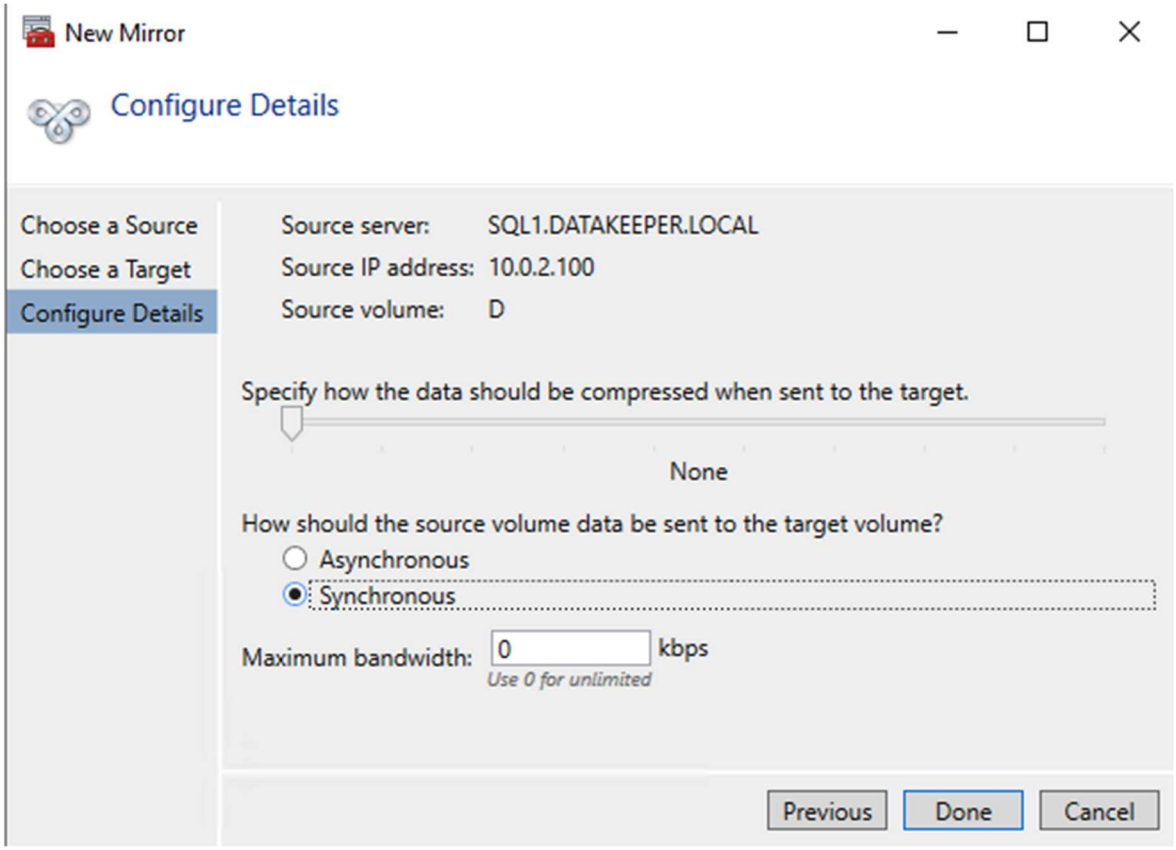




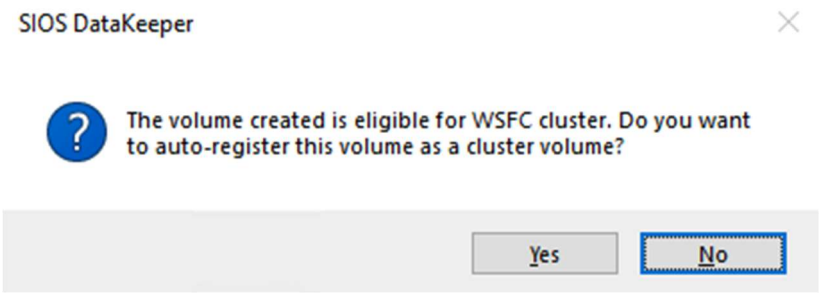

New Mirror
Choose a Source
Choose a Source
Choose a Target
Configure Details
Choose the server with the source volume.
Server:
SQL1.DATAKEEPER.LOCAL
Connect to Server
Choose the IP address to use on the server.
IP address:
10.0.2.100 / 24
Choose the volume on the selected server.
Volume:
D
Next
Cancel


New Mirror
Choose a Target
Choose a Source
Choose a Target
Configure Details
Source server:
SQL1.DATAKEEPER.LOCAL
Source IP address:
10.0.2.100
Source volume:
D
Choose the server with the target volume.
Server:
SQL2.DATAKEEPER.LOCAL
Connect to Server
Choose the IP address to use on the server.
IP address:
10.0.3.100 / 24
Choose the volume on the selected server.
Volume:
D
Previous
Next
Cancel

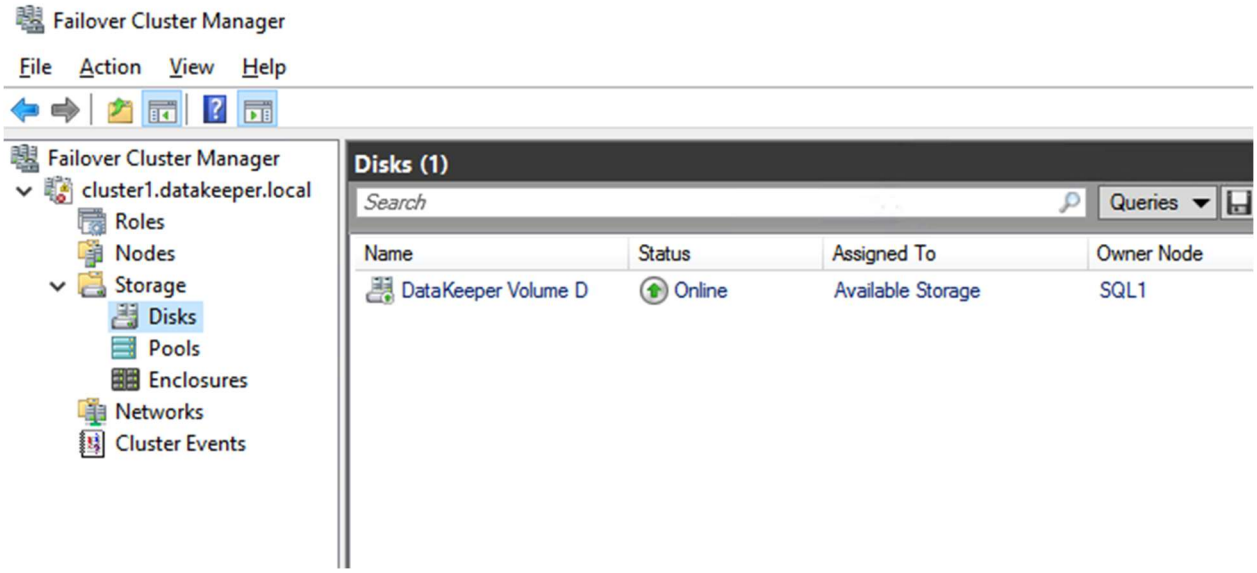
DataKeeper supports both synchronous and asynchronous replication. For replication between availability zones in the same region, choose synchronous. If you want to replicate across regions or even across cloud providers, choose asynchronous



Click “Yes” here to register the DataKeeper Volume resource in Available Storage in the cluster



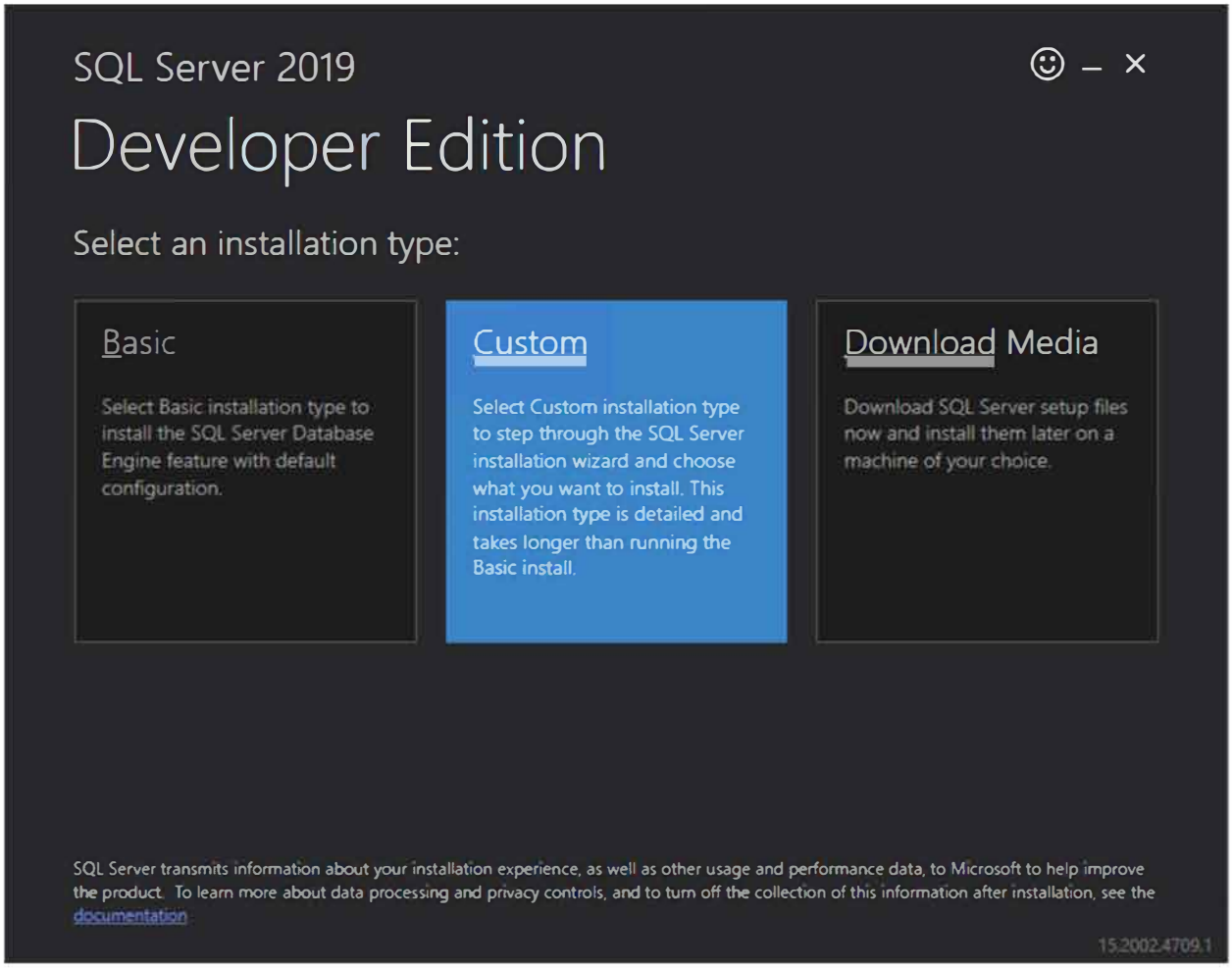
The DataKeeper Volume D now appears in Failover Cluster Manager in Available Storage.

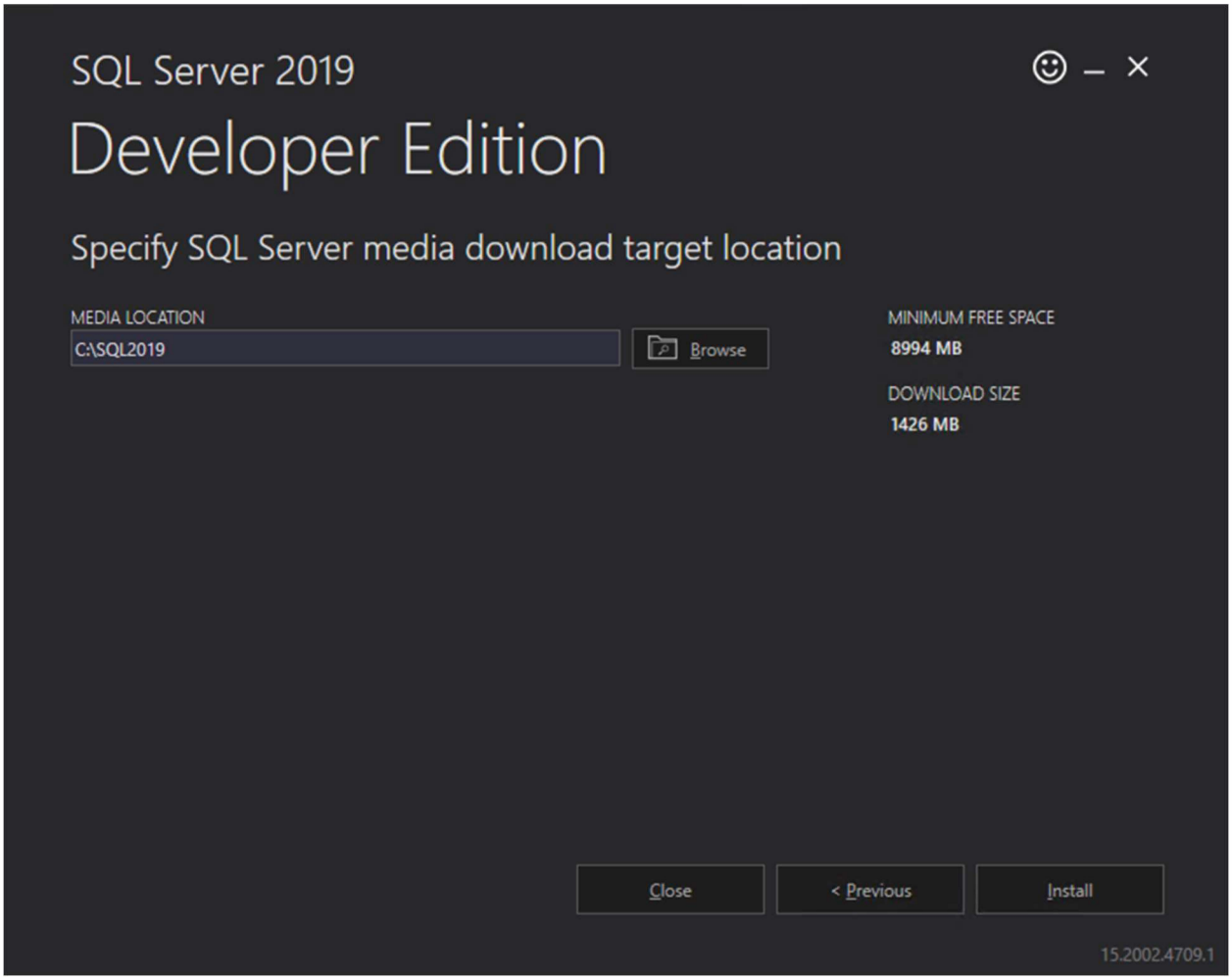


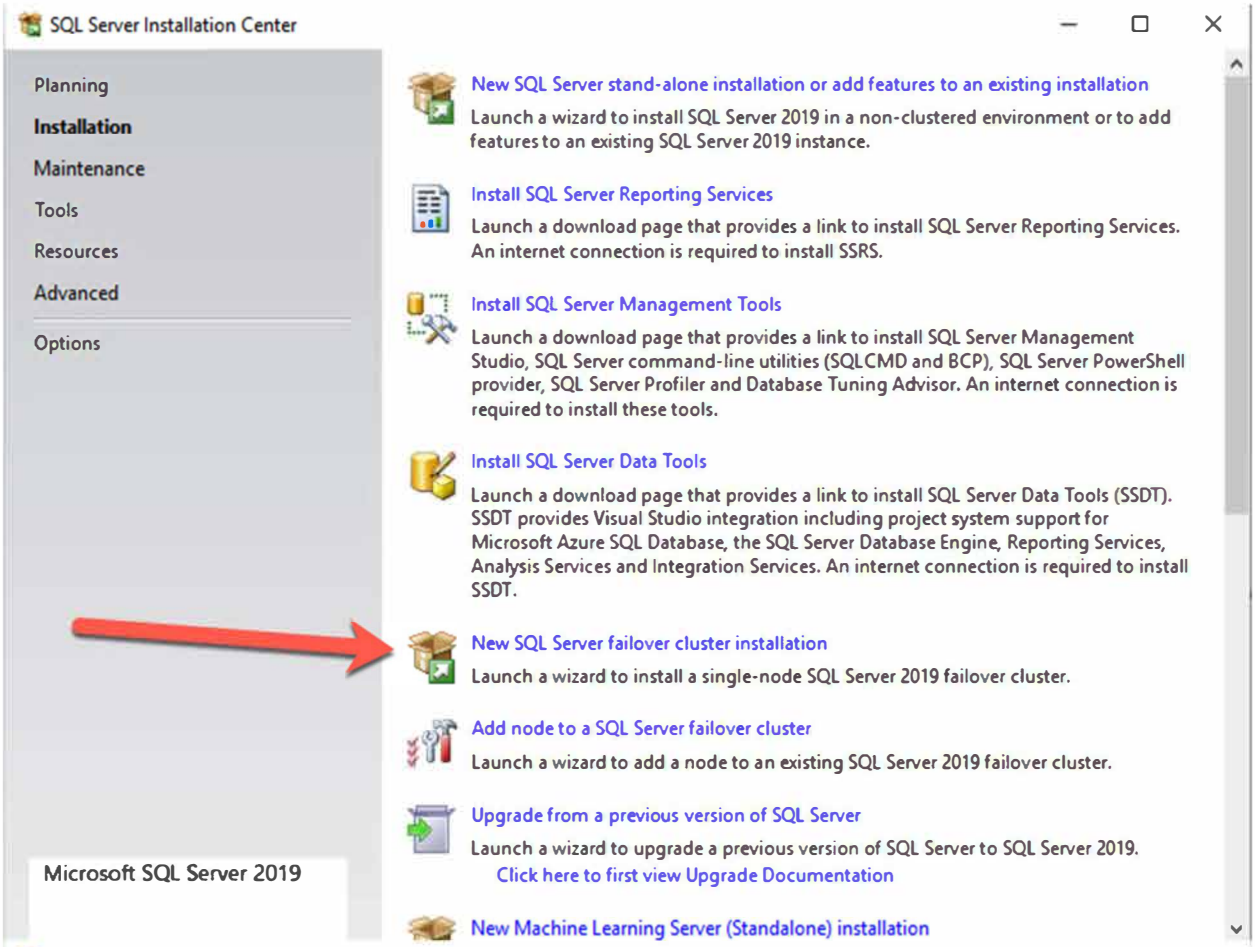
Install the First Node of the SQL Server FCI on SQL1

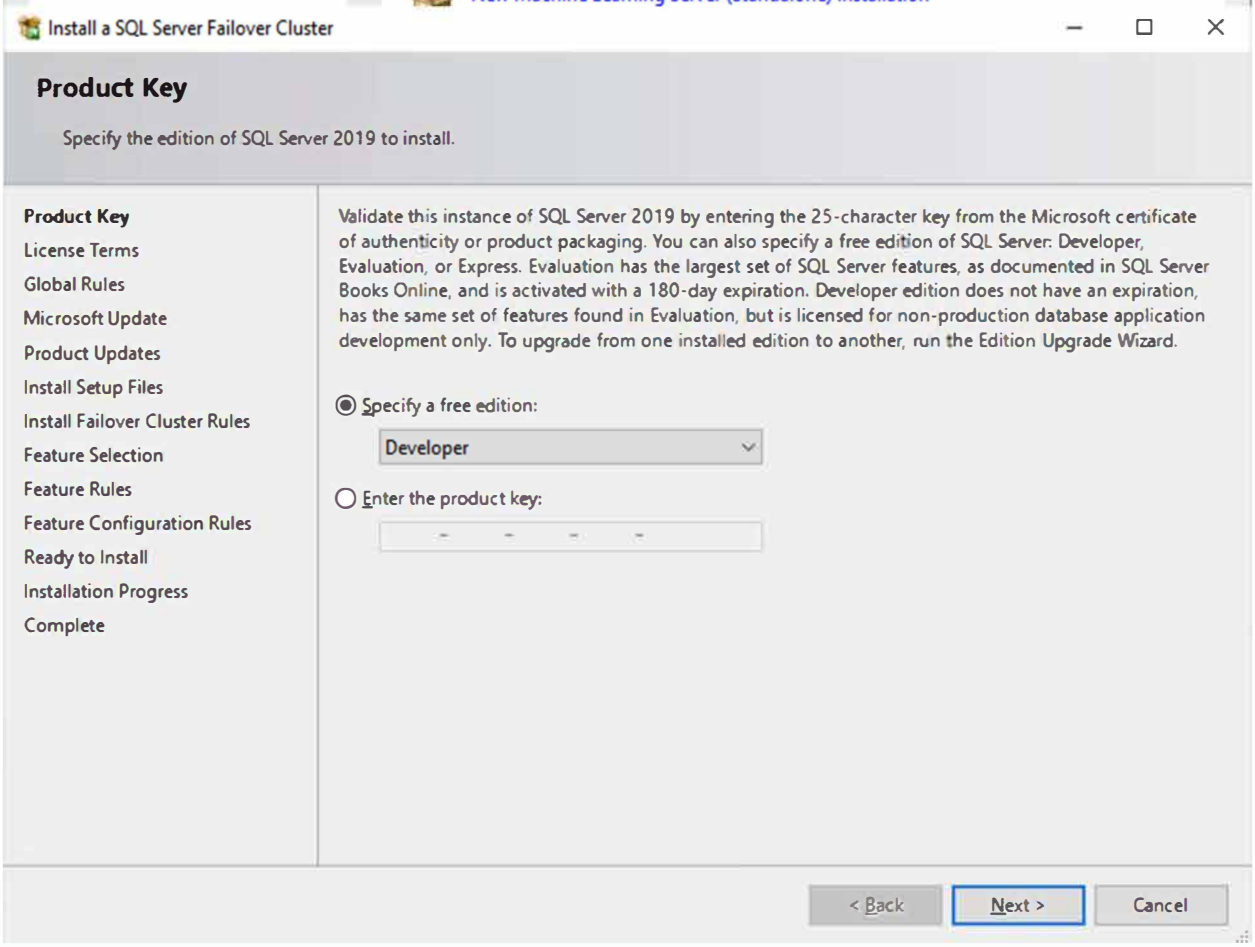
Now that the core cluster has been created and the DataKeeper volume resource is in Available Storage, it is time to install SQL Server on the first cluster node. As mentioned earlier, the example here illustrates a cluster configuration using SQL 2019 and Windows 2022, but all the steps described in this example are virtually identical, regardless of which version of Windows Server or SQL Server you are trying to deploy.

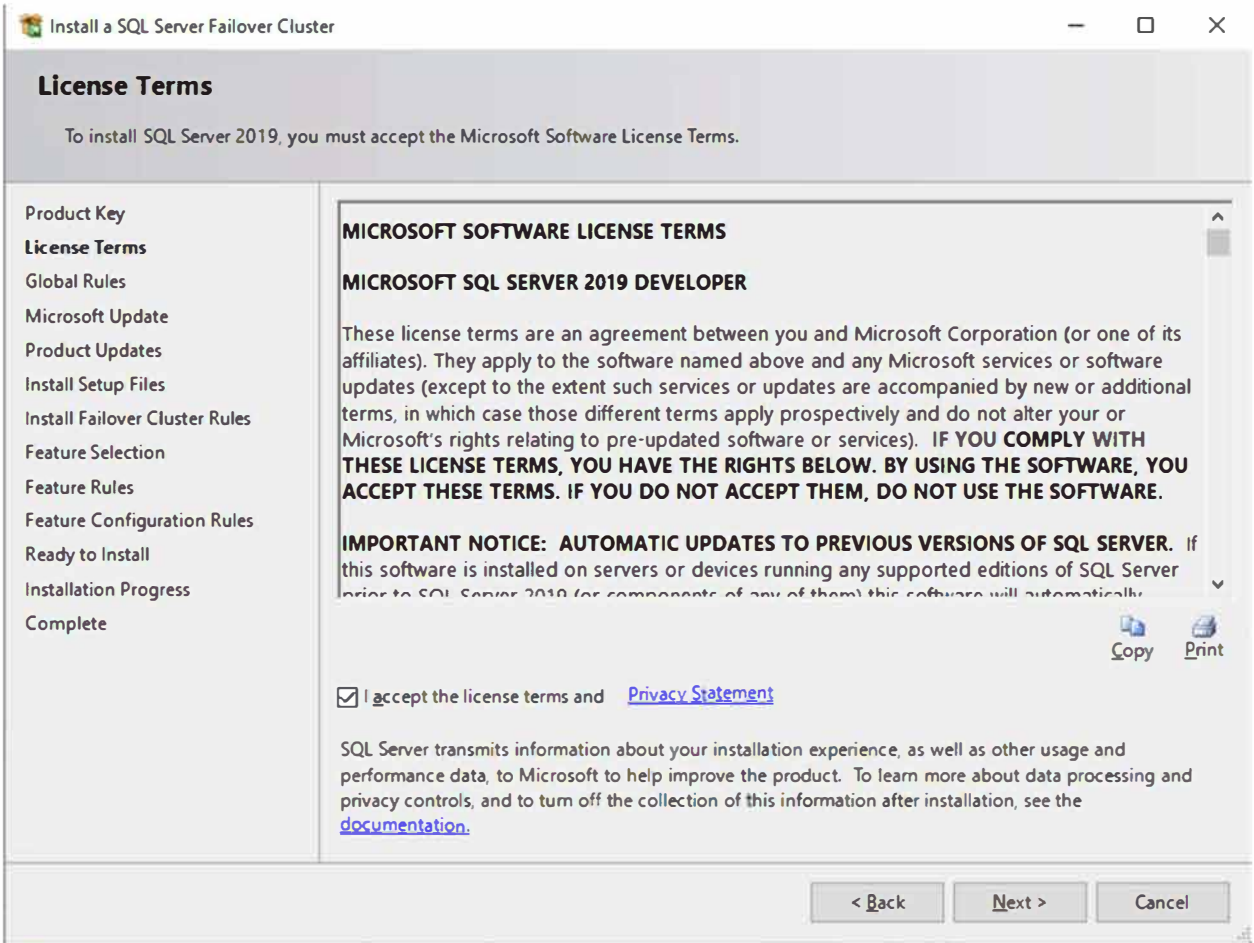
Follow the example below to install SQL Server on SQL1

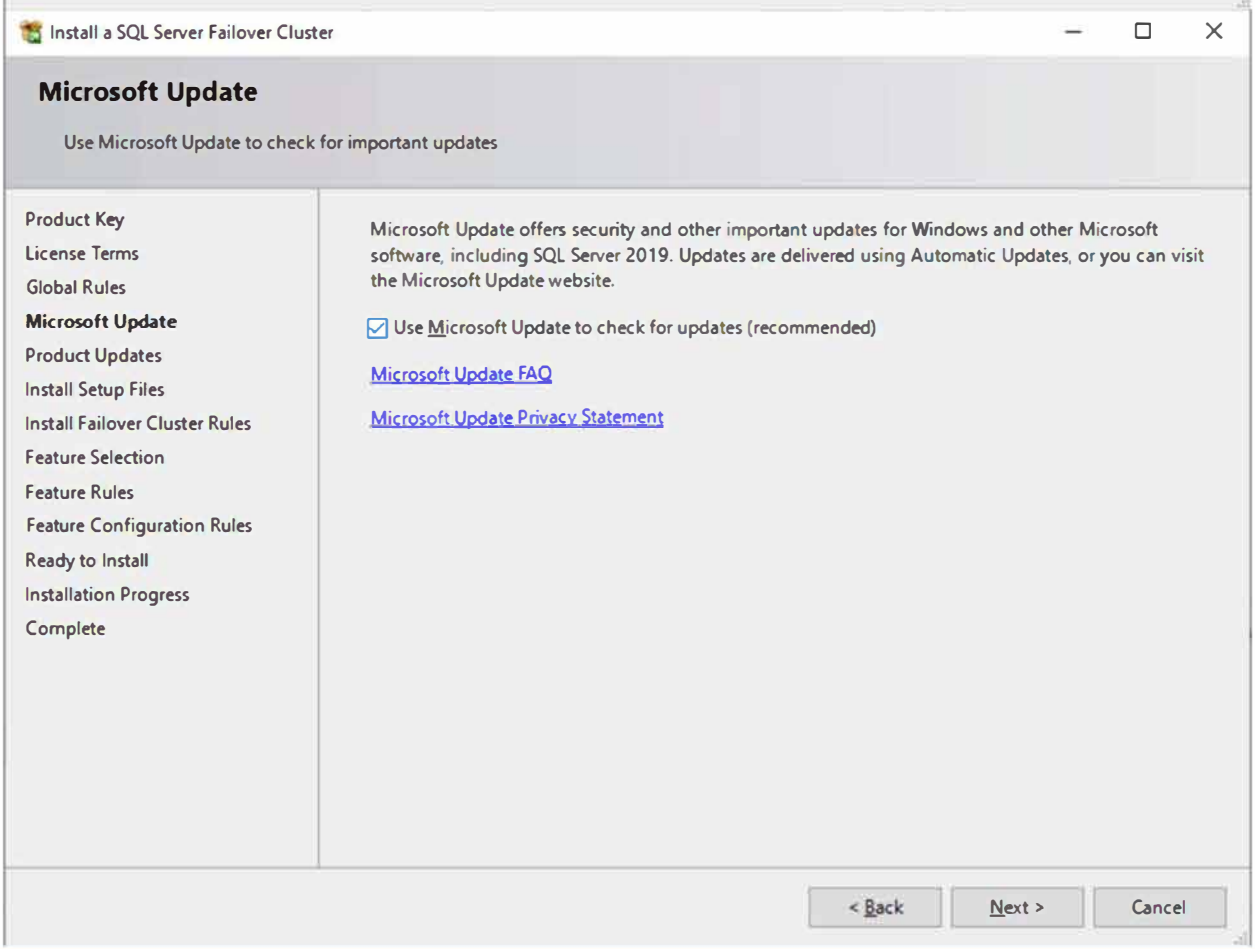

SQL Server 2019
Developer Edition
Select an installation type:
Basic
Select Basic installation type to install the SQL Server Database Engine feature with default configuration.
Custom
Select Custom installation type to step through the SQL Server installation wizard and choose what you want to install. This installation type is detailed and takes longer than running the Basic install.
Download Media
Download SQL Server setup files now and install them later on a machine of your choice.
SQL Server transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about data processing and privacy controls, and to turn off the collection of this information after installation, see the documentation.
15.2002.4709.1

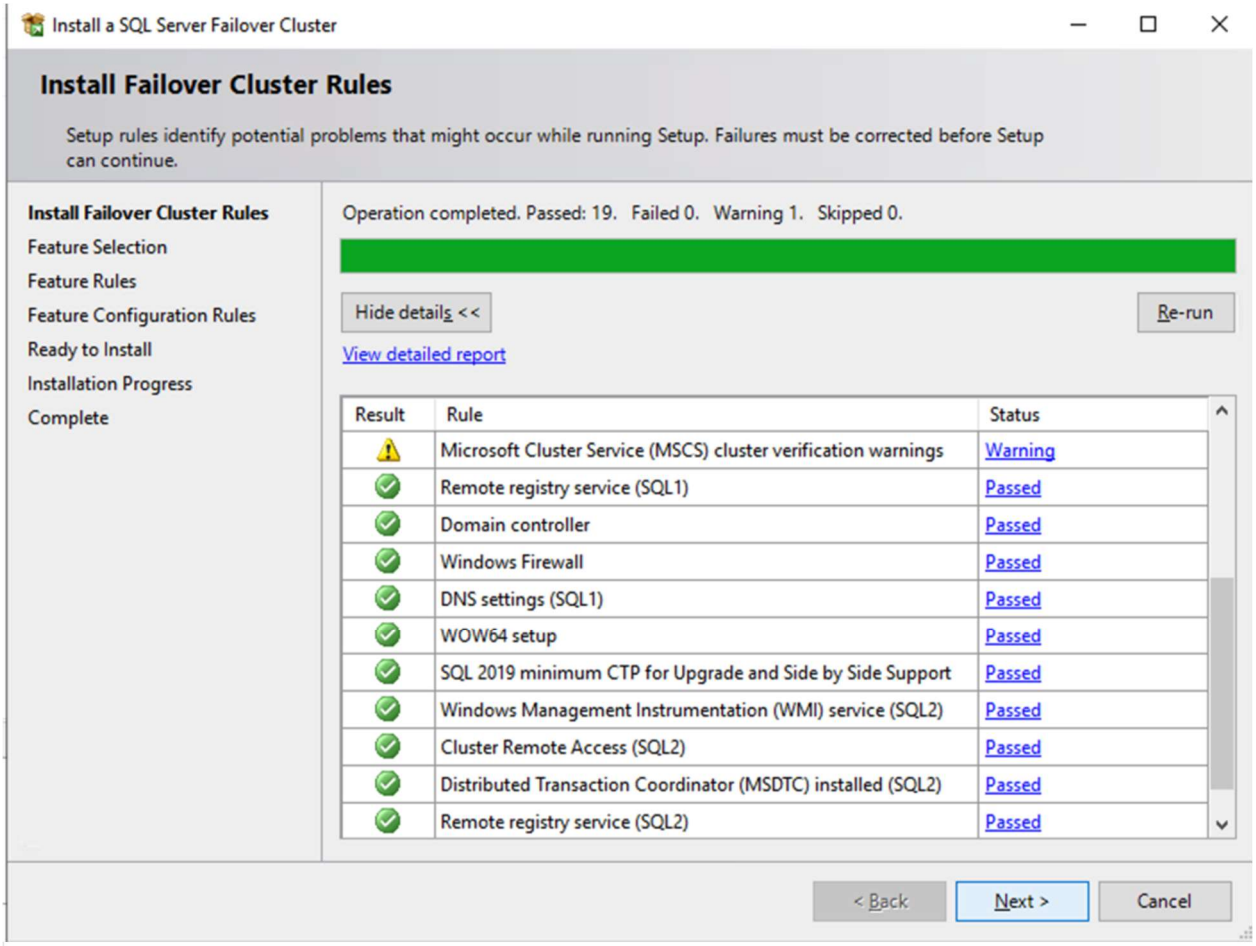

SQL Server 2019
Developer Edition
Specify SQL Server media download target location
MEDIA LOCATION
C:\SQL2019
Browse
MINIMUM FREE SPACE
8994 MB
DOWNLOAD SIZE
1426 MB
Close
< Previous
Install
15.2002.4709.1

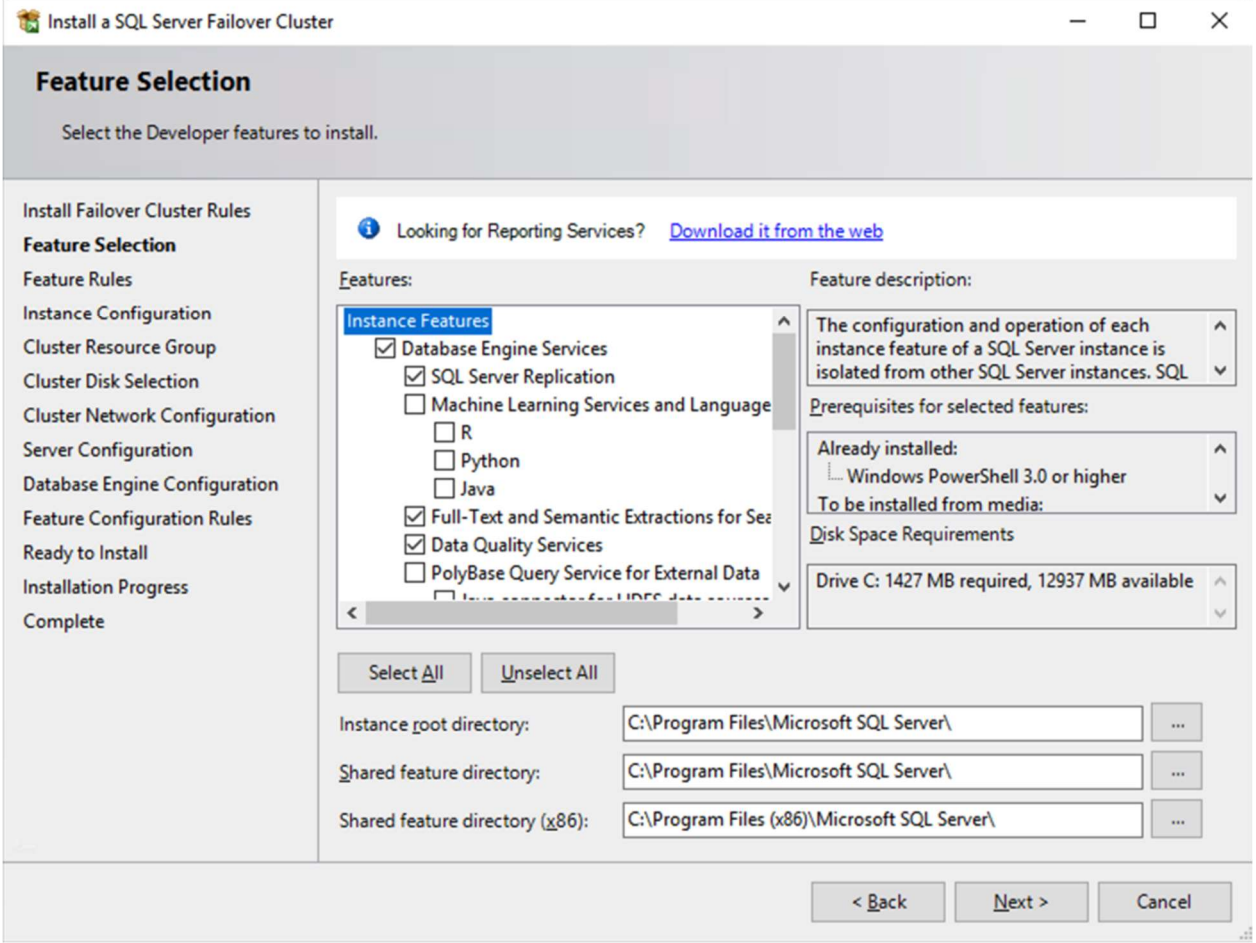

SQL Server Installation Center
Planning
Installation
Maintenance
Tools
Resources
Advanced
Options
New SQL Server stand-alone installation or add features to an existing installation
Launch a wizard to install SQL Server 2019 in a non-clustered environment or to add features to an existing SQL Server 2019 instance.
Install SQL Server Reporting Services
Launch a download page that provides a link to install SQL Server Reporting Services. An internet connection is required to install SSRS.
Install SQL Server Management Tools
Launch a download page that provides a link to install SQL Server Management Studio, SQL Server command-line utilities (SQLCMD and BCP), SQL Server PowerShell provider, SQL Server Profiler and Database Tuning Advisor. An internet connection is required to install these tools.
Install SQL Server Data Tools
Launch a download page that provides a link to install SQL Server Data Tools (SSDT). SSDT provides Visual Studio integration including project system support for Microsoft Azure SQL Database, the SQL Server Database Engine, Reporting Services, Analysis Services and Integration Services. An internet connection is required to install SSDT.
New SQL Server failover cluster installation
Launch a wizard to install a single-node SQL Server 2019 failover cluster.
Add node to a SQL Server failover cluster
Launch a wizard to add a node to an existing SQL Server 2019 failover cluster.
Upgrade from a previous version of SQL Server
Launch a wizard to upgrade a previous version of SQL Server to SQL Server 2019.
Click here to first view Upgrade Documentation
New Machine Learning Server (Standalone) installation
Microsoft SQL Server 2019


Install a SQL Server Failover Cluster
Product Key
Specify the edition of SQL Server 2019 to install.
Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Failover Cluster Rules
Feature Selection
Feature Rules
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Validate this instance of SQL Server 2019 by entering the 25-character key from the Microsoft certificate of authenticity or product packaging. You can also specify a free edition of SQL Server: Developer, Evaluation, or Express. Evaluation has the largest set of SQL Server features, as documented in SQL Server Books Online, and is activated with a 180-day expiration. Developer edition does not have an expiration, has the same set of features found in Evaluation, but is licensed for non-production database application development only. To upgrade from one installed edition to another, run the Edition Upgrade Wizard.
Specify a free edition:
Developer
Enter the product key:
< Back
Next >
Cancel

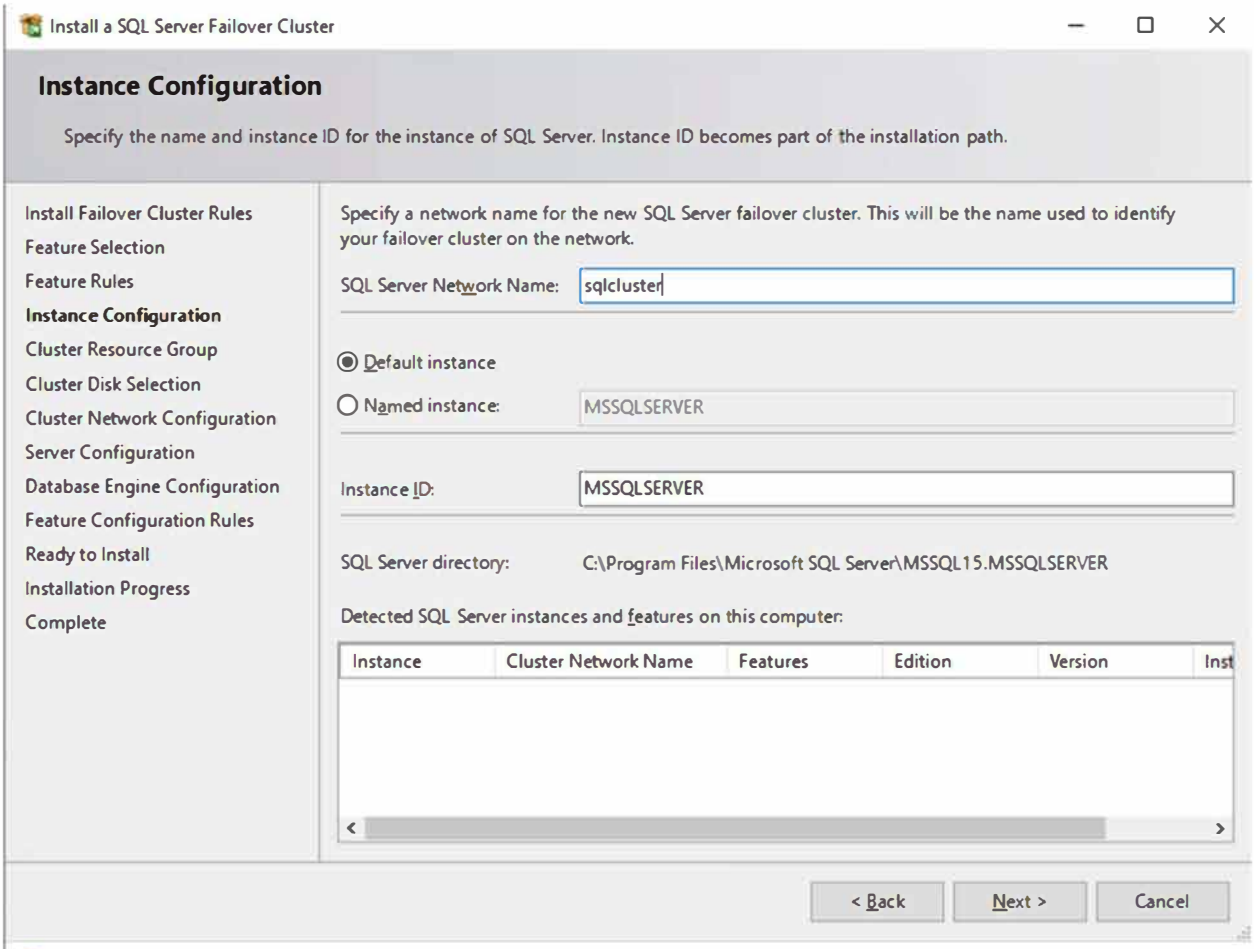

Install a SQL Server Failover Cluster
License Terms
To install SQL Server 2019, you must accept the Microsoft Software License Terms.
Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Failover Cluster Rules
Feature Selection
Feature Rules
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
MICROSOFT SOFTWARE LICENSE TERMS
MICROSOFT SQL SERVER 2019 DEVELOPER
These license terms are an agreement between you and Microsoft Corporation (or one of its affiliates). They apply to the software named above and any Microsoft services or software updates (except to the extent such services or updates are accompanied by new or additional terms, in which case those different terms apply prospectively and do not alter your or Microsoft's rights relating to pre-updated software or services). IF YOU COMPLY WITH THESE LICENSE TERMS, YOU HAVE THE RIGHTS BELOW. BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT USE THE SOFTWARE.
IMPORTANT NOTICE: AUTOMATIC UPDATES TO PREVIOUS VERSIONS OF SQL SERVER. If this software is installed on servers or devices running any supported editions of SQL Server
Copy
Print
I accept the license terms and
Privacy Statement
SQL Server transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about data processing and privacy controls, and to turn off the collection of this information after installation, see the documentation.
< Back
Next >
Cancel

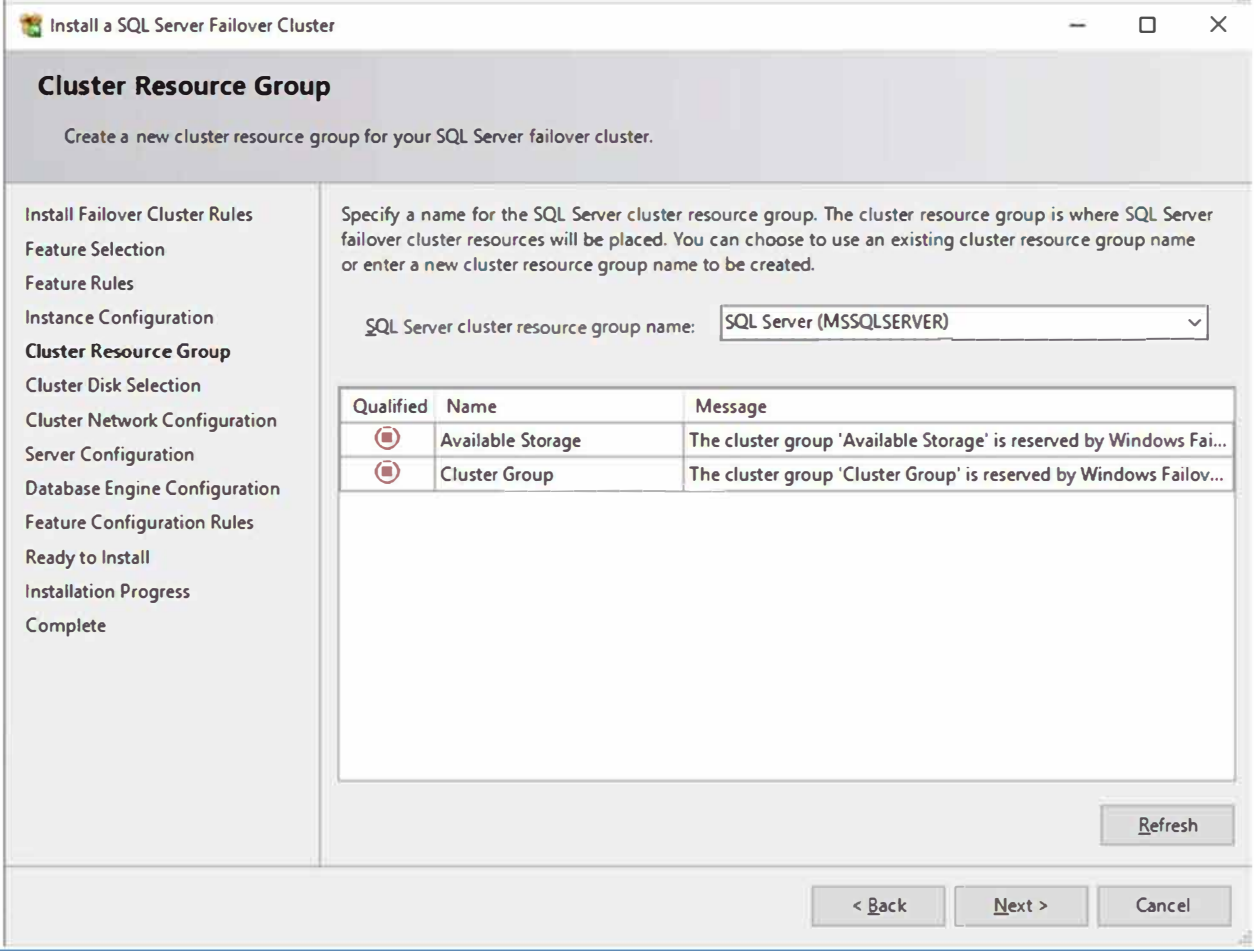

Install a SQL Server Failover Cluster
Microsoft Update
Use Microsoft Update to check for important updates
Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Failover Cluster Rules
Feature Selection
Feature Rules
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Microsoft Update offers security and other important updates for Windows and other Microsoft software, including SQL Server 2019. Updates are delivered using Automatic Updates, or you can visit the Microsoft Update website.
Use Microsoft Update to check for updates (recommended)
Microsoft Update FAQ
Microsoft Update Privacy Statement
< Back
Next >
Cancel

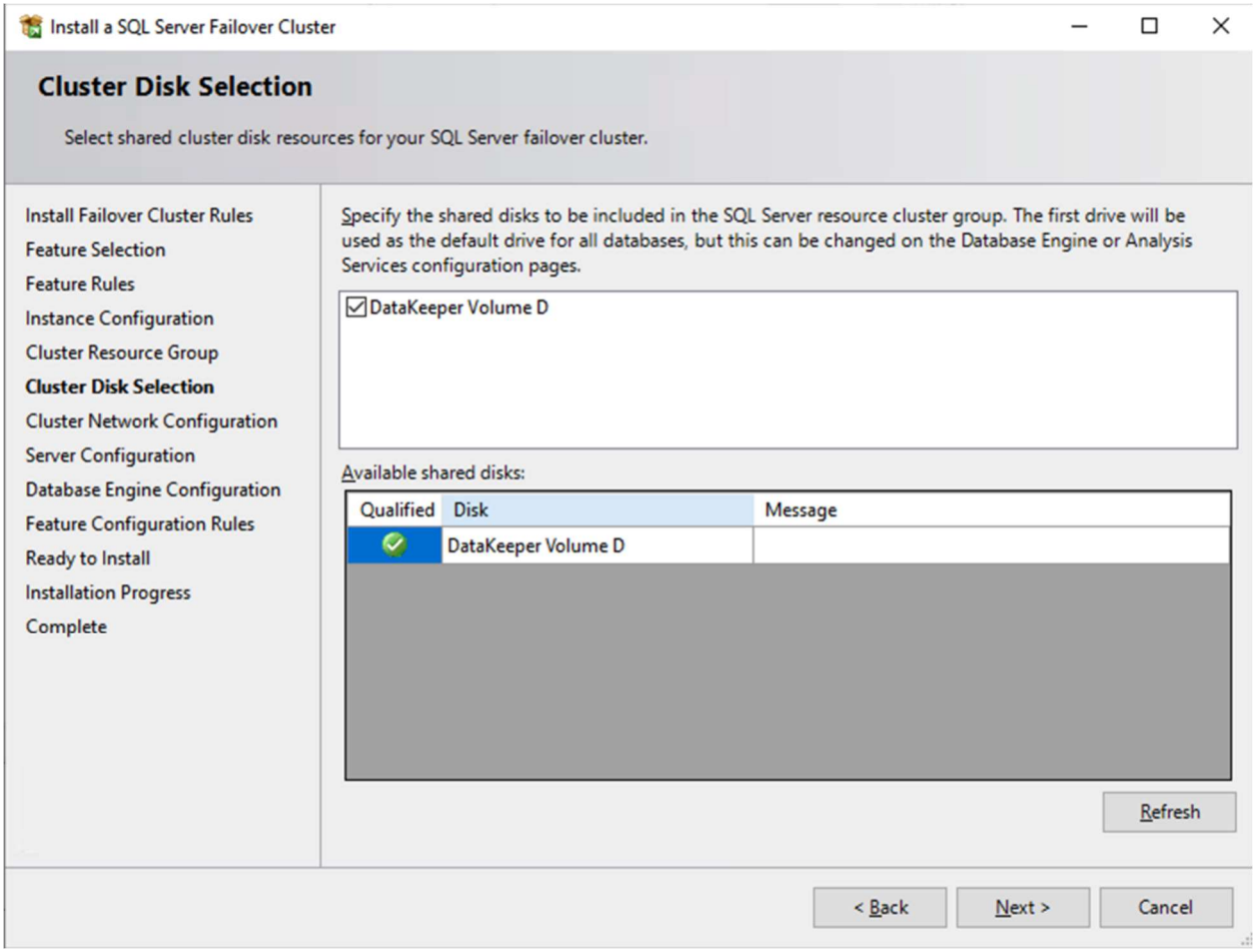

Install a SQL Server Failover Cluster
Install Failover Cluster Rules
Setup rules identify potential problems that might occur while running Setup. Failures must be corrected before Setup can continue.
Install Failover Cluster Rules
Feature Selection
Feature Rules
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Operation completed. Passed: 19. Failed 0. Warning 1. Skipped 0.
Hide details <<
Re-run
View detailed report
Result
Rule
Status
Microsoft Cluster Service (MSCS) cluster verification warnings
Warning
Remote registry service (SQL1)
Passed
Domain controller
Passed
Windows Firewall
Passed
DNS settings (SQL1)
Passed
WOW64 setup
Passed
SQL 2019 minimum CTP for Upgrade and Side by Side Support
Passed
Windows Management Instrumentation (WMI) service (SQL2)
Passed
Cluster Remote Access (SQL2)
Passed
Distributed Transaction Coordinator (MSDTC) installed (SQL2)
Passed
Remote registry service (SQL2)
Passed
< Back
Next >
Cancel


Install a SQL Server Failover Cluster
Feature Selection
Select the Developer features to install.
Install Failover Cluster Rules
Feature Selection
Feature Rules
Instance Configuration
Cluster Resource Group
Cluster Disk Selection
Cluster Network Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Looking for Reporting Services?
Download it from the web
Features:
Feature description:
Instance Features
Database Engine Services
SQL Server Replication
Machine Learning Services and Language
R
Python
Java
Full-Text and Semantic Extractions for Sea
Data Quality Services
PolyBase Query Service for External Data
The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL
Prerequisites for selected features:
Already installed:
Windows PowerShell 3.0 or higher
To be installed from media:
Disk Space Requirements
Drive C: 1427 MB required, 12937 MB available
Select All
Unselect All
Instance root directory:
C:\Program Files\Microsoft SQL Server\
Shared feature directory:
C:\Program Files\Microsoft SQL Server\
Shared feature directory (x86):
C:\Program Files (x86)\Microsoft SQL Server\
< Back
Next >
Cancel

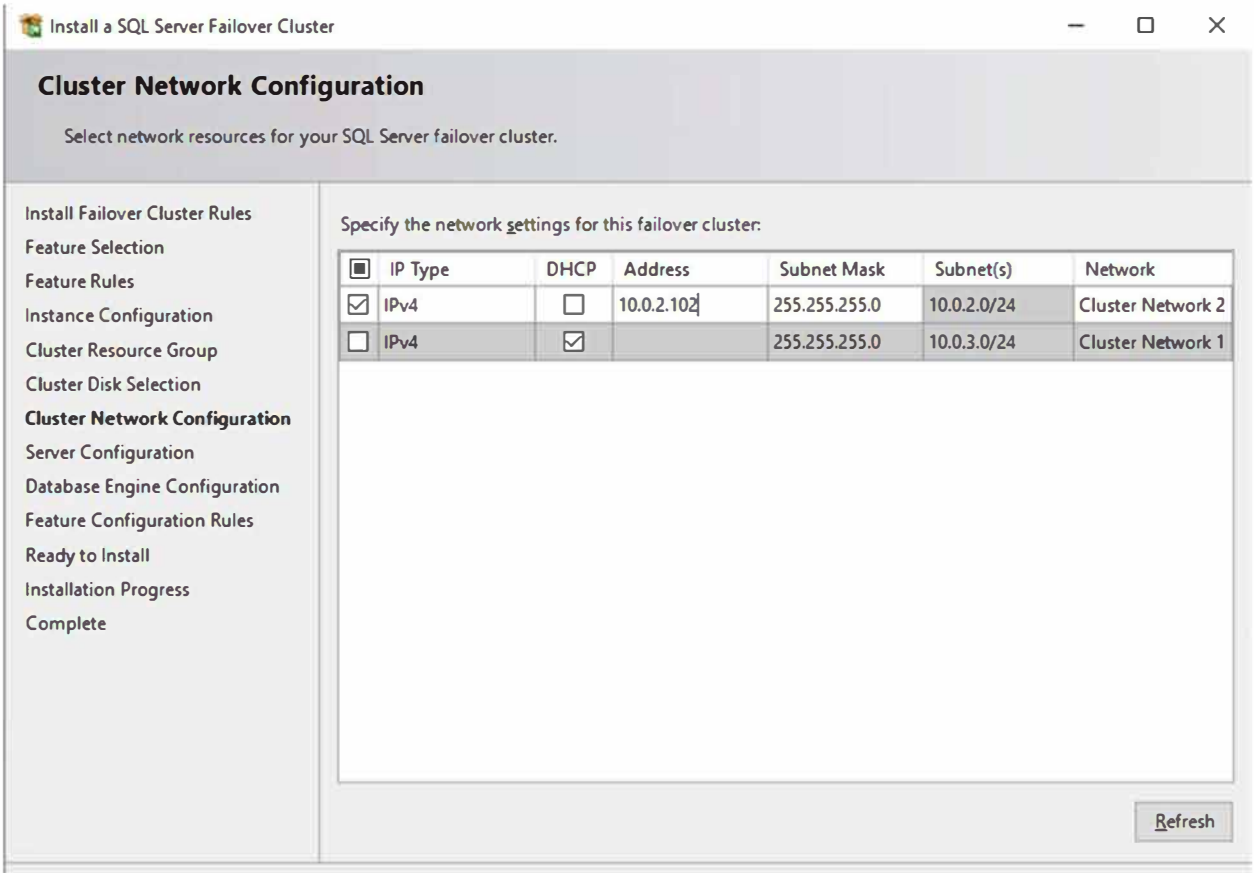
The name you specify below is the client access point. This is the name your application servers will use when they want to connect to the SQL Server FCI.

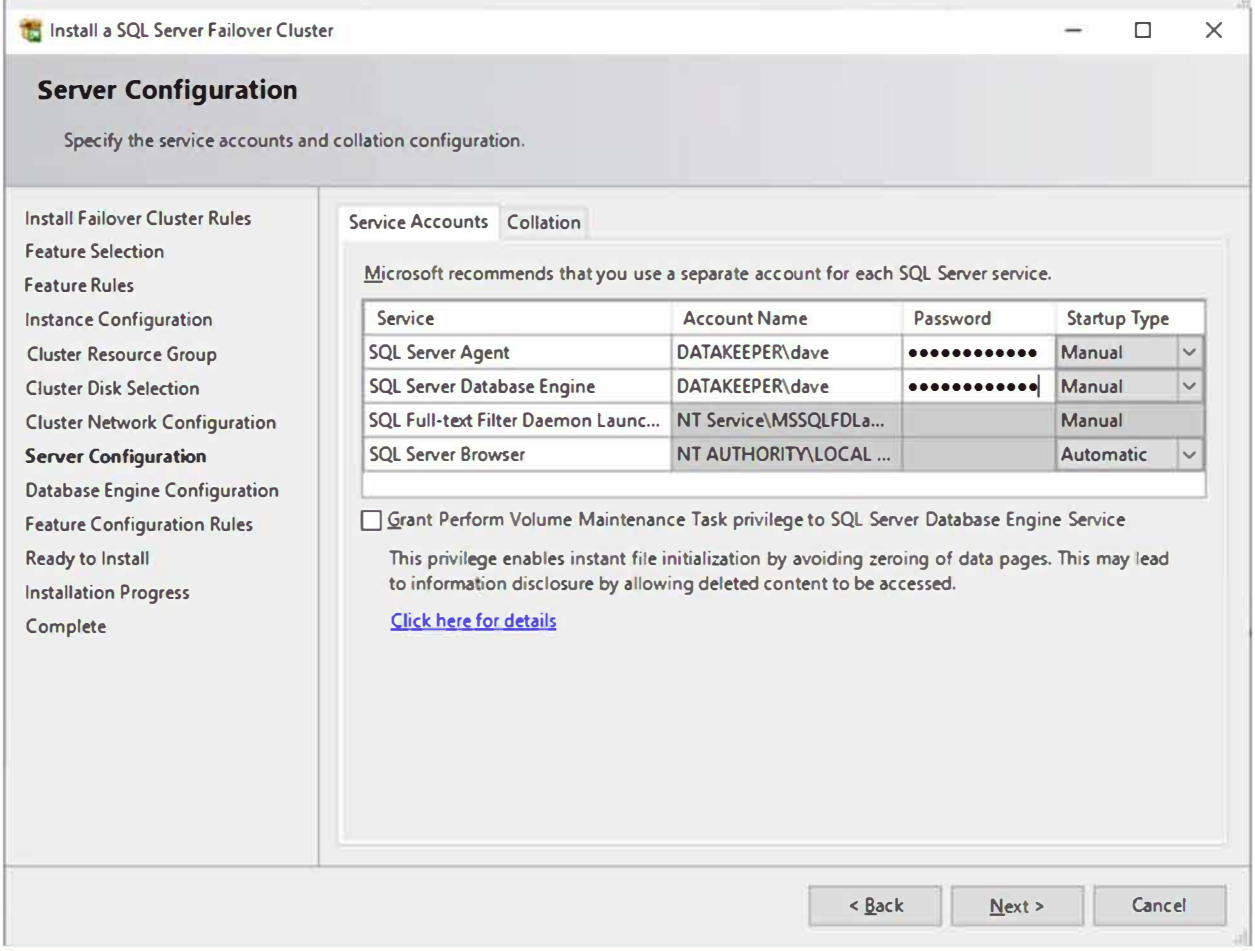

Install a SQL Server Failover Cluster
Instance Configuration
Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.
Install Failover Cluster Rules
Feature Selection
Feature Rules
Instance Configuration
Cluster Resource Group
Cluster Disk Selection
Cluster Network Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Specify a network name for the new SQL Server failover cluster. This will be the name used to identify your failover cluster on the network.
SQL Server Network Name: sqlcluster
Default instance
Named instance: MSSQLSERVER
Instance ID: MSSQLSERVER
SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER
Detected SQL Server instances and features on this computer:
Instance
Cluster Network Name
Features
Edition
Version
Inst
< Back
Next >
Cancel

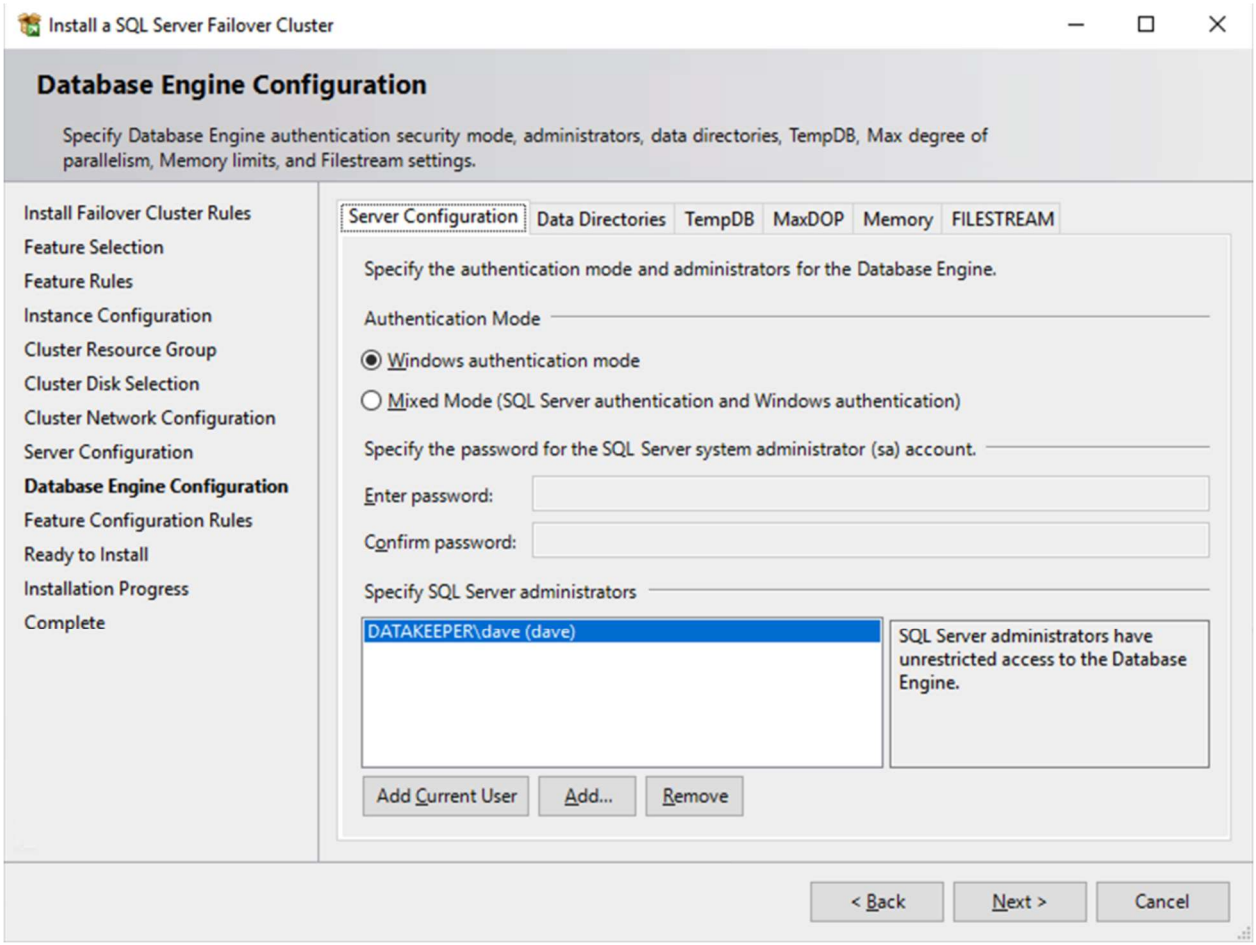

Install a SQL Server Failover Cluster
Cluster Resource Group
Create a new cluster resource group for your SQL Server failover cluster.
Install Failover Cluster Rules
Feature Selection
Feature Rules
Instance Configuration
Cluster Resource Group
Cluster Disk Selection
Cluster Network Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Specify a name for the SQL Server cluster resource group. The cluster resource group is where SQL Server failover cluster resources will be placed. You can choose to use an existing cluster resource group name or enter a new cluster resource group name to be created.
SQL Server cluster resource group name: SQL Server (MSSQLSERVER)
Qualified
Name
Message
Available Storage
The cluster group 'Available Storage' is reserved by Windows Fai...
Cluster Group
The cluster group 'Cluster Group' is reserved by Windows Failov...
Refresh
< Back
Next >
Cancel



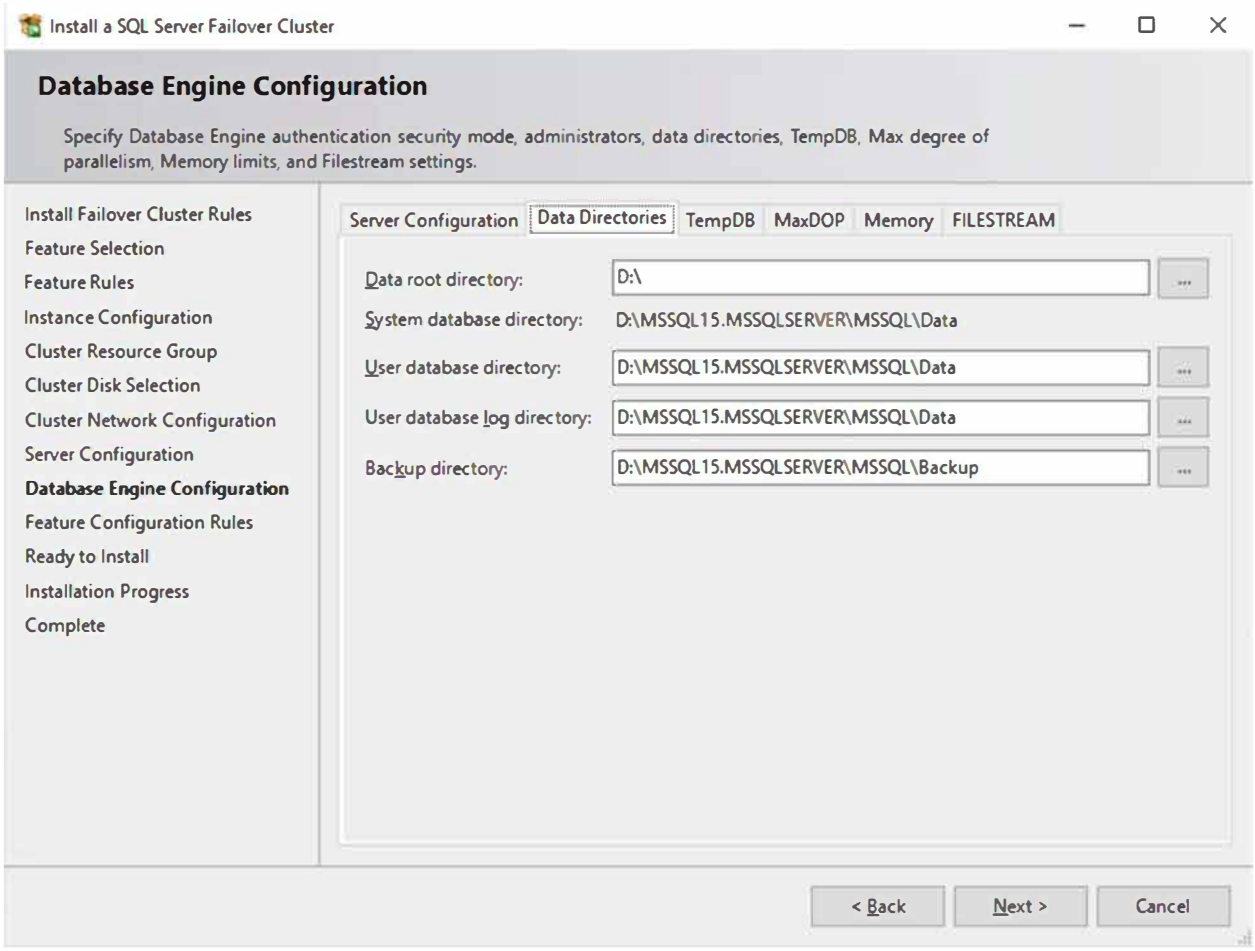
On this screen you will add the SQL1 secondary IP address we identified earlier in the planning section of Part 1 of this series.

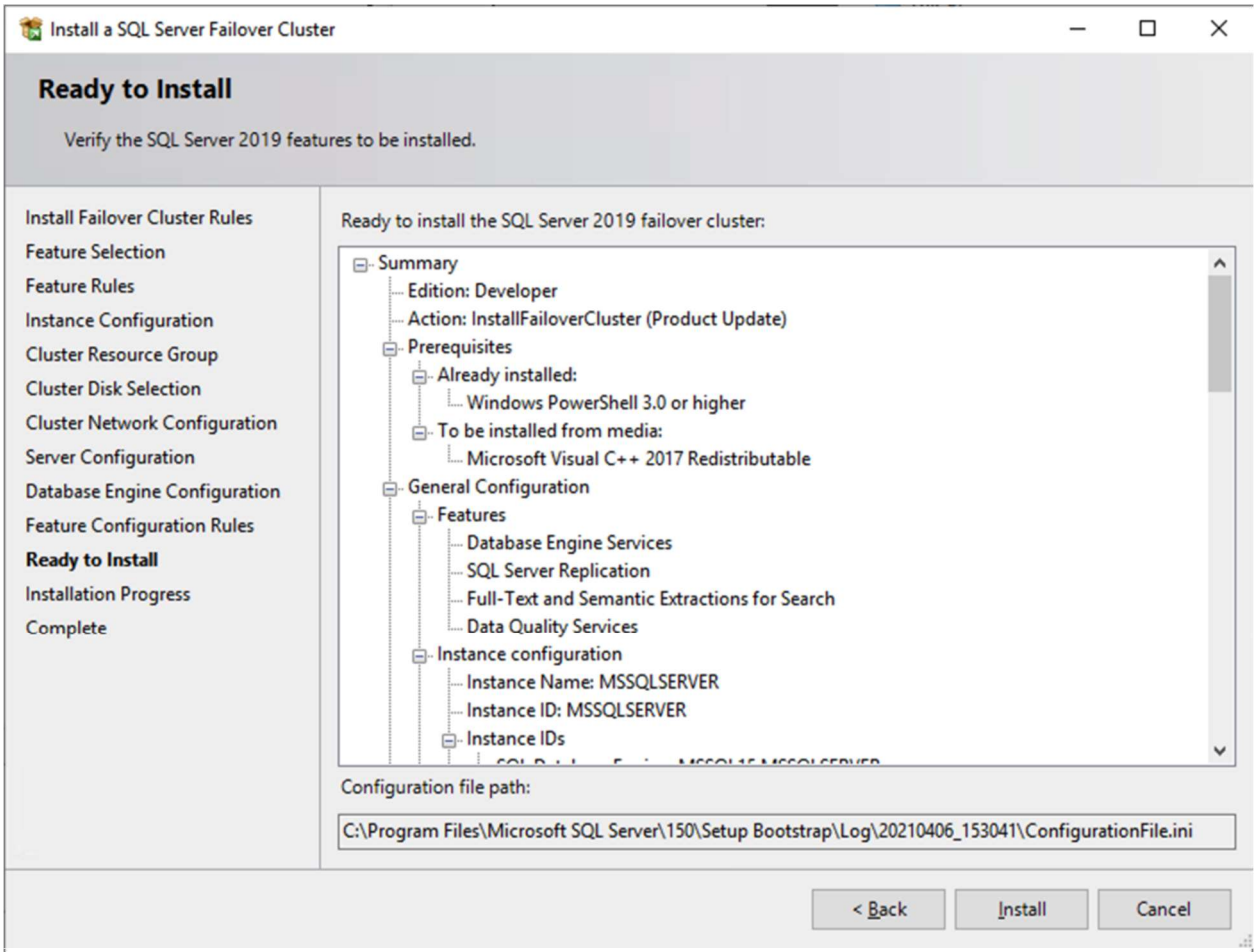

Install a SQL Server Failover Cluster
Cluster Network Configuration
Select network resources for your SQL Server failover cluster.
Install Failover Cluster Rules
Feature Selection
Feature Rules
Instance Configuration
Cluster Resource Group
Cluster Disk Selection
Cluster Network Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Specify the network settings for this failover cluster:
IP Type
DHCP
Address
Subnet Mask
Subnet(s)
Network
IPv4
10.0.2.102
255.255.255.0
10.0.2.0/24
Cluster Network 2
IPv4
255.255.255.0
10.0.3.0/24
Cluster Network 1
Refresh
< Back
Next >
Cancel

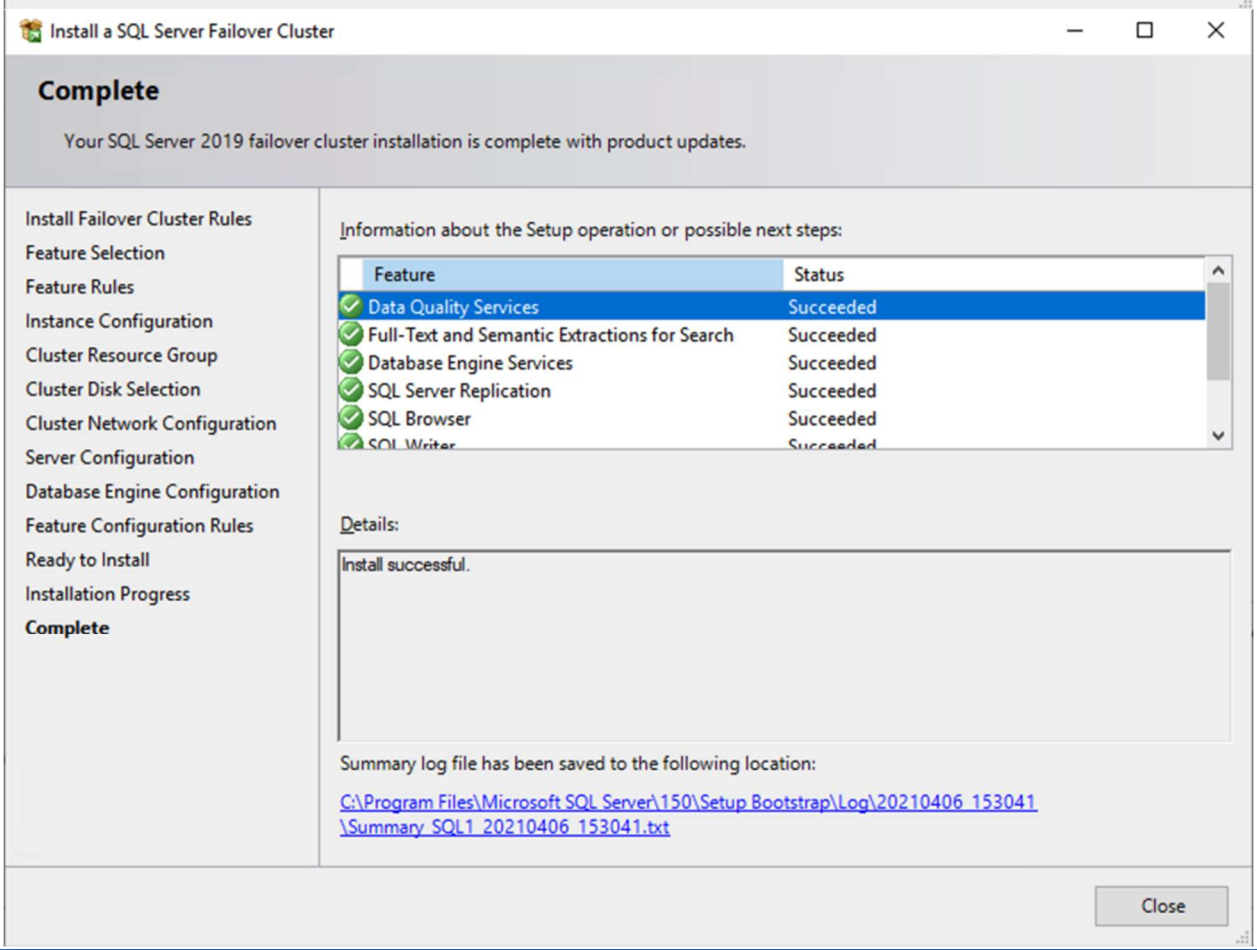

Install a SQL Server Failover Cluster
Server Configuration
Specify the service accounts and collation configuration.
Install Failover Cluster Rules
Feature Selection
Feature Rules
Instance Configuration
Cluster Resource Group
Cluster Disk Selection
Cluster Network Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Service Accounts
Collation
Microsoft recommends that you use a separate account for each SQL Server service.
Service
Account Name
Password
Startup Type
SQL Server Agent
DATAKEEPER\dave
Manual
SQL Server Database Engine
DATAKEEPER\dave
Manual
SQL Full-text Filter Daemon Launc...
NT Service\MSSQLFDLa...
Manual
SQL Server Browser
NT AUTHORITY\LOCAL ...
Automatic
Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service
This privilege enables instant file initialization by avoiding zeroing of data pages. This may lead to information disclosure by allowing deleted content to be accessed.
Click here for details
< Back
Next >
Cancel



In this example we left tempdb on the D drive. However, for best performance it is recommended that you locate tempdb on a non-replicated volume.

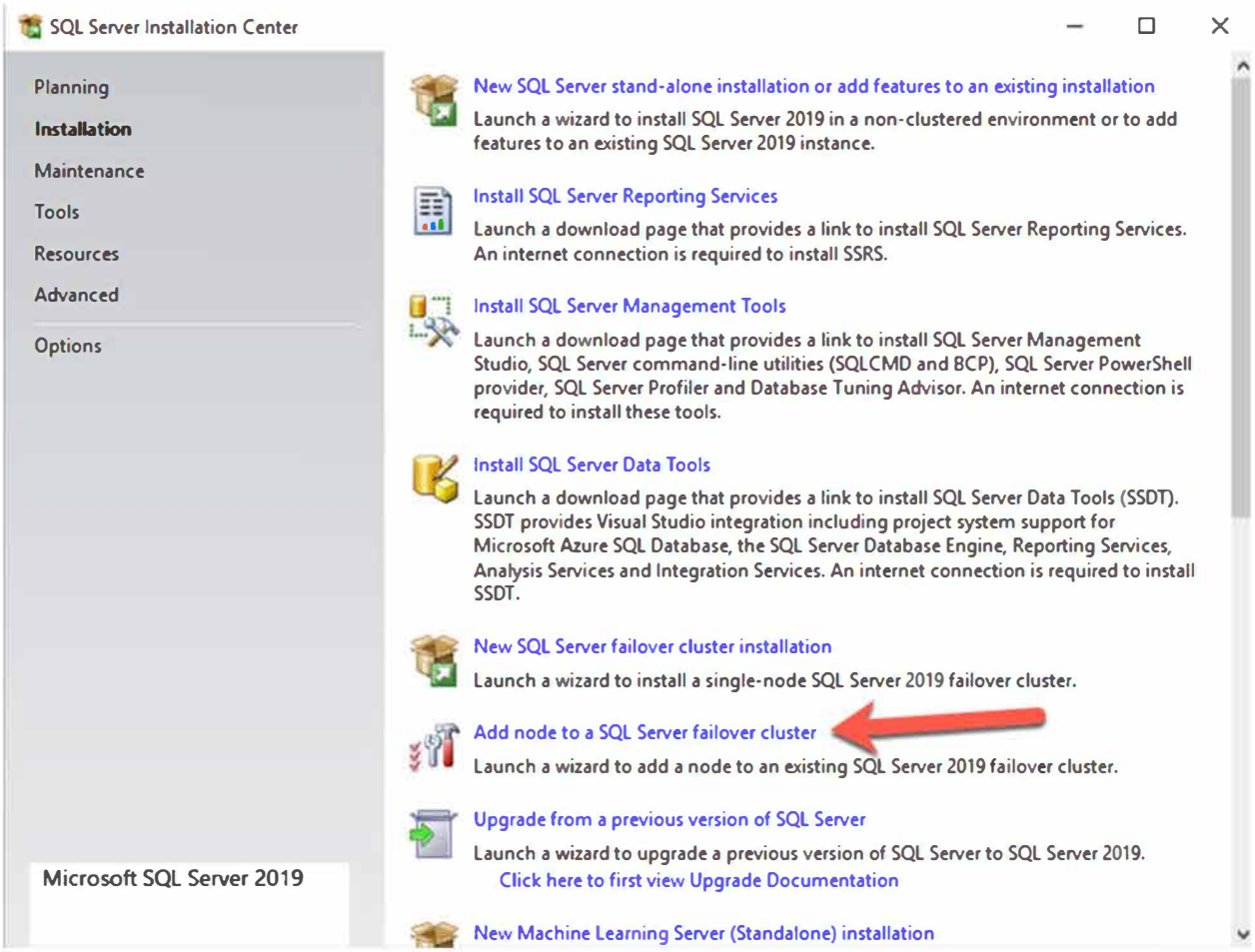

Install a SQL Server Failover Cluster
Database Engine Configuration
Specify Database Engine authentication security mode, administrators, data directories, TempDB, Max degree of parallelism, Memory limits, and Filestream settings.
Install Failover Cluster Rules
Feature Selection
Feature Rules
Instance Configuration
Cluster Resource Group
Cluster Disk Selection
Cluster Network Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Server Configuration
Data Directories
TempDB
MaxDOP
Memory
FILESTREAM
Data root directory:
D:\
System database directory:
D:\MSSQL15.MSSQLSERVER\MSSQL\Data
User database directory:
D:\MSSQL15.MSSQLSERVER\MSSQL\Data
User database log directory:
D:\MSSQL15.MSSQLSERVER\MSSQL\Data
Backup directory:
D:\MSSQL15.MSSQLSERVER\MSSQL\Backup
< Back
Next >
Cancel

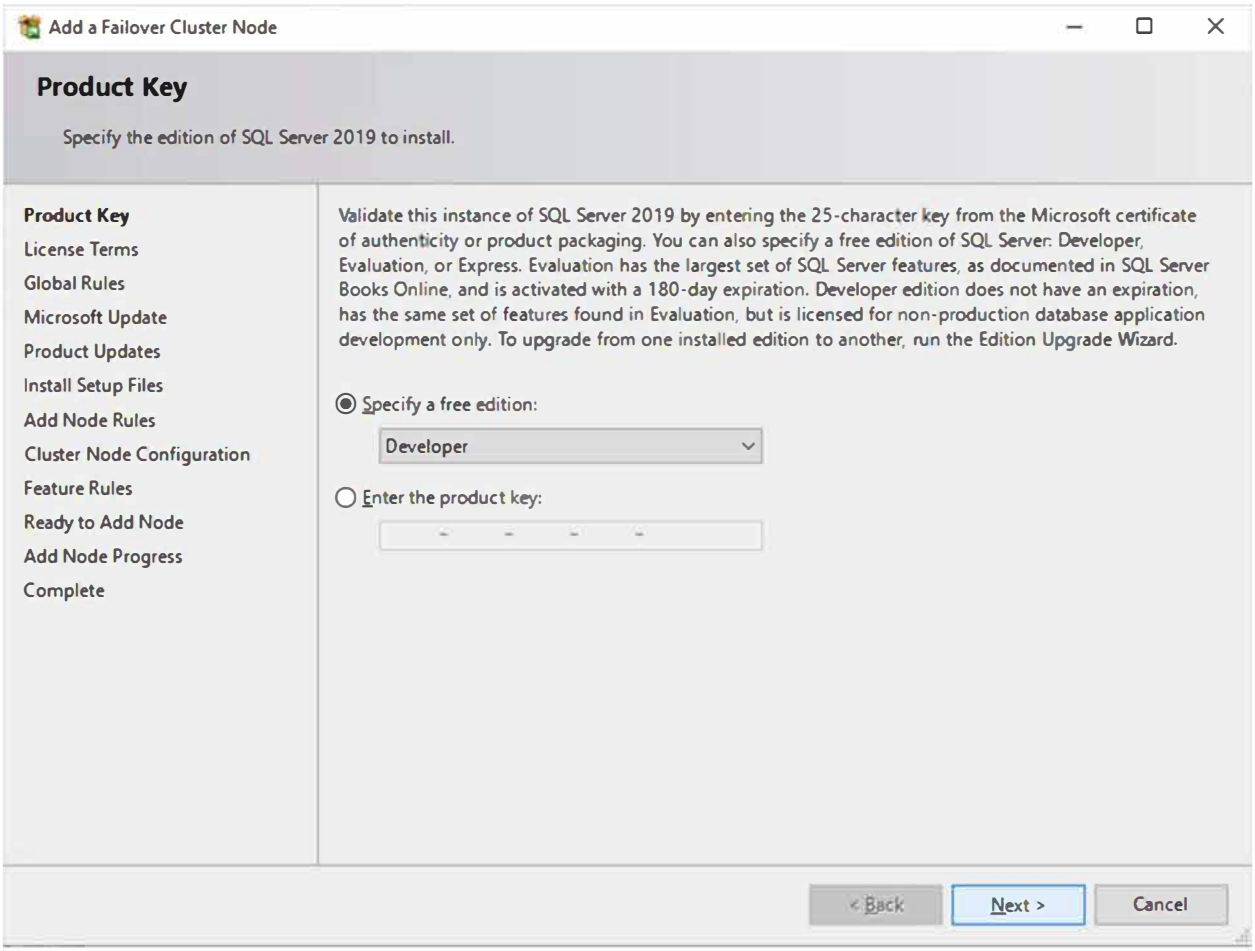

Install a SQL Server Failover Cluster
Ready to Install
Verify the SQL Server 2019 features to be installed.
Install Failover Cluster Rules
Feature Selection
Feature Rules
Instance Configuration
Cluster Resource Group
Cluster Disk Selection
Cluster Network Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Ready to install the SQL Server 2019 failover cluster:
Summary
Edition: Developer
Action: InstallFailoverCluster (Product Update)
Prerequisites
Already installed:
Windows PowerShell 3.0 or higher
To be installed from media:
Microsoft Visual C++ 2017 Redistributable
General Configuration
Features
Database Engine Services
SQL Server Replication
Full-Text and Semantic Extractions for Search
Data Quality Services
Instance configuration
Instance Name: MSSQLSERVER
Instance ID: MSSQLSERVER
Instance IDs
Configuration file path:
C:\Program Files\Microsoft SQL Server\150\Setup Bootstrap\Log\20210406_153041\ConfigurationFile.ini
< Back
Install
Cancel

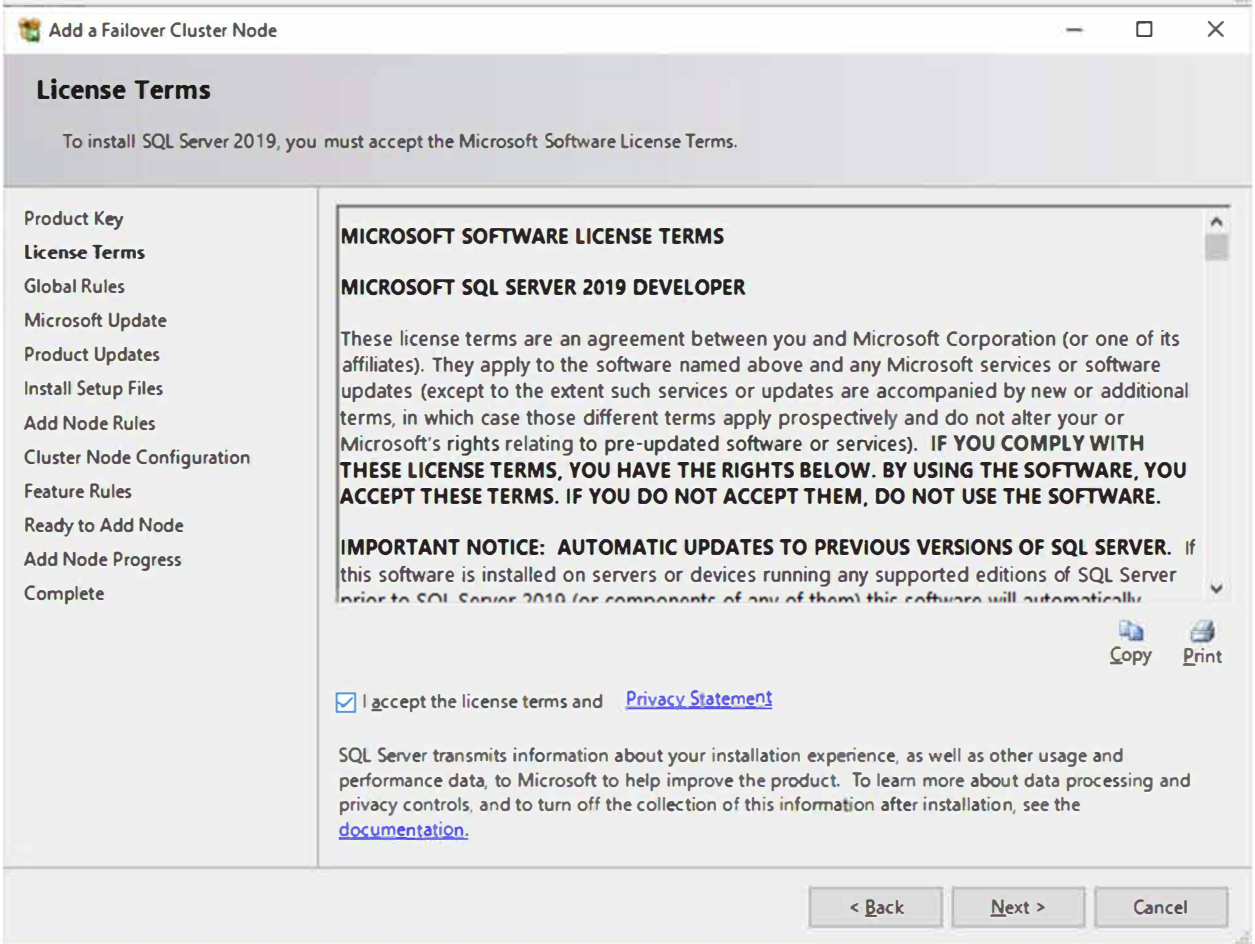

Install a SQL Server Failover Cluster
Complete
Your SQL Server 2019 failover cluster installation is complete with product updates.
Install Failover Cluster Rules
Feature Selection
Feature Rules
Instance Configuration
Cluster Resource Group
Cluster Disk Selection
Cluster Network Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Information about the Setup operation or possible next steps:
Feature
Status
Data Quality Services
Succeeded
Full-Text and Semantic Extractions for Search
Succeeded
Database Engine Services
Succeeded
SQL Server Replication
Succeeded
SQL Browser
Succeeded
Details:
Install successful.
Summary log file has been saved to the following location:
C:\Program Files\Microsoft SQL Server\150\Setup Bootstrap\Log\20210406_153041\Summary_SQL1_20210406_153041.txt
Close

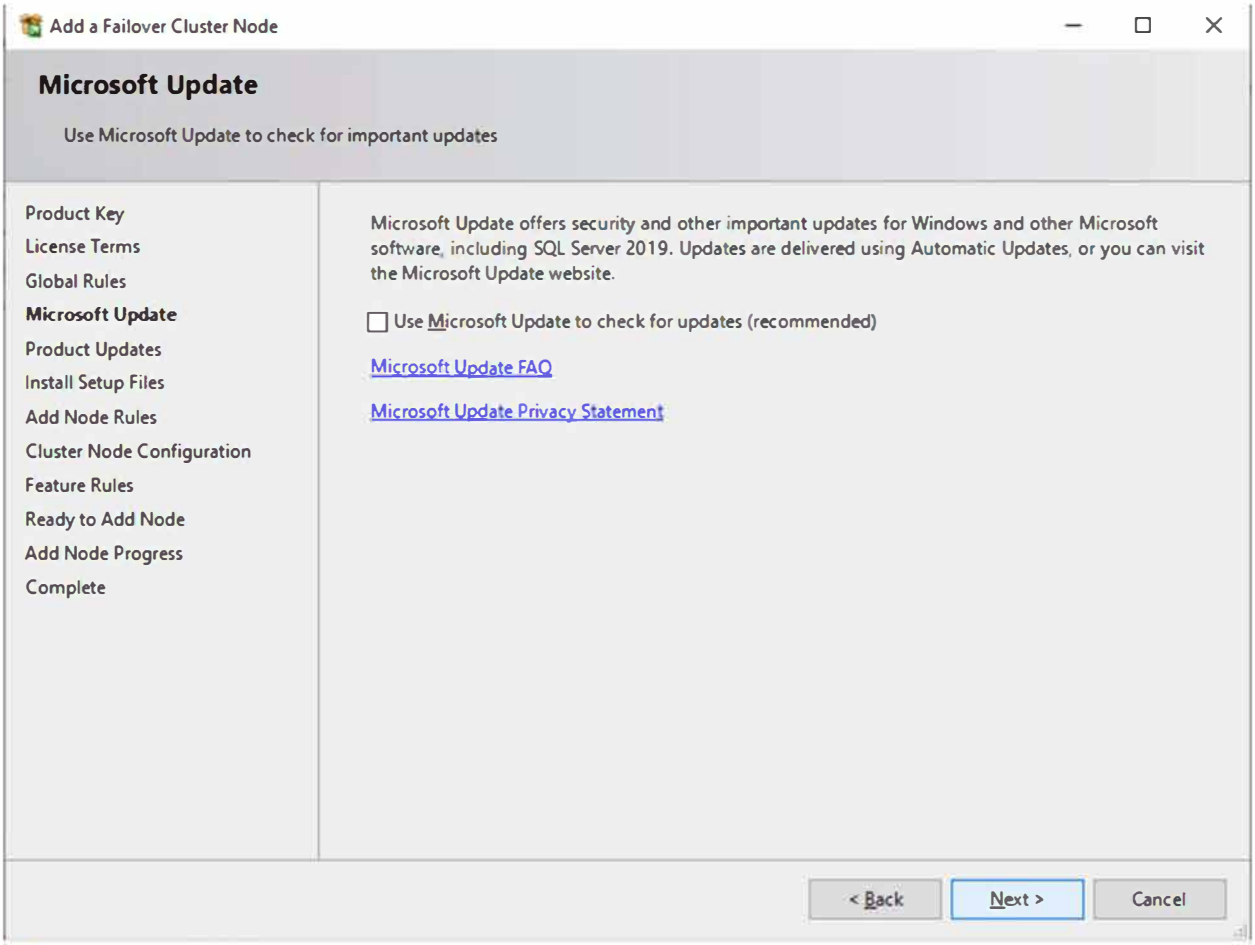
Install the second node of the SQL Server FCI on SQL2

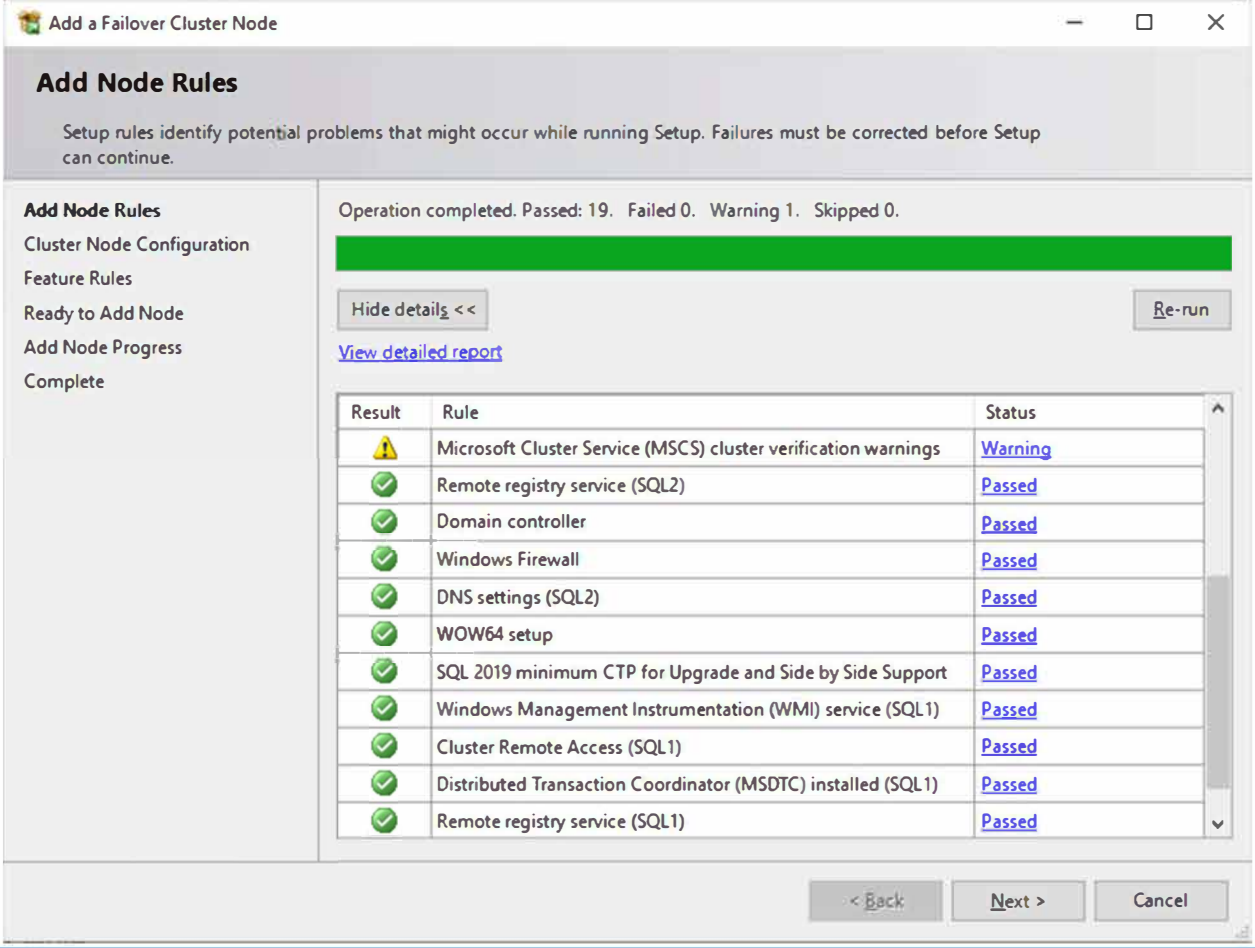
It is now time to install SQL Server on SQL2.

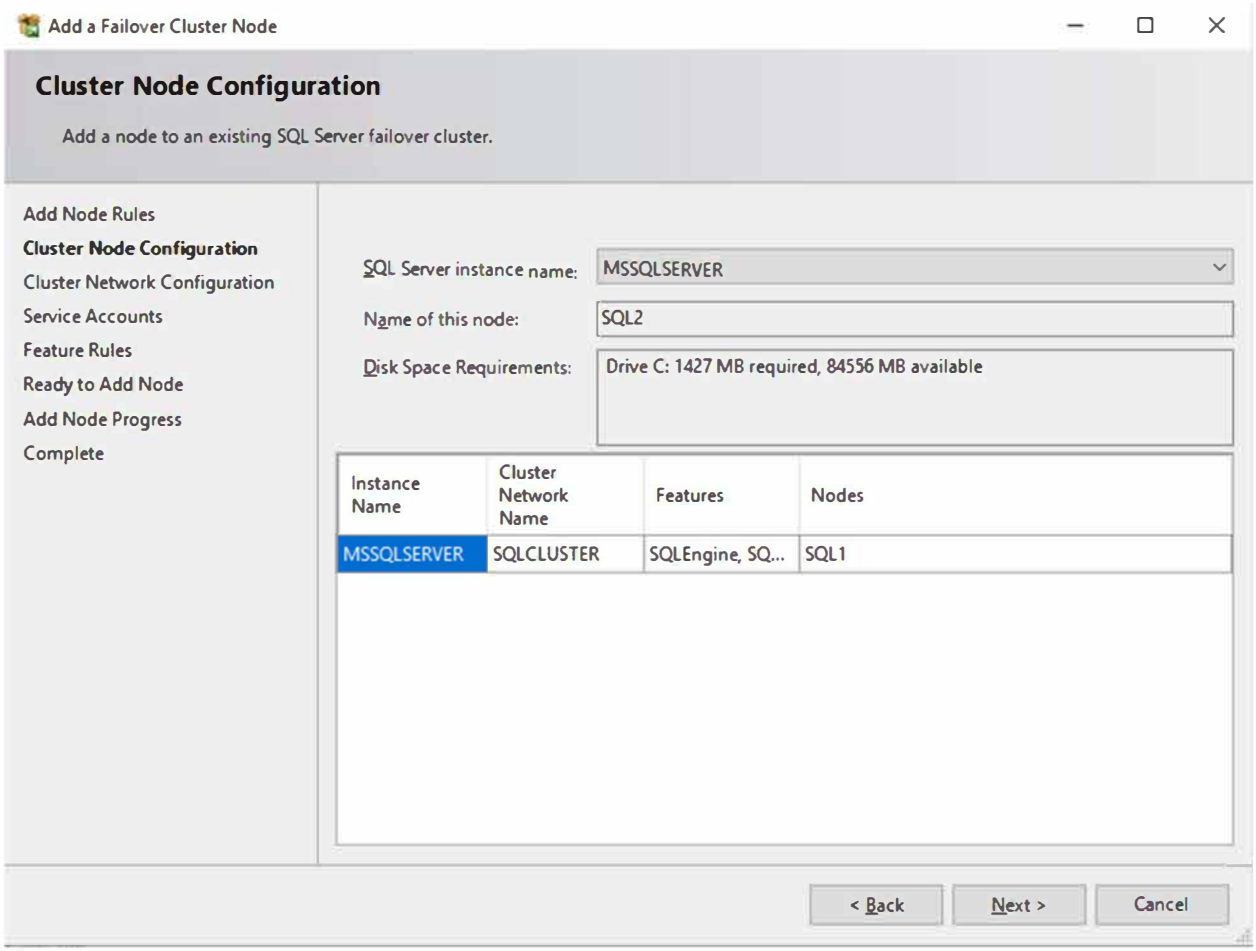

SQL Server Installation Center
Planning
Installation
Maintenance
Tools
Resources
Advanced
Options
Microsoft SQL Server 2019
New SQL Server stand-alone installation or add features to an existing installation
Launch a wizard to install SQL Server 2019 in a non-clustered environment or to add features to an existing SQL Server 2019 instance.
Install SQL Server Reporting Services
Launch a download page that provides a link to install SQL Server Reporting Services. An internet connection is required to install SSRS.
Install SQL Server Management Tools
Launch a download page that provides a link to install SQL Server Management Studio, SQL Server command-line utilities (SQLCMD and BCP), SQL Server PowerShell provider, SQL Server Profiler and Database Tuning Advisor. An internet connection is required to install these tools.
Install SQL Server Data Tools
Launch a download page that provides a link to install SQL Server Data Tools (SSDT). SSDT provides Visual Studio integration including project system support for Microsoft Azure SQL Database, the SQL Server Database Engine, Reporting Services, Analysis Services and Integration Services. An internet connection is required to install SSDT.
New SQL Server failover cluster installation
Launch a wizard to install a single-node SQL Server 2019 failover cluster.
Add node to a SQL Server failover cluster
Launch a wizard to add a node to an existing SQL Server 2019 failover cluster.
Upgrade from a previous version of SQL Server
Launch a wizard to upgrade a previous version of SQL Server to SQL Server 2019.
Click here to first view Upgrade Documentation
New Machine Learning Server (Standalone) installation

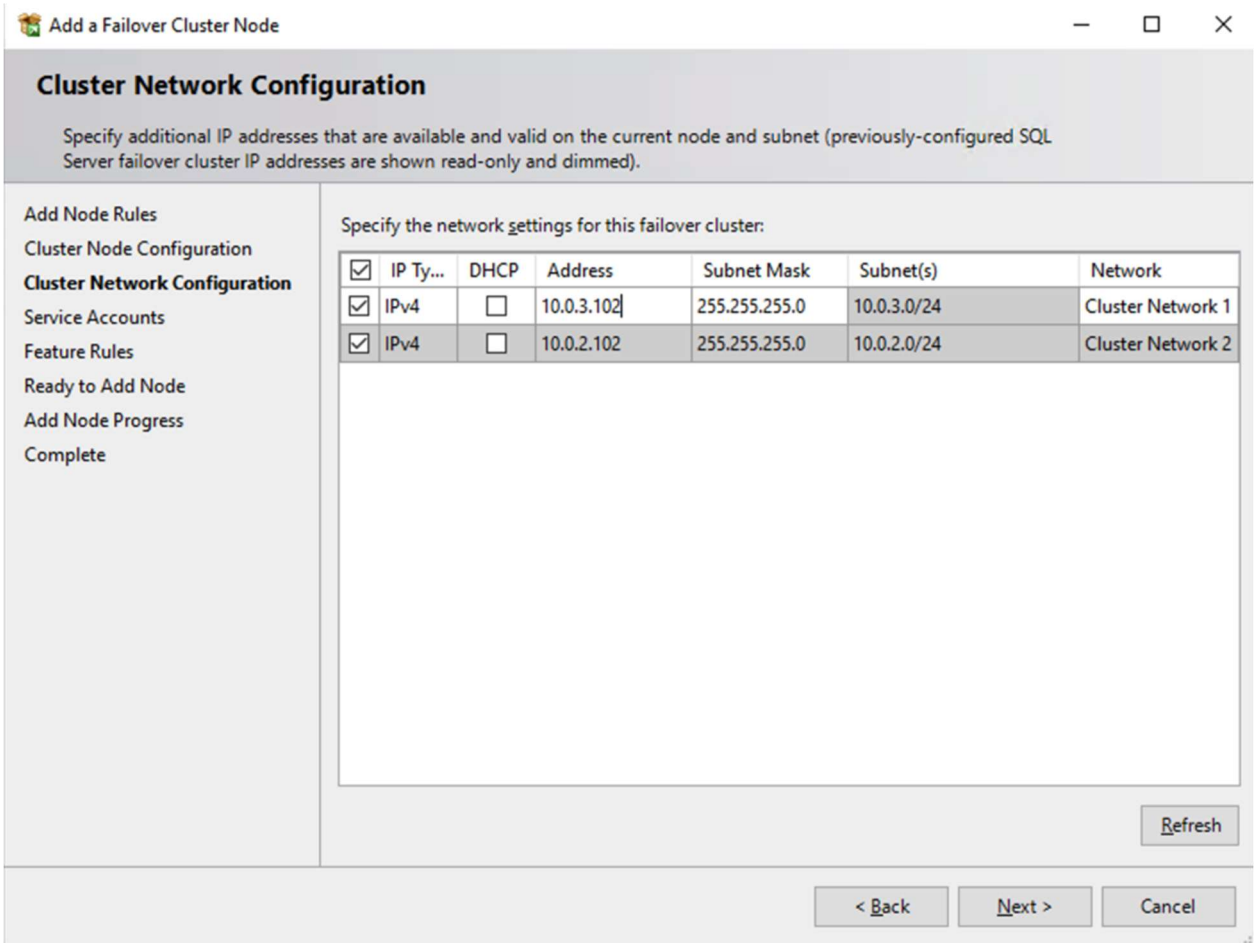

Add a Failover Cluster Node
Product Key
Specify the edition of SQL Server 2019 to install.
Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Add Node Rules
Cluster Node Configuration
Feature Rules
Ready to Add Node
Add Node Progress
Complete
Validate this instance of SQL Server 2019 by entering the 25-character key from the Microsoft certificate of authenticity or product packaging. You can also specify a free edition of SQL Server: Developer, Evaluation, or Express. Evaluation has the largest set of SQL Server features, as documented in SQL Server Books Online, and is activated with a 180-day expiration. Developer edition does not have an expiration, has the same set of features found in Evaluation, but is licensed for non-production database application development only. To upgrade from one installed edition to another, run the Edition Upgrade Wizard.
Specify a free edition:
Developer
Enter the product key:
< Back
Next >
Cancel

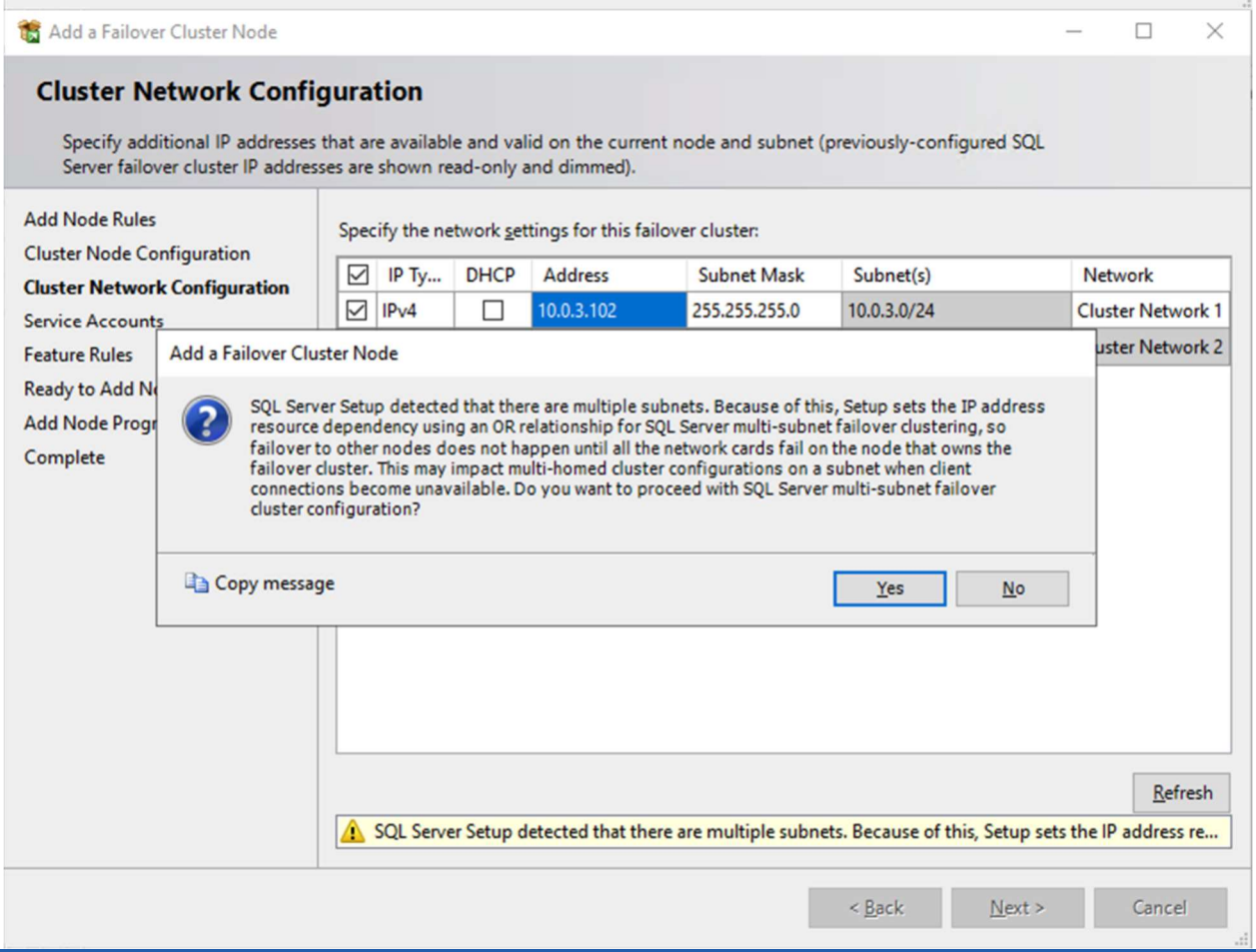

Add a Failover Cluster Node
License Terms
To install SQL Server 2019, you must accept the Microsoft Software License Terms.
Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Add Node Rules
Cluster Node Configuration
Feature Rules
Ready to Add Node
Add Node Progress
Complete
MICROSOFT SOFTWARE LICENSE TERMS
MICROSOFT SQL SERVER 2019 DEVELOPER
These license terms are an agreement between you and Microsoft Corporation (or one of its affiliates). They apply to the software named above and any Microsoft services or software updates (except to the extent such services or updates are accompanied by new or additional terms, in which case those different terms apply prospectively and do not alter your or Microsoft's rights relating to pre-updated software or services). IF YOU COMPLY WITH THESE LICENSE TERMS, YOU HAVE THE RIGHTS BELOW. BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT USE THE SOFTWARE.
IMPORTANT NOTICE: AUTOMATIC UPDATES TO PREVIOUS VERSIONS OF SQL SERVER. If this software is installed on servers or devices running any supported editions of SQL Server
Copy
Print
I accept the license terms and
Privacy Statement
SQL Server transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about data processing and privacy controls, and to turn off the collection of this information after installation, see the documentation.
< Back
Next >
Cancel

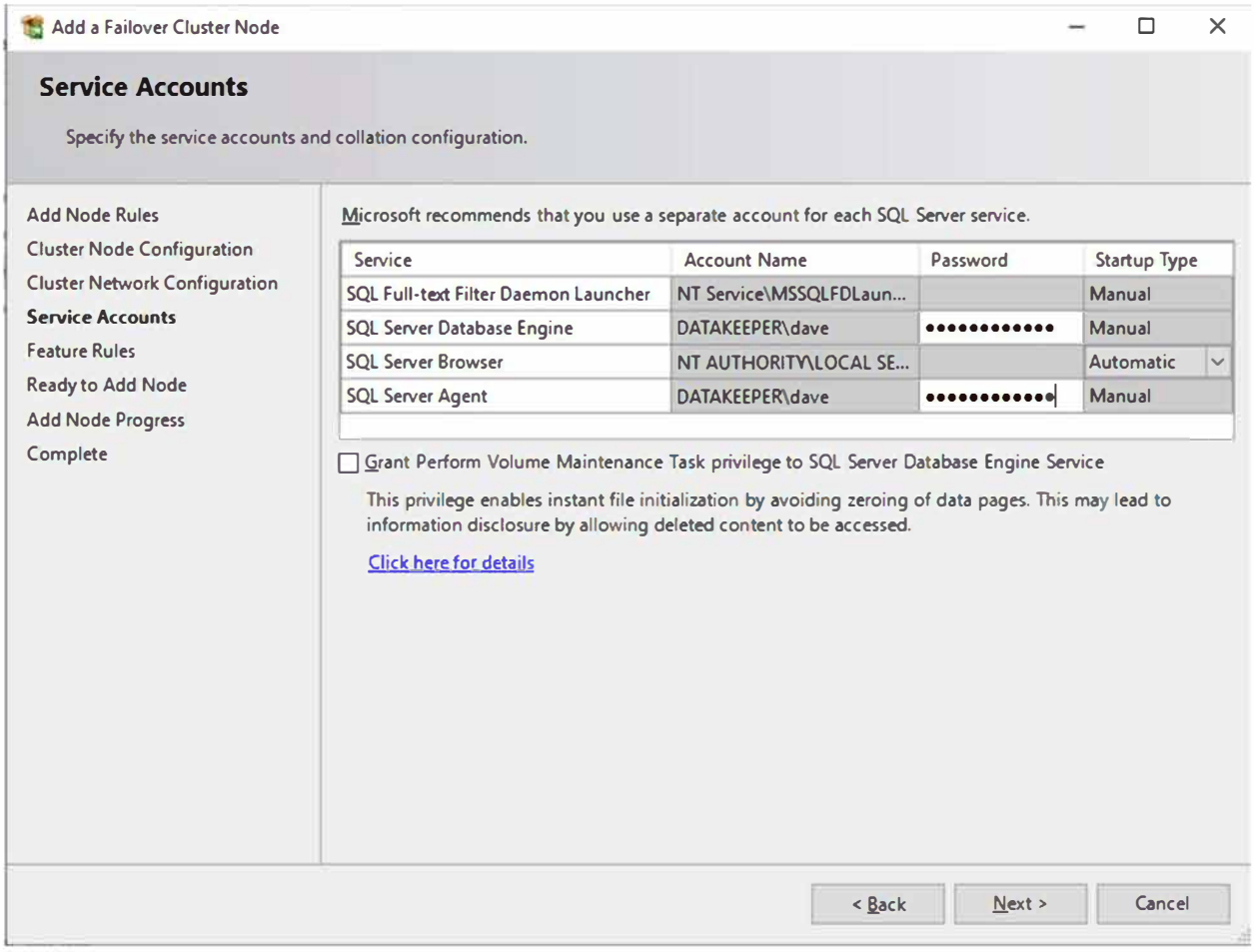

Add a Failover Cluster Node
Microsoft Update
Use Microsoft Update to check for important updates
Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Add Node Rules
Cluster Node Configuration
Feature Rules
Ready to Add Node
Add Node Progress
Complete
Microsoft Update offers security and other important updates for Windows and other Microsoft software, including SQL Server 2019. Updates are delivered using Automatic Updates, or you can visit the Microsoft Update website.
Use Microsoft Update to check for updates (recommended)
Microsoft Update FAQ
Microsoft Update Privacy Statement
< Back
Next >
Cancel

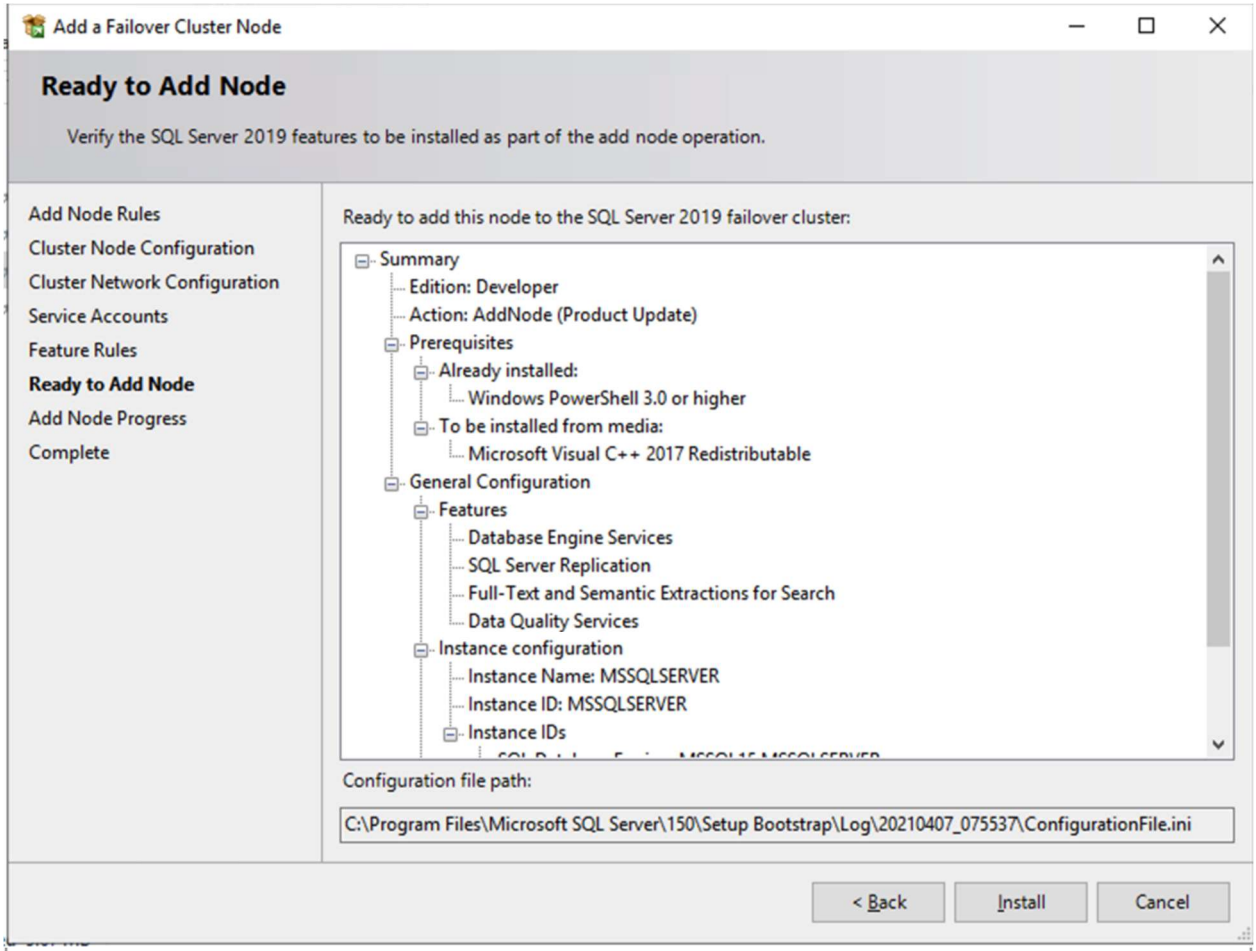

Add a Failover Cluster Node
Add Node Rules
Setup rules identify potential problems that might occur while running Setup. Failures must be corrected before Setup can continue.
Add Node Rules
Cluster Node Configuration
Feature Rules
Ready to Add Node
Add Node Progress
Complete
Operation completed. Passed: 19. Failed 0. Warning 1. Skipped 0.
Hide details <<
Re-run
View detailed report
Result
Rule
Status
Microsoft Cluster Service (MSCS) cluster verification warnings
Warning
Remote registry service (SQL2)
Passed
Domain controller
Passed
Windows Firewall
Passed
DNS settings (SQL2)
Passed
WOW64 setup
Passed
SQL 2019 minimum CTP for Upgrade and Side by Side Support
Passed
Windows Management Instrumentation (WMI) service (SQL1)
Passed
Cluster Remote Access (SQL1)
Passed
Distributed Transaction Coordinator (MSDTC) installed (SQL1)
Passed
Remote registry service (SQL1)
Passed
< Back
Next >
Cancel

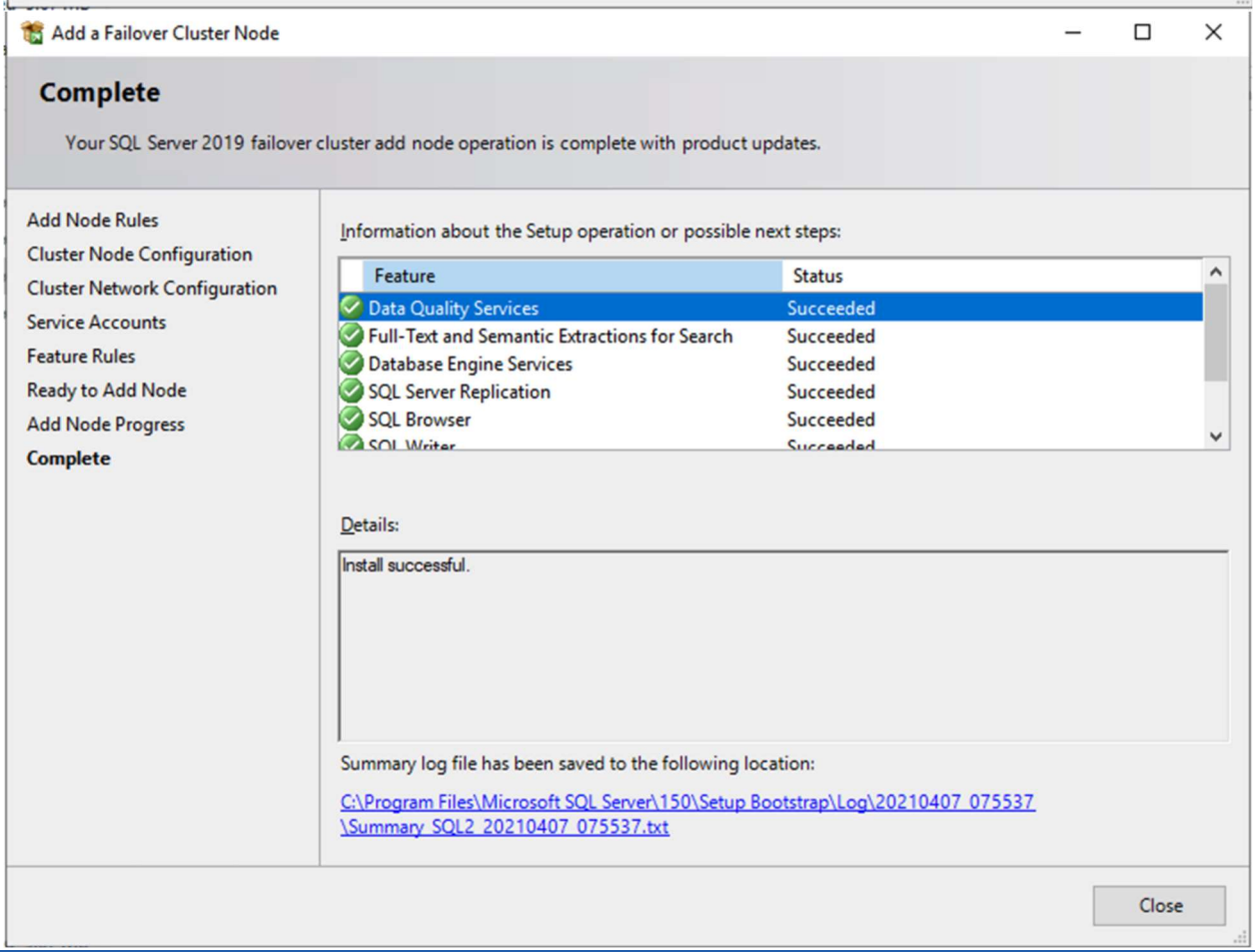

Add a Failover Cluster Node
Cluster Node Configuration
Add a node to an existing SQL Server failover cluster.
Add Node Rules
Cluster Node Configuration
Cluster Network Configuration
Service Accounts
Feature Rules
Ready to Add Node
Add Node Progress
Complete
SQL Server instance name:
MSSQLSERVER
Name of this node:
SQL2
Disk Space Requirements:
Drive C: 1427 MB required, 84556 MB available
Instance Name
Cluster Network Name
Features
Nodes
MSSQLSERVER
SQLCLUSTER
SQLEngine, SQ...
SQL1
< Back
Next >
Cancel


Add a Failover Cluster Node
Cluster Network Configuration
Specify additional IP addresses that are available and valid on the current node and subnet (previously-configured SQL Server failover cluster IP addresses are shown read-only and dimmed).
Add Node Rules
Cluster Node Configuration
Cluster Network Configuration
Service Accounts
Feature Rules
Ready to Add Node
Add Node Progress
Complete
Specify the network settings for this failover cluster:
IP Ty... DHCP Address Subnet Mask Subnet(s) Network
IPv4 10.0.3.102 255.255.255.0 10.0.3.0/24 Cluster Network 1
IPv4 10.0.2.102 255.255.255.0 10.0.2.0/24 Cluster Network 2
Refresh
< Back Next > Cancel

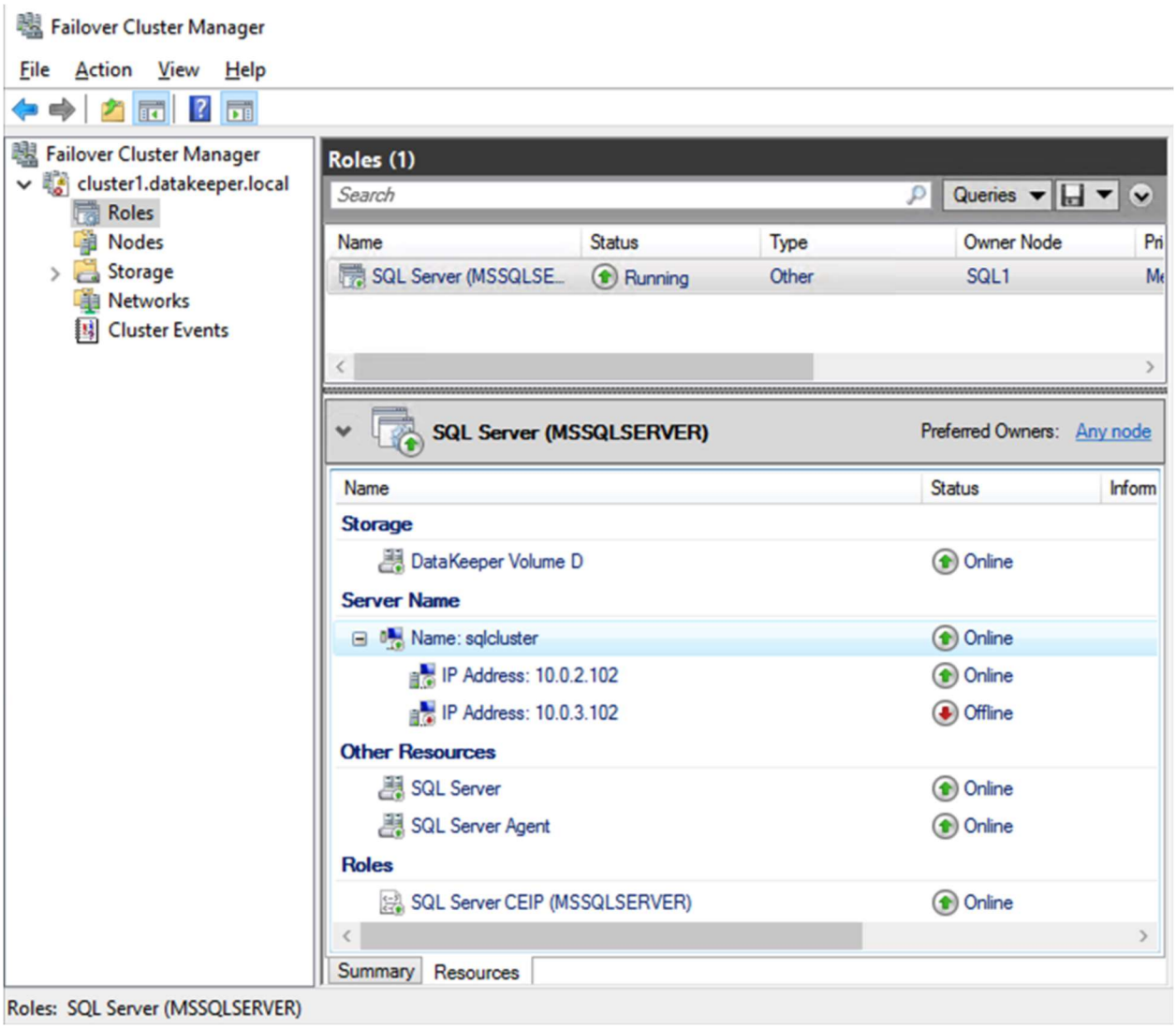

Add a Failover Cluster Node
Cluster Network Configuration
Specify additional IP addresses that are available and valid on the current node and subnet (previously-configured SQL Server failover cluster IP addresses are shown read-only and dimmed).
Add Node Rules
Cluster Node Configuration
Cluster Network Configuration
Service Accounts
Feature Rules
Ready to Add N
Add Node Progr
Complete
Specify the network settings for this failover cluster:
IP Ty... DHCP Address Subnet Mask Subnet(s) Network
IPv4 10.0.3.102 255.255.255.0 10.0.3.0/24 Cluster Network 1
Add a Failover Cluster Node
SQL Server Setup detected that there are multiple subnets. Because of this, Setup sets the IP address resource dependency using an OR relationship for SQL Server multi-subnet failover clustering, so failover to other nodes does not happen until all the network cards fail on the node that owns the failover cluster. This may impact multi-homed cluster configurations on a subnet when client connections become unavailable. Do you want to proceed with SQL Server multi-subnet failover cluster configuration?
Copy message
Yes No
Refresh
SQL Server Setup detected that there are multiple subnets. Because of this, Setup sets the IP address re...
< Back Next > Cancel


Add a Failover Cluster Node
Service Accounts
Specify the service accounts and collation configuration.
Add Node Rules
Cluster Node Configuration
Cluster Network Configuration
Service Accounts
Feature Rules
Ready to Add Node
Add Node Progress
Complete
Microsoft recommends that you use a separate account for each SQL Server service.
Service
Account Name
Password
Startup Type
SQL Full-text Filter Daemon Launcher
NT Service\MSSQLFDLaun...
Manual
SQL Server Database Engine
DATAKEEPER\dave
Manual
SQL Server Browser
NT AUTHORITY\LOCAL SE...
Automatic
SQL Server Agent
DATAKEEPER\dave
Manual
Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service
This privilege enables instant file initialization by avoiding zeroing of data pages. This may lead to information disclosure by allowing deleted content to be accessed.
Click here for details
< Back
Next >
Cancel


Add a Failover Cluster Node
Ready to Add Node
Verify the SQL Server 2019 features to be installed as part of the add node operation.
Add Node Rules
Cluster Node Configuration
Cluster Network Configuration
Service Accounts
Feature Rules
Ready to Add Node
Add Node Progress
Complete
Ready to add this node to the SQL Server 2019 failover cluster:
Summary
Edition: Developer
Action: AddNode (Product Update)
Prerequisites
Already installed:
Windows PowerShell 3.0 or higher
To be installed from media:
Microsoft Visual C++ 2017 Redistributable
General Configuration
Features
Database Engine Services
SQL Server Replication
Full-Text and Semantic Extractions for Search
Data Quality Services
Instance configuration
Instance Name: MSSQLSERVER
Instance ID: MSSQLSERVER
Instance IDs
Configuration file path:
C:\Program Files\Microsoft SQL Server\150\Setup Bootstrap\Log\20210407_075537\ConfigurationFile.ini
< Back
Install
Cancel

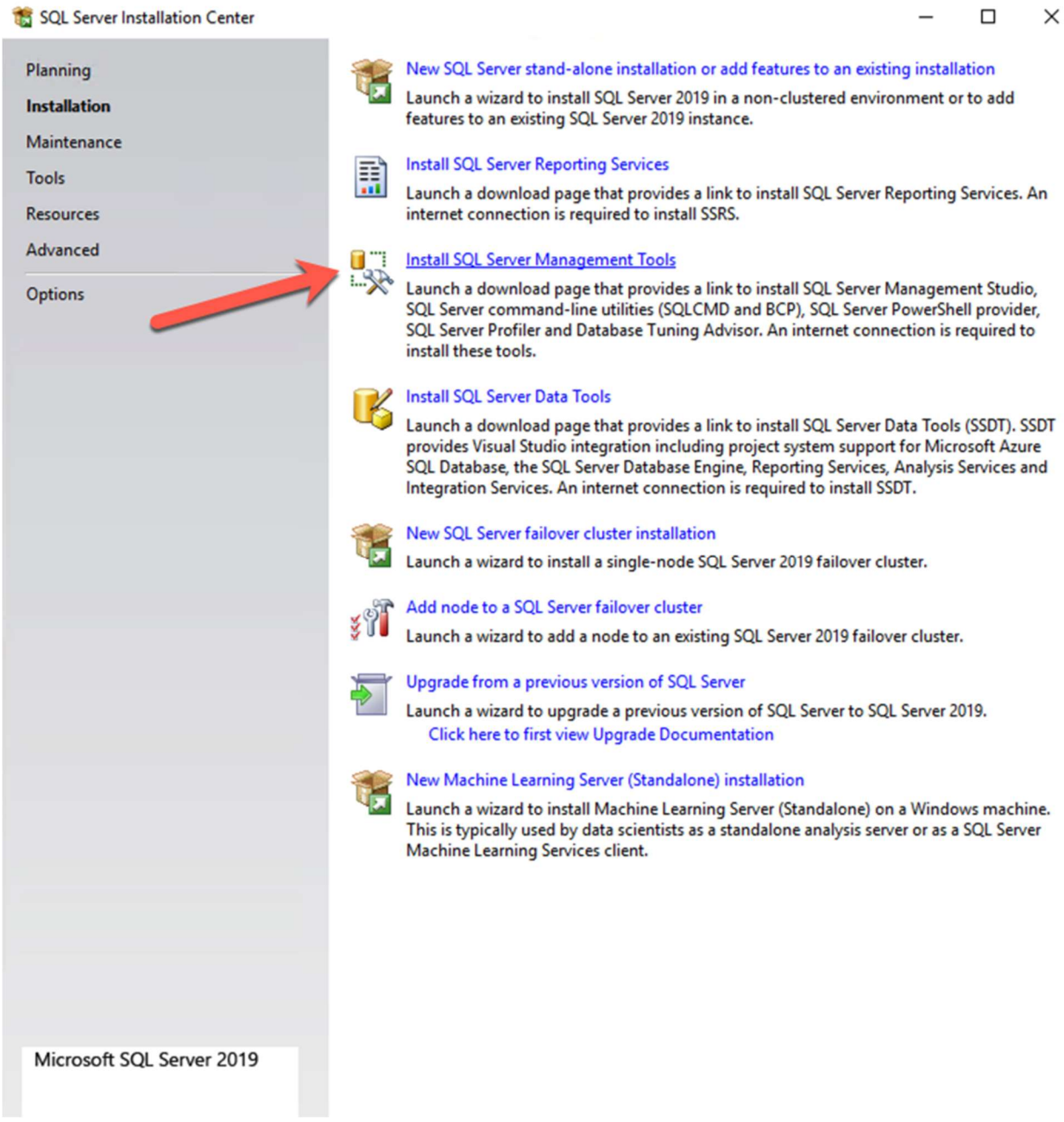

Add a Failover Cluster Node
Complete
Your SQL Server 2019 failover cluster add node operation is complete with product updates.
Add Node Rules
Cluster Node Configuration
Cluster Network Configuration
Service Accounts
Feature Rules
Ready to Add Node
Add Node Progress
Complete
Information about the Setup operation or possible next steps:
Feature
Status
Data Quality Services
Succeeded
Full-Text and Semantic Extractions for Search
Succeeded
Database Engine Services
Succeeded
SQL Server Replication
Succeeded
SQL Browser
Succeeded
Details:
Install successful.
Summary log file has been saved to the following location:
C:\Program Files\Microsoft SQL Server\150\Setup Bootstrap\Log\20210407_075537
\Summary_SQL2_20210407_075537.txt
Close

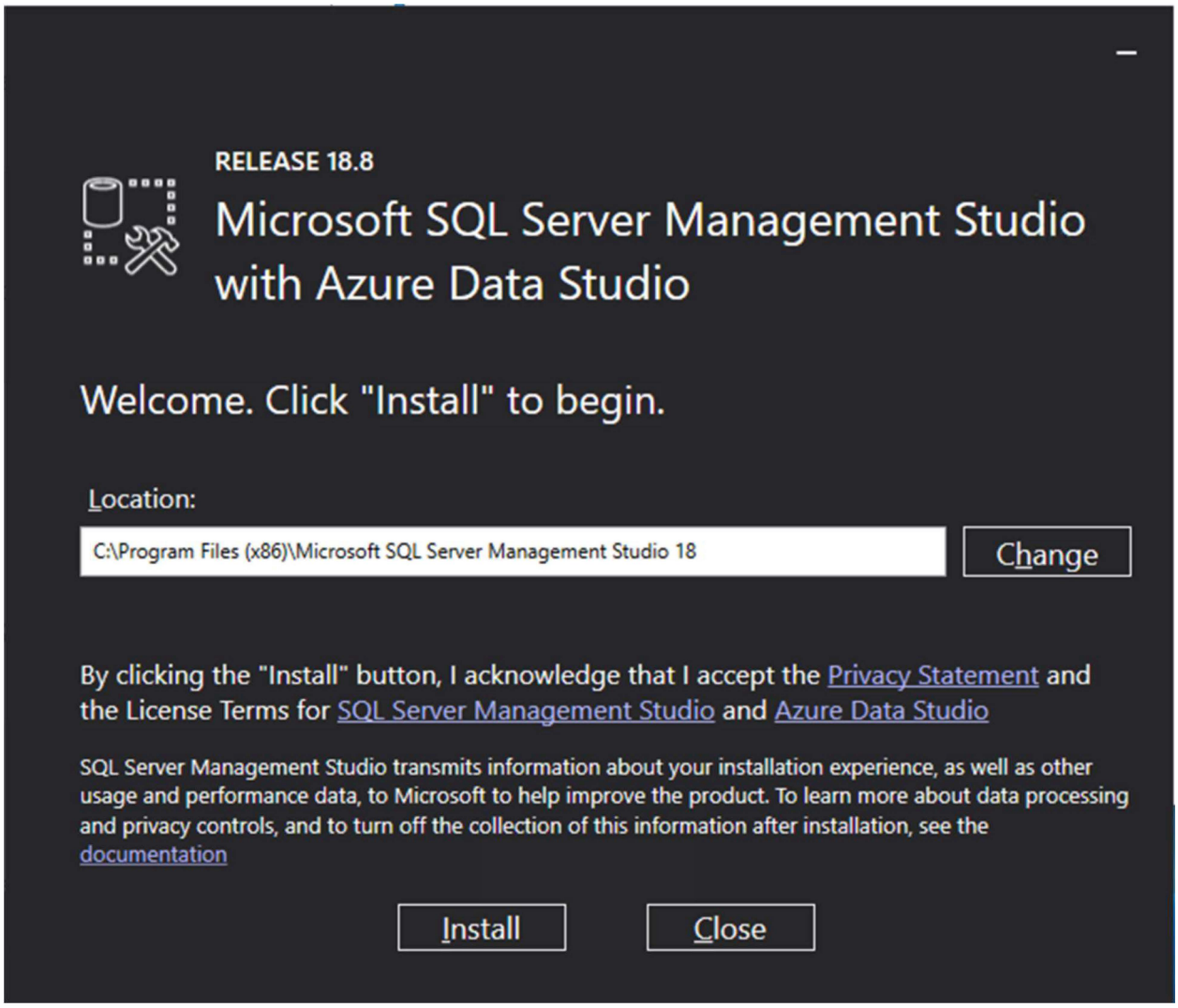
Once you have installed SQL Server on both cluster nodes, Failover Cluster Manager should look like this.

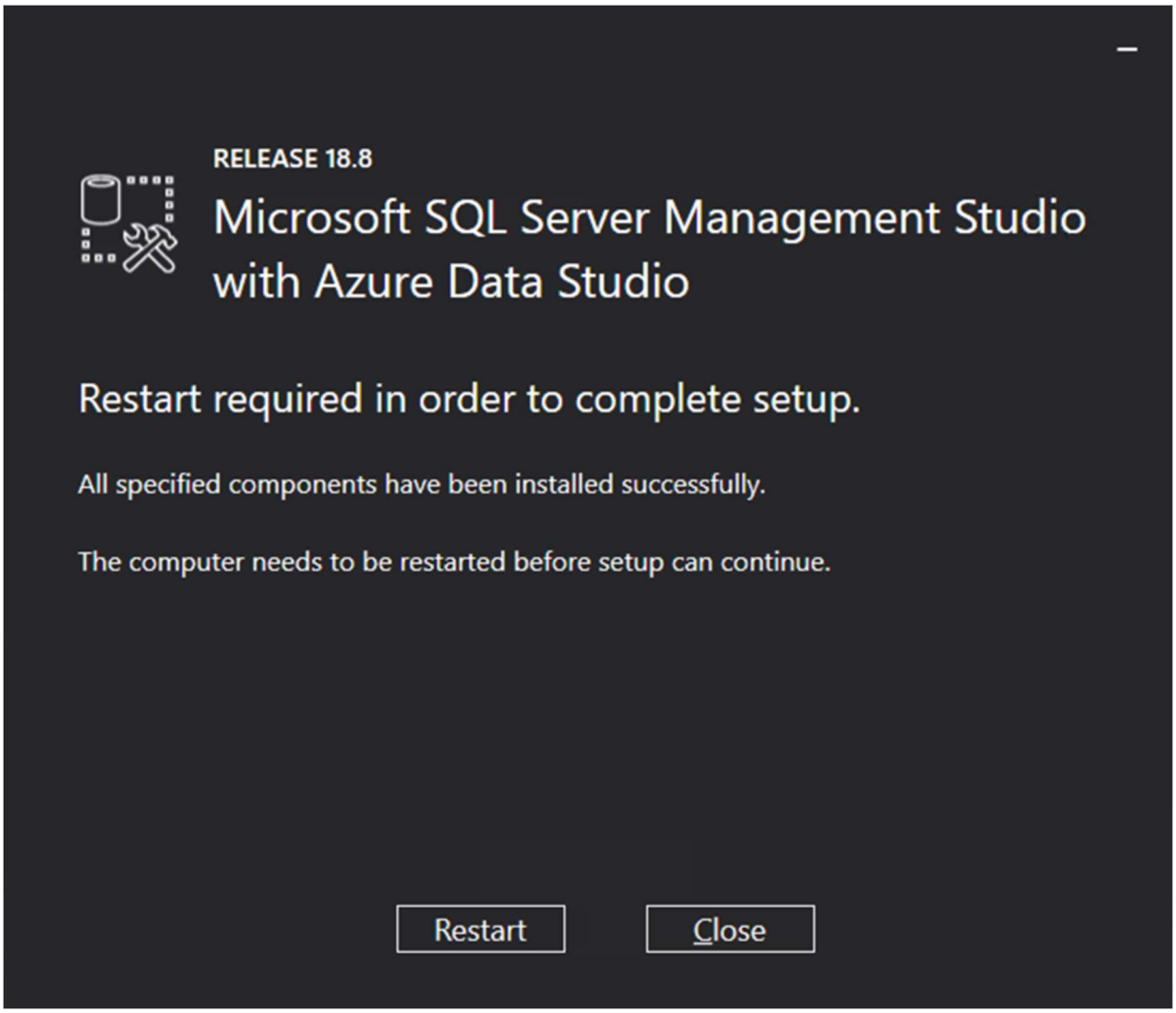


Install SQL Server Management Studio

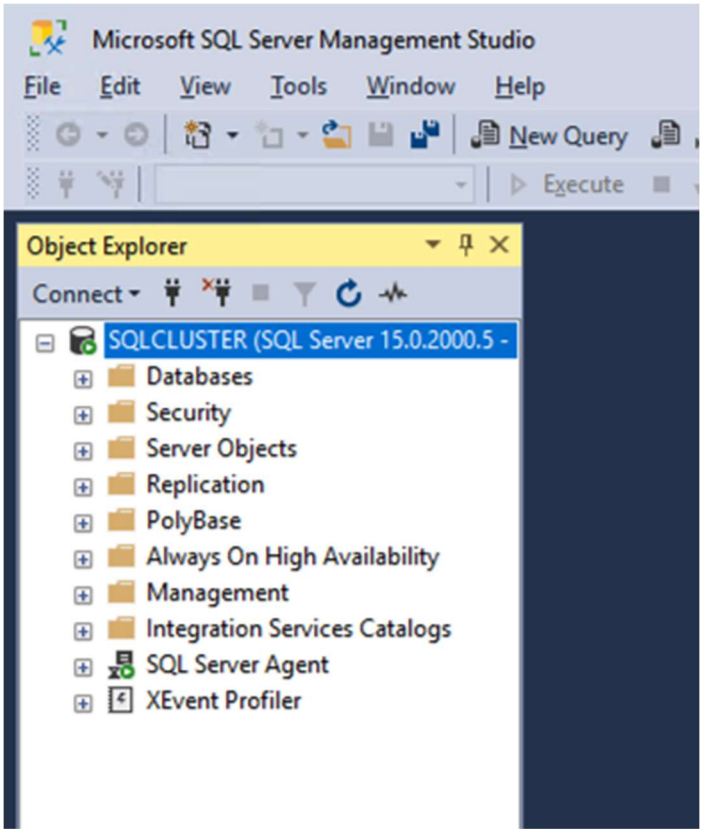
On SQL Server Versions 2016 and later, you must download and install SSMS as a separate option as shown below. Note: In earlier versions of SQL Server, SQL Server Management Studio (SSMS) was an option that you could choose to install during the SQL installation.




RELEASE 18.8
Microsoft SQL Server Management Studio with Azure Data Studio
Welcome. Click "Install" to begin.
Location:
C:\Program Files (x86)\Microsoft SQL Server Management Studio 18
Change
By clicking the "Install" button, I acknowledge that I accept the Privacy Statement and the License Terms for SQL Server Management Studio and Azure Data Studio
SQL Server Management Studio transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about data processing and privacy controls, and to turn off the collection of this information after installation, see the documentation
Install
Close

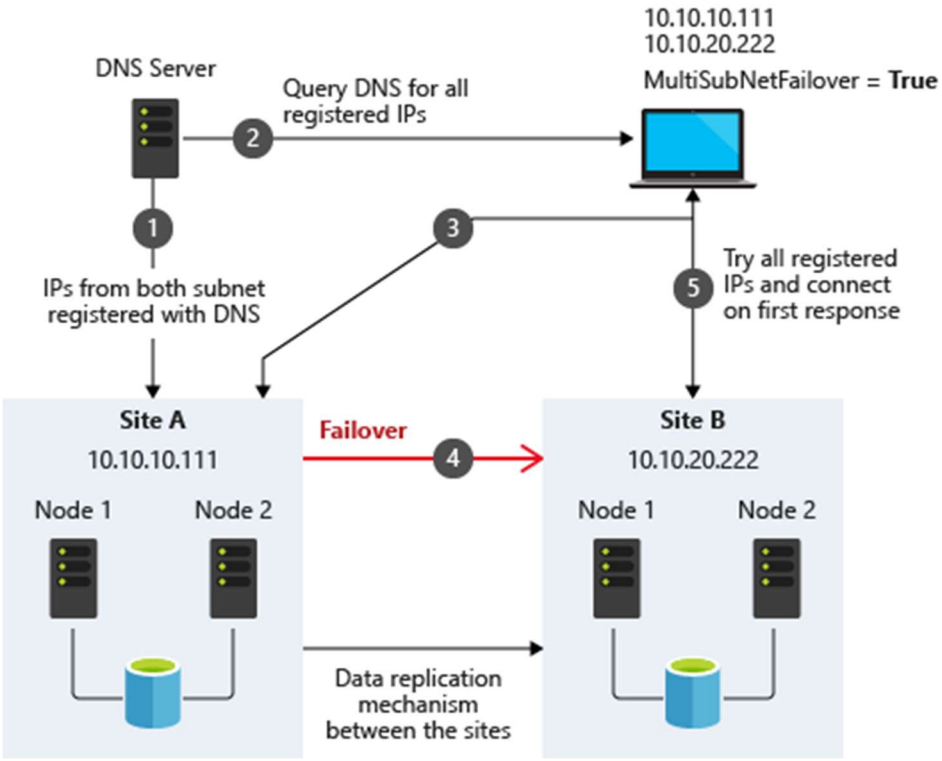

RELEASE 18.8
Microsoft SQL Server Management Studio with Azure Data Studio
Restart required in order to complete setup.
All specified components have been installed successfully.
The computer needs to be restarted before setup can continue.
Restart
Close

Once SSMS installs, connect to the cluster via the client access point. Your SQL Server FCI should look like this.



Multi-Subnet Considerations

One of the biggest considerations for running a SQL Server FCI in OCI is the fact that the cluster nodes reside in different subnets. Microsoft started to account for the fact that cluster nodes might reside in different subnets by adding the “OR” functionality in Windows Server 2008 R2 as described in the Microsoft documentation.



Taken from [SQL Server Multi-Subnet Clustering (SQL Server)]

The important thing described in the documentation is the concept of the RegisterAllProvidersIP on the network name resource, which is enabled by default when you create a SQL Server FCI. As described, when this is enabled, two A records will be registered in DNS with the network name resource, one for each IP address.

Using the “OR” functionality, only the IP address associated with the active subnet will ever be online and the other one will be shown as offline. If your client supports adding multisubnetfailover=true to the connection string, then both IP addresses will be tried at the same time and the client will automatically connect to the active node. That is the easiest, and the default method of client redirection in a multi-subnet cluster.

The documentation goes on to say that if your client does NOT support the multisubnetfailover=true functionality, that you should “try to adjust the connection timeout in the client connection string by 21 seconds for each additional IP address. This ensures that the client's reconnection attempt does not timeout before it is able to cycle through all IP addresses in your multi-subnet FCI.”

Disabling RegisterAllProvidersIP is another option that will work. By disabling the RegisterAllProvidersIP you will only have a single A record in DNS. The DNS A record will be updated each time the cluster fails over with the active cluster IP address associated with the name resource.

The downside of this scenario configuration is that your clients will cache the old IP address until

the time to live (TTL) expires. To minimize the delay in reconnection, it is recommended that you change the TTL on the name resource. This process is described here and an example is shown below that sets the TTL to 5 minutes

```
Get-ClusterResource -Name sqlcluster | Set-ClusterParameter
-Name HostRecordTTL -Value 300
```

Keep in mind that it also may take some time for the changes to your AD-integrated DNS server to propagate across your entire forest.

Summary

This technical guide provides a comprehensive overview of setting up a SQL Server 2019 Failover Cluster Instance (FCI) in Oracle Cloud Infrastructure (OCI). It begins by highlighting the importance of understanding OCI's availability SLAs, which differ based on deployment strategies: 99.99% for deployments across Availability Domains, 99.95% across Fault Domains, and 99.9% for single VM deployments. The guide emphasizes that the SLA covers VM availability, not the applications or services running on it, thus necessitating additional measures for application availability.

The guide details the initial steps of creating a Virtual Cloud Network (VCN) and subnets in OCI, emphasizing the need for a network plan that accommodates at least three Availability Domains for clustering purposes. Each Availability Domain must be in a different subnet, a requirement applicable to clusters spanning Fault Domains as well. It provides specific configurations for setting up three subnets across different Availability Domains within a single VCN.

Further, the guide describes the process of creating an internet gateway and editing default security lists and route tables to facilitate access and security across Availability Domains. It also covers the configuration of DHCP options for Active Directory compatibility and outlines the steps for provisioning VMs with Windows Server 2022 and SQL Server 2019, emphasizing the importance of planning server names, IP addresses, and availability zone placements.

The guide then delves into adding additional volumes for SQL Server FCI storage needs, detailing the process of creating and attaching block volumes to instances. It also instructs on configuring secondary IP addresses for Windows Server Failover Clustering in OCI.

Next, the guide addresses domain controller setup, including enabling Active Directory Domain Services and promoting the server to a domain controller. It walks through the preparation of storage and enabling of the Failover Clustering feature on SQL1 and SQL2, along with cluster validation and creation processes.

The guide further discusses adding a File Share Witness to maintain cluster quorum and installing DataKeeper Cluster Edition for volume replication. It provides a step-by-step approach to installing SQL Server on the cluster nodes and SQL Server Management Studio, along with considerations for multi-subnet deployments.

In summary, this guide offers a detailed blueprint for deploying and configuring a SQL Server 2019 FCI in OCI, covering aspects from network setup and VM provisioning to clustering, storage configuration, and domain control setup, ensuring maximum uptime and reliability for business-critical applications.

SIOS Technology Corp.
4 West 4th Ave
San Mateo, CA 94402
Tel: 650-645-7000

info@us.sios.com
https://us.sios.com

© 2024 SIOS Technology Corp. All rights reserved. SIOS, SIOS Technology, SIOS DataKeeper, SIOS LifeKeeper, SIOS Protection Suite and associated logos are registered trademarks or trademarks of SIOS Technology Corp. and/or its affiliates in the United States and/or other countries. All other trademarks are the property of their respective owners. SS-0412-A