Technical Report

Networking Configurations for NetApp Cloud ONTAP for Amazon Web Services

Kris Lippe, NetApp

January 2015 | TR-4352

TABLE OF CONTENTS

1 Introduction ... 4

1.1 Glossary of Terms ... 4

1.2 Overview ... 5

1.3 Scope ... 5

1.4 Assumptions ... 6

1.5 Target Audience ... 6

2 Before You Begin ... 6

2.1 Account Service Limits ... 6

2.2 Identity and Access Management Roles ... 6

2.3 Virtual Private Cloud Checklist ... 6

3 OnCommand Cloud Manager Setup ... 7

3.1 Proxy Server Configuration with Cloud Manager ... 8

4 Virtual Private Cloud Configurations ... 10

4.1 Private Virtual Private Cloud with Virtual Private Network (Hybrid Cloud Reference Architecture) ... 10

4.2 Public and Private Virtual Private Cloud and an Optional HTTP Proxy ... 12

4.3 Public and Private Virtual Private Cloud with Virtual Private Network ... 15

4.4 Public Virtual Private Cloud ... 17

5 Cloud ONTAP Security Group Rules ... 22

6 Cloud ONTAP Proxy Configuration ... 23

6.1 Verify Proxy Server ... 25

7 Connectivity Verification Testing ... 26

7.1 Cloud ONTAP AutoSupport Verification ... 26

7.2 Verify Cloud Manager AutoSupport Connectivity ... 27

References ... 29

Version History ... 29

LIST OF TABLES

Table 1) AWS networking requirements for Cloud Manager. ... 7

Table 2) AWS networking requirements for Cloud ONTAP. ... 8

Table 3) NAT security group inbound recommendations. ... 14

Table 4) NAT security group outbound recommendations. ... 15

Table 5) Inbound security group rules for Cloud ONTAP. ... 22

Table 6) Outbound security group rules for Cloud ONTAP. ... 23

LIST OF FIGURES

Figure 1) VPC with only a private subnet and hardware VPN access (graphic supplied by AWS). 11

Figure 2) VPC with public and private subnets (graphic supplied by AWS)...12

Figure 3) VPC with public and private subnets and hardware VPN access (graphic supplied by AWS). 16

Figure 4) VPC with a public subnet only (graphic supplied by AWS). 17

Figure 5) Assign a public IP address automatically. 18

1 Introduction

This document describes the configuration choices available when building a virtual private cloud (VPC) in the Amazon Web Services (AWS) cloud operating environment and the effect these choices have on the deployment and configuration of NetApp® Cloud ONTAP® systems.

1.1 Glossary of Terms

This section defines the terms used to describe the technical aspects of AWS described in this document.

Amazon region. An Amazon region is a pool of AWS cloud resources tied to a geographic site. Each Amazon region consists of multiple availability zones.

Amazon security group. An Amazon security group is the firewall for data ingress and egress for your Amazon Elastic Compute Cloud (EC2) instances. The rules of a security group control the inbound traffic attempting to reach associated instances and the outbound traffic leaving them. By default, security groups allow all outbound traffic.

Amazon Machine Image (AMI). An AMI is a virtual machine image in Amazon EC2, and EC2 virtual machines are deployed from AMIs. AMIs can be purchased from the AWS Marketplace, or customers can build their own.

Amazon Web Services (AWS). AWS is the public cloud platform offered by Amazon.com that includes services such as Amazon EC2.

Availability zone. Availability zones are distinct locations within an Amazon region that are engineered to be isolated from failures in other availability zones and provide inexpensive, low-latency network connectivity to other availability zones within the same region.

Elastic IP addresses (EIP). EIPs are static IP addresses that a customer may allocate and assign to instances that reside in EC2. EIPs are associated with an AWS account, not an instance, and can therefore be remapped at will.

Elastic Compute Cloud. EC2 provides computing resources through virtual machine (VM) operating systems (OSs) for the AWS cloud. VMs can run either Microsoft® Windows® or Linux® OSs.

Identity and Access Management (IAM). IAM allows customers to securely control access to AWS services and resources. Through IAM, an administrator creates user and group accounts and delegates rights and privileges by managing roles and assigning permissions.

Internet Gateway (IGW). IGW is a gateway (router) that forwards packets to and receives packets from the Internet.

Network address translation (NAT). NAT maps a network from one IP space into another by modifying network address information in IP packets that transmit across a network gateway. A NAT instance can be deployed into a VPC public subnet to allow instances in a private subnet to send outbound Internet traffic and prevent them from receiving inbound traffic.

Proxy. A proxy server can be configured within a VPC to allow network connectivity when no direct route is available. This can be used to provide access to specific web services (for example, HTTP and HTTPS) to systems that do not have Internet access.

Virtual private cloud. A VPC is an isolated, private (RFC 1918) IP address range (`10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16`) that can be connected to other VPCs, the Internet, or other networks through an AWS Direct Connect network connection.

Virtual private network (VPN). A VPN provides administrators with a secure mechanism for connecting to a private network over the Internet. In the context of AWS, a VPN is an IP Security (IPSec)–enabled network tunnel configured from a corporate data center to the AWS public cloud, allowing customers to securely access cloud resources from on-premise infrastructure. IPSec secures network communication by authenticating and encrypting IP packets.

1.2 Overview

Cloud ONTAP

NetApp Cloud ONTAP for AWS is a software-only storage appliance that runs the NetApp clustered Data ONTAP® storage OS in the cloud. Cloud ONTAP manages general-purpose Amazon Elastic Block Storage (GP2 EBS) with clustered Data ONTAP and provides enterprise-class features on top of EBS. This gives the customer access to NFS, CIFS, and iSCSI protocol support as well as to a rich feature set that enhances the management and efficiency of your storage. Customers also have access to industry-leading technologies like NetApp SnapMirror® and NetApp SnapVault® data replication, which enable seamless connectivity for hybrid cloud resources.

Cloud ONTAP is launched and managed using the NetApp OnCommand® Cloud Manager application. Cloud Manager is a web front end that enables the deployment and management of AWS public cloud resources associated with Cloud ONTAP. Cloud Manager provides a flexible, intuitive interface for activities such as deploying Cloud ONTAP working environments, intelligent allocation of additional AWS EBS storage, creation of NetApp flexible volumes, and so on.

Cloud Manager can be deployed several different ways, including:

- Into your local data center from the NetApp Support Software downloads site
- Into an existing EC2 instance running a supported version of Windows
- From the AWS Marketplace from an AMI into an EC2 instance

Refer to the OnCommand Cloud Manager Installation and Setup Guide and the OnCommand Cloud Manager User Guide for more information.

Amazon Web Services Virtual Private Cloud

Amazon Web Services allows customers to create logically isolated areas called VPCs within an EC2 environment. A VPC gives customers a secure container for the deployment and management of EC2 resources. When connected by an IPsec-based VPN, a VPC acts as an extension to a local data center, with security controls handled at several access points. Cloud ONTAP must be deployed within an AWS VPC and subnet. Deployments into AWS EC2 Classic are not supported.

Refer to the AWS Virtual Private Cloud documentation website for more information.

1.3 Scope

Amazon provides a series of guidelines concerning the deployment and configuration of VPCs. Reference configurations are documented online (with links provided in this document) that explain the various options available for AWS network isolation. This document discusses these various configurations and their effect on Cloud ONTAP network connectivity in terms of outbound Internet communication to the AWS application programming interfaces. This document also covers direct communication between the Cloud Manager and Cloud ONTAP systems and the NetApp AutoSupport™ feature in the Data ONTAP OS.

The following key topics are covered in this document:

- AWS IAM user and group prerequisites
- Identification of VPC configuration choices
- Deployment and configuration of Cloud ONTAP and Cloud Manager
- Cloud ONTAP network connectivity verification procedures

1.4 Assumptions

AWS is a large and complex array of heavily interconnected services. This document does not attempt to provide the context or background information necessary to familiarize a new user with AWS. Amazon provides extensive online documentation that thoroughly explains every aspect of its cloud offering. In an effort to keep this document as brief and focused as possible, we direct you to the applicable AWS documentation whenever possible.

1.5 Target Audience

This document is intended for intermediate-level cloud administrators who want to deploy Cloud ONTAP in a hybrid cloud environment. Such administrators should have:

- Some level of experience with NetApp systems
- A reasonable understanding of the various services in the AWS operating environment
- Familiarity with the AWS management console and terminology
- A basic understanding of clustered Data ONTAP and its feature set
- Network connectivity to the AWS cloud and the necessary routes required for hybrid cloud connectivity

2 Before You Begin

2.1 Account Service Limits

Amazon imposes service limits on AWS accounts as a safety precaution designed to minimize the financial consequences resulting from an unintentional deployment of cloud resources. Although these limits can be raised at the request of a customer, they are set low by design and, in certain situations, can affect the ability of Cloud ONTAP to purchase or provision necessary resources.

Verify that your account service limits are set correctly before deploying Cloud Manager and Cloud ONTAP. For more information, refer to the AWS Service Limits site.

2.2 Identity and Access Management Roles

In the AWS cloud environment, IAM controls allow the customer to create user and group policies that allow or deny access to AWS resources. These controls can be thought of as subaccounts or subgroups under the main account that grant or revoke access as needed without impacting the main account. To create a VPC, certain security privileges must be made available to the requesting user account. Assigning responsibility for granting and verifying these privileges is outside the scope of this document. This document assumes that the customer has a broader corporate strategy to govern access to cloud resources.

Refer to the OnCommand Cloud Manager Installation and Setup Guide for a detailed explanation of the IAM policies governing the deployment and management of Cloud ONTAP.

2.3 Virtual Private Cloud Checklist

Before attempting to deploy Cloud ONTAP into one of the VPC configurations listed in this document, verify that you have:

- An existing AWS account with a password and access credentials
- An Internet-connected computer with a web browser
- A VPC with an assigned AWS region and availability zones
- An existing AWS VPC and subnet for deploying Cloud ONTAP

- Network connectivity to the AWS VPC from the local data center

For more information on building and configuring VPCs, refer to the AWS VPC Portal and the AWS VPC FAQ.

3 OnCommand Cloud Manager Setup

OnCommand Cloud Manager can be deployed:

- As a standalone application running within the customer's data center
- As an AMI running in an AWS VPC

The OnCommand Cloud Manager Installation and Setup Guide provides a detailed description of the AWS networking requirements for Cloud Manager. Refer to this guide before attempting to install and configure Cloud Manager.

Network Requirements

Both Cloud Manager and Cloud ONTAP have network configuration prerequisites that must be met before attempting to install either product. These prerequisites are described in Table 1and Table 2, respectively.

Table 1) AWS networking requirements for Cloud Manager.

Requirement	Description
Internet access to AWS services	Cloud Manager requires Internet access to communicate with AWS services, launch and manage Cloud ONTAP instances, and configure a NetApp private storage connection. An Internet connection is also required to send AutoSupport messages to NetApp technical support. If you deploy Cloud Manager in your data center, you must set up a VPN connection to the VPC. If you deploy Cloud Manager in AWS, you must enable Internet access from your VPC through an Internet gateway, NAT instance, or proxy server.
A route to the subnets where Cloud ONTAP is deployed	Cloud Manager requires a connection to the subnets where Cloud ONTAP instances have been launched. If you deploy Cloud Manager in your data center, a VPN connection provides a route to the subnets in a VPC. If you deploy Cloud Manager in AWS, subnets are routed together by default. However, if you changed the routing tables, you must either reroute the subnets or make sure that users do not use nonroutable subnets for Cloud ONTAP instances.
A security group with the required rules	When you launch Cloud Manager in AWS, the AWS Marketplace page provides an option to create a security group that includes the required inbound and outbound rules. It is best to use that predefined security group, but if you must use your own, then it must include the required inbound and outbound rules.

Requirement	Description
Access to the Cloud Manager web console	Users must access Cloud Manager from a web browser. If you deploy Cloud Manager in AWS, the easiest way to provide access is by launching Cloud Manager in a public subnet with a public IP address. However, if you must use a private IP address instead, users can access the console through any of the following: • A jump host in the VPC that has a connection to Cloud Manager • A host in your data center that has a VPN connection to the private IP address • A remote desktop connection to the Cloud Manager host

Table 2) AWS networking requirements for Cloud ONTAP.

Requirement	Description
Internet access to send AutoSupport messages	Cloud ONTAP requires outbound Internet access to communicate with NetApp AutoSupport, a troubleshooting tool that proactively monitors the health of your system and automatically sends messages to NetApp technical support. You can use a NAT instance, VPN, or proxy server (in your data center or in AWS) to enable outbound traffic to AutoSupport. For a NAT instance, you must define an inbound security group rule that allows HTTPS traffic from the private subnet to the Internet.
A security group with the required rules	When you launch a Cloud ONTAP instance from Cloud Manager, you can select a predefined security group that includes the required rules. It is best to use that predefined security group, but if you must use your own, then it must include the required inbound and outbound rules.
DNS and Active Directory for CIFS	If you want to provision CIFS storage, you must set up DNS and Active Directory® in AWS or extend your on-premises setup to AWS. The DNS server must provide name resolution services for the Active Directory environment. You can configure DHCP option sets to use the default EC2 DNS server, which must not be the DNS server used by the Active Directory environment.

3.1 Proxy Server Configuration with Cloud Manager

Some of the VPC configurations refer to the optional use of a proxy server to provide Internet connectivity to AWS instances. In environments without direct Internet connectivity, it is important to provide Internet access to both Cloud Manager and Cloud ONTAP for the following reasons:

- Cloud Manager must have access to an AWS application programming interface (API) endpoint, which is only available through Internet-facing IP addresses.
- Both Cloud ONTAP and Cloud Manager can be configured to send AutoSupport messages, which must be sent to the Internet-facing NetApp support address.

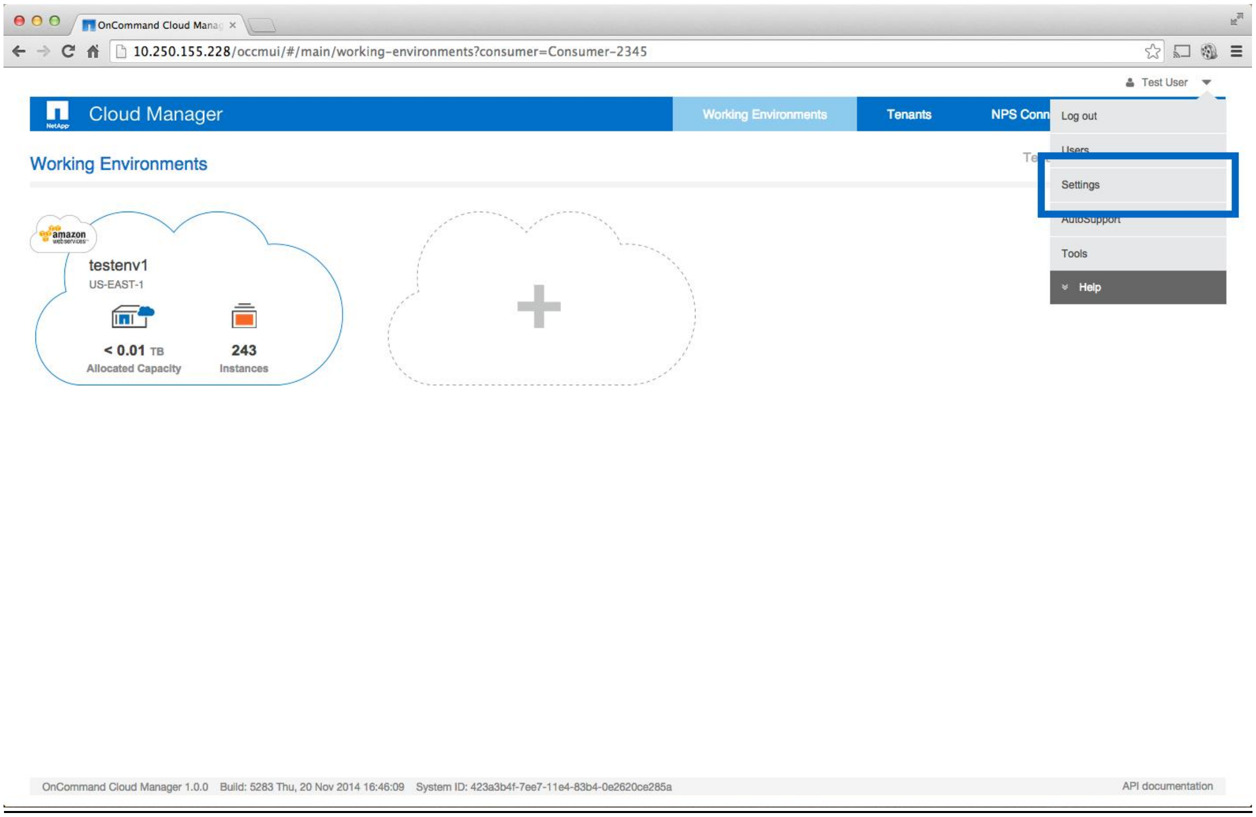
Proxy server configuration performed through Cloud Manager is passed to any Cloud ONTAP instances that are subsequently deployed. Therefore, if you intend to use a proxy server, it is important to configure it in Cloud Manager before deploying any Cloud ONTAP working environments. However, if a proxy server is added to your environment after Cloud ONTAP has been deployed, the server can be configured directly in Data ONTAP through the System Manager interface.

Additional information on the configuration of proxy servers is available in the OnCommand Cloud Manager Installation and Setup Guide.

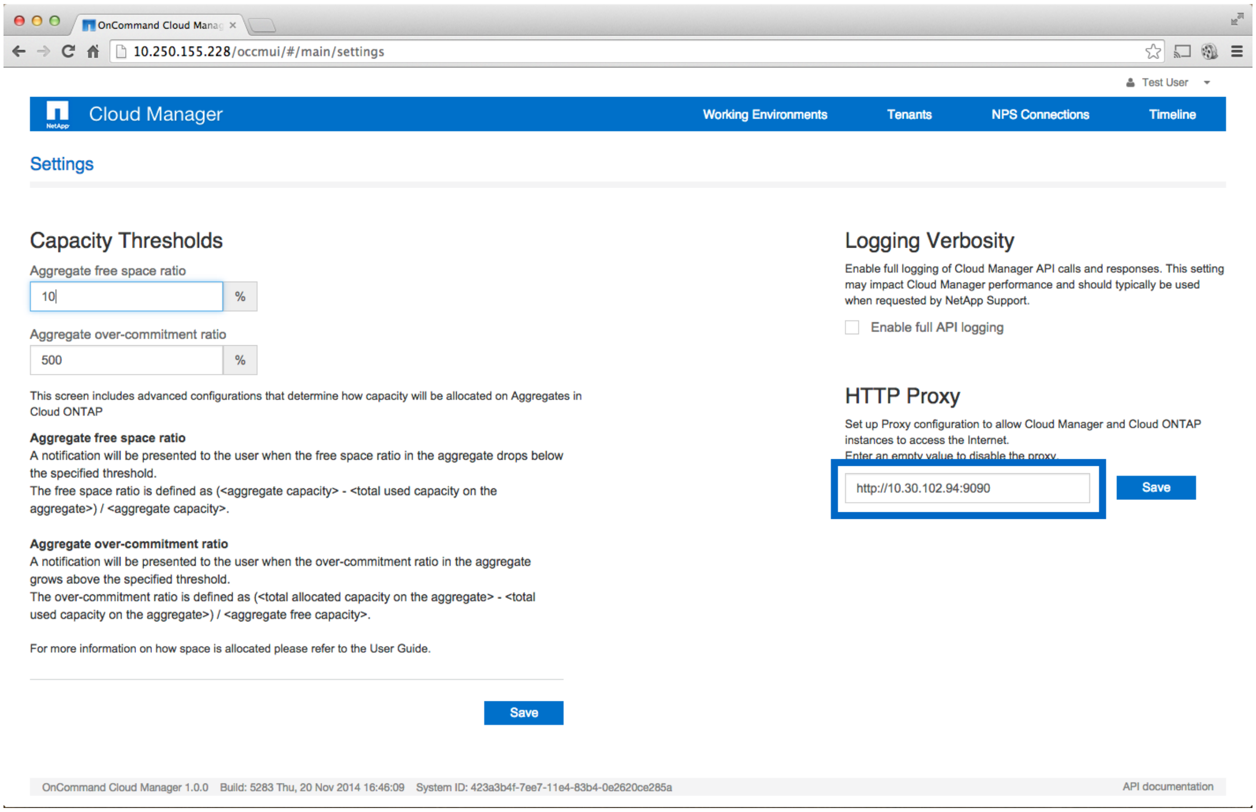
Configure a Proxy Server

To configure a proxy server within Cloud Manager, complete the following steps:

1. Start Cloud Manager by pointing a supported web browser at the applicable URL and login using the necessary credentials.
2. Click the arrow in the upper-right-hand corner of the browser and select Settings.



3. Enter the URL for the HTTP proxy in the appropriate text box and click Save.



Settings

Capacity Thresholds

Aggregate free space ratio: 10 %

Aggregate over-commitment ratio: 500 %

This screen includes advanced configurations that determine how capacity will be allocated on Aggregates in Cloud ONTAP

Aggregate free space ratio
A notification will be presented to the user when the free space ratio in the aggregate drops below the specified threshold.
The free space ratio is defined as (<aggregate capacity> - <total used capacity on the aggregate>) / <aggregate capacity>.

Aggregate over-commitment ratio
A notification will be presented to the user when the over-commitment ratio in the aggregate grows above the specified threshold.
The over-commitment ratio is defined as (<total allocated capacity on the aggregate> - <total used capacity on the aggregate>) / <aggregate free capacity>.

For more information on how space is allocated please refer to the User Guide.

Save

Logging Verbosity

Enable full logging of Cloud Manager API calls and responses. This setting may impact Cloud Manager performance and should typically be used when requested by NetApp Support.

□ Enable full API logging

HTTP Proxy

Set up Proxy configuration to allow Cloud Manager and Cloud ONTAP instances to access the Internet.
Enter an empty value to disable the proxy.

http://10.30.102.94:9090

Save

OnCommand Cloud Manager 1.0.0 Build: 5283 Thu, 20 Nov 2014 16:46:09 System ID: 423a3b4f-7ee7-11e4-83b4-0e2620ce285a

API documentation

4. Cloud Manager now routes all Internet requests through the defined proxy server.

4 Virtual Private Cloud Configurations

This section describes various possible VPC configurations in a customer environment and their impact on network connectivity from the perspective of Cloud ONTAP and Cloud Manager.

4.1 Private Virtual Private Cloud with Virtual Private Network (Hybrid Cloud Reference Architecture)

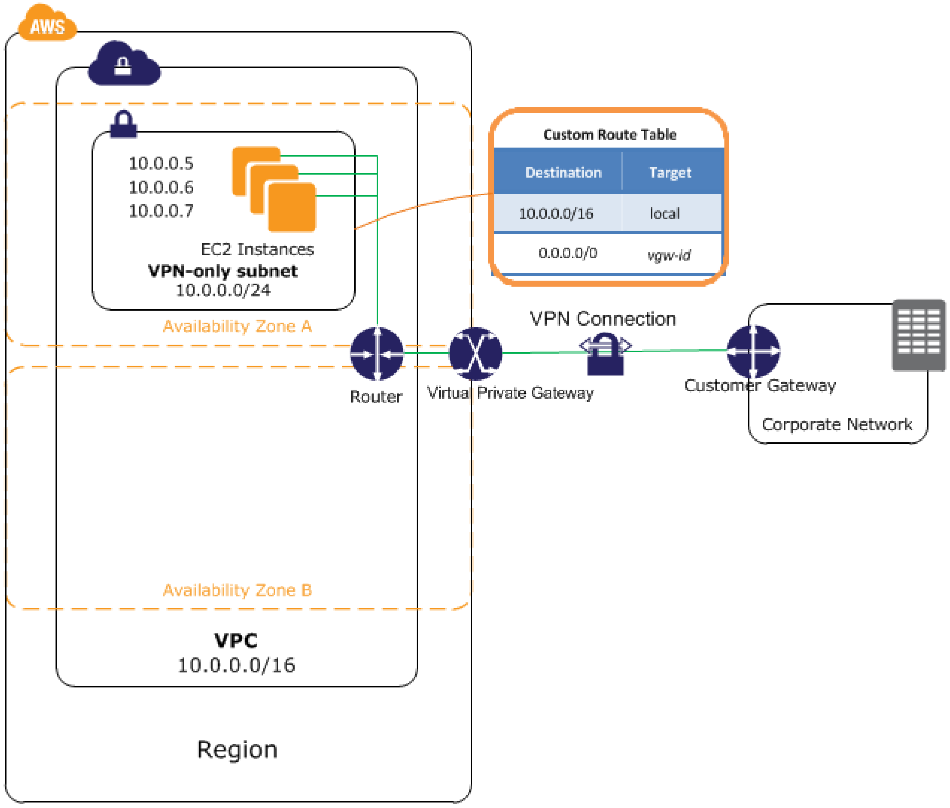
This section describes the hybrid cloud reference configuration, a deployment configuration recommended by AWS with support available through the VPC creation wizard.

In this configuration, the customer chooses to deploy a Cloud ONTAP instance into a VPC with a single private subnet with network connectivity back to a local data center enabled through an IPsec-supported VPN tunnel. There is no Internet gateway configured, and the customer has followed AWS documentation to enable routing across the VPN tunnel and to allow EC2 instances to access the Internet through their on-premises network and firewalls.

This configuration can also contain an HTTP proxy configured to provide AWS instances with Internet connectivity. Refer to the section “Proxy Server Configuration with Cloud Manager” for detailed instructions on how to configure a proxy server for Cloud ONTAP and Cloud Manager. Figure 1 depicts the organization of this configuration.

Additional information on the configuration of VPN connections can be found in the AWS Virtual Private Gateway documentation.

Figure 1) VPC with only a private subnet and hardware VPN access (graphic supplied by AWS).



Deploying Cloud Manager

Cloud Manager can be deployed into either the local data center or the AWS cloud.

If Cloud Manager is deployed into the local data center, verify that the network connectivity requirements described in the section “OnCommand Cloud Manager Setup” are met. This may require the modification of corporate firewall policies to allow traffic to pass to the necessary endpoints.

If Cloud Manager is deployed into a VPC, an AWS EIP is not required because connectivity is governed by AWS instance security-group policies and ingress corporate firewall settings. Cloud Manager makes AWS API calls, which, in this scenario, are routed to the necessary Internet endpoint over the VPN connection.

Deploy Cloud ONTAP

To deploy and configure Cloud ONTAP into this environment, complete the following steps:

1. Identify the desired target AWS region, VPC, and subnet for Cloud ONTAP.

   Note: Verify that Cloud Manager has network connectivity to the designated subnet.

2. If a proxy server is part of this configuration, refer to the section “Proxy Server Configuration with Cloud Manager” to verify that Cloud Manager is configured correctly prior to deploying Cloud ONTAP.
3. After Cloud Manager has been properly configured, follow the OnCommand Cloud Manager 1.0 Installation and Setup Guide to deploy Cloud ONTAP using Cloud Manager.
4. Because outbound Internet routing is handled through a local data center gateway, both Cloud ONTAP and Cloud Manager should be able to transmit AutoSupport messages without any additional

configuration, provided that corporate routing and firewall policies have been modified to allow AWS HTTP and HTTPS traffic to pass through unrestricted.

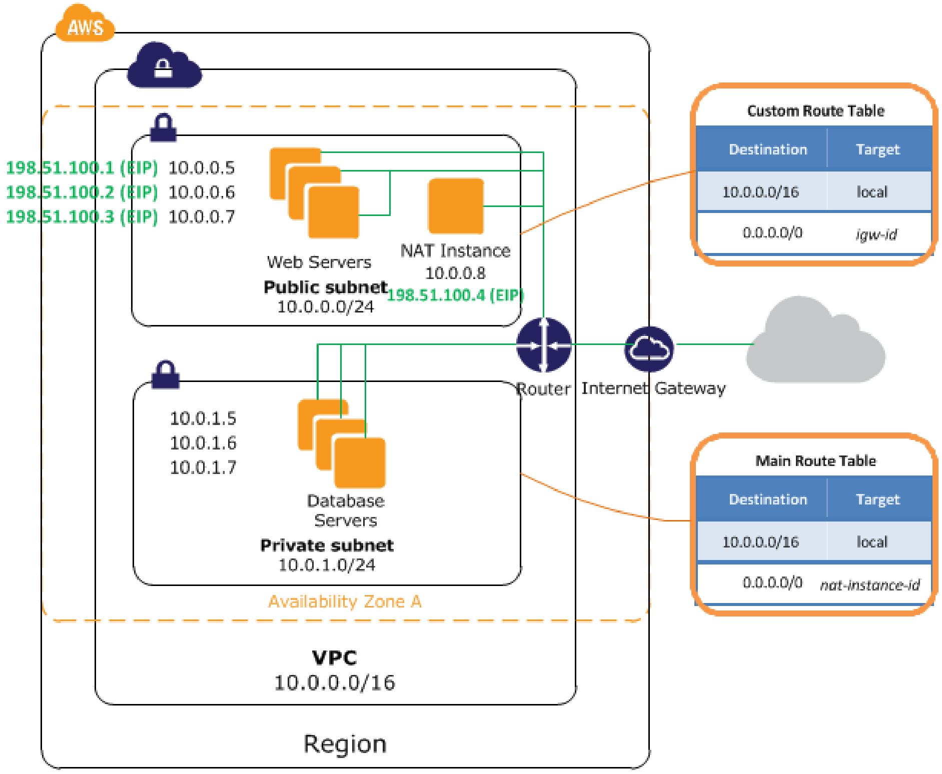
Note: AutoSupport traffic is sent to support.netapp.com, which both Cloud ONTAP and Cloud Manager can access through configured routes over the VPN connection.

4.2 Public and Private Virtual Private Cloud and an Optional HTTP Proxy

This scenario uses two subnets to logically isolate systems that require inbound connectivity (those configured on the public subnet) from those that only provide back-end services (those configured on the private subnet). In this configuration, a NAT instance is provisioned in the public subnet and allows outgoing and select incoming Internet traffic to systems that reside in the private subnet. An IGW is configured to provide systems in the public subnet and the private subnet through the NAT instance, with Internet access. Figure 2 depicts the organization of this configuration.

Alternatively, an HTTP proxy, instead of the NAT instance, can be configured to provide systems in the private subnet with Internet connectivity. If a proxy server is part of your configuration, follow the steps detailed in the section “Proxy Server Configuration with Cloud Manager.”

Figure 2) VPC with public and private subnets (graphic supplied by AWS).



Custom Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*igw-id*

Main Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*nat-instance-id*

Deploy Cloud Manager

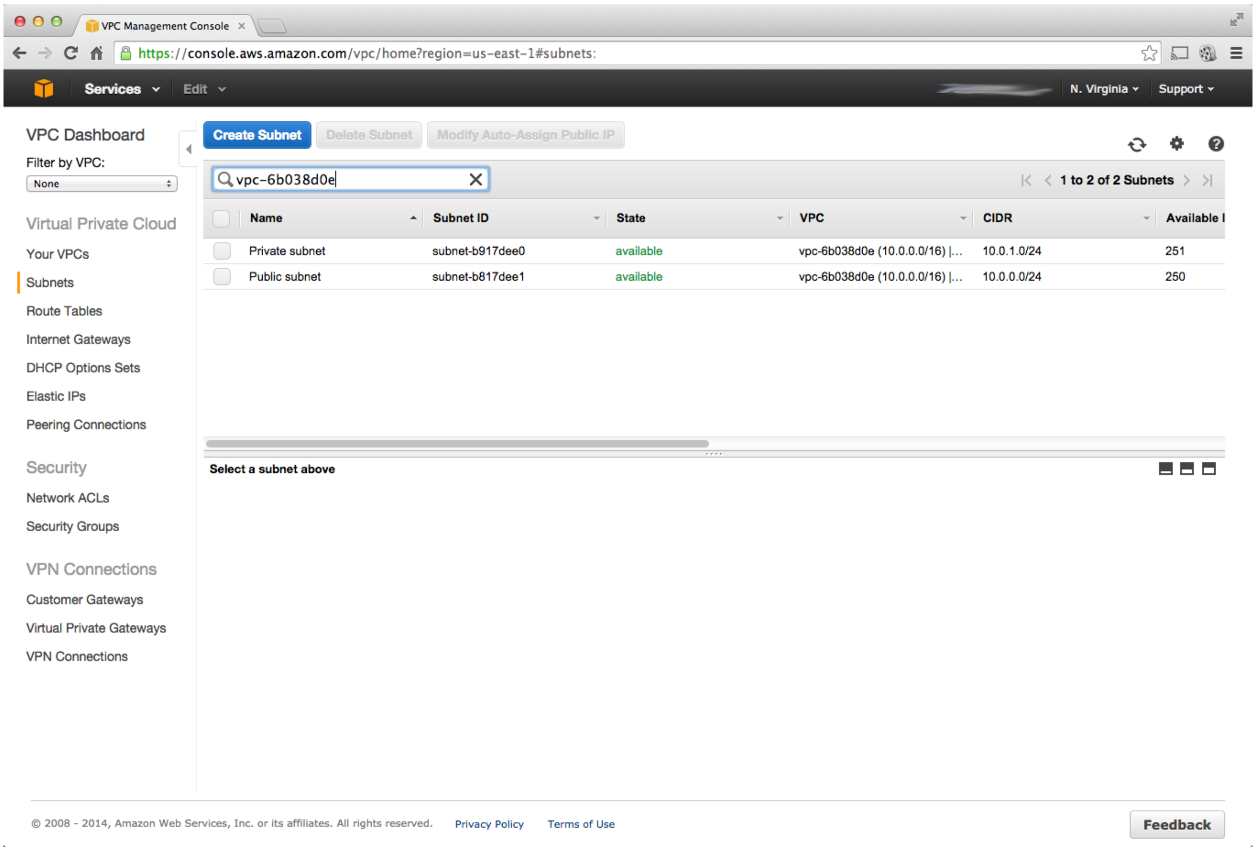
Although administrators can deploy Cloud Manager in either the private or public subnet, NetApp recommends using the public subnet, because the Cloud Manager instance should be accessible by hosts outside of the VPC. Cloud ONTAP, however, should be deployed into the private subnet. The following example assumes that the customer is deploying Cloud Manager into the public subnet and Cloud ONTAP into the private subnet.

Deploy Cloud ONTAP

To deploy and configure Cloud ONTAP into this environment, complete the following steps:

1. Identify the desired target AWS region, VPC, and subnet for Cloud ONTAP. To view the available subnets for the VPC, search for the VPC ID from the Subnets section of the VPC Dashboard. Both public and private subnets should be listed. Remember, although Cloud Manager can be deployed into either public or private subnets, Cloud ONTAP should be deployed into a private subnet.

   Note: In this example, the private subnet is configured as `10.0.1.0/24`, and the public subnet is configured as `10.0.0.0/24`.



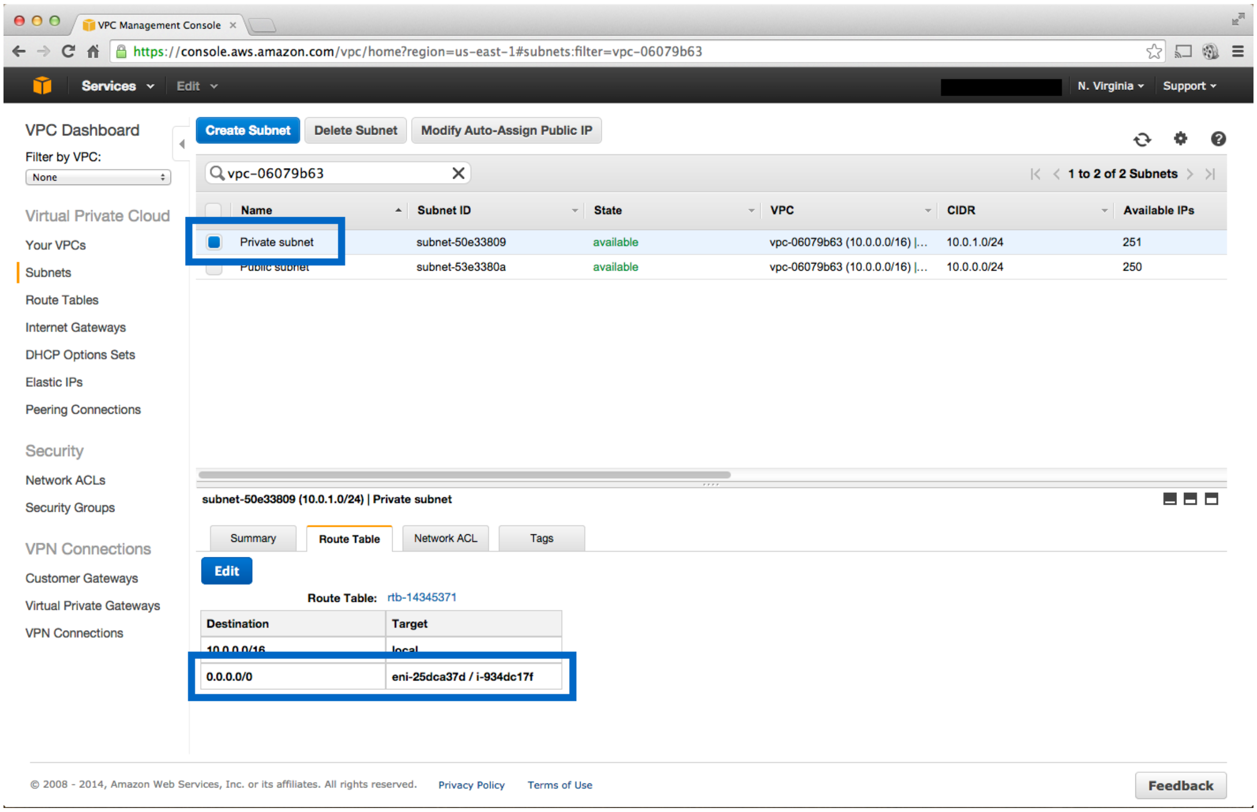
https://console.aws.amazon.com/vpc/home?region=us-east-1#subnets:

vpc-6b038d0e

Name	Subnet ID	State	VPC	CIDR	Available I
Private subnet	subnet-b917dee0	available	vpc-6b038d0e (10.0.0.0/16) |...	10.0.1.0/24	251
Public subnet	subnet-b817dee1	available	vpc-6b038d0e (10.0.0.0/16) |...	10.0.0.0/24	250

© 2008 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved.

2. The private subnet contains a default route that points to the network interface of the NAT instance. This routes all external traffic to the NAT instance, which then routes traffic out of the IGW. Select the private subnet and click the Route Table tab to confirm the selection.



https://console.aws.amazon.com/vpc/home?region=us-east-1#subnets:filter=vpc-06079b63

vpc-06079b63

Name	Subnet ID	State	VPC	CIDR	Available IPs
Private subnet	subnet-50e33809	available	vpc-06079b63 (10.0.0.0/16) |...	10.0.1.0/24	251
Public subnet	subnet-53e3380a	available	vpc-06079b63 (10.0.0.0/16) |...	10.0.0.0/24	250

subnet-50e33809 (10.0.1.0/24) | Private subnet

Route Table: rtb-14345371

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	eni-25dca37d / i-934dc17f

3. After Cloud Manager has been properly deployed into the public subnet and the private subnet has been identified for Cloud ONTAP, follow the OnCommand Cloud Manager 1.0 Installation and Setup Guide to deploy Cloud ONTAP using Cloud Manager.

The NAT instance handles outbound Internet routing. Access from systems on the private subnet is controlled through the AWS security group policies of both the local system and the NAT instance. The AWS security group that is assigned to the NAT instance may require modifications to allow Cloud ONTAP to transmit AutoSupport messages to the NetApp Support URL.

NAT Security Group Configuration

In the preceding example, the public and private VPC was configured with the following subnets:

- A single public subnet (`10.0.0.0/24)` hosts the Cloud Manager instance
- A single private subnet (`10.0.1.0/24)` hosts the Cloud ONTAP instance

Using this sample subnet configuration, Table 3 and Table 4 describe, respectively, the inbound and outbound rules required to verify that the NAT security group has made the necessary services available to the Cloud ONTAP instance.

Table 3) NAT security group inbound recommendations.

NAT Security Group Rules: Inbound			
Source	Protocol	Port Range	Comments
`10.0.1.0/24`	TCP	80	All inbound HTTP traffic from the private subnet
`10.0.1.0/24`	TCP	443	All inbound HTTPS traffic from the private subnet

NAT Security Group Rules: Inbound			
Local network public IP address range	TCP	22	Allow inbound SSH access to the NAT instance from the local data center (over IGW)

Table 4) NAT security group outbound recommendations.

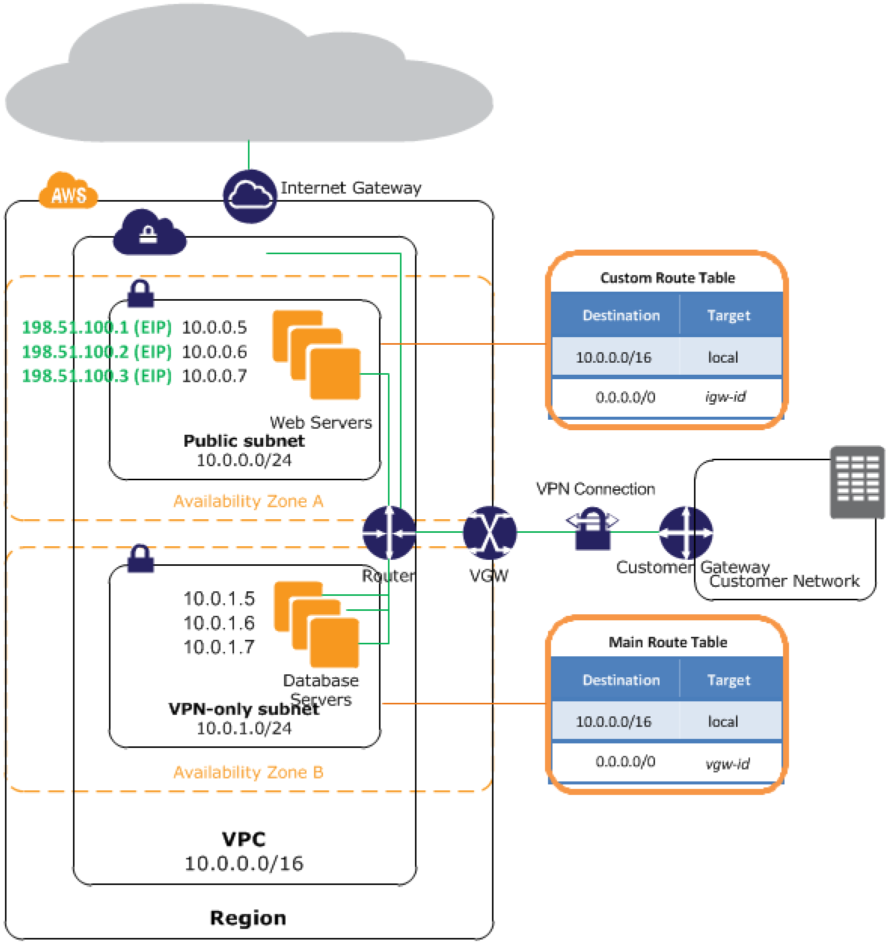
NAT Security Group Rules: Outbound			
Destination	Protocol	Port Range	Comments
`0.0.0.0/0`	TCP	80	Allows outbound HTTP access to Internet
`0.0.0.0/0`	TCP	443	Allows outbound HTTPS access to Internet

4.3 Public and Private Virtual Private Cloud with Virtual Private Network

This scenario uses two subnets to logically isolate systems that require inbound connectivity (a public subnet) from those that do not (a private subnet). An IPSec-enabled VPN connection provides connectivity back to the local data center with the subnet routes configured back to the on-premises infrastructure. Internet connectivity for AWS instances in the public subnet is provided by an IGW, while Internet traffic originating from the private subnet routes back over the VPN connection and is therefore subject to corporate firewall policies. The organization of this configuration is depicted in Figure 3.

This configuration can be used when the customer runs a web server farm in the AWS cloud (public subnet) while providing back-end services and on-premises resources from Cloud ONTAP (private subnet).

Figure 3) VPC with public and private subnets and hardware VPN access (graphic supplied by AWS).



Custom Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*igw-id*

Main Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*vgw-id*

Deploying Cloud Manager

Cloud Manager can be deployed into either the public or private subnets, with the VPN connection providing access to the web service for any corporate system. If a private subnet is used, however, verify that Cloud Manager has access to the appropriate services, as outlined in the section “OnCommand Cloud Manager Setup.” NetApp recommends deploying Cloud ONTAP into the private subnet, because Cloud ONTAP is likely to provide back-end support services.

Deploying Cloud ONTAP

To deploy and configure Cloud ONTAP in this environment, complete the following steps:

1. Identify the desired target AWS Region, VPC, and private subnet for Cloud ONTAP.

   Note: Verify that Cloud Manager has network connectivity to the designated subnet.

2. If a proxy server is part of this configuration, refer to the section “Proxy Server Configuration with Cloud Manager” to verify that Cloud Manager is configured correctly prior to deploying Cloud ONTAP.
3. After Cloud Manager has been properly configured, follow the OnCommand Cloud Manager 1.0 Installation and Setup Guide to deploy Cloud ONTAP using Cloud Manager.
4. Because outbound Internet routing for the private subnet is handled through a local data center gateway, Cloud ONTAP (and possibly Cloud Manager) should be able to transmit AutoSupport messages without additional configuration, provided that corporate routing and firewall policies have

been modified to allow AWS HTTP and HTTPS traffic to pass through unrestricted. If Cloud Manager is deployed into the public subnet, the IGW provides Internet routing services that allow AutoSupport transmission.

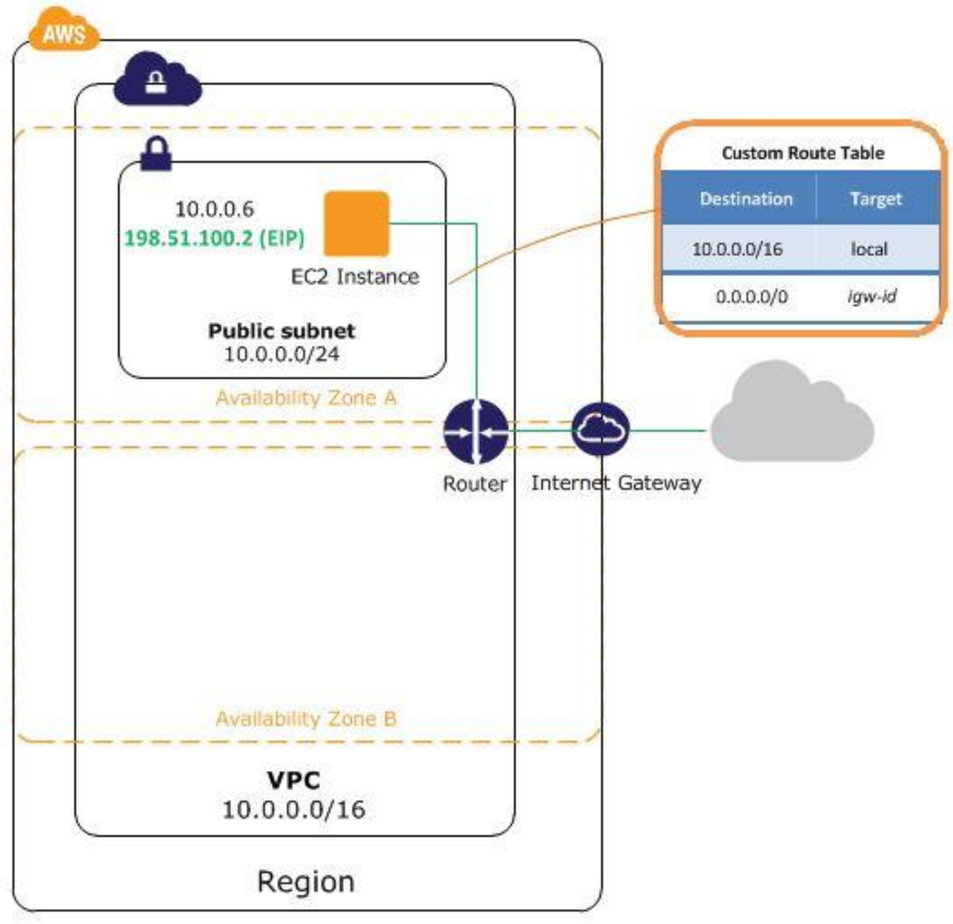
4.4 Public Virtual Private Cloud

The configuration described in this section is not a NetApp recommended deployment for production instances of Cloud ONTAP. This networking configuration is intended for use with Internet-facing services, such as public web servers, rather than infrastructure that provides secure, private back-end services, such as database servers, Cloud ONTAP, and so on. This configuration may be useful, however, if the user would like to create a new VPC environment to export the Cloud ONTAP product without incurring the overhead of configuring NAT or VPN connectivity.

In this configuration, the customer deploys the Cloud ONTAP instance into a VPC with a single public subnet. In this instance, a public subnet is defined as an AWS VPC subnet with Internet access enabled through an IGW that has been configured in the customer’s VPC. Connectivity to hosts deployed into this subnet occurs through the use of public IP addresses and/or EIPs that have been assigned to specific network interfaces on select AWS instances.

Because there is an IGW present, no proxy server is needed to provide Internet connectivity to AWS instances.

Figure 4) VPC with a public subnet only (graphic supplied by AWS).



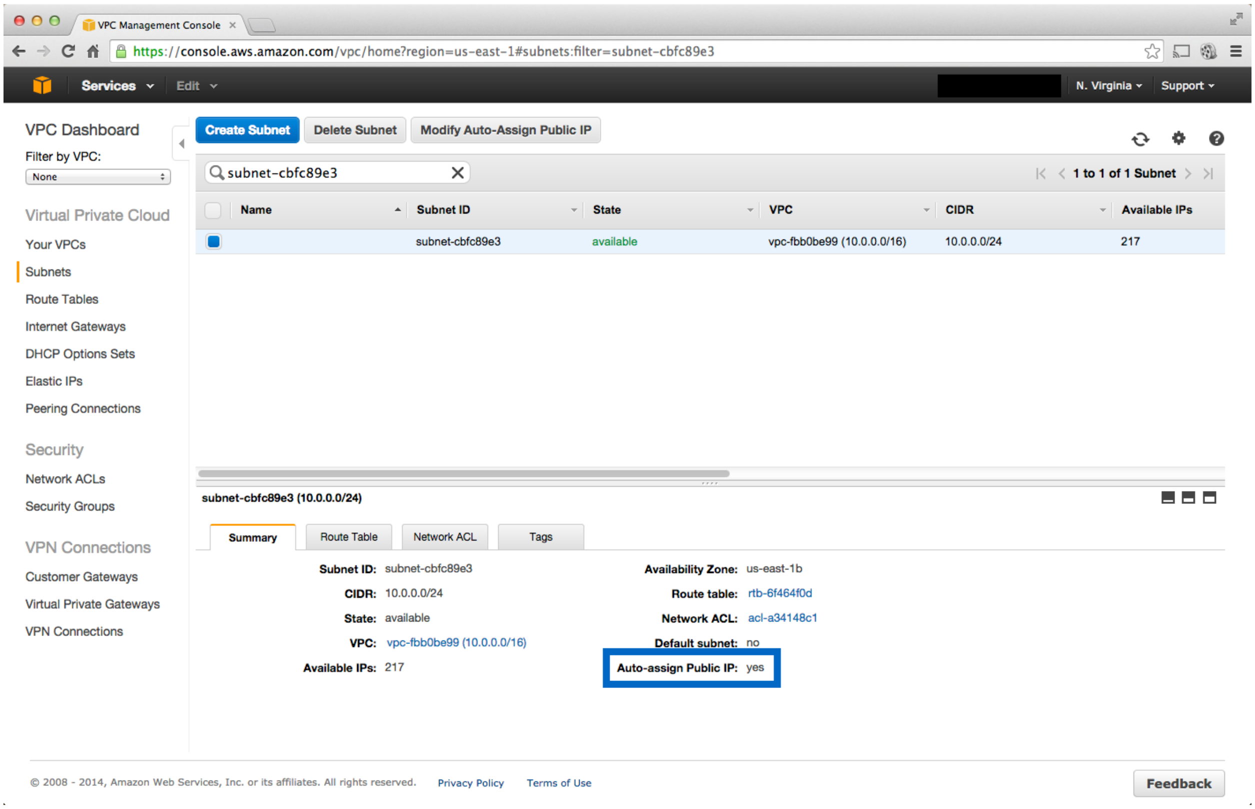
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*igw-id*

Deploying Cloud Manager

In this scenario, NetApp recommends deploying the Cloud Manager AMI into the subnet that hosts Cloud ONTAP. This allows the administrator to use AWS public IP address allocation procedures to enable access to the Cloud Manager system. There are two options available to the administrator:

- Acquire a public IP address automatically at the time of deployment. This can be done by toggling the Auto-Assign Public IP address flag to Yes in the target subnet, as is shown in Figure 5.

Figure 5) Assign a public IP address automatically.



Name	Subnet ID	State	VPC	CIDR	Available IPs
	subnet-cbfc89e3	available	vpc-fbb0be99 (10.0.0.0/16)	10.0.0.0/24	217

subnet-cbfc89e3 (10.0.0.0/24)

Subnet ID: subnet-cbfc89e3
CIDR: 10.0.0.0/24
State: available
VPC: vpc-fbb0be99 (10.0.0.0/16)
Available IPs: 217
Availability Zone: us-east-1b
Route table: rtb-6f464f0d
Network ACL: acl-a34148c1
Default subnet: no
Auto-assign Public IP: yes

- Manually assign an EIP to the Cloud Manager instance postdeployment.

  Note: The instance is deployed with a private IP address that is inaccessible from hosts external to the VPC. The allocation and assignment of an EIP allow the host to receive incoming remote-desktop or HTTP requests.

After Cloud Manager has been deployed and a public IP address has been allocated either automatically or manually, no additional network configuration is necessary. That is because all further IP connectivity is governed through the assigned AWS security group policies and defined network routes.

Deploy Cloud ONTAP

To deploy and configure Cloud ONTAP in this environment, complete the following steps:

1. Identify the desired target AWS region, VPC, and subnet for Cloud ONTAP.

   Note: Verify that Cloud Manager has network connectivity to the designated subnet.

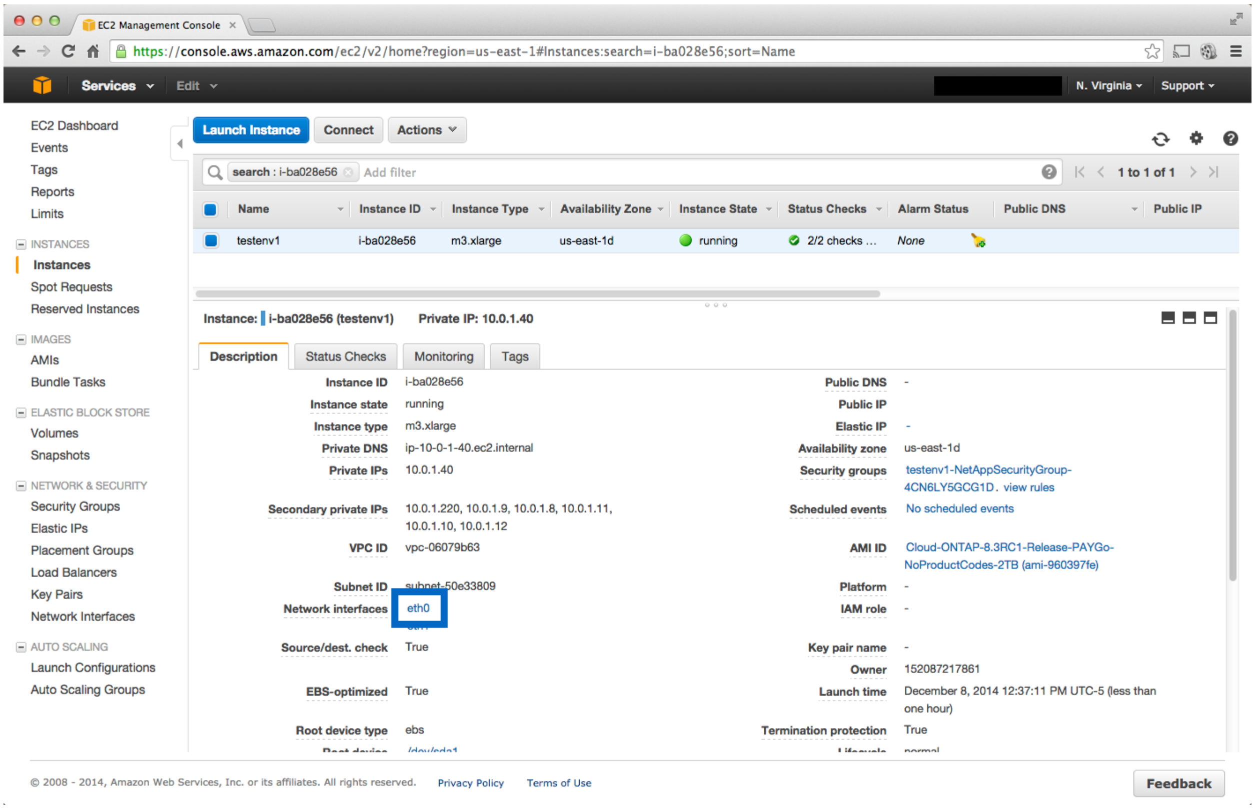
2. After Cloud Manager has been properly configured, follow the OnCommand Cloud Manager 1.0 Installation and Setup Guide to deploy Cloud ONTAP using Cloud Manager.

Outbound Internet connectivity is required for Cloud ONTAP to perform actions such as sending AutoSupport messages back to the NetApp support center, downloading new Data ONTAP software releases, and providing web-based management access through System Manager. These requests are handled by two separate network interfaces.

- Network interface eth0 hosts the cluster management interface, which handles incoming System Manager network requests.
- Network interface eth1 hosts the node management interface, which is used to transmit AutoSupport messages and download Data ONTAP software updates.

In this configuration, the customer must assign an EIP to both eth0 and eth1, the elastic network interfaces of the Cloud ONTAP instance. Once assigned, the EIP associates with the primary IP of the network interface. No further actions are required by the user. Unlike Cloud Manager, Cloud ONTAP does not support the use of an automatically assigned public IP address in a VPC subnet and ignores this setting, even when it is toggled to True. To configure Cloud ONTAP with an EIP, complete the following steps:

1. From the EC2 Dashboard section of the AWS management console, click on the newly deployed Cloud ONTAP instance.
2. From the bottom pane, scroll down to the section that lists network interfaces and select eth0.

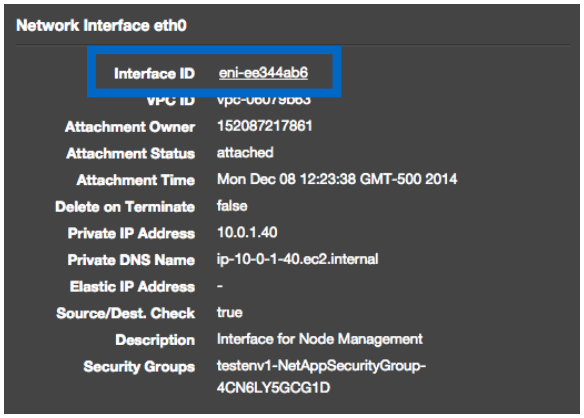


Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS	Public IP
testenv1	i-ba028e56	m3.xlarge	us-east-1d	running	2/2 checks ...	None		

Instance: i-ba028e56 (testenv1) Private IP: 10.0.1.40

Instance ID	i-ba028e56	Public DNS	-
Instance state	running	Public IP	
Instance type	m3.xlarge	Elastic IP	-
Private DNS	ip-10-0-1-40.ec2.internal	Availability zone	us-east-1d
Private IPs	10.0.1.40	Security groups	testenv1-NetAppSecurityGroup-4CN6LY5GCG1D. view rules
Secondary private IPs	10.0.1.220, 10.0.1.9, 10.0.1.8, 10.0.1.11, 10.0.1.10, 10.0.1.12	Scheduled events	No scheduled events
VPC ID	vpc-06079b63	AMI ID	Cloud-ONTAP-8.3RC1-Release-PAYGo-NoProductCodes-2TB (ami-960397fe)
Subnet ID	subnet-50e33809	Platform	-
Network interfaces	eth0 eth1	IAM role	-
Source/dest. check	True	Key pair name	-
		Owner	152087217861
EBS-optimized	True	Launch time	December 8, 2014 12:37:11 PM UTC-5 (less than one hour)
Root device type	ebs	Termination protection	True
Root device	/dev/sda1	Lifecycle	normal

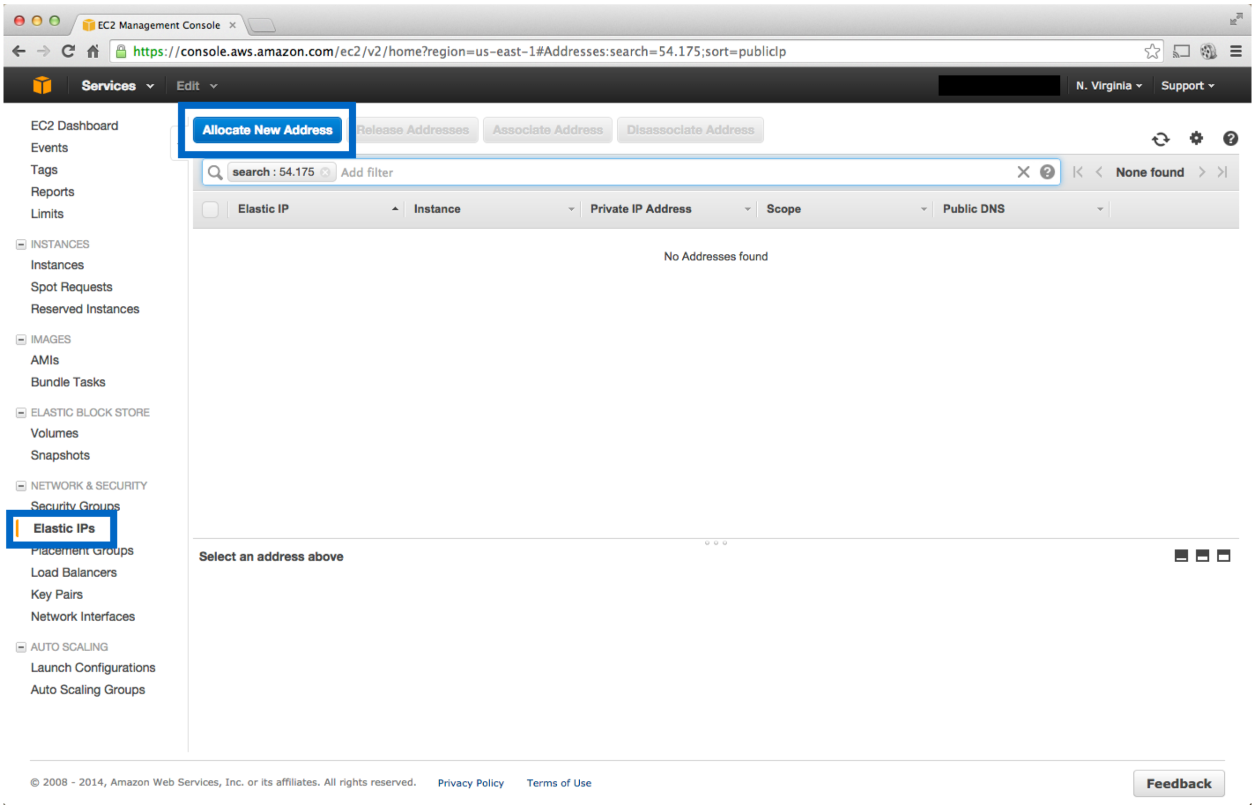
3. Copy the Interface ID. This information is used later.



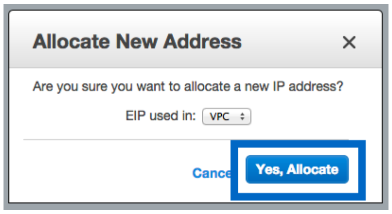
Network Interface eth0

Interface ID eni-ee344ab6
VPC ID vpc-06079b63
Attachment Owner 152087217861
Attachment Status attached
Attachment Time Mon Dec 08 12:23:38 GMT-500 2014
Delete on Terminate false
Private IP Address 10.0.1.40
Private DNS Name ip-10-0-1-40.ec2.internal
Elastic IP Address -
Source/Dest. Check true
Description Interface for Node Management
Security Groups testenv1-NetAppSecurityGroup-4CN6LY5GCG1D

4. Navigate to the elastic IP address section of the management console in the left-hand menu and click Allocate New Address.



5. From the Allocate New Address confirmation dialog box, select VPC and click Yes, Allocate.

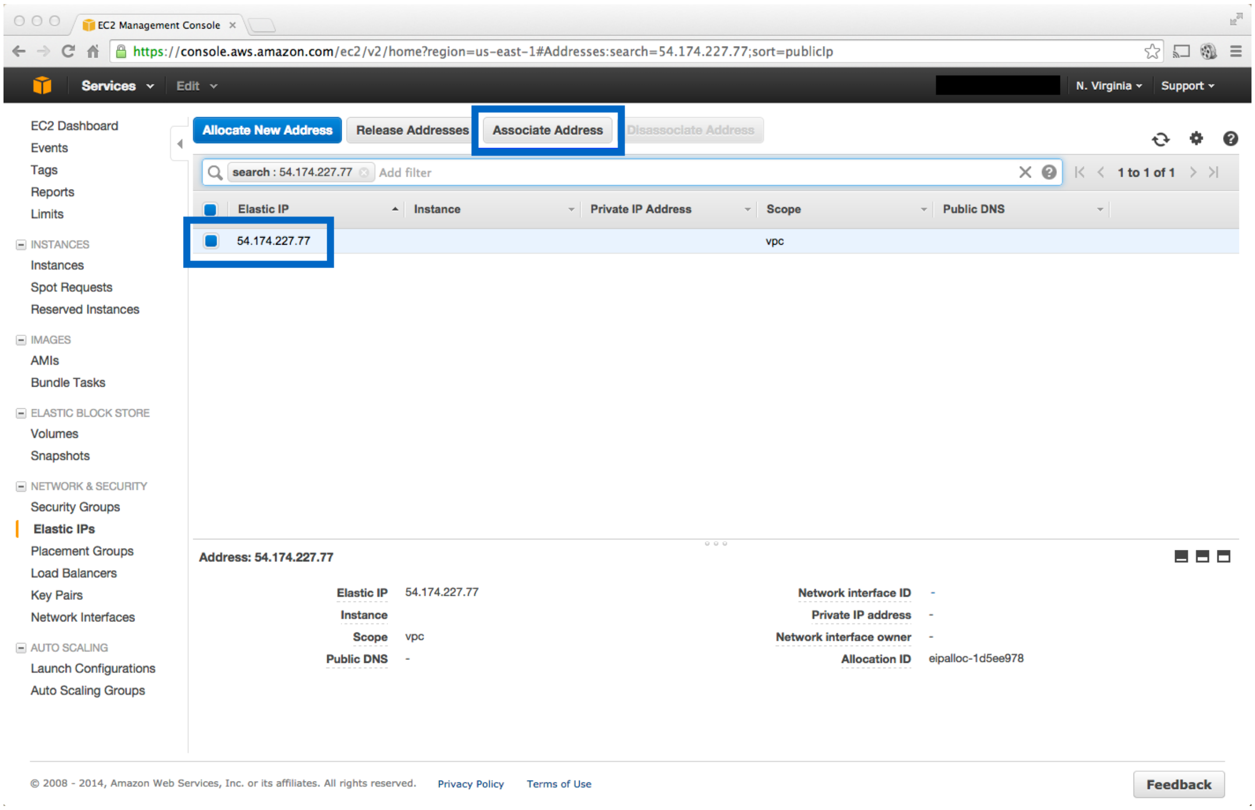


Allocate New Address

Are you sure you want to allocate a new IP address?

EIP used in: VPC

6. Click on the newly allocated EIP and select Associate Address.



https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#Addresses:search=54.174.227.77;sort=publicIp

search : 54.174.227.77

1 to 1 of 1

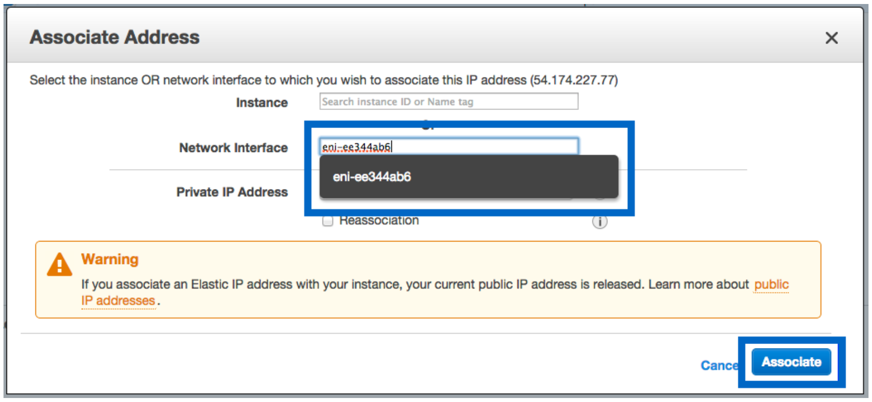
Elastic IP	Instance	Private IP Address	Scope	Public DNS
54.174.227.77			vpc	

Address: 54.174.227.77

Elastic IP	54.174.227.77	Network interface ID	-
Instance		Private IP address	-
Scope	vpc	Network interface owner	-
Public DNS	-	Allocation ID	eipalloc-1d5ee978

© 2008 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved.

7. Enter the Interface ID identified in step 5 into the Network Interface textbox and click Associate.



Select the instance OR network interface to which you wish to associate this IP address (54.174.227.77)

Instance

Network Interface: eni-ee344ab6

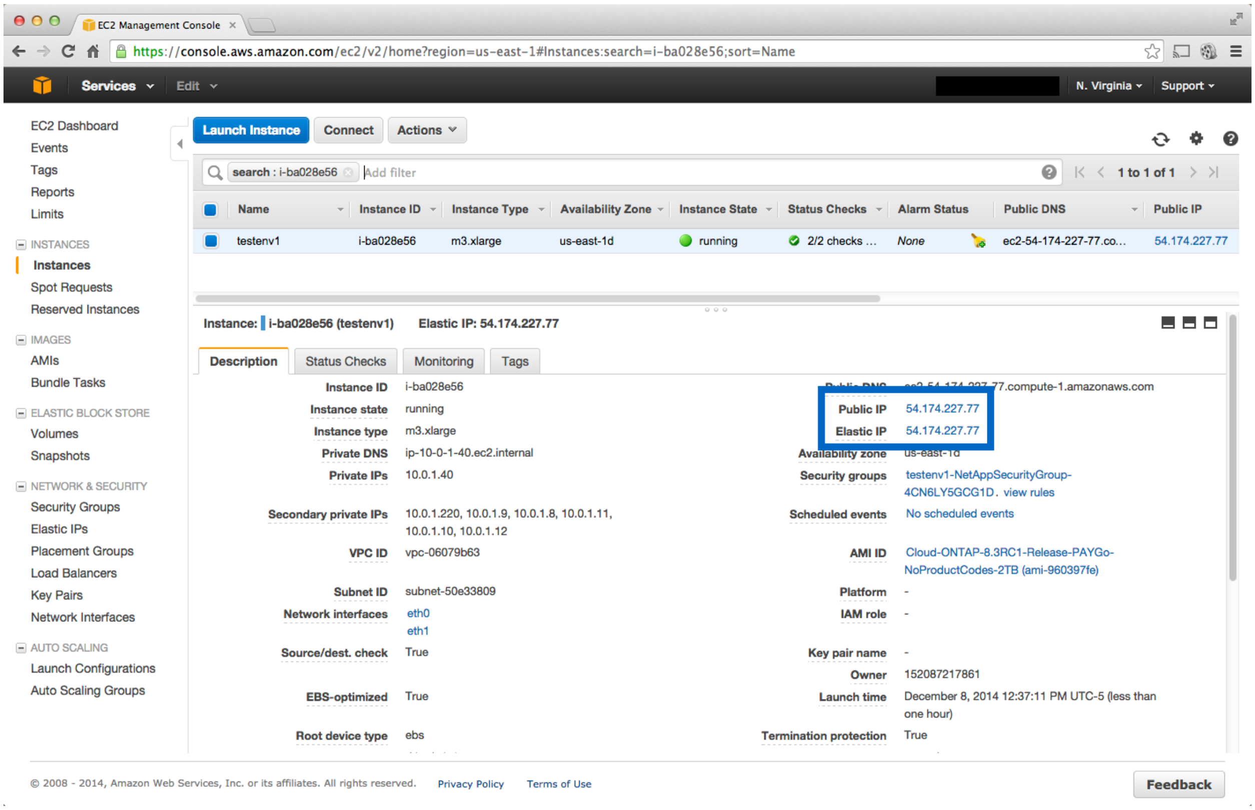
eni-ee344ab6

Private IP Address

Warning

If you associate an Elastic IP address with your instance, your current public IP address is released. Learn more about public IP addresses.

8. A public IP address is now associated with Cloud ONTAP interface eth0. Cloud ONTAP can now send Internet packets from the cluster management logical interface (LIF) associated with eth0.



https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:search=i-ba028e56;sort=Name

[redacted]

search : i-ba028e56

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS	Public IP
testenv1	i-ba028e56	m3.xlarge	us-east-1d	running	2/2 checks ...	None	ec2-54-174-227-77.co...	54.174.227.77

Instance: i-ba028e56 (testenv1) Elastic IP: 54.174.227.77

Instance ID	i-ba028e56	Public DNS	ec2-54-174-227-77.compute-1.amazonaws.com
Instance state	running	Public IP	54.174.227.77
Instance type	m3.xlarge	Elastic IP	54.174.227.77
Private DNS	ip-10-0-1-40.ec2.internal	Availability zone	us-east-1d
Private IPs	10.0.1.40	Security groups	testenv1-NetAppSecurityGroup-4CN6LY5GCG1D. view rules
Secondary private IPs	10.0.1.220, 10.0.1.9, 10.0.1.8, 10.0.1.11, 10.0.1.10, 10.0.1.12	Scheduled events	No scheduled events
VPC ID	vpc-06079b63	AMI ID	Cloud-ONTAP-8.3RC1-Release-PAYGo-NoProductCodes-2TB (ami-960397fe)
Subnet ID	subnet-50e33809	Platform	-
Network interfaces	eth0 eth1	IAM role	-
Source/dest. check	True	Key pair name	-
		Owner	152087217861
EBS-optimized	True	Launch time	December 8, 2014 12:37:11 PM UTC-5 (less than one hour)
Root device type	ebs	Termination protection	True

© 2008 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved.

9. Repeat steps 1 through 8 and allocate an EIP to network interface eth1.
10. The public IP address is now associated with Cloud ONTAP interface eth1. Cloud ONTAP can now send Internet packets from the node management LIF associated with eth1.

5 Cloud ONTAP Security Group Rules

When deploying Cloud ONTAP, the user has the option to create a default security group or use a group that was created previously. If the user chooses the first option, the security group created for the Cloud ONTAP instance contains the inbound (Table 5) and outbound (Table 6) rules necessary for connectivity for all supported Data ONTAP features. If an administrator decides to use a different security group, the administrator must verify that these ports are open to provide proper connectivity.

Table 5) Inbound security group rules for Cloud ONTAP.

Type	Port Range	Used for:
All ICMP	All	Pinging the instance
Custom TCP Rule	111	Portmapper
Custom TCP Rule	139	NetBIOS
Custom TCP Rule	161 to 162	SNMP
Custom TCP Rule	445	Microsoft SMB
Custom TCP Rule	635	NFS mount service
Custom TCP Rule	749	Kerberos

Type	Port Range	Used for:
Custom TCP Rule	2049	NFS
Custom TCP Rule	3260	iSCSI
Custom TCP Rule	4045 to 4046	NFS (lockd, mountd)
Custom TCP Rule	10,000	NDMP
Custom TCP Rule	11,104 to 11,105	Intercluster management and data
Custom UDP Rule	111	Portmapper
Custom UDP Rule	161 to 162	SNMP
Custom UDP Rule	635	NFS mount service
Custom UDP Rule	2049	NFS
Custom UDP Rule	4045 to 4046	NFS (lockd, mountd)
HTTP	80	System Manager access
HTTPS	443	System Manager access
SSH	22	SSH to the CLI

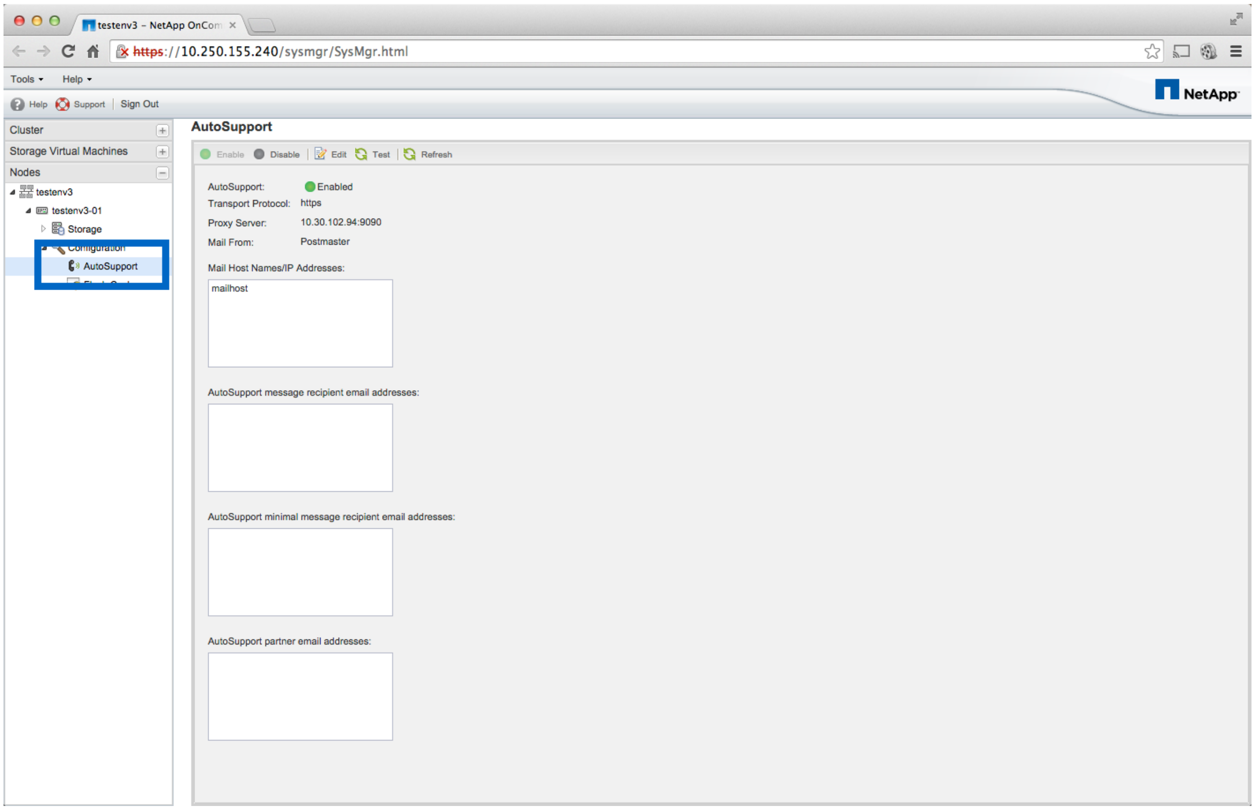
Table 6) Outbound security group rules for Cloud ONTAP

Type	Port range	Used for
All ICMP	All	All outbound traffic
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

6 Cloud ONTAP Proxy Configuration

If a proxy server is defined, Cloud Manager automatically configures a proxy server when deploying a Cloud ONTAP instance. If not, a proxy server can be manually configured in Cloud ONTAP by completing the following steps:

1. Start System Manager by pointing a supported web browser at the cluster management interface of the Cloud ONTAP system and log in using the necessary credentials.
2. Click Configuration > AutoSupport to navigate to the AutoSupport page.



AutoSupport

AutoSupport: Enabled
Transport Protocol: https
Proxy Server: 10.30.102.94:9090
Mail From: Postmaster

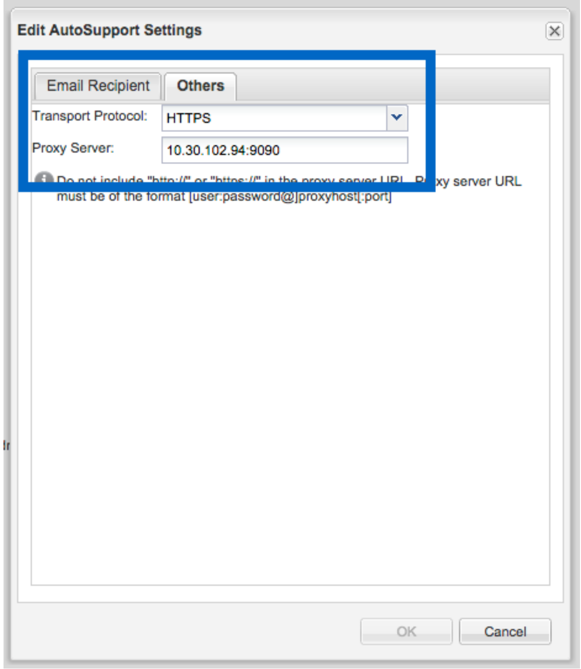
Mail Host Names/IP Addresses:
mailhost

AutoSupport message recipient email addresses:

AutoSupport minimal message recipient email addresses:

AutoSupport partner email addresses:

3. Click Edit and then click on the Others tab.
4. Enter the proxy server information and click OK.



Edit AutoSupport Settings

Transport Protocol: HTTPS

Proxy Server: 10.30.102.94:9090

Do not include "http://" or "https://" in the proxy server URL. Proxy server URL must be of the format [user:password@]proxyhost[:port]

6.1 Verify Proxy Server

Cloud ONTAP proxy server verification can be performed by using either the Cloud ONTAP CLI or System Manager.

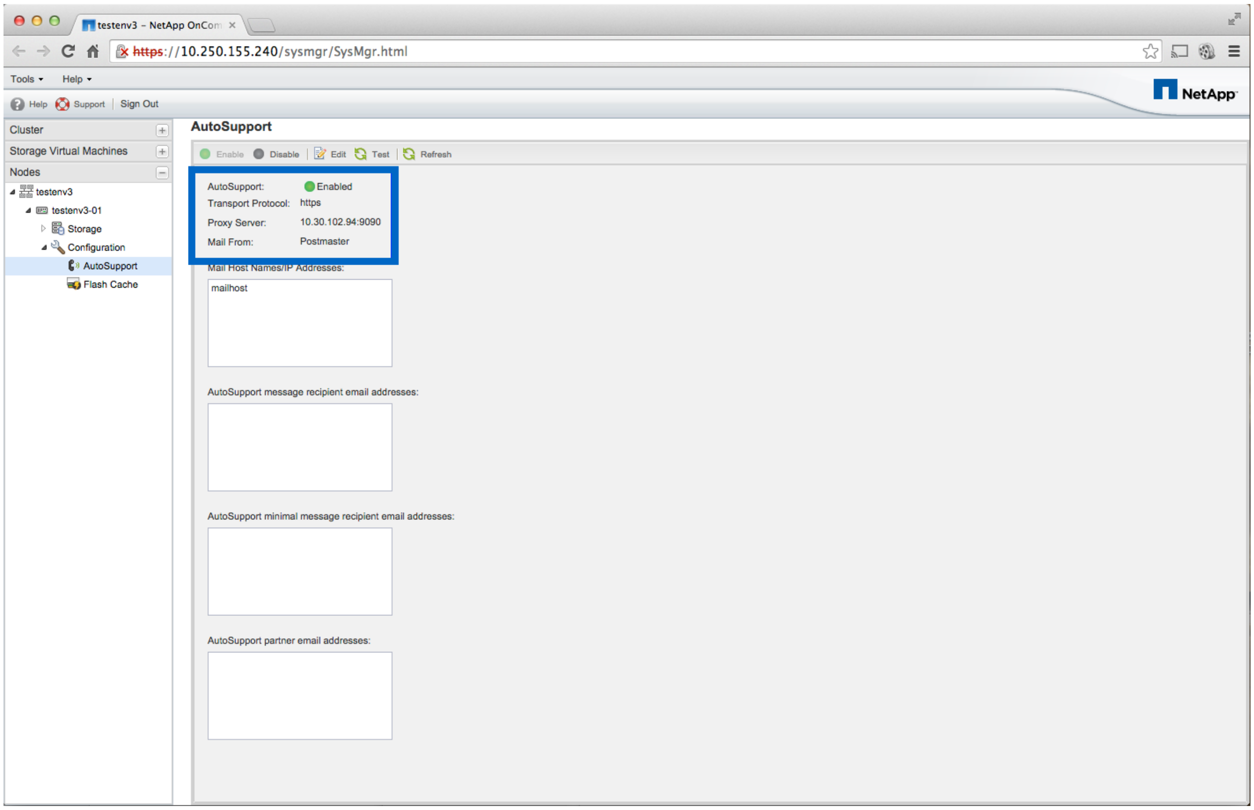
To verify Cloud ONTAP proxy settings with the Cloud ONTAP CLI, run the following command:

```
testwe1::> autosupport show –instance

                                       Node: testwe1
                                      State: enable
                            SMTP Mail Hosts: mailhost
                               From Address: Postmaster
                       List of To Addresses: -
                   List of Noteto Addresses: -
                  List of Partner Addresses: -
Send AutoSupport Messages to Vendor Support: enable
                Protocol to Contact Support: https
                 Support URL for HTTP/HTTPS: support.netapp.com/asupprod/post/1.0/postAsup
                 Support URL for HTTP/S PUT: support.netapp.com/put/AsupPut
                          Support Proxy URL: 10.30.102.94:9090
                            Support Address: autosupport@netapp.com
                           Hostname Subject: false
                                 NHT Enable: true
                    Performance Data Enable: true
                             Retry Interval: 4m
                                Retry Count: 15
                            Reminder Enable: true
                          Last Subject Sent: MANAGEMENT_LOG
                             Last Time Sent: 10/31/2014 00:35:28
                          Maximum HTTP Size: 10MB
                          Maximum SMTP Size: 5MB
                      Remove Sensitive Data: false
      Validate Digital Certificate Received: true
            AutoSupport OnDemand Server URL: https://support.netapp.com/aods/asupmessage
```

To verify Cloud ONTAP proxy settings with System Manager, complete the following steps:

1. Start System Manager by pointing a web browser at the cluster management IP address of the Cloud ONTAP instance.
2. Log in to the Cloud ONTAP system using the proper administrator credentials.
3. On the left-hand side of the screen, click Nodes to show the host name of your Cloud ONTAP system.
4. Select Configuration > AutoSupport.
5. The AutoSupport settings are indicated in the following screenshot.



AutoSupport

AutoSupport: ● Enabled
Transport Protocol: https
Proxy Server: 10.30.102.94:9090
Mail From: Postmaster

Mail Host Names/IP Addresses:
mailhost

AutoSupport message recipient email addresses:

AutoSupport minimal message recipient email addresses:

AutoSupport partner email addresses:

7 Connectivity Verification Testing

This section provides procedures for verifying that AutoSupport transmissions can be sent by both Cloud ONTAP and Cloud Manager.

7.1 Cloud ONTAP AutoSupport Verification

The procedures documented in the section “Virtual Private Cloud Configurations” describe the steps necessary to allow Cloud ONTAP to transmit AutoSupport messages to NetApp support. This section documents the process for testing this connectivity by manually invoking an AutoSupport message through the clustered Data ONTAP CLI.

Before attempting to verify the functionality of AutoSupport on your Cloud ONTAP instance, note the following:

- There is a 24 hour opt-out period before manual AutoSupport invocations transmit from a Cloud ONTAP instance. This period allows customers to disable AutoSupport, if desired.
- Both manual and scheduled AutoSupport invocations of a Cloud ONTAP instance configured with a proxy server transmit immediately after deployment. There is no opt-out period.
- Cloud Manager transmits both manual and scheduled AutoSupport invocations immediately after deployment. There is no opt-out period.

The NetApp support URL is support.netapp.com. Before attempting to invoke an AutoSupport request, please verify that corporate firewall settings allow access to this URL.

Test AutoSupport Using the Clustered Data ONTAP CLI

To test AutoSupport network connectivity using the clustered Data ONTAP CLI, complete the following steps:

1. Using a Linux host or Windows terminal emulator, initiate an SSH session into the cluster management interface of the Cloud ONTAP instance.
2. Log in to the instance using the administrative account and the applicable password.

```
megatron:~ testuser$ ssh 10.250.155.95 -l admin
Password:
testwe1::>
```

3. From the clustered Data ONTAP CLI, run the `autosupport invoke –type test` command.

```
testwe1::> autosupport invoke -type test
The AutoSupport was successfully invoked on node "testwe1-01". To view the status of the
AutoSupport, use the "system node autosupport history show" command. Note: It may take several
minutes for the AutoSupport to appear in the history list.
```

4. Wait approximately 60 seconds, and then run the `autosupport history show` command.

```
testwe1::> autosupport history show
             Seq                                       Attempt  Percent  Last
Node         Num   Destination Status                  Count    Complete Update
------------ ----- ----------- -------------------- -------- -------- --------
testwe1-01  19
                   smtp        ignore                  1        -        11/4/2014 01:19:58
                   http        sent-successful         1        100      11/4/2014 01:21:07
                   noteto      ignore                  1        -        11/4/2014 01:19:58
```

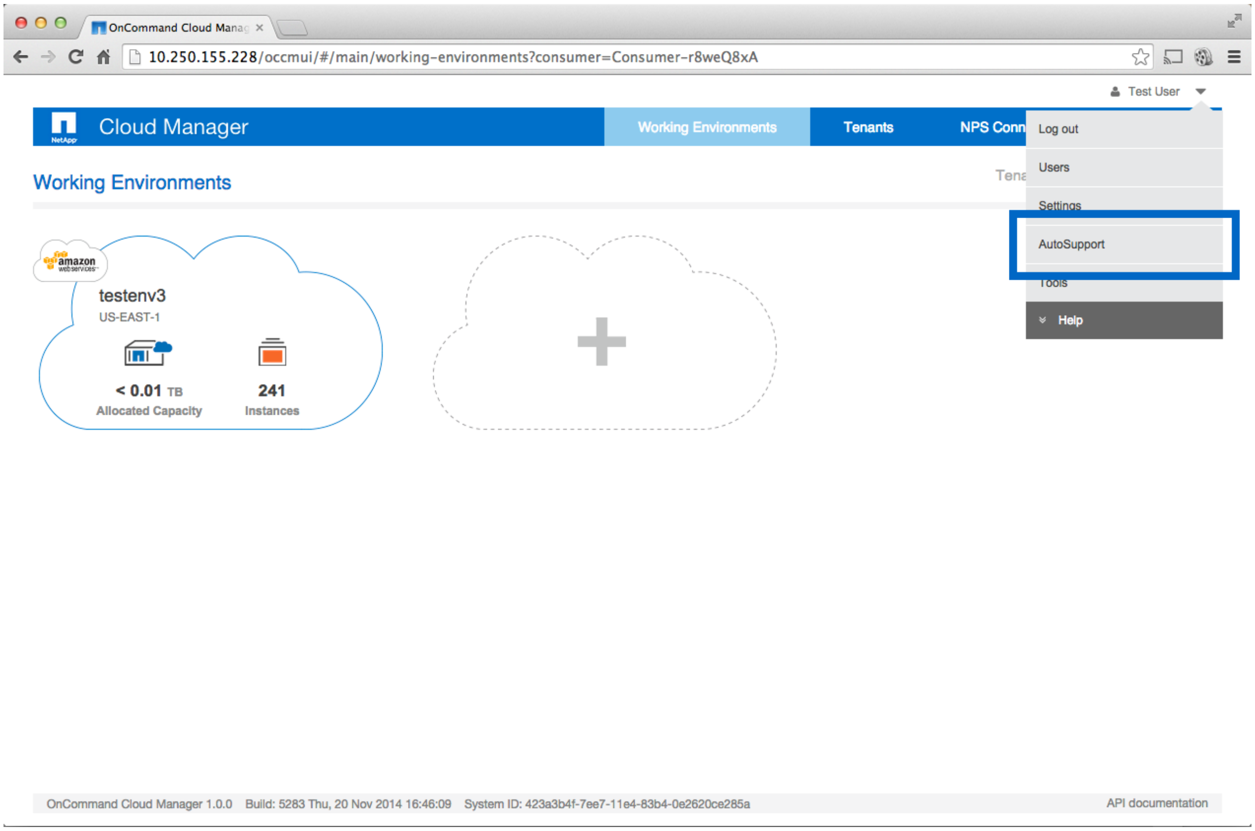
5. The message status should read `sent–successful`. If the status is `transmitting`, wait another 60 seconds and rerun the command. Any other output might indicate a connectivity problem to the NetApp Support site.

7.2 Verify Cloud Manager AutoSupport Connectivity

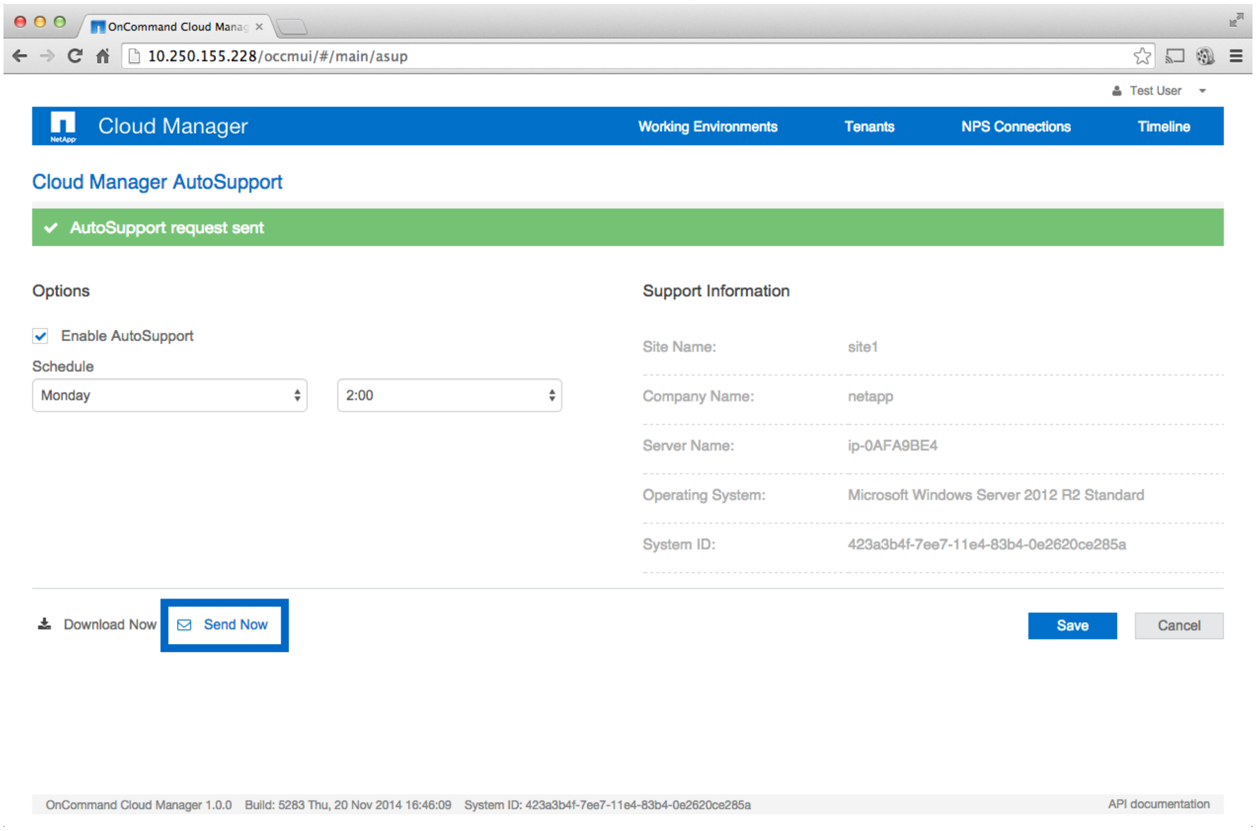
This section describes how to test network connectivity between Cloud Manager and NetApp support by manually invoking an AutoSupport test message from within Cloud Manager.

To test AutoSupport network connectivity by using Cloud Manager, complete the following steps:

1. Start Cloud Manager by pointing a supported web browser at the applicable URL and log in using the necessary credentials.
2. From the drop-down menu in the upper-right-hand corner of the browser, select AutoSupport.



3. Click Send Now. If the system is able to send an AutoSupport message, an AutoSupport Request Sent banner is displayed at the top of the screen. Any other output might indicate a connectivity problem to the NetApp Support site. For help in debugging connectivity issues, contact NetApp support.



Cloud Manager AutoSupport

✓ AutoSupport request sent

Options

☑ Enable AutoSupport

Schedule: Monday, 2:00

Support Information

Site Name:	site1
Company Name:	netapp
Server Name:	ip-0AFA9BE4
Operating System:	Microsoft Windows Server 2012 R2 Standard
System ID:	423a3b4f-7ee7-11e4-83b4-0e2620ce285a

OnCommand Cloud Manager 1.0.0 Build: 5283 Thu, 20 Nov 2014 16:46:09 System ID: 423a3b4f-7ee7-11e4-83b4-0e2620ce285a

References

The following references were used in this technical report:

- OnCommand Cloud Manager 1.0 Installation and Setup Guide
  https://library.netapp.com/ecm/ecm_get_file/ECMP1651524
- OnCommand Cloud Manager 1.0 User Guide
  https://library.netapp.com/ecm/ecm_get_file/ECMP1651525
- OnCommand Cloud Manager 1.0 Administration Guide
  https://library.netapp.com/ecm/ecm_get_file/ECMP1651526
- OnCommand Cloud Manager 1.0 Release Notes
  https://library.netapp.com/ecm/ecm_get_file/ECMP1651527
- Cloud ONTAP 8.3 RC1 for Amazon Web Services Release Notes
  https://library.netapp.com/ecm/ecm_get_file/ECMP1658441
- AWS Virtual Private Cloud Documentation
  http://aws.amazon.com/documentation/vpc/

Version History

Version	Date	Document Version History
Version 1.0	January 2015	Initial release

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

TR-4352-0115

NetApp®
www.netapp.com