## Contents

- About This Guide ................................................................................................................... 3
- Quick Links ............................................................................................................................ 3
- About Quick Starts ................................................................................................................. 4
- Overview .................................................................................................................................... 4
- SQL Server and WSFC on AWS ............................................................................................. 4
- Costs and Licenses ................................................................................................................. 5
- AWS Services .......................................................................................................................... 6
- Architecture ............................................................................................................................... 7
- Best Practices ......................................................................................................................... 9
  - High Availability and Disaster Recovery ........................................................................... 9
  - Automatic Failover ............................................................................................................. 9
  - Security Groups and Firewalls .......................................................................................... 11
- Implementation Details ........................................................................................................... 11
  - SQL Server Enterprise Edition ......................................................................................... 11
  - Storage on the WSFC Nodes .............................................................................................. 12
  - IP Addressing on the WSFC Nodes .................................................................................... 14
  - Windows Server Failover Clustering ................................................................................ 14
  - Always On Configuration ................................................................................................. 15
- Deployment Options ............................................................................................................... 16
- Deployment Steps ................................................................................................................... 17
  - Step 1. Prepare an AWS Account ....................................................................................... 17
  - Step 2. Launch the Quick Start .......................................................................................... 20
  - Step 3. Configure a SQL Server Always On Availability Group ......................................... 30
    - Set up Permissions for the Cluster Object ....................................................................... 30
    - Create a Test Database or Attach an Existing Database .................................................. 31
    - Create an Availability Group ......................................................................................... 32
  - Step 4: Test the Cluster and Availability Group ................................................................. 38
About This Guide

This Quick Start deployment guide discusses architectural considerations and configuration steps for deploying a Microsoft Windows Server Failover Clustering (WSFC) cluster and a SQL Server Always On Availability Group on the Amazon Web Services (AWS) Cloud. It also provides links for viewing and launching AWS CloudFormation templates that automate the deployment.

Note  Always On Availability Groups is a feature supported by SQL Server Enterprise edition. Running WSFC nodes in the same subnet is currently not supported on the AWS Cloud.

The guide is for IT infrastructure architects, administrators, and DevOps professionals who are planning to implement or extend their WSFC and SQL Server workloads on the AWS Cloud.

This Quick Start supports SQL Server versions 2014, 2016, and 2017.

Quick Links

The links in this section are for your convenience. Before you launch the Quick Start, please review the architecture, configuration, network security, and other considerations discussed in this guide.

Note  You are responsible for the costs related to your use of any AWS services used while running this Quick Start reference deployment. See the pricing pages of the AWS services you will be using for full details.

- If you have an AWS account, and you’re already familiar with AWS services, SQL Server, and WSFC, you can launch the Quick Start to build the architecture shown in Figure 1 in a new or existing virtual private cloud (VPC). The deployment takes approximately
three hours. If you’re new to AWS or to SQL Server, please review the implementation details and follow the step-by-step instructions provided later in this guide.

- If you want to take a look under the covers, you can view the AWS CloudFormation templates that automate the deployment.

About Quick Starts

Quick Starts are automated reference deployments for key workloads on the AWS Cloud. Each Quick Start launches, configures, and runs the AWS compute, network, storage, and other services required to deploy a specific workload on AWS, using AWS best practices for security and availability.

Overview

SQL Server and WSFC on AWS

This Quick Start implements a high availability solution built with Microsoft Windows Server and SQL Server running on Amazon Elastic Compute Cloud (Amazon EC2), using the Always On Availability Groups feature of SQL Server Enterprise edition. This infrastructure provides the underpinnings for many Microsoft technology-based solutions for the enterprise, including Microsoft SharePoint and .NET Framework applications.

A prerequisite for deploying a SQL Server Always On Availability Group is Windows Server Failover Clustering (WSFC). SQL Server Always On uses WSFC to increase application availability. WSFC provides infrastructure features that complement the high availability and disaster recovery scenarios supported in the AWS Cloud.

Implementing WSFC in the AWS Cloud is very similar to deploying it in an on-premises setting as long as you meet two key requirements:

- You must deploy the cluster nodes inside a virtual private cloud (VPC).
- You must deploy the cluster nodes in separate subnets.
This Quick Start provides an automated deployment of WSFC that meets these requirements and handles some of the configuration steps for you.

This guide provides step-by-step instructions and discusses AWS-specific considerations. The guide doesn’t provide general configuration and usage information for WSFC and SQL Server. For general guidance and best practices, consult the product documentation.

**Costs and Licenses**

The Quick Start provides three licensing options for SQL Server Enterprise edition. You can:

- Install a trial version of SQL Server 2014, 2016, or 2017 Enterprise edition from the Microsoft download site.
- Use the Amazon Machine Image (AMI) with license costs for SQL Server Enterprise edition included.
- Use your volume licensing software and mobilize the license. For details, see the [Microsoft License Mobility through Software Assurance](https://docs.microsoft.com/en-us/compatible-software/qlm) program. For development and test environments, you can leverage your existing MSDN licenses for SQL Server using Amazon EC2 Dedicated Instances. For details, see the [MSDN on AWS](https://aws.amazon.com/microsoft/) webpage.

This Quick Start launches one of the following Windows Server AMIs, depending on which version of SQL Server you choose to deploy, and includes the license for the Windows Server operating system:

- AMI for Windows Server 2012 R2, if you choose to deploy SQL Server 2014 or 2016
- AMI for Windows Server 2016, if you choose to deploy SQL Server 2017

The AMI is updated on a regular basis with the latest service pack for the operating system.

You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using the Quick Start.

The AWS CloudFormation template for this Quick Start includes configuration parameters that you can customize. Some of these settings, such as instance type, volume size, or opting to use the Amazon-provided AMI for SQL Server, will affect the cost of deployment. See the pricing pages for each AWS service you will be using for cost estimates.
AWS Services

The core AWS components used by this Quick Start include the following AWS services. (If you are new to AWS, see the Getting Started Resource Center.)

- **Amazon EC2** – The Amazon Elastic Compute Cloud (Amazon EC2) service enables you to launch virtual machine instances with a variety of operating systems. You can choose from existing AMIs or import your own virtual machine images.

- **Amazon EBS** – Amazon Elastic Block Store (Amazon EBS) provides persistent block-level storage volumes for use with Amazon EC2 instances in the AWS Cloud. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. Amazon EBS volumes provide the consistent and low-latency performance needed to run your workloads.

- **Amazon VPC** – The Amazon Virtual Private Cloud (Amazon VPC) service lets you provision a private, isolated section of the AWS Cloud where you can launch AWS services and other resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

In addition, you should be familiar with the following:

- Windows Server 2012 R2 or 2016, depending on the SQL Server version
- Windows Server Active Directory and DNS
- Windows Server Failover Clustering (WSFC)
- SQL Server Always On Availability Groups

For information, see the Microsoft product documentation for these technologies.
Architecture

Deploying this Quick Start for a new VPC with the default parameters builds the following environment in the AWS Cloud.

Figure 1: WSFC and SQL Server architecture on AWS (default configuration)
You can also choose to build an architecture with three Availability Zones, as shown in Figure 2.

![Figure 2: WSFC and SQL Server architecture on AWS with three Availability Zones](image)

The deployment includes the following components.

**Note** If you use the option to deploy the Quick Start into your existing VPC and AD DS infrastructure, the components marked by asterisks are skipped. For details about the underlying Active Directory and network design, see the [Quick Start for Active Directory Domain Services](#).

- A virtual private cloud (VPC) configured with public and private subnets across two Availability Zones. This provides the network infrastructure for your SQL Server deployment. You can optionally choose a third Availability Zone for the file share witness or for an additional SQL cluster node, as shown in Figure 2.*
- An internet gateway to provide access to the internet.*
• In the public subnets, Windows Server-based Remote Desktop Gateway (RDGW) instances and network address translation (NAT) gateways for outbound internet access.*

• Elastic IP addresses associated with the NAT gateway and RDGW instances.*

• In the private subnets, Active Directory domain controllers.*

• In the private subnets, Windows Server-based instances as WSFC nodes.

• SQL Server Enterprise edition with SQL Server Always On Availability Groups on each WSFC node. This architecture provides redundant databases along with a witness server to ensure that a quorum can vote for the node to be promoted to master. The default architecture mirrors an on-premises architecture of two SQL Server instances spanning two subnets placed in two different Availability Zones, as shown in Figure 3.

• Security groups to ensure the secure flow of traffic between the instances deployed in the VPC.

Best Practices
The architecture built by this Quick Start supports AWS best practices for high availability and security.

High Availability and Disaster Recovery
Amazon EC2 provides the ability to place instances in multiple locations composed of AWS Regions and Availability Zones. Regions are dispersed and located in separate geographic areas. Availability Zones are distinct locations within a region that are engineered to be isolated from failures in other Availability Zones and that provide inexpensive, low-latency network connectivity to other Availability Zones in the same region.

By launching your instances in separate regions, you can design your application to be closer to specific customers or to meet legal or other requirements. By launching your instances in separate Availability Zones, you can protect your applications from the failure of a single location. WSFC provides infrastructure features that complement the high availability and disaster recovery scenarios supported in the AWS Cloud.

Automatic Failover
Deploying the Quick Start with the default parameters configures a two-node automatic failover cluster with a file share witness. On this cluster, it deploys an Always On Availability Group with two availability replicas.
Figure 3: SQL Server Always On Availability Groups and automatic failover

The Quick Start implementation supports the following scenarios:

- Protection from the failure of a single instance
- Automatic failover between the cluster nodes
- Automatic failover between Availability Zones

However, the Quick Start default implementation doesn’t provide automatic failover in every case. For example, the loss of Availability Zone 1, which contains the primary node and file share witness, would prevent automatic failover to Availability Zone 2. This is because the cluster would fail as it loses quorum. In this scenario, you could follow manual disaster recovery steps that include restarting the cluster service and forcing quorum on the second cluster node (e.g., WSFCNode2) to restore application availability. The Quick Start also provides an option to deploy into three Availability Zones. This deployment option can mitigate this loss of quorum in the case of a failure of a single node. However, you can select this option only in AWS Regions that include three or more Availability Zones; for a current list, see the AWS Global Infrastructure webpage.

We recommend that you consult the Microsoft SQL Server documentation and customize some of the steps described in this guide or add additional ones (e.g., deploy additional
cluster nodes and configure them as readable secondary replicas) to deploy a solution that best meets your business, IT, and security requirements.

**Security Groups and Firewalls**

When the EC2 instances are launched, they must be associated with a security group, which acts as a stateful firewall. You have complete control over the network traffic entering or leaving the security group, and you can build granular rules that are scoped by protocol, port number, and source or destination IP address or subnet. By default, all traffic egressing a security group is permitted. Ingress traffic, on the other hand, must be configured to allow the appropriate traffic to reach your instances.

The [Securing the Microsoft Platform on Amazon Web Services](#) whitepaper discusses the different methods for securing your AWS infrastructure. Recommendations include providing isolation between application tiers using security groups. We recommend that you tightly control ingress traffic in order to reduce the attack surface of your EC2 instances.

Domain controllers and member servers require several security group rules to allow traffic for services such as AD DS replication, user authentication, Windows Time services, and Distributed File System (DFS), among others. The WSFC nodes running SQL Server will need to permit several additional ports to communicate with each other as well. Finally, instances launched into the application server tier will need to establish SQL client connections to the WSFC nodes.

The Quick Start creates a number of security groups and rules for you. For a detailed list of port mappings, see the Security section of the Active Directory deployment guide, and the Security section of this guide.

In addition to security groups, the Windows firewall also needs to be modified on the SQL Server instances. During the bootstrapping process, a script will run on each instance that opens the TCP ports 1433, 1434, 4022, 5022, 5023, and 135 on the Windows firewall.

**Implementation Details**

**SQL Server Enterprise Edition**

Amazon Machine Images (AMIs) for the SQL Server 2014 and 2016 Enterprise edition are available for launch on AWS, with the limitations discussed in the [Costs and Licenses](#) section. If you keep the default (no) setting for the **Amazon-Provided SQL License (SQLLicenseProvided)** parameter, this Quick Start automatically connects to the
Microsoft download site and installs the trial software for SQL Server Enterprise edition. If you set the parameter to **yes**, the Quick Start uses the Amazon-provided AMI, which includes a license for SQL Server Enterprise edition.

You’ll find the installation software on each node in the `C:\sqlinstall\` folder. If you have to re-run the installation, make sure you select **Run as Administrator** to start the installation.

The SQL services are configured to run under the `sqlsa` account that is created in Active Directory. This account is also added to the local administrators groups on each WSFC node.

---

**Note**  
AWS does not provide installation media for Microsoft software. If you are not using the AWS CloudFormation templates, you can set up a test or evaluation environment by downloading a trial version of SQL Server at [http://www.microsoft.com/evalcenter/](http://www.microsoft.com/evalcenter/).

---

### Storage on the WSFC Nodes

Storage capacity and performance are key aspects of any production SQL Server installation. Although capacity and performance will vary from one deployment to the next, this Quick Start provides a reference configuration that you can use as a starting point. The AWS CloudFormation template deploys the WSFC nodes using the memory-optimized **r4.2xlarge** instance type by default.

In an effort to provide highly performant and durable storage, we’ve also included Amazon Elastic Block Store (Amazon EBS) volumes in this reference architecture. EBS volumes are network-attached disk storage, which you can create and attach to EC2 instances. Once these are attached, you can create a file system on top of these volumes, run a database, or use them in any other way you would use a block device. EBS volumes are placed in a specific Availability Zone, where they are automatically replicated to protect you from the failure of a single component.

Provisioned IOPS EBS volumes offer storage with consistent and low-latency performance. They are backed by solid state drives (SSDs) and are designed for applications with I/O-intensive workloads such as databases.

Amazon EBS-optimized instances, such as the R4 instance type, deliver dedicated throughput between Amazon EC2 and Amazon EBS. The dedicated throughput minimizes
contention between Amazon EBS I/O and other traffic from your EC2 instance, and provides the best performance for your EBS volumes.

By default, on each WSFC node, the Quick Start deploys three 500-GiB General Purpose SSD volumes to store databases, logs, tempdb, and backups. This is in addition to the root General Purpose SSD volume used by the operating system. This volume type delivers a consistent baseline of 3 IOPS/GiB, which provides a total of 1,500 IOPS per volume for SQL Server database and log volumes. You can customize the volume size, and you can also switch to using dedicated IOPS volumes with the volume you specify. If you need more IOPS per volume, consider using Provisioned IOPS SSD volumes by changing the SQL Server Volume Type and SQL Server Volume IOPS parameters, or use disk striping within Windows.

The default disk layout for SQL Server in this Quick Start uses the following EBS volumes:

- One General Purpose SSD volume (100 GiB) for the operating system (C:)
- One General Purpose SSD volume (500 GiB) to host the SQL Server database files (D:)
- One General Purpose SSD volume (500 GiB) to host the SQL Server log files (E:)
- One General Purpose SSD volume (500 GiB) to host the SQL Server tempdb and backup files (F:)

Figure 4 shows the disk layout on each SQL Server node. The Z: drive is instance storage that can be used for ephemeral data, such as the operating system page file. Keep in mind that data on instance storage will be lost when you stop your EC2 instance.

![Device Layout](https://via.placeholder.com/150)

**Figure 4: WSFC node disk layout**
IP Addressing on the WSFC Nodes

In order to support WSFC and Always On Availability Group listeners, each node hosting the SQL Server instances participating in the cluster will need to have three IP addresses assigned:

- One IP address is used as the primary IP address for the instance.
- A second IP address acts as the WSFC IP resource.
- A third IP address is used to host the Always On Availability Group listener.

When you launch the AWS CloudFormation template, you can specify the addresses for each node. By default, the 10.0.0.0/19, 10.0.32.0/19, and 10.0.64.0/19 CIDR blocks are used for the private subnets.

![Figure 4: Defining WSFC node IP addresses](image)

Windows Server Failover Clustering

Once your Windows Server instances have been deployed and domain-joined, you’re ready to build the cluster. The AWS CloudFormation templates carry out this task when deploying the second node. If you use the default template parameter settings, the Quick Start executes the following Windows PowerShell commands to complete this task:

```
Install-WindowsFeature failover-clustering -IncludeManagementTools
New-Cluster -Name WSFCluster1 -Node WSFCNODE1,WSFCNODE2
-StaticAddress 10.0.0.101,10.0.64.101
```

The first command runs on each instance during the bootstrapping process. It installs the required components and management tools for the failover clustering services. The second
command runs near the end of the bootstrapping process on the second node and is responsible for creating the cluster and for defining the server nodes and IP addresses.

By default, the Quick Start configures an even number of servers in the cluster. You’ll need a third resource to maintain a majority vote to keep the cluster online in the event of an individual server failure. For this, the Quick Start uses a dedicated file share witness instance, which requires modifying the cluster settings to NodeAndFileShareMajority. The first step in making this configuration change is to create the share. By default, the Quick Start creates a dedicated instance in the first Availability Zone to host this share. For production environments, you can also set the Third AZ parameter to witness to create a dedicated instance with a file share in a third Availability Zone. Alternatively, you can use any domain-joined server for this task. (This isn’t included in the Quick Start.) If you set the Third AZ parameter to full, the Quick Start will keep the quorum settings to the default node majority and will create a third SQL Server node in the third Availability Zone. Note that some AWS Regions support only two Availability Zones; for a current list, see the AWS Global Infrastructure webpage.

By default, the witness file share is \WSFCFileServer\witness. The Active Directory computer account that is created when forming the cluster (e.g., WSFCNODE1) is given NTFS permissions to access the share. After that, the cluster is updated to use the share as the file share witness resource.

```
Set-ClusterQuorum -NodeAndFileShareMajority \WSFCFileServer\witness
```

**Always On Configuration**

After SQL Server Enterprise edition has been installed and the Windows Server failover cluster has been built, the Quick Start enables SQL Server Always On with the following PowerShell command:

```
Enable-SqlAlwaysOn -ServerInstance WSFCNODE1
```

The Quick Start runs this command on each node, and the proper server name is provided as a value for the **ServerInstance** parameter.

The Quick Start automated solution ends after enabling SQL Server Always On. When the deployment is complete, you can create your databases and make them highly available by creating an Always On Availability Group. This process is covered in step 3 of the deployment instructions.
When you create an availability group, you’ll need to provide a network share used to perform an initial data synchronization. As you progress through the **New Availability Group** wizard, a full backup for each selected database is taken and placed in the share. The secondary node connects to the share and restores the database backups before joining the availability group.

To accommodate this initial synchronization, the Quick Start creates a folder called **C:\replica** on the first domain controller, using the share name **replica**. By default, the file share is defined as **\\WSFCFileServer\replica**. If you set the **Third AZ** parameter to **full**, the Quick Start creates the **replica** share on the first WSFC node in the first Availability Zone. Since SQL services run in this account, the **sqlsa** Active Directory user account is given NTFS permissions to this share.

**Deployment Options**

This Quick Start provides two deployment options:

- **Deploy SQL Server into a new VPC** (end-to-end deployment). This option builds a new AWS environment consisting of the VPC, subnets, NAT gateways, security groups, domain controllers, and other infrastructure components, and then deploys WSFC and SQL Server into this new VPC.

- **Deploy SQL Server into an existing VPC**. This option provisions WSFC in your existing AWS infrastructure. It creates one Windows Server–based instance to host a sample application that can test your cluster and allow you to see the failover occur between the different nodes in your deployment. Your AWS environment must include a VPC with two or three Availability Zones, public and private subnets in each Availability Zone, Remote Desktop Gateway and NAT gateways deployed into the public subnet, and Active Directory Domain Services deployed into the private subnet.

The Quick Start provides separate templates for these options. It also lets you configure additional settings such as the version of SQL Server you’d like to install, CIDR blocks, instance types, and software settings, as discussed later in this guide.
Deployment Steps

The procedure for deploying SQL Server on AWS consists of the following steps. For detailed instructions, follow the links for each step.

**Step 1. Prepare an AWS account**
This involves signing up for an AWS account, choosing a region, creating a key pair, and requesting increases for account limits, if necessary.

**Step 2. Launch the Quick Start**
In this step, you’ll launch the AWS CloudFormation template into your AWS account, specify parameter values, and create the stack. The Quick Start provides separate templates for end-to-end deployment and deployment into an existing VPC.

**Step 3. Configure a SQL Server Always On Availability Group**
After deployment is complete, you’ll configure the WSFC nodes with a SQL Server database and create an Always On Availability Group.

**Step 4. Test the cluster and availability group**
Before putting the availability group into production, you’ll test your deployment and the cluster’s behavior during an automatic failover or a disaster recovery event.

**Step 1. Prepare an AWS Account**

1. If you don’t already have an AWS account, create one at https://aws.amazon.com by following the on-screen instructions. Part of the sign-up process involves receiving a phone call and entering a PIN using the phone keypad.

2. Use the region selector in the navigation bar to choose the AWS Region where you want to deploy the software on AWS. For more information, see Regions and Availability Zones. Regions are dispersed and located in separate geographic areas. Each Region includes at least two Availability Zones that are isolated from one another but connected through low-latency links. Deploying your cloud applications across multiple Availability Zones helps you achieve high availability, even in the face of natural disasters that might impact a single Availability Zone.
Consider choosing a region closest to your data center or corporate network to reduce network latency between systems running on AWS and the systems and users on your corporate network.

If you’re planning to use a third Availability Zone for a file share witness instance or a third SQL Server node, choose an AWS Region that includes three or more Availability Zones; see the AWS Global Infrastructure webpage for a list.

3. Create a key pair in your preferred region. To do this, in the navigation pane of the Amazon EC2 console, choose Key Pairs, Create Key Pair, type a name, and then choose Create.
Amazon EC2 uses public-key cryptography to encrypt and decrypt login information. To be able to log in to your instances, you must create a key pair. With Windows instances, we use the key pair to obtain the administrator password via the Amazon EC2 console and then log in using Remote Desktop Protocol (RDP) as explained in the step-by-step instructions in the Amazon EC2 User Guide.

4. If necessary, request a service limit increase for the Amazon EC2 r4.2xlarge instance type. To do this, in the AWS Support Center, choose Create Case, Service Limit Increase, EC2 instances, and then complete the fields in the limit increase form. You might need to request an increase if you already have an existing deployment that uses this instance type, and you think you might exceed the default limit with this reference deployment. It might take a few days for the new service limit to become effective. For more information, see Amazon EC2 Service Limits in the AWS documentation.
Step 2. Launch the Quick Start

1. Choose one of the following options to launch the AWS CloudFormation template into your AWS account. For help choosing an option and prerequisites for deploying the software into an existing VPC, see deployment options earlier in this guide.

<table>
<thead>
<tr>
<th>Option 1</th>
<th>Option 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy software into a new VPC on AWS</td>
<td>Deploy software into an existing VPC on AWS</td>
</tr>
<tr>
<td>![Launch Button]</td>
<td>![Launch Button]</td>
</tr>
</tbody>
</table>

Each stack takes approximately three hours to create.
Note  You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using this Quick Start. For full details, see the pricing pages for each AWS service you will be using in this Quick Start.

2. Check the region that’s displayed in the upper-right corner of the navigation bar, and change it if necessary. This is where the network infrastructure will be built. The template is launched in the US East (Ohio) Region by default.

3. On the Select Template page, keep the default setting for the template URL, and then choose Next.

4. On the Specify Details page, change the stack name if needed. Review the parameters for the template. Provide values for the parameters that require input. For all other parameters, review the default settings and customize them as necessary. When you finish reviewing and customizing the parameters, choose Next.

In the following tables, parameters are listed and described separately for the two deployment scenarios:

–  Parameters for deployment into a new VPC
–  Parameters for deployment into an existing VPC

**Scenario 1: Parameters for deployment into a new VPC**

View the template for a new VPC

**Network Configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability Zones (AvailabilityZones)</td>
<td>Requires input</td>
<td>The list of Availability Zones to use for the subnets in the VPC. You must specify two zones if the Third AZ parameter is set to no, or three zones if the Third AZ parameter is set to yes. The Quick Start preserves the logical order you specify.</td>
</tr>
<tr>
<td>Third AZ (ThirdAZ)</td>
<td>no</td>
<td>Change this setting if you’d like to use three Availability Zones in your deployment. Choose witness to use the third zone for the file share witness, or full to use the third zone as a full SQL Server cluster node. If you choose witness, you must set the File Server Private IP Address parameter under Failover Cluster Configuration to an IP in the third subnet range.</td>
</tr>
<tr>
<td>VPC CIDR (VPCCIDR)</td>
<td>10.0.0.0/16</td>
<td>CIDR block for the VPC to create.</td>
</tr>
<tr>
<td>Parameter label (name)</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Public Subnet 1 CIDR</strong>&lt;br&gt;(PublicSubnet1CIDR)</td>
<td>10.0.128.0/20</td>
<td>CIDR block for the public (DMZ) subnet located in Availability Zone 1.</td>
</tr>
<tr>
<td><strong>Public Subnet 2 CIDR</strong>&lt;br&gt;(PublicSubnet2CIDR)</td>
<td>10.0.144.0/20</td>
<td>CIDR block for the public (DMZ) subnet located in Availability Zone 2.</td>
</tr>
<tr>
<td><strong>Public Subnet 3 CIDR</strong>&lt;br&gt;(PublicSubnet3CIDR)</td>
<td>10.0.160.0/20</td>
<td>CIDR block for the optional public (DMZ) subnet located in Availability Zone 3, if you’ve chosen to use a third zone.</td>
</tr>
<tr>
<td><strong>Private Subnet 1 CIDR</strong>&lt;br&gt;(PrivateSubnet1CIDR)</td>
<td>10.0.0.0/19</td>
<td>CIDR block for the private subnet located in Availability Zone 1.</td>
</tr>
<tr>
<td><strong>Private Subnet 2 CIDR</strong>&lt;br&gt;(PrivateSubnet2CIDR)</td>
<td>10.0.32.0/19</td>
<td>CIDR block for the private subnet located in Availability Zone 2.</td>
</tr>
<tr>
<td><strong>Private Subnet 3 CIDR</strong>&lt;br&gt;(PrivateSubnet3CIDR)</td>
<td>10.0.64.0/19</td>
<td>CIDR block for the optional private subnet located in Availability Zone 3, if you’ve chosen to use a third zone.</td>
</tr>
</tbody>
</table>

**Amazon EC2 Configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Pair Name</strong>&lt;br&gt;(KeyPairName)</td>
<td>Requires input</td>
<td>Public/private key pair, which allows you to connect securely to your instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region.</td>
</tr>
<tr>
<td><strong>Tenancy</strong>&lt;br&gt;(HostType)</td>
<td>Shared</td>
<td>Host type. If you choose Dedicated or Dedicated Host, hosts will be created in each Availability Zone.</td>
</tr>
<tr>
<td><strong>BYOL AMI to Use on Dedicated Host</strong>&lt;br&gt;(DedicatedHostAMI)</td>
<td>Requires input</td>
<td>Your imported bring your own license (BYOL) AMI ID, if you set the Tenancy parameter to Dedicated or Dedicated Host.</td>
</tr>
</tbody>
</table>

**Standard Active Directory Configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AD Scenario Type</strong>&lt;br&gt;(ADScenarioType)</td>
<td>AWS Directory Service for Microsoft AD</td>
<td>The type of Active Directory deployment to use. You can use AWS Directory Service for Active Directory, or choose Microsoft AD on Amazon EC2 to manage your own EC2 instances for Active Directory.</td>
</tr>
<tr>
<td><strong>Domain DNS Name</strong>&lt;br&gt;(DomainDNSName)</td>
<td>example.com</td>
<td>Fully qualified domain name (FQDN) of the forest root domain.</td>
</tr>
<tr>
<td><strong>Domain NetBIOS Name</strong>&lt;br&gt;(DomainNetBIOSName)</td>
<td>example</td>
<td>NetBIOS name of the domain for users of earlier versions of Windows. This can be up to 15 characters long.</td>
</tr>
<tr>
<td><strong>Domain Admin Password</strong>&lt;br&gt;(DomainAdminPassword)</td>
<td>Requires input</td>
<td>Password for the domain administrator user. This must be a complex password that’s at least 8 characters long.</td>
</tr>
</tbody>
</table>
Self-Managed Active Directory Configuration (for non-AWS Directory Service architecture):

**Note**  The parameters in this section are ignored if you have selected AWS Directory Service for Microsoft AD as the AD Scenario Type.

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Admin User Name (DomainAdminUser)</td>
<td>StackAdmin</td>
<td>User name for the account that is added as domain administrator. This is separate from the default administrator account.</td>
</tr>
<tr>
<td>Domain Controller 1 Instance Type (ADServer1InstanceType)</td>
<td>m4.xlarge</td>
<td>EC2 instance type for the first Active Directory instance.</td>
</tr>
<tr>
<td>Domain Controller 1 NetBIOS Name (ADServer1NetBIOSName)</td>
<td>DC1</td>
<td>NetBIOS name of the first Active Directory server. This can be up to 15 characters long.</td>
</tr>
<tr>
<td>Domain Controller 1 Private IP Address (ADServer1PrivateIP)</td>
<td>10.0.0.10</td>
<td>Fixed private IP for the first Active Directory server located in Availability Zone 1.</td>
</tr>
<tr>
<td>Domain Controller 2 Instance Type (ADServer2InstanceType)</td>
<td>m4.xlarge</td>
<td>EC2 instance type for the second Active Directory instance.</td>
</tr>
<tr>
<td>Domain Controller 2 NetBIOS Name (ADServer2NetBIOSName)</td>
<td>DC2</td>
<td>NetBIOS name of the second Active Directory server. This can be up to 15 characters long.</td>
</tr>
<tr>
<td>Domain Controller 2 Private IP Address (ADServer2PrivateIP)</td>
<td>10.0.32.10</td>
<td>Fixed private IP for the second Active Directory server located in Availability Zone 2.</td>
</tr>
<tr>
<td>Restore Mode Password (RestoreModePassword)</td>
<td>Requires input</td>
<td>Password for a separate administrator account when the domain controller is in restore mode. This must be a complex password that’s at least 8 characters long.</td>
</tr>
</tbody>
</table>

Remote Desktop Configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed Remote Desktop Gateway External Access CIDR (RDGWCIDR)</td>
<td>Requires input</td>
<td>Allowed CIDR block for external access to the Remote Desktop Gateway instances. We recommend that you set this value to a trusted CIDR block.</td>
</tr>
<tr>
<td>Number of RDGW hosts (NumberOfRDGWHosts)</td>
<td>1</td>
<td>The number of RD Gateway instances to create. You can choose 1-4 instances.</td>
</tr>
<tr>
<td>Remote Desktop Gateway Instance Type (RDGWInstanceType)</td>
<td>t2.large</td>
<td>EC2 instance type for the Remote Desktop Gateway instances.</td>
</tr>
</tbody>
</table>
### Microsoft SQL Server Configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Account Name</strong> (SQLServiceAccount)</td>
<td>sqlsa</td>
<td>User name for the SQL Server service account. This account is a domain user.</td>
</tr>
<tr>
<td><strong>Service Account Password</strong> (SQLServiceAccountPassword)</td>
<td>Requires input</td>
<td>Password for the SQL Server service account. This must be a complex password that's at least 8 characters long.</td>
</tr>
<tr>
<td><strong>Amazon-Provided SQL Server License</strong> (SQLLicenseProvided)</td>
<td>no</td>
<td>Set to yes to use the license-included SQL Server AMI from AWS. For more information about licensing options, see the Cost and Licenses section.</td>
</tr>
<tr>
<td><strong>SQL Server Volume IOPS</strong> (VolumeIops)</td>
<td>1000</td>
<td>Provisioned IOPS for the SQL Server data, logs, and tempdb volumes. This setting applies only when the SQL Server Volume Type parameter is set to io1.</td>
</tr>
<tr>
<td><strong>SQL Server Volume Size</strong> (VolumeSize)</td>
<td>500</td>
<td>Volume size for the SQL Server data, logs, and tempdb volumes, in GiB.</td>
</tr>
<tr>
<td><strong>SQL Server Volume Type</strong> (VolumeType)</td>
<td>gp2</td>
<td>Volume type (gp2 or io1) for the SQL Server data, logs, and tempdb volumes.</td>
</tr>
</tbody>
</table>

### Failover Cluster Configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Instance Type for Cluster Nodes</strong> (WSFCNodeInstanceType)</td>
<td>r4.2xlarge</td>
<td>EC2 instance type for the WSFC nodes.</td>
</tr>
<tr>
<td><strong>Cluster Node 1 NETBIOS Name</strong> (WSFCNode1NetBIOSName)</td>
<td>WSFCNode1</td>
<td>NetBIOS name of the first WSFC node. This can be up to 15 characters long.</td>
</tr>
<tr>
<td><strong>Cluster Node 1 Private IP Address 1</strong> (WSFCNode1PrivateIP1)</td>
<td>10.0.0.100</td>
<td>Primary private IP for the first WSFC node.</td>
</tr>
<tr>
<td><strong>Cluster Node 1 Private IP Address 2</strong> (WSFCNode1PrivateIP2)</td>
<td>10.0.0.101</td>
<td>Secondary private IP for the first WSFC node.</td>
</tr>
<tr>
<td><strong>Cluster Node 1 Private IP Address 3</strong> (WSFCNode1PrivateIP3)</td>
<td>10.0.0.102</td>
<td>Third private IP for the first WSFC node.</td>
</tr>
<tr>
<td><strong>Cluster Node 2 NETBIOS Name</strong> (WSFCNode2NetBIOSName)</td>
<td>WSFCNode2</td>
<td>NetBIOS name of the second WSFC node. This can be up to 15 characters long.</td>
</tr>
<tr>
<td><strong>Cluster Node 2 Private IP Address 1</strong> (WSFCNode2PrivateIP1)</td>
<td>10.0.32.100</td>
<td>Primary private IP for the second WSFC node.</td>
</tr>
</tbody>
</table>
### Parameter label (name) | Default | Description
--- | --- | ---
Cluster Node 2 Private IP Address 2 (WSFCNode2PrivateIP2) | 10.0.32.101 | Secondary private IP for the second WSFC node.

Cluster Node 2 Private IP Address 3 (WSFCNode2PrivateIP3) | 10.0.32.102 | Third private IP for the second WSFC node.

Cluster Node 3 NETBIOS Name (WSFCNode3NetBIOSName) | WSFCNode3 | NetBIOS name of the third (optional) WSFC node. This can be up to 15 characters long.

Cluster Node 3 Private IP Address 1 (WSFCNode3PrivateIP1) | 10.0.64.100 | Primary private IP for the third (optional) WSFC node.

Cluster Node 3 Private IP Address 2 (WSFCNode3PrivateIP2) | 10.0.64.101 | Secondary private IP for the third (optional) WSFC node.

Cluster Node 3 Private IP Address 3 (WSFCNode3PrivateIP3) | 10.0.64.102 | Third private IP for the third (optional) WSFC node.

File Server Instance Type (WSFCFileServerInstanceType) | t2.small | EC2 instance type for the file server used to share installation media, witness, and replication folders.

File Server Private IP Address (WSFCFileServerPrivateIP) | 10.0.0.200 | Primary private IP for the file server located in Availability Zone 1. If you choose **witness** for the Third AZ parameter in the Network Configuration section, you must specify an IP in the third subnet range.

---

**AWS Quick Start Configuration:**

### Parameter label (name) | Default | Description
--- | --- | ---
Quick Start S3 Bucket Name (QSS3BucketName) | quickstart-reference | S3 bucket where the Quick Start templates and scripts are installed. Use this parameter to specify the S3 bucket name you've created for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. The bucket name can include numbers, lowercase letters, uppercase letters, and hyphens, but should not start or end with a hyphen.

Quick Start S3 Key Prefix (QSS3KeyPrefix) | microsoft/sql/latest/ | The [S3 key name prefix](https://docs.aws.amazon.com/QuickStart/latest/SQLServerAWS/keywords.html) used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes.
- **Parameters for deployment into an existing VPC**

  [View the template for existing VPC](#)

**Network Configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third AZ (ThirdAZ)</td>
<td>no</td>
<td>Change this setting if you’d like to use three Availability Zones in your deployment. Choose <strong>witness</strong> to use the third zone for the file share witness, or <strong>full</strong> to use the third zone as a full SQL Server cluster node. If you choose <strong>witness</strong>, you must set the <strong>File Server Private IP Address</strong> parameter under <strong>Failover Cluster Configuration</strong> to an IP in the third subnet range.</td>
</tr>
<tr>
<td><strong>VPC ID (VPCID)</strong></td>
<td><strong>Requires input</strong></td>
<td>ID of your existing VPC (e.g., vpc-0343606e).</td>
</tr>
<tr>
<td><strong>Private Subnet 1 ID (PrivateSubnet1ID)</strong></td>
<td><strong>Requires input</strong></td>
<td>ID of the private subnet in Availability Zone 1 in your existing VPC (e.g., subnet-a0246dcd).</td>
</tr>
<tr>
<td><strong>Private Subnet 2 ID (PrivateSubnet2ID)</strong></td>
<td><strong>Requires input</strong></td>
<td>ID of the private subnet in Availability Zone 2 in your existing VPC (e.g., subnet-b58c3d67).</td>
</tr>
<tr>
<td><strong>Private Subnet 3 ID (PrivateSubnet3ID)</strong></td>
<td>—</td>
<td>ID of the private subnet in Availability Zone 3 in your existing VPC (e.g., subnet-7f16e910), if you’re using three Availability Zones.</td>
</tr>
</tbody>
</table>

**Amazon EC2 Configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Pair Name (KeyPairName)</strong></td>
<td><strong>Requires input</strong></td>
<td>Public/private key pair, which allows you to connect securely to your instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region.</td>
</tr>
<tr>
<td><strong>Tenancy (HostType)</strong></td>
<td>Shared</td>
<td>Host type. If you choose <strong>Dedicated</strong> or <strong>Dedicated Host</strong>, hosts will be created in each Availability Zone.</td>
</tr>
<tr>
<td><strong>BYOL AMI to Use on Dedicated Host (DedicatedHostAMI)</strong></td>
<td><strong>Requires input</strong></td>
<td>Your imported bring your own license (BYOL) AMI ID, if you set the <strong>Tenancy</strong> parameter to <strong>Dedicated</strong> or <strong>Dedicated Host</strong>.</td>
</tr>
</tbody>
</table>

**Microsoft Active Directory Configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain DNS Name (DomainDNSName)</strong></td>
<td>example.com</td>
<td>Fully qualified domain name (FQDN) of the forest root domain.</td>
</tr>
<tr>
<td>Parameter label (name)</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------------</td>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Domain NetBIOS Name (DomainNetBIOSName)</td>
<td>example</td>
<td>NetBIOS name of the domain for users of earlier versions of Windows. This can be up to 15 characters long.</td>
</tr>
<tr>
<td>Domain Admin User Name (DomainAdminUser)</td>
<td>StackAdmin</td>
<td>User name for the account that is added as domain administrator. This is separate from the default administrator account.</td>
</tr>
<tr>
<td>Domain Admin Password (DomainAdminPassword)</td>
<td>Requires input</td>
<td>Password for the domain administrator user. This must be a complex password that’s at least 8 characters long.</td>
</tr>
<tr>
<td>Security Group ID for AD Domain Members (DomainMemberSGID)</td>
<td>Requires input</td>
<td>ID of the domain name security group (e.g., sq-7f16e910).</td>
</tr>
</tbody>
</table>

**Microsoft SQL Server Configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Account Name (SQLServiceAccount)</td>
<td>sqlsa</td>
<td>User name for the SQL Server service account. This account is a domain user.</td>
</tr>
<tr>
<td>Service Account Password (SQLServiceAccountPassword)</td>
<td>Requires input</td>
<td>Password for the SQL Server service account. This must be a complex password that’s at least 8 characters long.</td>
</tr>
<tr>
<td>Amazon-Provided SQL Server License (SQLLicenseProvided)</td>
<td>no</td>
<td>Set to yes to use the license-included SQL Server AMI from AWS. For more information about licensing options, see the Cost and Licenses section.</td>
</tr>
<tr>
<td>Data Volume Size (Volume1Size)</td>
<td>500</td>
<td>Volume size for the SQL Server data drive, in GiB.</td>
</tr>
<tr>
<td>Data Volume Type (Volume1Type)</td>
<td>gp2</td>
<td>Volume type (gp2 or io1) for the SQL Server data drive.</td>
</tr>
<tr>
<td>Data Volume IOPS (Volume1Iops)</td>
<td>1000</td>
<td>Provisioned IOPS for the SQL Server data drive. This setting applies only when the Data Volume Type parameter is set to io1.</td>
</tr>
<tr>
<td>Logs Volume Size (Volume2Size)</td>
<td>500</td>
<td>Volume size for the SQL Server Logs drive, in GiB.</td>
</tr>
<tr>
<td>Logs Volume Type (Volume2Type)</td>
<td>gp2</td>
<td>Volume type (gp2 or io1) for the SQL Server Logs drive.</td>
</tr>
<tr>
<td>Logs Volume IOPS (Volume2Iops)</td>
<td>1000</td>
<td>Provisioned IOPS for the SQL Server Logs drive. This setting applies only when the Logs Volume Type parameter is set to io1.</td>
</tr>
<tr>
<td>TempDB Volume Size (Volume3Size)</td>
<td>500</td>
<td>Volume size for the SQL Server tempdb drive, in GiB.</td>
</tr>
<tr>
<td>Parameter label (name)</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>TempDB Volume Type</strong> (Volume3Type)</td>
<td>gp2</td>
<td>Volume type (gp2 or io1) for the SQL Server tempdb drive.</td>
</tr>
<tr>
<td><strong>TempDb Volume IOPS</strong> (Volume3Iops)</td>
<td>1000</td>
<td>Provisioned IOPS for the SQL Server tempdb drive. This setting applies only when the TempDB Volume Type parameter is set to io1.</td>
</tr>
</tbody>
</table>

**Failover Cluster Configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File Server Instance Type</strong> (WSFCFileServerInstanceType)</td>
<td>t2.small</td>
<td>EC2 instance type for the file server used to share installation media, witness, and replication folders.</td>
</tr>
<tr>
<td><strong>File Server NetBIOS Name</strong> (WSFCFileServerNetBIOSName)</td>
<td>WSFCFileServer</td>
<td>NetBIOS name of the WSFC file server (up to 15 characters).</td>
</tr>
<tr>
<td><strong>File Server Private IP Address</strong> (WSFCFileServerPrivateIP)</td>
<td>10.0.0.200</td>
<td>Primary private IP for the file server in Availability Zone 1. If you choose witness for the Third AZ parameter in the Network Configuration section, you must specify an IP in the third subnet range.</td>
</tr>
<tr>
<td><strong>Instance Type for Cluster Node 1</strong> (WSFCNode1InstanceType)</td>
<td>r4.2xlarge</td>
<td>EC2 instance type for the first WSFC node.</td>
</tr>
<tr>
<td><strong>Cluster Node 1 NETBIOS Name</strong> (WSFCNode1NetBIOSName)</td>
<td>WSFCNode1</td>
<td>NetBIOS name of the first WSFC node. This can be up to 15 characters long.</td>
</tr>
<tr>
<td><strong>Cluster Node 1 Private IP Address 1</strong> (WSFCNode1PrivateIP1)</td>
<td>10.0.0.100</td>
<td>Primary private IP for the first WSFC node.</td>
</tr>
<tr>
<td><strong>Cluster Node 1 Private IP Address 2</strong> (WSFCNode1PrivateIP2)</td>
<td>10.0.0.101</td>
<td>Secondary private IP for the first WSFC node.</td>
</tr>
<tr>
<td><strong>Cluster Node 1 Private IP Address 3</strong> (WSFCNode1PrivateIP3)</td>
<td>10.0.0.102</td>
<td>Third private IP for the first WSFC node.</td>
</tr>
<tr>
<td><strong>Dedicated Host ID for Node 1</strong> (DedicatedHostIDNode1)</td>
<td>—</td>
<td>Dedicated host ID for the first WSFC node. This parameter is used only if you set the Tenancy parameter to Dedicated Host.</td>
</tr>
<tr>
<td><strong>Instance Type for Cluster Node 2</strong> (WSFCNode2InstanceType)</td>
<td>r4.2xlarge</td>
<td>EC2 instance type for the second WSFC node.</td>
</tr>
<tr>
<td><strong>Cluster Node 2 NETBIOS Name</strong> (WSFCNode2NetBIOSName)</td>
<td>WSFCNode2</td>
<td>NetBIOS name of the second WSFC node. This can be up to 15 characters long.</td>
</tr>
<tr>
<td><strong>Cluster Node 2 Private IP Address 1</strong> (WSFCNode2PrivateIP1)</td>
<td>10.0.32.100</td>
<td>Primary private IP for the second WSFC node.</td>
</tr>
</tbody>
</table>
### Parameter label (name) | Default | Description
--- | --- | ---
**Cluster Node 2 Private IP Address 2** (WSFCNode2PrivateIP2) | 10.0.32.101 | Secondary private IP for the second WSFC node.

**Cluster Node 2 Private IP Address 3** (WSFCNode2PrivateIP3) | 10.0.32.102 | Third private IP for the second WSFC node.

**Dedicated HostID for Node 2** (DedicatedHostIDNode2) | — | Dedicated host ID for the second WSFC node. This parameter is used only if you set the **Tenancy** parameter to **Dedicated Host**.

**Instance Type for Cluster Node 3** (WSFCNode3InstanceType) | r4.2xlarge | EC2 instance type for the third (optional) WSFC node.

**Cluster Node 3 NETBIOS Name** (WSFCNode3NetBIOSName) | WSFCNode3 | NetBIOS name of the third (optional) WSFC node. This can be up to 15 characters long.

**Cluster Node 3 Private IP Address 1** (WSFCNode3PrivateIP1) | 10.0.64.100 | Primary private IP for the third (optional) WSFC node.

**Cluster Node 3 Private IP Address 2** (WSFCNode3PrivateIP2) | 10.0.64.101 | Secondary private IP for the third (optional) WSFC node.

**Cluster Node 3 Private IP Address 3** (WSFCNode3PrivateIP3) | 10.0.64.102 | Third private IP for the third (optional) WSFC node.

**Dedicated HostID for Node 3** (DedicatedHostIDNode3) | — | Dedicated host ID for the optional third WSFC node. This parameter is used only if you set the **Tenancy** parameter to **Dedicated Host**.

---

**AWS Quick Start Configuration:**

### Parameter label (name) | Default | Description
--- | --- | ---
**Quick Start S3 Bucket Name** (QSS3BucketName) | quickstart-reference | S3 bucket where the Quick Start templates and scripts are installed. Use this parameter to specify the S3 bucket name you’ve created for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. The bucket name can include numbers, lowercase letters, uppercase letters, and hyphens, but should not start or end with a hyphen.

**Quick Start S3 Key Prefix** (QSS3KeyPrefix) | microsoft/sql/latest/ | The **S3 key name prefix** used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes.
5. On the **Options** page, you can **specify tags** (key-value pairs) for resources in your stack and **set advanced options**. When you’re done, choose **Next**.

6. On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the check box to acknowledge that the template will create IAM resources.

7. Choose **Create** to deploy the stack.

8. Monitor the status of the stack. When the status is **CREATE_COMPLETE**, the WSFC cluster is ready.

9. You can use the URLs displayed in the **Outputs** tab for the stack to view the resources that were created.

---

### Step 3. Configure a SQL Server Always On Availability Group

**Note**  If you’re using a third Availability Zone as a full SQL Server cluster node (that is, if you set the **Third AZ** parameter to **full**), take that into consideration when following the steps in this section.

After you have successfully deployed the Quick Start, you can set up permissions for AWS Directory Service (if applicable), configure the WSFC nodes by choosing and backing up a database, and create and configure an availability group.

#### Set up Permissions for the Cluster Object

If you’re using the AWS Directory Service (that is, if the **AD Scenario Type** parameter in step 2 is set to **AWS Directory Service for Microsoft AD**, which is the default), follow these steps to set up permissions:

1. Run Windows PowerShell as an administrator, and use the following command to install Active Directory Management Services:

   ```powershell
   Add-WindowsFeature RSAT-ADDS-Tools
   ```

2. Open **Active Directory Users and Computers** on one of your two cluster node instances.

3. In the navigation bar, choose **View, Advanced Features** to see the advanced features for **Active Directory Users and Computers**.

4. Expand the organizational unit (OU) for your domain name.
5. Open the context (right-click) menu for the Computers OU within your domain name, and then choose Properties.


7. In the Advanced Security Settings dialog box, choose Add.

8. Next to Principal, choose Select a principal.

9. Choose Object Types, select Computers, and then choose OK.

10. Type the name of your cluster object (WSFCLUSTER1 for the default name), choose Check Names, and then choose OK.

11. When your object has been verified, choose OK.

12. Add the Create Computer objects permission to this principal, and then choose OK.

13. In the Advanced Security Settings for Computers screen, choose OK.

14. In the Computer Properties screen, choose OK.

Create a Test Database or Attach an Existing Database

1. Open the Desktop Connection application (mstsc.exe) and connect to the first cluster node (e.g., WSFCNode1).

2. Open SQL Server Management Studio (SSMS).

3. In the Connect to Server dialog box, connect to the first cluster node (e.g., WSFCNode1).

4. Create a new database or attach a test database.

5. Make sure that the Recovery model on the database is set to Full.
6. Open the context (right-click) menu for the database in SSMS, and then choose **Tasks, Backup**.

**Create an Availability Group**

1. In **Object Explorer**, open the context (right-click) menu for **AlwaysOn High Availability** and launch the **New Availability Group** wizard.
2. Complete the **New Availability Group** wizard:
   a. On the **Introduction** page, choose **Next**.
   b. On the **Specify Availability Group Name** page, type **SQLAG1**, and then choose **Next**.
   c. On the **Select Databases** page, choose the database you created or attached in the previous section, and then choose **Next**.
   d. On the **Specify Replicas** page, add the second cluster node (e.g., WSFCNode2), and then choose **Automatic Failover**.
On the Listener tab, choose Create an availability group listener, provide a Listener DNS Name (e.g., AG1-Listener), and then specify the TPC port used by this listener (e.g., 1433). Add the two private subnets the cluster nodes were deployed into and a corresponding IPv4 address.

**Note** We will use the secondary private IP addresses we assigned earlier to the nodes (e.g., 10.0.0.102 and 10.0.32.102). If you’re using the third Availability Zone with a SQL node, you’ll also want to add 10.0.64.102.
Figure 11: Creating an availability group listener

f. On the Select Initial Data Synchronization page, choose Full. In the shared network location box, type `\\WSFCFileServer\replica` if you’re using a file share witness, or `\\WSFCNode1\replica` if you have three SQL nodes (that is, if you set the Third AZ parameter to full). Then choose Next.

g. On the Validation page, choose Next.

h. On the Summary page, choose Finish, and then close the wizard.

3. Run Windows PowerShell as an administrator and change the availability group listener host record TTL to 300.
4. Open DNS Manager:
   - If you’re using AWS Directory Service:
     a. On the Remote Desktop Gateway instance, install Remote Server Administration Tools for DNS Server, by running this command in a PowerShell window with administrator privileges:

```
Install-WindowsFeature RSAT-DNS-Server
```

b. In the same PowerShell window, run the command:

```
Get-NetIPConfiguration
```

c. Select one of the DNS server addresses from the command output.

d. Use that address to connect to the DNS server when you open DNS Manager.
   - If you’re not using AWS Directory Service:
     a. Open the Desktop Connection application (mstsc.exe) and connect to the primary domain controller in Availability Zone 1, using its NetBIOS name (e.g., DC1).
b. Use the credentials of the domain admin user and domain admin password to log into the instance.

c. Open DNS Manager.

5. In DNS Manager, check to make sure that all availability group listener (e.g., AG1-Listener) IP addresses are listed.

![DNS Manager](image)

**Figure 13: Verifying DNS configuration**

**Note** Client connectivity to an availability group database can be established via the availability group listener. The availability group listener (in this case, AG1-Listener) is a virtual network name that clients can connect to. This configuration allows clients to connect to a database without knowing the name of an individual server in the WSFC cluster. The availability group listener can share TCP port 1433 with an individual SQL Server instance. However, when running multiple side-by-side SQL Server instances, you will need to use a non-standard port to avoid a port conflict.
The security groups and ingress rules created by the AWS CloudFormation template permit all required traffic between WSFC nodes and client connections to TCP port 1433 from the remaining server tiers within the VPC. See the **Security** section of this guide for a detailed list of port mappings.

When you complete the steps in this section, you will have a WSFC cluster and SQL Server Always On Availability Group successfully deployed in the AWS Cloud, as illustrated previously in Figure 1.

**Step 4: Test the Cluster and Availability Group**

**Note** If you’re using a third Availability Zone as a full SQL Server cluster node (that is, if you set the Third AZ parameter to full), take that into consideration when following the steps in this section.

Before you put the availability group into production, you should test your deployment and familiarize yourself with the cluster’s behavior during a high availability automatic failover or a disaster recovery event.

1. Open the Remote Desktop Connection application (mstsc.exe), connect to the Remote Desktop Gateway instance, and then connect to the WSFC node (e.g., WSFCNode1) in that zone.

2. On the first cluster node instance, open the Failover Cluster Manager to view the cluster core resources. Make sure the cluster, one of the two listed IP addresses, and the file share witness are online.
Figure 14: Viewing the Failover Cluster Manager

3. Open SQL Server Management Studio. In Object Explorer, open the context (right-click) menu for the **AlwaysOn High Availability** node, and launch the dashboard for the availability group you created earlier (e.g., SQLAG1).

4. In the dashboard, view the availability replicas and make sure their synchronization state is **Synchronized**.
Figure 15: Viewing the Always On High Availability dashboard with all nodes synchronized

5. Make sure that the primary instance and the IP address in the Cluster Core Resources pane of Failover Cluster Manager are coordinated. That is, if the primary instance is WSFCNode1, the IP address 10.0.0.101 should be online. If you need to move the cluster core resources to WSFCNode1, you can do so through PowerShell by using the command:

   ```powershell
   Get-ClusterGroup 'Cluster Group' | Move-ClusterGroup -Node WSFCNode1
   ```

6. Sign in to the AWS Management Console, and open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.

7. Stop the primary instance (e.g., WSFCNode1).

8. Open the Remote Desktop Connection application (mstsc.exe), connect to the second cluster node (e.g., WSFCNode2) in Availability Zone 2.

9. On the second cluster node instance, use the Failover Cluster Manager to view the cluster core resources. Note that the IP address that was previously offline (e.g., 10.0.32.101) is now online.
10. Open SQL Server Management Studio. In Object Explorer, open the context (right-click) menu for the **AlwaysOn High Availability** node, and launch the dashboard for the availability group you created earlier (e.g., SQLAG1).

11. In the dashboard, view the availability replicas. Note that now the primary instance has switched to WSFCNode2, and that the synchronization state of WSFCNode1 is **Not Synchronizing**.
At this point, you can start the WSFCNode1 instance again in the Amazon EC2 console. When the instance is online, use the **Failover wizard** in the Availability Group dashboard and switch the primary instance back to WSFCNode1.

**Note** We recommend that you use `MultiSubnetFailover=true` in your SQL client connection string. This property enables faster failover for all availability groups in SQL Server and will significantly reduce failover time for single and multi-subnet Always On topologies. If you have legacy clients that need to connect to an availability group listener and cannot use `MultiSubnetFailover`, we recommend that you change the `RegisterAllProvidersIP` setting to 0 by using the `Set-ClusterParameter` cmdlet.
Troubleshooting

Q. I encountered a CREATE_FAILED error when I launched the Quick Start. What should I do?

A. If AWS CloudFormation, we recommend that you relaunch the template with **Rollback on failure** set to **No**. (This setting is under **Advanced** in the AWS CloudFormation console, **Options** page.) With this setting, the stack’s state will be retained and the instance will be left running, so you can troubleshoot the issue. (You’ll want to look at the log files in %ProgramFiles%\Amazon\EC2ConfigService and in the C:\cfn\log folder.)

**Important** When you set **Rollback on failure** to **No**, you’ll continue to incur AWS charges for this stack. Please make sure to delete the stack when you’ve finished troubleshooting.

The following table lists specific CREATE_FAILED error messages you might encounter.

<table>
<thead>
<tr>
<th>Error message</th>
<th>Possible cause</th>
<th>What to do</th>
</tr>
</thead>
<tbody>
<tr>
<td>API: ec2: RunInstances Not authorized for images: ami-ID</td>
<td>The template is referencing an AMI that has expired</td>
<td>We refresh AMIs on a regular basis, but our schedule isn’t always synchronized with AWS AMI updates. If you get this error message, notify us, and we’ll update the template with the new AMI ID. If you’d like to fix the template yourself, you can download it and update the Mappings section with the latest AMI ID for your region.</td>
</tr>
<tr>
<td>We currently do not have sufficient r4.2xlarge capacity in the AZ you requested</td>
<td>The WSFC node requires a larger instance type</td>
<td>Switch to an instance type that supports higher capacity, or complete the request form in the AWS Support Center to increase the Amazon EC2 limit for the instance type or region. Limit increases are tied to the region they were requested for.</td>
</tr>
<tr>
<td>Instance ID did not stabilize</td>
<td>You have exceeded your IOPS for the region</td>
<td>Request a limit increase by completing the request form in the AWS Support Center.</td>
</tr>
<tr>
<td>System Administrator password must contain at least 8 characters</td>
<td>The master password contains $ or other special characters</td>
<td>Change the password for the domain administrator or SQL Server service account, and then relaunch the Quick Start. The password must be at least 8 characters, consisting of uppercase and lowercase letters and numbers. Avoid using special characters such as @ or $.</td>
</tr>
</tbody>
</table>

For additional information, see [Troubleshooting AWS CloudFormation](#) on the AWS website. If the problem you encounter isn’t covered on that page or in the table, please visit the [AWS Support Center](#). If you’re filing a support ticket, please attach the install.log file.
from the master instance (this is the log file that is located in the /root/install folder) to the ticket.

**Q.** I encountered a size limitation error when I deployed the AWS Cloudformation templates.

**A.** We recommend that you launch the Quick Start templates from the location we’ve provided or from another S3 bucket. If you deploy the templates from a local copy on your computer, you might encounter template size limitations when you create the stack. For more information about AWS CloudFormation limits, see the [AWS documentation](https://aws.amazon.com/documentation/cloudformation/).

## Security

AWS provides a set of building blocks (e.g., Amazon EC2 and Amazon VPC) that customers can use to provision infrastructure for their applications. In this model, some security capabilities, such as physical security, are the responsibility of AWS and are highlighted in the [AWS security whitepaper](https://aws.amazon.com/security/). Other areas, such as controlling access to applications, fall on the application developer and the tools provided in the Microsoft platform.

This Quick Start configures the following security groups for SQL Server:

<table>
<thead>
<tr>
<th>Security group</th>
<th>Associated with</th>
<th>Inbound source</th>
<th>Port(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WSFCSecurityGroup</strong></td>
<td>WSFCNode1, WSFCNode2, WSFCNode3, WSFCFileServer</td>
<td>WSFCSecurityGroup</td>
<td>ICMP-1, TCP135, TCP137, UDP137, TCP445, TCP1433, TCP1434, UDP3343, TCP5022, TCP5985</td>
</tr>
<tr>
<td><strong>WSFCClientSecurityGroup</strong></td>
<td>WSFCNode1, WSFCNode2, WSFCNode3, WSFCFileServer</td>
<td>SQLServerAccessSecurityGroup</td>
<td>TCP1433</td>
</tr>
<tr>
<td><strong>SQLServerAccessSecurity Group</strong></td>
<td>Add instances that require access to SQL to this security group</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Additional Resources

AWS services
- AWS CloudFormation
  https://aws.amazon.com/documentation/cloudformation/
- Amazon EBS
- Amazon EC2
- Amazon VPC
  https://aws.amazon.com/documentation/vpc/

WSFC with SQL Server
- Windows Server Failover Clustering (WSFC) with SQL Server
  https://msdn.microsoft.com/library/79d2ea5a-edd8-4b3b-9502-96202057b01a
- Always On Availability Groups

Deploying Microsoft software on AWS
- Microsoft on AWS
  https://aws.amazon.com/microsoft/
- Secure Microsoft applications on AWS
- Microsoft Licensing Mobility
  https://aws.amazon.com/windows/mslicensemobility/
- MSDN on AWS
  https://aws.amazon.com/windows/msdn/
- AWS Windows and .NET Developer Center on AWS
  https://aws.amazon.com/net/

Quick Start reference deployments
- AWS Quick Start home page
  https://aws.amazon.com/quickstart/
- Microsoft Active Directory DS on the AWS Cloud
  [https://docs.aws.amazon.com/quickstart/latest/active-directory-ds/](https://docs.aws.amazon.com/quickstart/latest/active-directory-ds/)

- Microsoft Remote Desktop Gateway on the AWS Cloud
  [https://docs.aws.amazon.com/quickstart/latest/rd-gateway/](https://docs.aws.amazon.com/quickstart/latest/rd-gateway/)

- Microsoft SharePoint on the AWS Cloud
  [https://docs.aws.amazon.com/quickstart/latest/sharepoint/](https://docs.aws.amazon.com/quickstart/latest/sharepoint/)

- Microsoft Servers on the AWS Cloud
  [https://docs.aws.amazon.com/quickstart/latest/accelerator-msservers/](https://docs.aws.amazon.com/quickstart/latest/accelerator-msservers/)

### Send Us Feedback

You can visit our [GitHub repository](https://github.com/aws/QuickStarts) to download the templates and scripts for this Quick Start, to post your comments, and to share your customizations with others.

### Document Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Changes</th>
<th>In sections</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>December 2017</strong></td>
<td>Added support for SQL Server 2017; deprecated SQL Server 2012.</td>
<td>Template updates and changes throughout guide</td>
</tr>
<tr>
<td></td>
<td>Added instructions for setting up permissions for the cluster object.</td>
<td>Set up permissions</td>
</tr>
<tr>
<td><strong>August 2017</strong></td>
<td>Refactored templates with submodules following Quick Start best practices, and added support for:</td>
<td>Template updates and changes throughout guide</td>
</tr>
<tr>
<td></td>
<td>- AWS Directory Service for Microsoft Active Directory (set as default)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2016 and license-included AMI provided by Amazon</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Three tenancy options (default, dedicated, dedicated hosts)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Choice of two or three Availability Zones</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Choice of two SQL nodes plus dedicated file share witness, or three SQL nodes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Customizable EBS volume types (gp2, io1) and adjustable IOPS (for io1)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- New R4 instance types</td>
<td></td>
</tr>
<tr>
<td><strong>September 2015</strong></td>
<td>Changed the default type for Active Directory and RD Gateway instances to m4.xlarge for better performance and price.</td>
<td>Template parameters</td>
</tr>
<tr>
<td><strong>April 2015</strong></td>
<td>Updated the storage configuration on the WSFC nodes.</td>
<td>Storage on the WSFC Nodes</td>
</tr>
</tbody>
</table>
© 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Notices

This document is provided for informational purposes only. It represents AWS’s current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS’s products or services, each of which is provided “as is” without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

The software included with this paper is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at http://aws.amazon.com/apache2.0/ or in the "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.