NetApp ONTAP Cloud with SQL Server on the AWS Cloud

Quick Start Reference Deployment

April 2017

Kevin Hill and Mudassar Shafique, NetApp
Saulo Cruz and Shivansh Singh, Amazon Web Services

Contents
Overview.................................................................................................................................2
Costs and Licenses..................................................................................................................3
Architecture............................................................................................................................3
Prerequisites ..........................................................................................................................5
Deployment Options ..............................................................................................................5
Deployment Steps ..................................................................................................................6
  Step 1. Prepare Your AWS Account ..................................................................................6
  Step 2. Subscribe to the AMIs for NetApp Software .........................................................6
  Step 3. Launch the Quick Start .......................................................................................9
  Step 4. Access Your ONTAP Cloud with SQL Server Deployment .............................13
Cleaning Up ..........................................................................................................................17
  Removing the ONTAP Cloud System ............................................................................17
  Removing the Quick Start CloudFormation Stacks .......................................................20
Troubleshooting ...................................................................................................................23
Security .................................................................................................................................25
  AWS Identity and Access Management (IAM) ...............................................................26
This Quick Start deployment guide was created by Amazon Web Services (AWS) in partnership with NetApp.

Quick Starts are automated reference deployments that use AWS CloudFormation templates to launch, configure, and run the AWS compute, network, storage, and other services required to deploy a specific workload on AWS.

Overview

This Quick Start reference deployment guide provides step-by-step instructions for deploying an environment with NetApp ONTAP Cloud and Microsoft SQL Server on the AWS Cloud.

NetApp data storage systems are used by enterprises that require complete control, efficiency, durability, and resiliency of their data. NetApp ONTAP Cloud is a software-only version of Data ONTAP, which is the data management operating system from NetApp that is used on physical NetApp storage appliances. With ONTAP Cloud, the operating system has been customized to run as an Amazon Elastic Compute Cloud (Amazon EC2) instance.

The features of ONTAP Cloud include:

- Storage efficiencies that enable you to use less underlying storage capacity for your data needs
- Instant backup and recovery for data of all sizes
- Space-efficient, intuitive, bi-directional data transfer
- Instant, writable data clones that consume no additional storage capacity
- Ability to use multiple protocols (NFS, CIFS, and iSCSI) from the same storage system, at the same time

With ONTAP Cloud on AWS, you can spin up a new enterprise-class data management system in minutes on the cloud. This Quick Start automatically sets up a SQL Server 2014
environment that receives its storage and enterprise-class data management capabilities from a NetApp ONTAP Cloud system running on AWS. The Quick Start uses NetAPP OnCommand Cloud Manager to deploy and configure ONTAP Cloud.

The Quick Start is for IT infrastructure architects, storage administrators, SQL DBAs, and DevOps professionals who are planning to deploy ONTAP Cloud with SQL Server 2014 on AWS. This guide provides links to automated AWS CloudFormation templates that you can launch directly into your AWS account. You can modify the templates to suit your specific business requirements, or use them as is.

For more in-depth information about OnCommand Cloud Manager and ONTAP Cloud, see the Cloud Manager and ONTAP Cloud documentation.

Costs and Licenses
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.

This Quick Start uses the AWS Marketplace offerings for NetApp products. To use this Quick Start, you will need to subscribe to the Amazon Machine Images (AMIs) for NetApp OnCommand Cloud Manager and NetApp ONTAP Cloud in the AWS Marketplace. Subscription instructions are provided in the Deployment Steps section.

The AWS CloudFormation template for this Quick Start includes configuration parameters that you can customize. Some of these settings, such as database size, will affect the cost of deployment. For cost estimates, see the pricing pages for each AWS service you will be using. Prices are subject to change.

Note that this Quick Start includes nested AWS CloudFormation templates that launch multiple stacks.

Architecture
Deploying this Quick Start for a new virtual private cloud (VPC) with default parameters builds the following NetApp ONTAP Cloud with SQL Server environment in the AWS Cloud.
This Quick Start will either set up the virtual network and create the networking resources needed for the deployment, or deploy the resources into a VPC and subnet of your choice. The Quick Start sets up the following:

- A VPC configured with one public subnet

**Note**  If you choose the option to create a new VPC, the Quick Start creates and configures the VPC and the public subnets for you. If you choose the option to deploy the Quick Start into an existing VPC, the Quick Start requires you to select an existing VPC and subnet.
• An AWS Identity and Access Management (IAM) role with fine-grained permissions for access to AWS services necessary for the deployment process

• Security groups for each instance or function to restrict access to only necessary protocols and ports

• A fully configured OnCommand Cloud Manager instance that deploys the ONTAP Cloud instance used in this Quick Start

• A Windows Server 2012 R2 RTM with SQL Server 2014 Standard instance connected to storage from the ONTAP Cloud instance

Prerequisites

Before you launch this Quick Start you’ll need to subscribe to the Amazon Machine Images (AMIs) for NetApp OnCommand Cloud Manager and NetApp ONTAP Cloud for AWS. To subscribe, follow the instructions in step 2.

If you are planning to launch this Quick Start into your own VPC, you’ll need to ensure that you use a subnet with an Internet gateway to allow limited, outbound public Internet access. OnCommand Cloud Manager automates the deployment of ONTAP Cloud and uses AWS APIs that require outbound public Internet connectivity. On AWS, this is facilitated via a public subnet with an attached Internet gateway.

Deployment Options

This Quick Start provides two deployment options:

• **Deploy ONTAP Cloud with SQL Server into a new VPC** (end-to-end deployment). This option builds a new AWS environment consisting of the VPC, public subnet, Internet gateway, security group, security ACLs, and other infrastructure components, and then deploys ONTAP Cloud with SQL Server into this new VPC.

• **Deploy ONTAP Cloud with SQL Server into an existing VPC.** This option provisions ONTAP Cloud with SQL Server in your existing AWS infrastructure.

The Quick Start also lets you customize additional settings, such as CIDR blocks and security credentials for ONTAP Cloud with SQL Server, as discussed later in this guide.
Deployment Steps

Step 1. Prepare Your 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.

   When you create an AWS account, you’ll gain access to all AWS services, including Amazon EC2, which you’ll use in the next step. You are charged only for the services that you use.

2. Use the region selector in the navigation bar to choose the AWS Region where you want to deploy ONTAP Cloud with SQL Server on AWS.

   **Note** This Quick Start is available in all commercial AWS Regions except for the China (Beijing) Region.

3. Create a key pair in your preferred region.

4. If necessary, request a service limit increase for the Amazon EC2 r4.xlarge instance type. You might need to do this 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.

Step 2. Subscribe to the AMIs for NetApp Software


2. Subscribe to the NetApp ONTAP Cloud AMI:
   a. Open the webpage for NetApp ONTAP Cloud.
   b. Choose Continue to view the license terms and launch information.
c. Select the **Manual Launch** tab, and then choose **Accept Software Terms**.

3. Subscribe to the NetApp OnCommand Cloud Manager AMI:
   a. Open the [webpage for NetApp OnCommand Cloud Manager](#).
b. Choose **Continue** to view the license terms and launch information.

![Image of OnCommand Cloud Manager in the AWS Marketplace](image1)

**Figure 4: OnCommand Cloud Manager in the AWS Marketplace**

(c) Select the **Manual Launch** tab, and then choose **Accept Software Terms**.

![Image of Launching the Cloud Manager AMI](image2)

**Figure 5: Subscribing to the Cloud Manager AMI**

There is no need to subscribe to the AMI for Windows Server 2012 R2 RTM with SQL Server 2014 Standard—the Quick Start template will automatically launch it for you.
Step 3. Launch the Quick Start

Note  You are responsible for the cost of subscribing to the NetApp ONTAP Cloud and OnCommand Cloud Manager AMIs. You are also responsible for the cost of 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. Prices are subject to change.

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

<table>
<thead>
<tr>
<th>Option 1</th>
<th>Option 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy ONTAP Cloud with SQL into a new VPC on AWS</td>
<td>Deploy ONTAP Cloud with SQL into an existing VPC on AWS</td>
</tr>
<tr>
<td><img src="Launch" alt="Launch" /></td>
<td><img src="Launch" alt="Launch" /></td>
</tr>
</tbody>
</table>

Important  If you’re deploying ONTAP Cloud into an existing VPC, make sure that your VPC has a public subnet with an attached Internet gateway. OnCommand Cloud Manager will be deployed into that subnet, and requires minimal outbound Internet connectivity in order to use the AWS APIs to deploy the ONTAP Cloud instance into your AWS account.

Each deployment takes about 45 minutes to complete.

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 for ONTAP Cloud with SQL Server will be built. The template is launched in the US West (Oregon) 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 by category and described separately for the two deployment options:

- Parameters for deploying ONTAP Cloud with SQL into a new VPC
- Parameters for deploying ONTAP Cloud with SQL into an existing VPC

- **Option 1: Parameters for deploying ONTAP Cloud with SQL into a new VPC**

  View template

**Network Configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC CIDR (VPCCIDR)</td>
<td>172.18.0.0</td>
<td>The CIDR block for the VPC that will be created. The Quick Start will automatically create the appropriate /22 subnet based on your VPC CIDR selection.</td>
</tr>
<tr>
<td>Remote Access CIDR (RemoteAccessCIDR)</td>
<td>Requires input</td>
<td>The CIDR IP range that is permitted to access ONTAP Cloud with SQL Server. We recommend that you set this value to a trusted IP range (for example, to restrict access to your corporate network). Note that the setting 0.0.0.0/0 will allow full public access to the software.</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>Key Name (KeyPair)</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>
</tbody>
</table>

**ONTAP Cloud General Configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name (CompanyName)</td>
<td>Requires input</td>
<td>The name of your company. This 4-35 character string should start with an alphabetic character and may contain only numbers, letters, or underscores (_).</td>
</tr>
<tr>
<td>Cloud Manager User Email (CloudManagerUserEmail)</td>
<td>Requires input</td>
<td>Your email address. This email address will be used as the user ID for logging in to OnCommand Cloud Manager after deployment.</td>
</tr>
<tr>
<td>Cloud Manager Password (CloudManagerPassword)</td>
<td>Requires input</td>
<td>The password (6-20 characters) you would like to use for OnCommand Cloud Manager. This password will also be used for the admin user on ONTAP Cloud.</td>
</tr>
</tbody>
</table>
Microsoft SQL Node Configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB Size (Capacity)</td>
<td>100</td>
<td>The size of the SQL Server database, in gibibytes (up to 2,000 GiB).</td>
</tr>
</tbody>
</table>

AWS Quick Start Configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick Start S3 Bucket Name (QSS3BucketName)</td>
<td>aws-quickstart</td>
<td>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.</td>
</tr>
<tr>
<td>Quick Start S3 Key Prefix (QSS3KeyPrefix)</td>
<td>quickstart-netapp-ontapcloud-sql/</td>
<td>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, but should not start or end with a forward slash (which is automatically added).</td>
</tr>
</tbody>
</table>

- **Option 2: Parameters for deploying ONTAP Cloud with SQL into an existing VPC**

View template

Network Configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC Id (VPCId)</td>
<td>Requires input</td>
<td>The ID of the target VPC in your preferred region where you would like to deploy the Quick Start (e.g., vpc-0343606c).</td>
</tr>
<tr>
<td>Subnet Id (SubnetId)</td>
<td>Requires input</td>
<td>The target subnet in your selected VPC where you would like to deploy the Quick Start (e.g., subnet-a0246dcd). This should be a public subnet with an attached Internet gateway.</td>
</tr>
<tr>
<td>Remote Access CIDR (RemoteAccessCIDR)</td>
<td>Requires input</td>
<td>The CIDR IP range that is permitted to access ONTAP Cloud with SQL Server. We recommend that you set this value to a trusted IP range (for example, to restrict access to your corporate network). Note that the setting 0.0.0.0/0 will allow full public access to the software.</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>Key Name (KeyPair)</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>
</tbody>
</table>

ONTAP Cloud General Configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique Resource Identifier (UniqueResourceId)</td>
<td>NetApp-ONTAP-Cloud</td>
<td>A unique identifier that will be used to identify the AWS resources deployed as part of this Quick Start. The default is the stack name used in the launch links provided in this guide.</td>
</tr>
<tr>
<td>Company Name (CompanyName)</td>
<td>Requires input</td>
<td>The name of your company. This 4-35 character string should start with an alphabetic character and may contain only numbers, letters, or underscores (_).</td>
</tr>
<tr>
<td>Cloud Manager User Email (CloudManagerUserEmail)</td>
<td>Requires input</td>
<td>Your email address. This email address will be used as the user ID for logging in to OnCommand Cloud Manager after deployment.</td>
</tr>
<tr>
<td>Cloud Manager Password (CloudManagerPassword)</td>
<td>Requires input</td>
<td>The password (6-20 characters) you would like to use for OnCommand Cloud Manager. This password will also be used for the admin user on ONTAP Cloud.</td>
</tr>
</tbody>
</table>

Microsoft SQL Node Configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB Size (Capacity)</td>
<td>100</td>
<td>The size of the SQL Server database, in gibibytes (up to 2,000 GiB).</td>
</tr>
</tbody>
</table>

AWS Quick Start Configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick Start S3 Bucket Name (QSS3BucketName)</td>
<td>aws-quickstart</td>
<td>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.</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>Quick Start S3 Key Prefix (QSS3KeyPrefix)</td>
<td>quickstart-netapp-ontapcloud-sql/</td>
<td>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, but should not start or end with a forward slash (which is automatically added).</td>
</tr>
</tbody>
</table>

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 ONTAP Cloud with SQL deployment is ready.

**Step 4. Access Your ONTAP Cloud with SQL Server Deployment**

Now that the ONTAP Cloud with SQL Server deployment is complete, you can access Windows Server or OnCommand Cloud Manager to manage your ONTAP Cloud system. To access the software, you can connect either to the SQL Server 2014 instance or to the OnCommand Cloud Manager instance. We’ve provided step-by-step instructions for both options.

**Connecting to the SQL Server 2014 Standard instance**

1. Make sure that you’re in the region where you launched the Quick Start, and open the Amazon EC2 console at [https://console.aws.amazon.com/ec2/](https://console.aws.amazon.com/ec2/).

2. Choose the SQL Server 2014 instance, and then choose **Connect**.
3. Follow the instructions in the AWS documentation to connect to the instance.

4. Connect to Windows Server with your preferred Remote Desktop application using the credentials from step 3.

5. In Windows Server, confirm that your data and log LUNs are available from Windows Explorer. You’ll see two NetApp LUNs attached to the Windows Server 2012 R2 with SQL Server 2014 instance. These are available for you to use for your database data and logs.

Figure 6: Connecting to the SQL Server instance

Figure 7: Confirming that NetApp storage is attached and usable on Windows Server
If you’d like to find out more about using SQL Server on NetApp enterprise-class storage, see Best Practices Guide for Microsoft SQL Server and SnapManager 7.1 for SQL Server with Clustered Data ONTAP in the NetApp documentation.

**Connecting to the OnCommand Cloud Manager instance**

You can also manage your NetApp ONTAP Cloud storage by using OnCommand Cloud Manager.

1. Make sure that you’re in the region where you launched the Quick Start, and open the Amazon EC2 console at [https://console.aws.amazon.com/ec2/](https://console.aws.amazon.com/ec2/).

2. Choose the Cloud Manager instance, and copy its public or private IP address from the Description section.

![Figure 8: Finding the IP addresses for OnCommand Cloud Manager](image)

3. Paste the IP address into a web browser window to open the OnCommand Cloud Manager login screen.

**Note** If you choose the private IP address, you’ll have to use it from a system that has access to the private AWS subnet (that is, from a jump host in that subnet).
4. Type in the email address and password you specified in the `CloudManagerUserEmail` and `CloudManagerPassword` parameters in step 3, and then choose **Log in**.

Once you’re logged in, you’ll see your ONTAP Cloud system.

![The OnCommand Cloud Manager login screen](image)

**Figure 9: The OnCommand Cloud Manager login screen**

![ONTAP Cloud in Cloud Manager](image)

**Figure 10: ONTAP Cloud in Cloud Manager**
5. To see the storage provided for the SQL Server database, double-click the ONTAP Cloud system to access the resources.

![ONTAP Cloud system](image)

**Figure 11: SQL Server database data and log storage volumes**

To find out more about how to manage your ONTAP Cloud system or to use OnCommand Cloud Manager, see the [OnCommand Cloud Manager Documentation Center](#).

### Cleaning Up

When you complete your work with ONTAP Cloud on AWS, you can clean up your account. The easiest method for cleaning up is to delete the AWS CloudFormation stacks that were generated as part of this Quick Start. However, the Quick Start provisions the ONTAP Cloud system with termination protection in place. This means that you should remove the ONTAP Cloud system first. You will then need to delete the other resources created by the Quick Start.

### Removing the ONTAP Cloud System

To remove the ONTAP Cloud system, you can use either Cloud Manager or the Amazon EC2 console. We’ve provided step-by-step instructions for both methods.

**Using Cloud Manager**

1. In Cloud Manager, double-click the ONTAP Cloud system to access the resources.
2. From the three-bar icon in the upper-right corner of the screen, choose the option to delete the ONTAP Cloud system.
3. In the confirmation screen, type the name of your ONTAP Cloud system, and then choose **Delete**.

You’ll receive a message that the ONTAP Cloud system is being deleted in Cloud Manager.
Using the Amazon EC2 Console

If you’d rather use the Amazon EC2 console to remove the ONTAP Cloud system, follow these steps:

1. Make sure that you’re in the region where you launched the Quick Start, and open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.

2. Open the context (right-click) menu for your ONTAP Cloud instance, and then chooseInstance Settings, Change Termination Protection.

3. In the confirmation dialog box, choose Yes, Disable to disable termination protection.
4. Open the context (right-click) menu for your ONTAP Cloud instance again, and then choose **Instance State, Terminate**.

You’ll see the ONTAP Cloud instance being shut down before it is deleted.

**Removing the Quick Start CloudFormation Stacks**

To remove the remaining resources created as part of this Quick Start, follow these steps:

1. Make sure that you’re in the region where you launched the Quick Start, and open the AWS CloudFormation console at [https://console.aws.amazon.com/cloudformation/](https://console.aws.amazon.com/cloudformation/).
Your console should look something like Figure 17 if you launched the stack in a new VPC.

![AWS CloudFormation console](image)

**Figure 17: AWS CloudFormation console**

2. You’ll have to delete the stacks in reverse order of deployment. To start, open the context (right-click) menu for the SQL stack, and then choose **Delete Stack**.

![Delete Stack](image)

**Figure 18: Deleting the SQL stack**

3. In the confirmation dialog box, choose **Yes, Delete**.

You’ll see that the stack is being deleted in the AWS CloudFormation console.
4. Perform the same steps to delete the two OTC stacks.

Figure 20: Deleting the OTC stacks

The stack deletions should only take a few minutes. When the stacks are deleted, they will be removed from the console.

5. Remove the main AWS CloudFormation stack (in this example, netapp).
Figure 21: Deleting the netapp stack

This will remove the main netapp stack as well as the netapp-NetApp and netapp-VPC substacks.

6. You can also delete the security group (SG) stack at any time. This stack was created by Cloud Manager for use with the ONTAP Cloud system we’ve already removed.

If you haven’t launched any other AWS CloudFormation templates, you should no longer see any active stacks once you have performed these steps.

Troubleshooting

If you run into any problems deploying this Quick Start, review the following FAQ for troubleshooting tips and guidance.

Q. How can I see the deployment progress for the Quick Start?

A. In the lower section of the AWS CloudFormation console, choose the Events tab and select your stack in the upper section. You will see all the events taking place for your stack. You can also choose substacks and see their events as well.
Q. I launched the Quick Start template and I see additional templates being launched in the AWS CloudFormation console. Why?

A. The master template for launching the Quick Start creates additional stacks to launch different components and resources. You will see separate stacks for Cloud Manager, ONTAP Cloud, a security group, and SQL Server. You will also see a stack for a new VPC if you chose the template to deploy the Quick Start into a new VPC.

Q. I received a CREATE_FAILED message but not all the stacks have been rolled back. Will I incur AWS charges?

A. Some of the stacks will require a manual deletion in case of a failure. You can manually delete the stack from the AWS CloudFormation console by following the instructions in the Cleaning Up section. Before deleting stacks, make sure to disable termination protection in the Amazon EC2 console for the servers created by this Quick Start.

Q. I am unable to launch the Quick Start, I am receiving a CREATE_FAILED message in the AWS CloudFormation console.

A. Here are some troubleshooting tips:
• Verify that you’ve prepared your AWS account as explained in step 1 of the deployment instructions, and that you’ve subscribed to the ONTAP Cloud and OnCommand Cloud Manager AMIs, as explained in step 2.

• Verify that you’ve accepted the default values for the QSS3BucketName and QSS3KeyPrefix parameters (unless you’ve copied the Quick Start assets into your own S3 bucket for customization purposes).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>QSS3KeyPrefix</td>
<td>aws-quickstart</td>
</tr>
<tr>
<td>QSS3KeyPrefix</td>
<td>quickstart-netapp-ontapcloud-sql/</td>
</tr>
</tbody>
</table>

• 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 C:\cfn\log.)

**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.

For additional information, see Troubleshooting AWS CloudFormation on the AWS website.

**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 or from a non-S3 location, you might encounter template size limitations when you create the stack. For more information about AWS CloudFormation limits, see the AWS documentation.

**Security**

The AWS Cloud provides a scalable, highly reliable platform that helps customers deploy applications and data quickly and securely. When you build systems on the AWS infrastructure, security responsibilities are shared between you and AWS. This shared model can reduce your operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical
security of the facilities in which the services operate. In turn, you assume responsibility and management of the guest operating system (including updates and security patches), other associated applications, as well as the configuration of the AWS-provided security group firewall. For more information about security on AWS, visit the AWS Security Center.

We highly recommend that you update the passwords for the administrator and database administrator accounts in accordance with your IT standards after you deploy the Quick Start.

**AWS Identity and Access Management (IAM)**

This solution leverages an IAM role with least privileged access while allowing access to the various functions needed by ONTAP Cloud. We recommend that you review the IAM role to further restrict access as needed once the deployment is up and running. We do not require or recommend storing SSH keys, secret keys, or access keys on the provisioned instances.

**IAM Policy**

<table>
<thead>
<tr>
<th>Description</th>
<th>Actions</th>
</tr>
</thead>
</table>
| Cloud Manager automating EC2 instance actions | "ec2:DescribeInstances"  
"ec2:DescribeInstanceStatus"  
"ec2:RunInstances"  
"ec2:ModifyInstanceAttribute"  
"ec2:DescribeRouteTables"  
"ec2:DescribeImages" |
| Cloud Manager automating tag creation | "ec2:CreateTags" |
| Cloud Manager automating EBS volume actions | "ec2:CreateVolume"  
"ec2:DescribeVolumes"  
"ec2:ModifyVolumeAttribute"  
"ec2:DeleteVolume" |
| Cloud Manager automating security group actions | "ec2:CreateSecurityGroup"  
"ec2:DeleteSecurityGroup"  
"ec2:DescribeSecurityGroups" |
| Cloud manager automating data ingress/egress rules | "ec2:RevokeSecurityGroupEgress"  
"ec2:AuthorizeSecurityGroupEgress"  
"ec2:AuthorizeSecurityGroupIngress" |
| Cloud Manager automating ENI actions | "ec2:CreateNetworkInterface"  
"ec2:DescribeNetworkInterfaces"  
"ec2:DeleteNetworkInterface"  
"ec2:ModifyNetworkInterfaceAttribute" |
<table>
<thead>
<tr>
<th>Description</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Manager describing VPC/subnet information</td>
<td>&quot;ec2:DescribeSubnets&quot; &lt;br&gt; &quot;ec2:DescribeVpcs&quot; &lt;br&gt; &quot;ec2:DescribeDhcpOptions&quot;</td>
</tr>
<tr>
<td>Cloud Manager creating/describing/deleting EBS snapshots</td>
<td>&quot;ec2:CreateSnapshot&quot; &lt;br&gt; &quot;ec2:DeleteSnapshot&quot; &lt;br&gt; &quot;ec2:DescribeSnapshots&quot;</td>
</tr>
<tr>
<td>Cloud Manager listing console output (to display error messages in Cloud Manager)</td>
<td>&quot;ec2:GetConsoleOutput&quot;</td>
</tr>
<tr>
<td>Describe key pair files and AWS Regions</td>
<td>&quot;ec2:DescribeKeyPairs&quot; &lt;br&gt; &quot;ec2:DescribeRegions&quot;</td>
</tr>
<tr>
<td>Describe and delete tags</td>
<td>&quot;ec2:DeleteTags&quot; &lt;br&gt; &quot;ec2:DescribeTags&quot;</td>
</tr>
<tr>
<td>Cloud Manager uses AWS CloudFormation to create the ONTAP Cloud systems</td>
<td>&quot;cloudformation:CreateStack&quot; &lt;br&gt; &quot;cloudformation:DeleteStack&quot; &lt;br&gt; &quot;cloudformation:DescribeStacks&quot; &lt;br&gt; &quot;cloudformation:DescribeStackEvents&quot; &lt;br&gt; &quot;cloudformation:ValidateTemplate&quot;</td>
</tr>
<tr>
<td>Ability to create an IAM role a custom policy (this whole policy) instead of supplying an AWS access key and secret key</td>
<td>&quot;iam:PassRole&quot; &lt;br&gt; &quot;iam:CreateRole&quot; &lt;br&gt; &quot;iam:DeleteRole&quot; &lt;br&gt; &quot;iam:PutRolePolicy&quot; &lt;br&gt; &quot;iam:CreateInstanceProfile&quot; &lt;br&gt; &quot;iam:DeleteRolePolicy&quot; &lt;br&gt; &quot;iam:AddRoleToInstanceProfile&quot; &lt;br&gt; &quot;iam:RemoveRoleFromInstanceProfile&quot; &lt;br&gt; &quot;iam:DeleteInstanceProfile&quot;</td>
</tr>
<tr>
<td>Cloud Manager enables users to specify their own KMS or leverage the AWS Key Management Service (AWS KMS)</td>
<td>&quot;kms:List*&quot; &lt;br&gt; &quot;kms:Describe*&quot;</td>
</tr>
</tbody>
</table>

**Operating System Security**

The root user on ONTAP Cloud and Cloud Manager can be accessed only by using the SSH key specified during the deployment process. AWS doesn’t store these SSH keys, so if you lose your SSH key you can lose access to these instances.

Operating system patches are your responsibility and should be performed on a periodic basis.
Security Groups

A security group acts as a firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time. The new rules are automatically applied to all instances that are associated with the security group.

The security groups created and assigned to the individual instances as part of this solution are restricted as much as possible while allowing access to the various functions needed by ONTAP Cloud and SQL Server. We recommend that you review security groups to further restrict access as needed once the deployment is up and running.

This Quick Start creates two security groups: **OCCMSecurityGroup** and **SQLServerSecurityGroup**. After the Quick Start deployment, you are responsible for maintaining these security groups and including or excluding rules.

### OCCMSecurityGroup

<table>
<thead>
<tr>
<th>Direction</th>
<th>Source or destination</th>
<th>Protocol/port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>Requires input</td>
<td>22</td>
<td>SSH</td>
</tr>
<tr>
<td>Inbound</td>
<td>Requires input</td>
<td>80</td>
<td>HTTP</td>
</tr>
<tr>
<td>Inbound</td>
<td>Requires input</td>
<td>443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Outbound</td>
<td>0.0.0.0/0</td>
<td>All</td>
<td>Allows all outbound traffic</td>
</tr>
</tbody>
</table>

### SQLServerSecurityGroup

<table>
<thead>
<tr>
<th>Direction</th>
<th>Source or destination</th>
<th>Protocol/port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>Requires input</td>
<td>80</td>
<td>HTTP</td>
</tr>
<tr>
<td>Inbound</td>
<td>Requires input</td>
<td>3389</td>
<td>RDP</td>
</tr>
</tbody>
</table>

### Additional Resources

**AWS services**

- AWS CloudFormation  
  [https://aws.amazon.com/documentation/cloudformation/](https://aws.amazon.com/documentation/cloudformation/)

- Amazon EC2  
• Amazon IAM
  https://aws.amazon.com/documentation/iam/
• Amazon VPC
  https://aws.amazon.com/documentation/vpc/

**NetApp**

• ONTAP Cloud
  https://cloud.netapp.com/cloud-ontap
• OnCommand Cloud Manager and ONTAP Cloud Documentation Center
• ONTAP Cloud and Cloud Manager videos
• Best Practices Guide for Microsoft SQL Server and SnapManager 7.1 for SQL Server with Clustered Data ONTAP

**Quick Start reference deployments**

• AWS Quick Start home page
  https://aws.amazon.com/quickstart/

**GitHub Repository**

You can visit our GitHub repository to download the templates and scripts for this Quick Start, to post your feedback, and to share your customizations with others.

**Document Revisions**

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>In sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 2017</td>
<td>Initial publication</td>
<td>—</td>
</tr>
</tbody>
</table>