Cloud Appliance: CT800/CT800-128

Requirements and Installation Guide

Original Publication Date: May 2021

Table of Contents

About This Document

The purpose of this document is to provide the reader with an understanding of how to install Cloud Appliances in the Amazon Web Services (AWS) cloud. It covers requirements, preparation, and installation for typical deployment scenarios. The reader of this document is expected to be a network administrator, or a network architect and familiar with AWS and its conventions.

Audience

This document was designed for network administrators and network architects who are familiar with Talari terminology and with the Talari solution

References

The following documents are available on the Talari Support site (www.talari.com/support):

- *Talari Glossary*
- *Talari APN 4.1 New Features Guide*
- *Talari APN 7.3 New Features Guide*
- *Talari APN 4.1 Configuration File Reference*
- *Talari APN 7.3 GA P4 Configuration Guide File Reference*

Request for Comments

We value the opinions and experiences of our readers. To offer feedback or corrections for this guide, please contact us.

Revision History

This section provides a revision history for this document.

Date	Description
May 2021	• Initial release

Requirements

AWS Resources

The Cloud Appliance on AWS has the following requirements:

Appliance Model	License Level	Dedicated VCPUs	RAM	Instance Type
CT800	20 Mbps	4	7.5 GB	c4.xlarge
CT800	200 Mbps	8	15 GB	c4.2xlarge
CT800-128	500 Mbps	16	32 GB	c5.4xlarge

Note: At minimum, Cloud Appliances requires 2 Network Interfaces (1 for MGT and 1 for LAN/WAN). However, Cloud Appliances can support up to 4 Network Interfaces.

WAN Optimization System Specifications

WAN Optimization is supported on CT800s running APN 7.1 or above and CT800-128s running APN 7.3 P4 or above at the following levels with the specified resources:

License Level	WANOp Capacity	VCPUs	RAM	Max WANOp Sessions	Disk Size	Instance Type
20 Mbps	8 Mbps	8	15GB	5,000	160GB	c4.xlarge
200 Mbps	50 Mbps	8	15GB	5,000	160GB	c4.2xlarge
500 Mbps	50 Mbps	16	32GB	16,000	160GB	c5.4xlarge

Software License

The Cloud Appliance on AWS requires a license, otherwise the Talari Service cannot be enabled. A properly licensed Cloud Appliance can function either as a Network Control Node (NCN) or as a Client Node within a Talari Adaptive Private Network (APN). A license must be acquired by submitting the AWS EC2 Instance ID for the Cloud Appliance to your Talari Sales Representative, who will then issue a Talari License file. The AWS EC2 Instance ID functions in place of a hardware identifier.

Upgrading from CT800 to CT800-128

An existing CT800 instance cannot be converted directly into a CT800-128. To upgrade a site from a CT800 to a CT800-128, deploy a new virtual appliance and cut over when ready, as with hardware appliance upgrades.

Preparation

The preparation process involves making a number of deployment decisions. Talari recommends documenting these decisions in a network diagram to guide the user through installation.

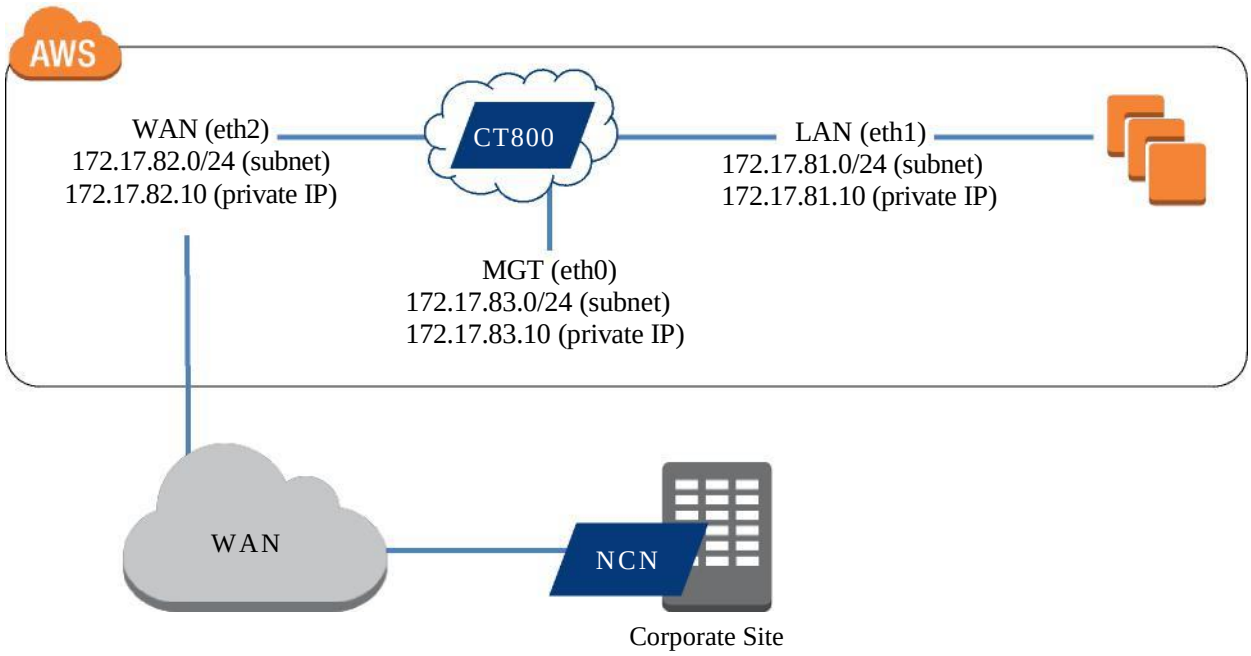
Select Topology, Subnets, and IP Addresses

The Cloud Appliance must reside within the existing topology of your network. This document assumes that the Cloud Appliance will be connected to a *previously deployed* Talari APN Appliance functioning as a Network Control Node (NCN). The Cloud Appliance and NCN can be connected over a variety of WAN infrastructure (e.g. Broadband, MPLS, AWS Direct Connect).

A subnet and IP address must be defined for each Cloud Appliance interface. The number of interfaces utilized depends on the deployment use case. If the goal is to reliably access application resources that are on the LAN side of the Cloud Appliance (e.g. inside of the same Region), the appliance can be configured with three Ethernet interfaces: MGT (eth0), LAN (eth1), and WAN (eth2). This topology separates the MGT, LAN, and WAN ports of the Talari into individual Ethernet segments. Alternatively, if the goal is to hairpin traffic through the Cloud Appliance to some other Region or to the public Internet, the appliance can be configured with two Ethernet interfaces: MGT (eth0) and LAN/WAN (eth1). The Cloud Appliance can support other interface configurations; these are just two examples. The Cloud Appliance can support up to 4 interfaces.

Note: This document assumes the use case of separate MGT, LAN, and WAN interfaces.

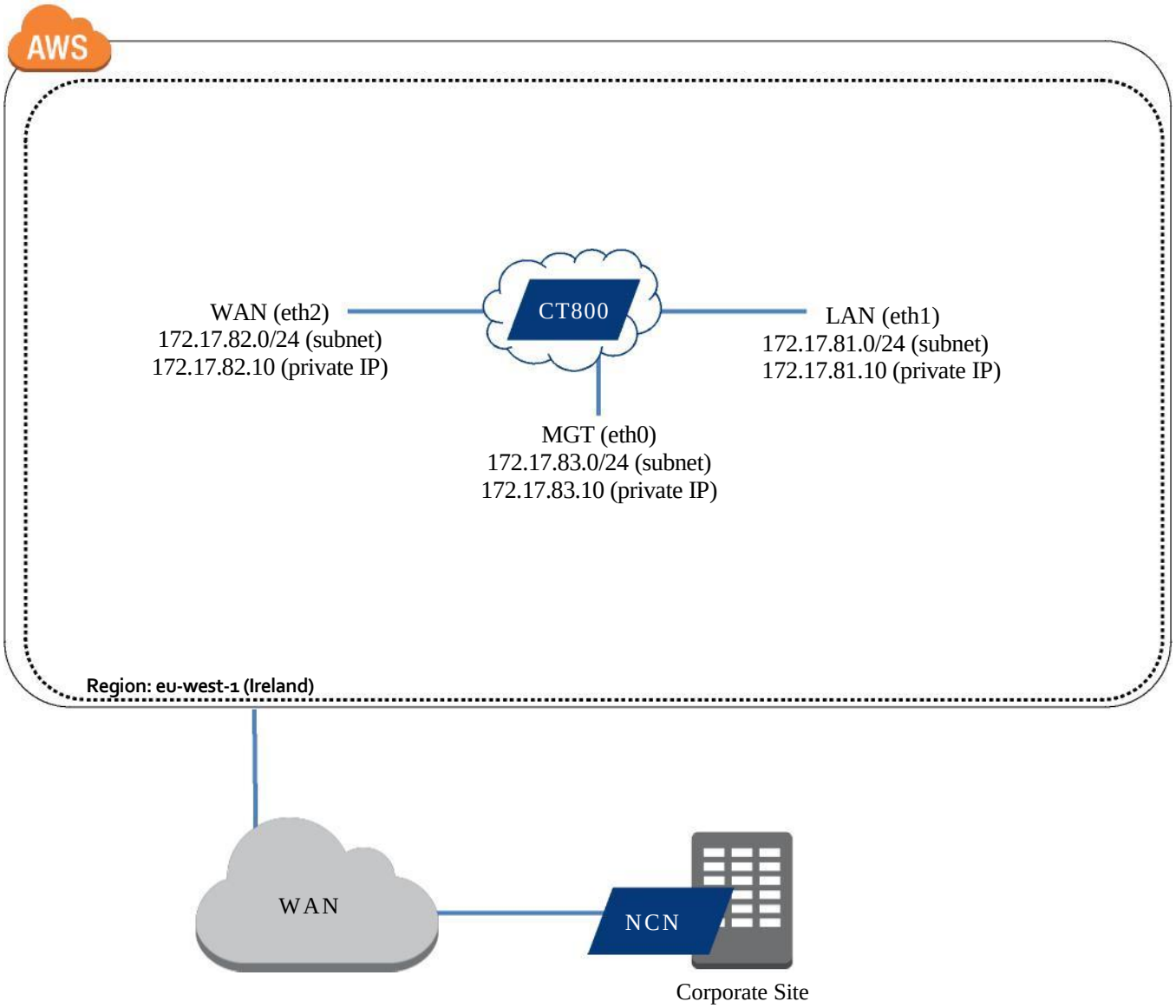
Topology, subnets, and IP addresses are selected in the example network diagram:



Select Region

AWS has multiple Data Centers (known as "Regions") across the globe that allow users to configure virtual networks. The Regions are independent of one another. When selecting a Region, the cost of resources within each region and the latency associated with accessing each region should be fully understood. Cloud Appliances are supported in all Regions.

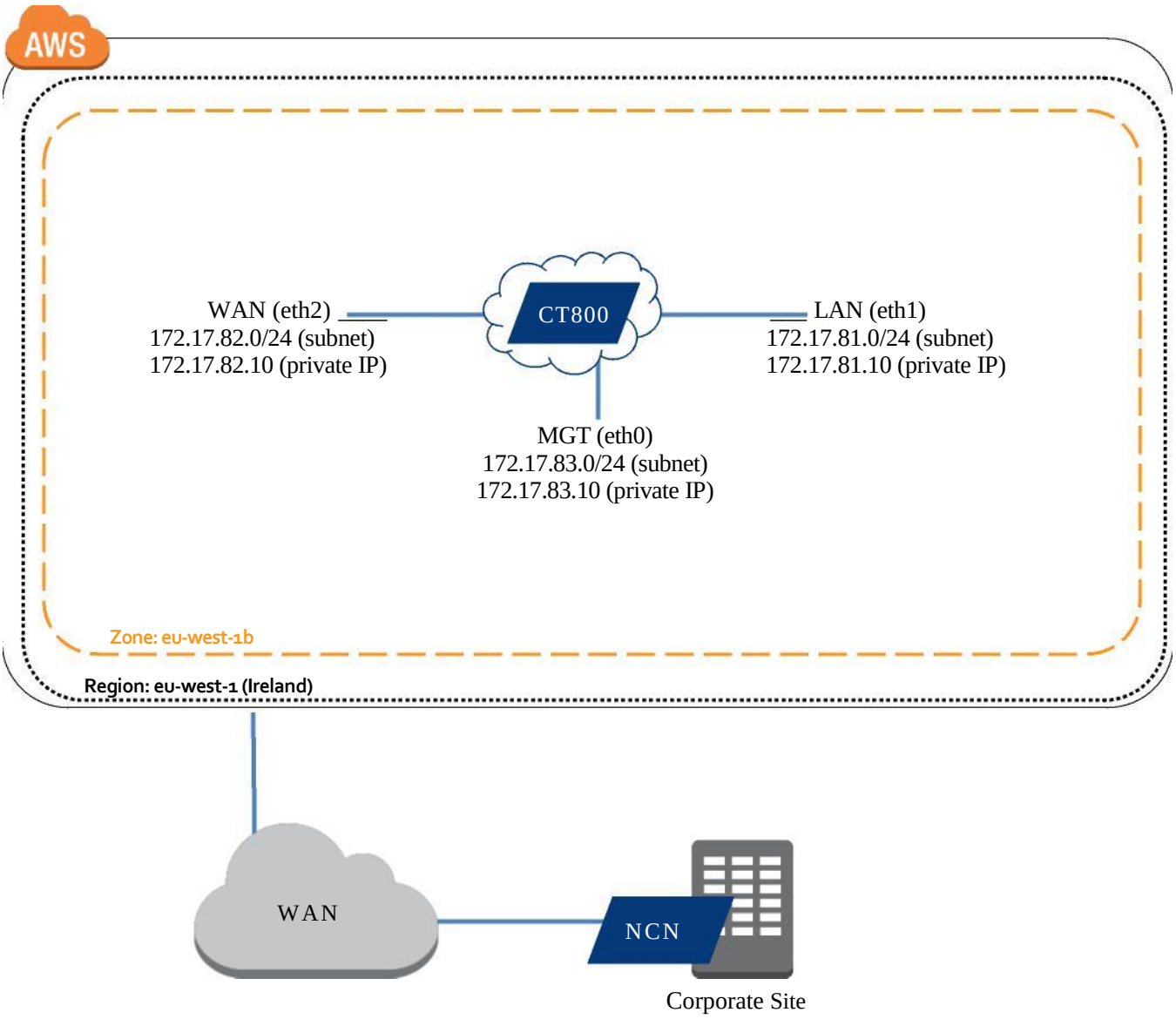
Region eu-west-1 (Ireland) is selected in the example network diagram:



Select Availability Zone

Within each Region, there are multiple Availability Zones. Each Availability Zone has different underlying hardware resources, such that events within that Availability Zone are contained within that Zone and should not impact the Region as a whole. If desired, users can deploy software resources in different Zones within the same Region in order to ensure maximum uptime. However, if performance is of most importance, resources should be deployed within the same Zone.

Availability Zone eu-west-1b is selected in the example network diagram:

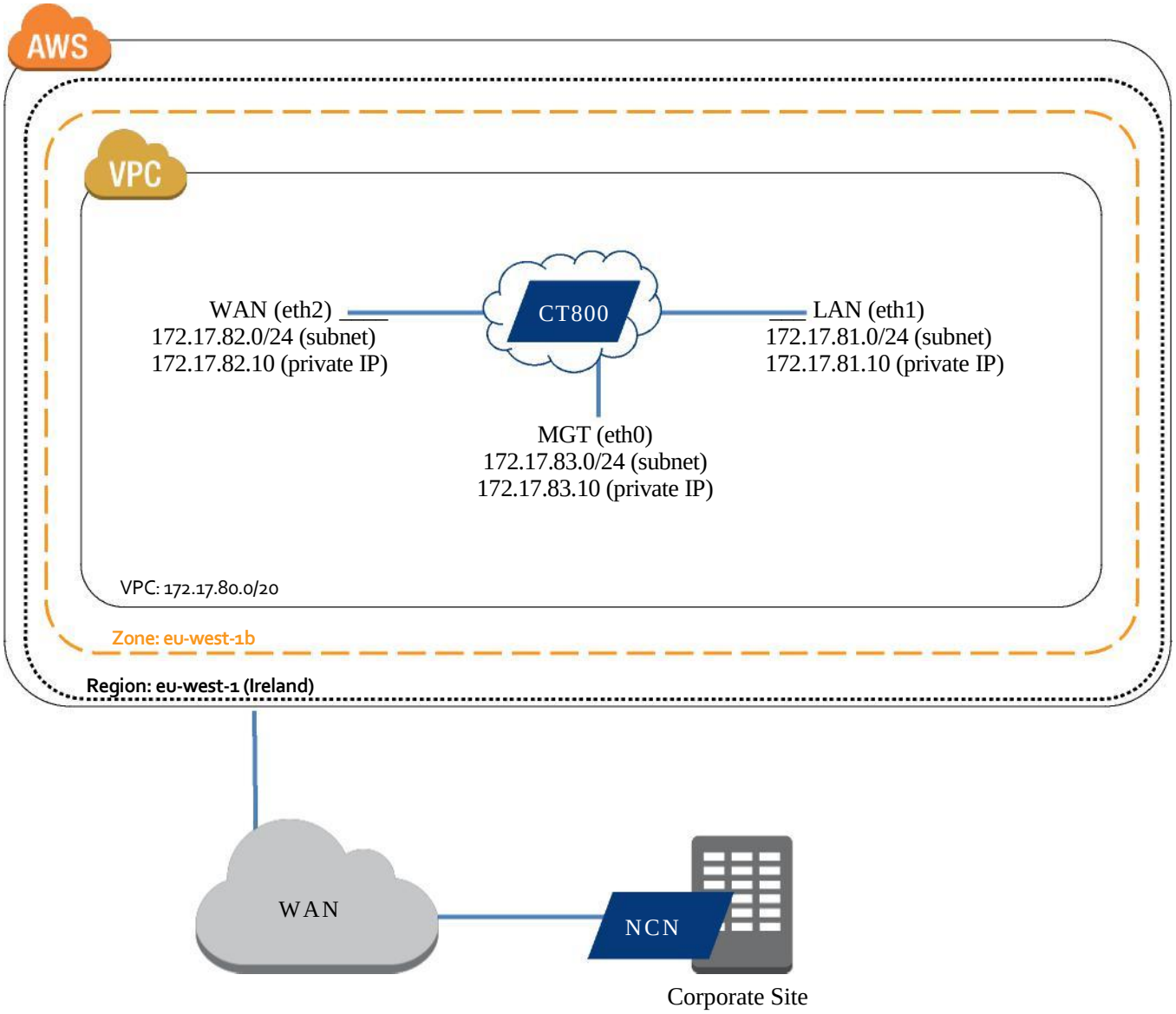


Define VPC CIDR Block

Virtual Private Clouds (VPC) enable the user to define a virtual private networks within AWS. These virtual networks closely resemble traditional networks, with the benefits of using scalable AWS infrastructure.

A Classless Inter-Domain Routing (CIDR) block must be defined for each VPC. The block of IP addresses selected should correspond to the current IP addressing scheme for the user's network and should also account for the subnets that have been selected for use by the Cloud Talari Appliance interfaces (see above).

CIDR block 172.17.80.0/20 is selected for the VPC in the example network diagram:

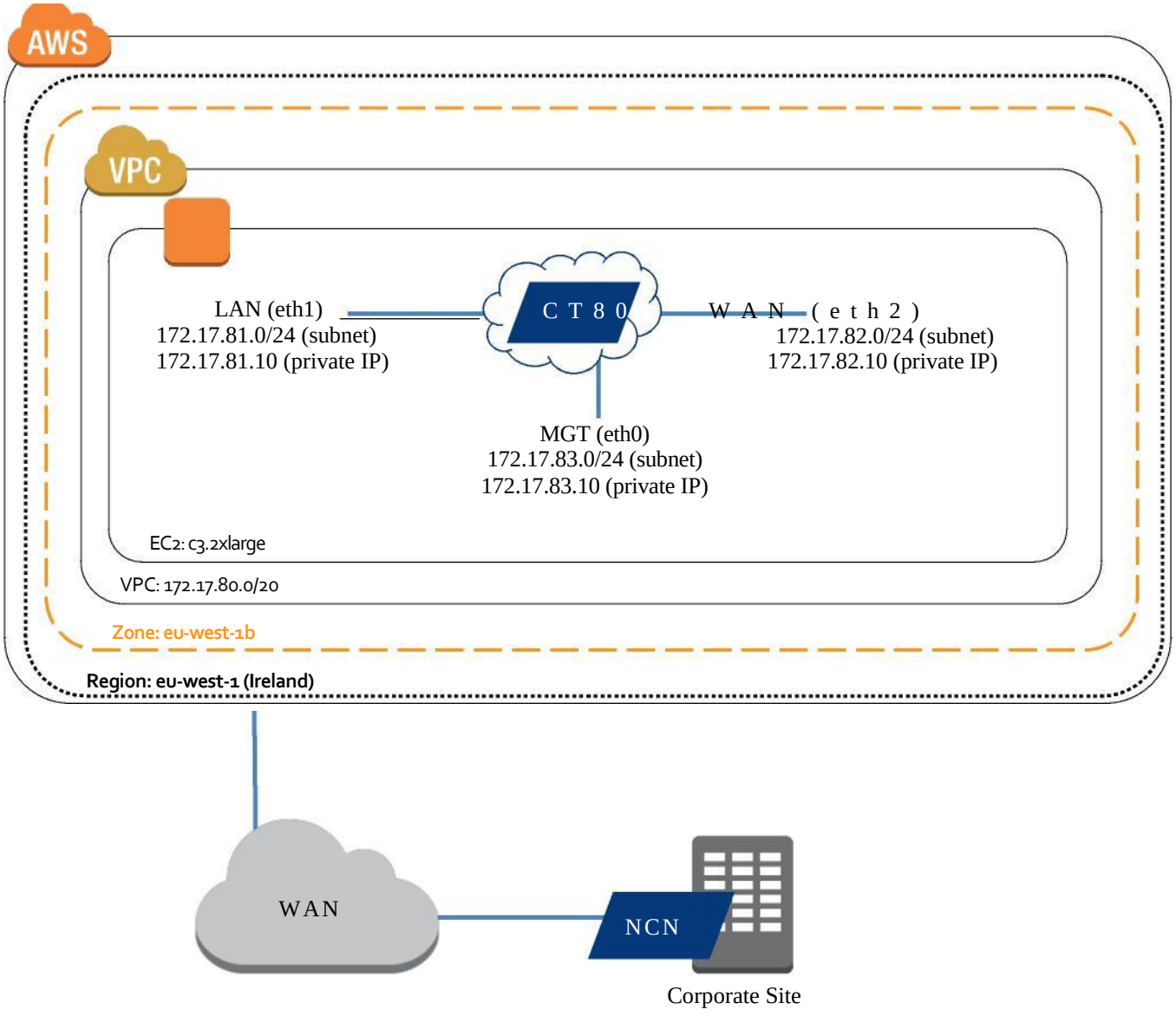


Select EC2 Instance Type

The Cloud Appliance will reside inside of an Elastic Compute Cloud (EC2). There are various types of EC2 instances. Refer to the section on Requirements (above) for guidance on which EC2 Instance Types are supported by the Cloud Appliance.

For more information on EC2 Instance Types, visit:
http://aws.amazon.com/ec2/instance-types/.

EC2 Instance Type c3.2xlarge is selected in the example network diagram:



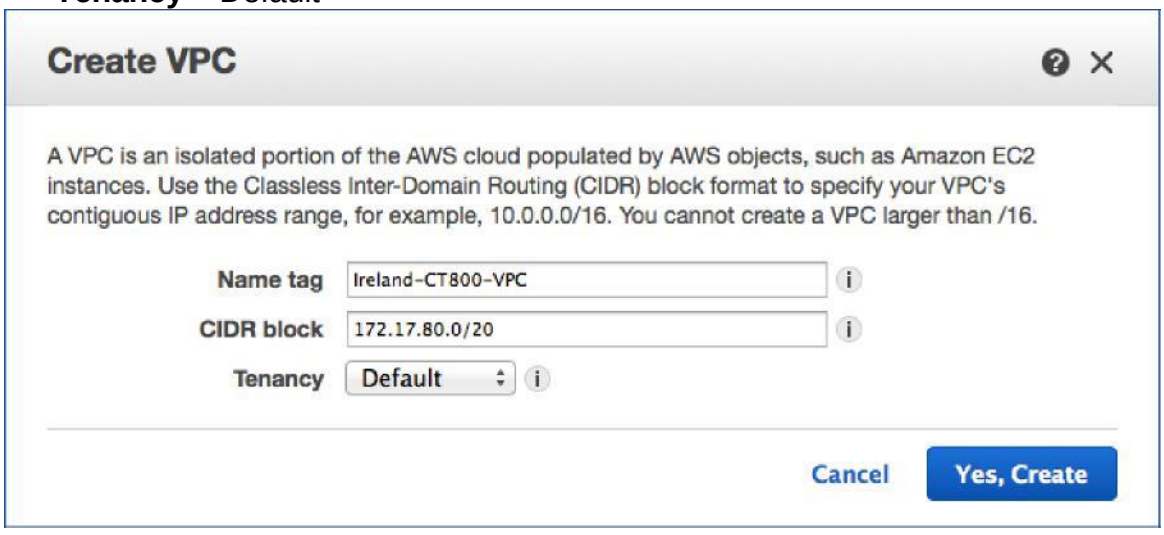
Installation

The installation process involves configuring multiple items in AWS:

1. Create a VPC
    a. Create an Internet Gateway for the VPC
    b. Create Subnets for the VPC
    c. Create Route Tables for Each Subnet
2. Create an EC2 instance
    d. Create Network Interfaces for the EC2 Instance
    e. Create Elastic IPs for the EC2 Instance
    f. Define security for the EC2 Instance and Network Interfaces
3. Connect to the MGT interface of the Cloud Talari Appliance and complete the installation

Create a VPC

1. From the top tool bar of the AWS management console, select **Services > VPC** to navigate to the VPC Dashboard.
2. From the left menu bar of the VPC Dashboard, select **Your VPCs > Create VPC** in order to create a virtual private cloud (VPC).
3. In the Create VPC dialog, enter the following information, then select **Yes, Create**:
    - **Name tag** = <A user user-defined name for the VPC>
    - **CIDR block** = <The VPC CIDR block previously defined during preparation>
    - **Tenancy** = Default



Create an Internet Gateway for the VPC

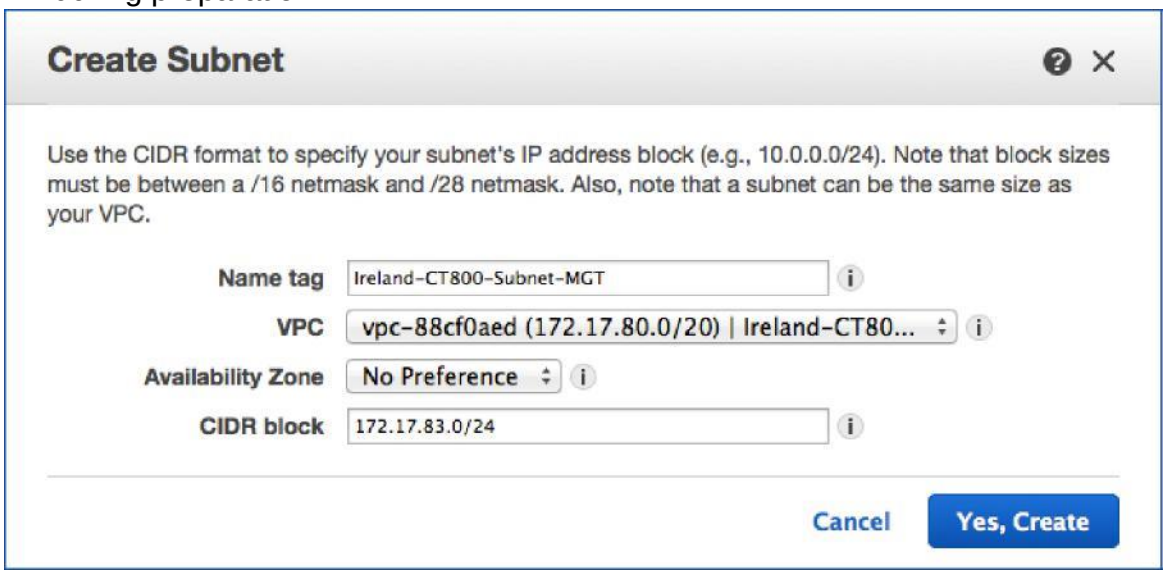
4. From the left menu bar of the VPC Dashboard, select **Internet Gateways > Create Internet Gateway** to create in Internet Gateway for the VPC.
5. In the Create Internet Gateway dialog, enter the following information, then select **Yes, Create**:
   - **Name tag** = <A user-defined name for the Internet Gateway>

6. With the newly created Internet Gateway still highlighted, select Attach to VPC to attach the Internet Gateway to the VPC:

Note: The Internet Gateway allows traffic matching the 0.0.0.0/0 route to be configured in the route table (see below). It is also required for external access to the Cloud Talari Appliance MGT interface during initial configuration.

Create Subnets for the VPC

7. From the left menu bar of the VPC Dashboard, select **Subnets > Create Subnet** to create subnets for the MGT, LAN, and WAN interfaces of the Cloud Talari Appliance.
8. In the Create Subnet dialog, enter the following information, then select **Yes, Create**:
   - **Name tag** = <A user user-defined name for the subnet>
   - **VPC** = <The VPC previously defined>
   - **Availability Zone** = <Set at your own discretion; Cloud Talari Appliance has no fixed requirement >
   - **CIDR block** = <The Subnet CIDR block previously defined during preparation>



3. Repeat this process until you have created a subnet for the MGT, LAN, and WAN interfaces of the Cloud Talari Appliance:

Name	Subnet ID	State	VPC	CIDR
Ireland-CT800-Subnet-LAN	subnet-422e8227	available	vpc-88cf0aed (172.17.80.0/20) ...	172.17.81.0/24
Ireland-CT800-Subnet-WAN	subnet-2e2d814b	available	vpc-88cf0aed (172.17.80.0/20) ...	172.17.82.0/24
Ireland-CT800-Subnet-MGT	subnet-da2c80bf	available	vpc-88cf0aed (172.17.80.0/20) ...	172.17.83.0/24

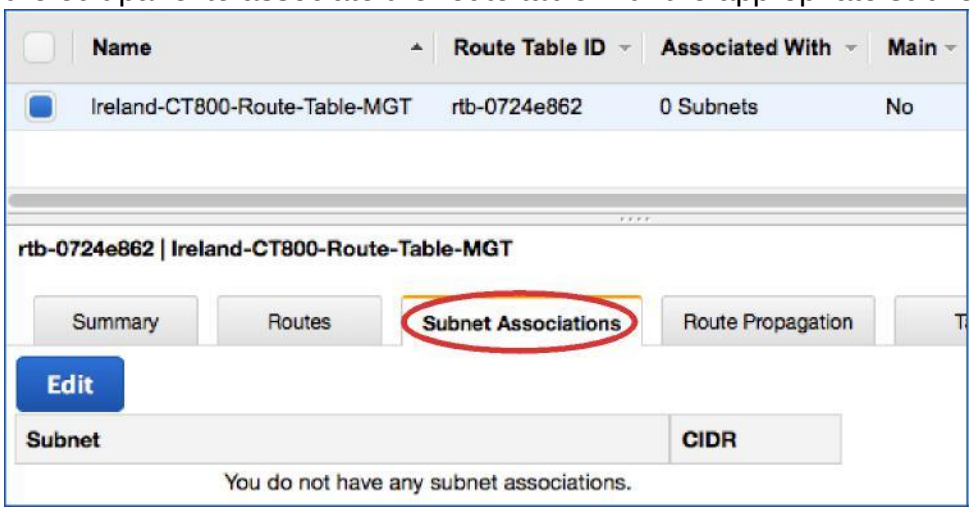
Create Route Tables for Each Subnet

9. From the left menu bar of the VPC Dashboard, **select Route Tables > Create Route Table** to create route tables for the MGT, LAN, and WAN subnets.

Note: AWS provides a global route table for the EC2 Instance but the Cloud Talari Appliance will use local route tables so that the user can control traffic forwarding to the Cloud Talari Appliance for Talari Conduit access.

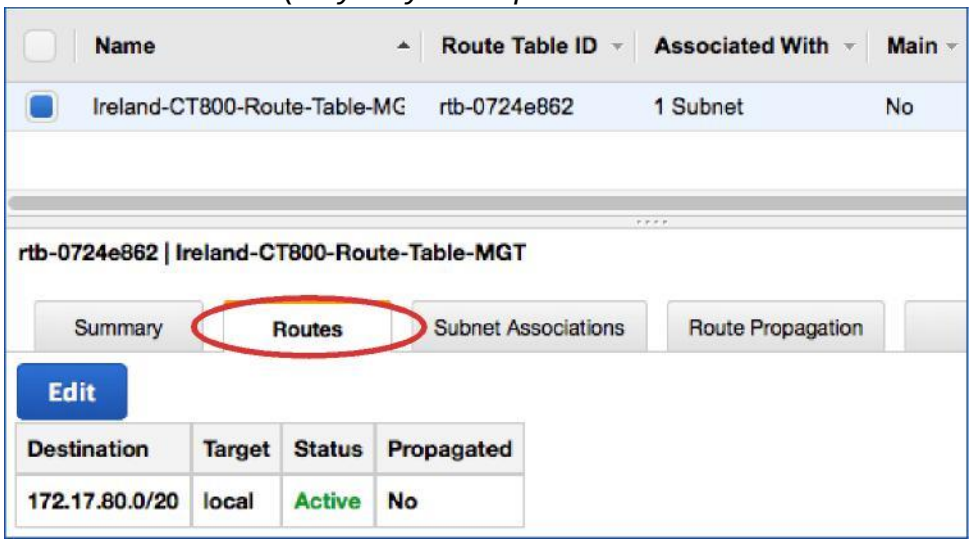
10. In the Create Route Table dialog, enter the following information, then select **Yes, Create**:
    - **Name tag** = <A user user-defined name for the route table>
    - **VPC** = <The VPC previously defined>

3. With the route table still highlighted, select **Subnet Associations > Edit** in the edit panel to associate the route table with the appropriate subnet:



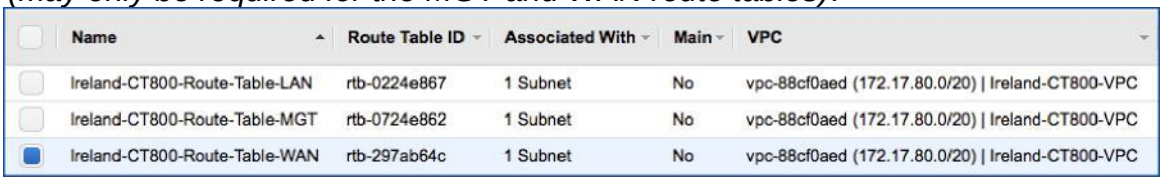
11. Select the appropriate subnet for the route table, then select **Save**.

5. With the route table still highlighted, select **Routes > Edit** in the edit panel to add route 0.0.0.0/0 *(may only be required for the MGT and WAN subnets)*.



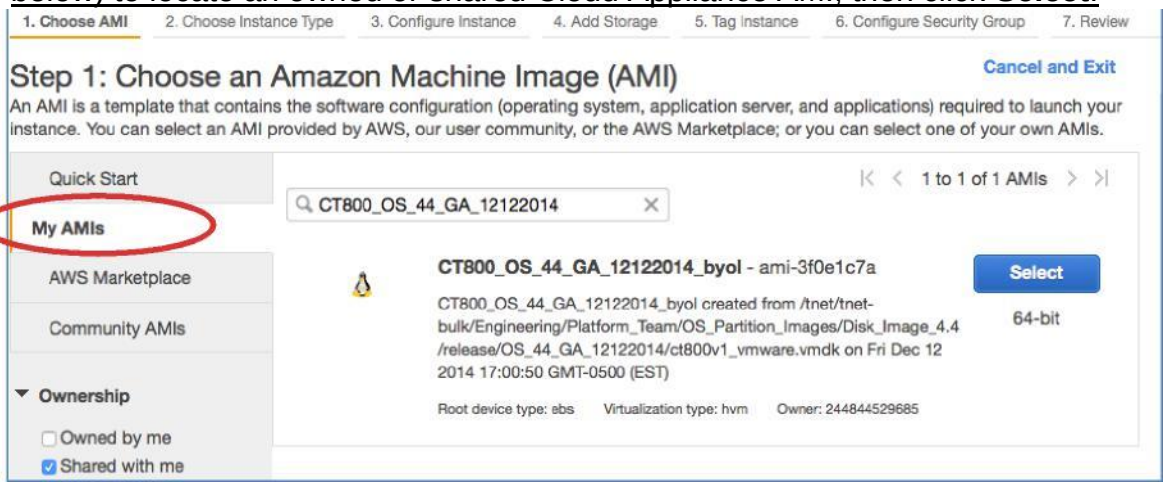
12. Enter the following information, then select **Save**:
    - **Destination** = 0.0.0.0/0
    - **Target** = <The Internet Gateway (igw-xxxxxxxx) previously defined>

7. Repeat this process until you have created route tables for the MGT, LAN, and WAN subnets, and have added route 0.0.0.0/0 to each table as appropriate *(may only be required for the MGT and WAN route tables)*.



Create an EC2 Instance

13. From the AWS tool bar, select **Services > EC2** to navigate to the EC2 dashboard.
14. From the left menu bar of the EC2 Dashboard, select **Instances > Launch Instance** to create an EC2 instance for the Cloud Appliance:
15. In the Choose AMI screen, use the **AWS Marketplace** tab to locate the Cloud Appliance Amazon Machine Image (AMI) or use the **My AMIs** tab (as shown below) to locate an owned or shared Cloud Appliance AMI, then click **Select**:

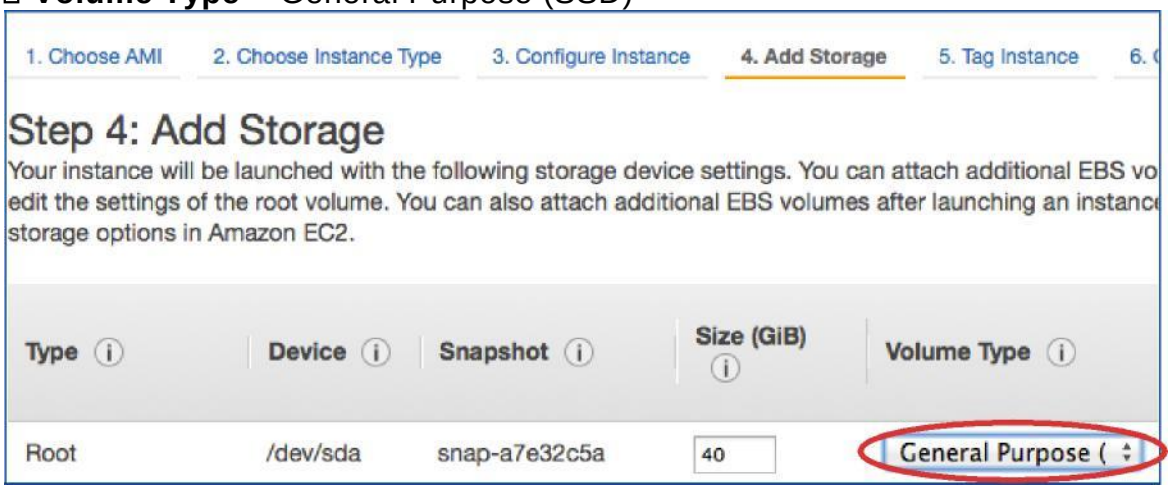


16. In the Choose Instance Type screen, select the appropriate EC2 Instance Type as determined by reference to the **AWS Resources** table, then select **Next: Configure Instance Details**.
17. In the Configure Instance Details screen, enter the following information *(anything not specified should be left unset/default)*:
    - **Number of instances** = 1
    - **Network** = <The VPC previously defined>
    - **Subnet** = <The MGT subnet >
    - **Auto-assign Public IP** = Disabled
    - **Tenancy** = Shared tenancy

IMPORTANT: You must associate the EC2 Instance with the MGT subnet in order to associate the first EC2 interface (eth0) with the Cloud Talari Appliance MGT interface. If eth0 is not associated with the Cloud Talari Appliance MGT interface, connectivity to the Cloud Talari Appliance will be lost following a reboot.

6. In the Configure Instance Details screen, under Network Interfaces, enter the following information for eth0, then select **Next: Add Storage**:
    - Primary IP = <The private IP for the MGT interface previously defined during preparation>

7. In the Add Storage screen, enter the following information for the Root storage, then select **Next: Tag Instance**:
   - **Volume Type** = General Purpose (SSD)



8. In the Tag Instance screen, give the EC2 instance a name by specifying a value for the default "Name" Tag. Create other desired Tags, then select **Next: Configure Security Group**.
18. In the Configure Security Group screen, either select an existing Security Group or create a new Security Group (depending on the user's AWS environment), then select **Review and Launch**.

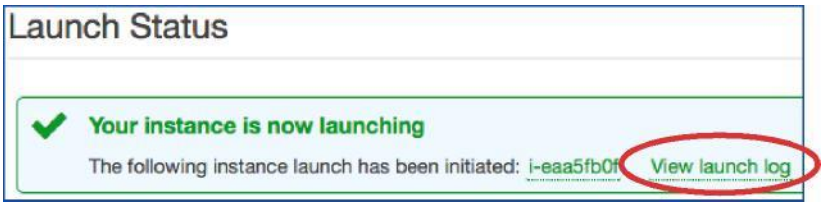
Note: A Security Group is a set of firewall rules that controls traffic for an EC2 Instance. Inbound and outbound rules can be edited during and after EC2 launch. Each EC2 Instance must have a Security Group assigned. Additionally, each Network Interface must have a Security Group assigned. Multiple Security Groups can be used to apply distinct sets of rules to individual Interfaces. The default Security Groups added by AWS only allow traffic within the VPC.

IMPORTANT: The Security Group(s) assigned to the Cloud Talari Appliance and its interfaces should at minimum accept SSH, ICMP, HTTP, and HTTPS. The Security Group assigned to the WAN interface must also accept UDP on port 2156 (for support of Talari Conduits). See AWS help for more details on Security Group configuration information.

19. In the Review Instance Launch screen, review the Instance details; then select **Launch**.
20. In the Key Pair dialog, either select an existing key pair or create a new key pair (depending on the user's AWS environment), then select **Launch Instances**.

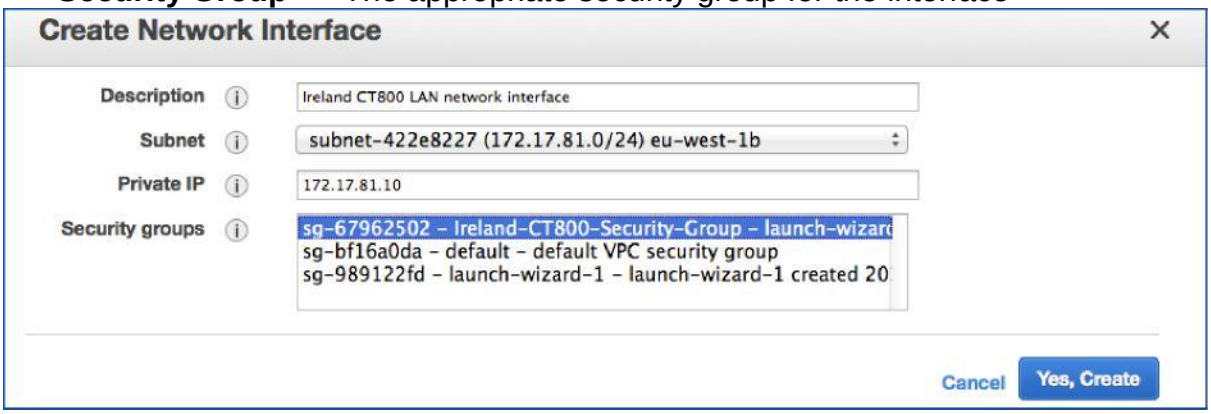
IMPORTANT: If a new key pair is created, be sure to download and store it in a safe location.

21. In the Launch Status screen, select **View launch log** to confirm that launch was successful, then return to the EC2 Dashboard:

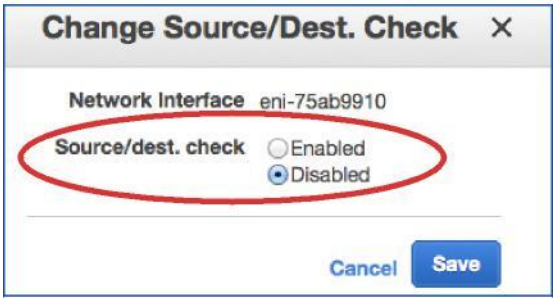


Create Network Interfaces for the EC2 Instance

22. From the left menu bar of the EC2 Dashboard select **Network Interfaces** to locate the MGT interface that was created during EC2 instance launch. Highlight the interface and edit the **Name** tag to give the interface a useful name.
23. Select **Create Network Interface** to create the WAN and LAN interfaces
24. In the Create Network Interface dialog, enter the following information, then select **Yes, Create**:
    - **Description** = <A user-defined description for the interface>
    - **Subnet** = <The subnet previously defined for the interface>
    - **Private IP** = <The private IP for the interface previously defined during preparation>
    - **Security Group** = <The appropriate security group for the interface>



    Highlight the interface and edit the **Name** tag to give the interface a useful name.
25. Highlight the interface and select **Actions > Networking > Change Source/Dest. Check** to disable **Source/dest. check**, then select **Save**:



IMPORTANT: Disabling the Source/Dest. Check attribute enables the interface to handle network traffic that isn't specifically destined for the EC2 Instance. As the Cloud Talari Appliance acts as a go-between for network traffic, the Source/Dest. Check attribute must be disabled for proper operation.

6. Repeat this process until you have Network Interfaces for MGT, LAN, and WAN, each with a Name, a Primary Private IP, and a disabled Source/Dest. Check attribute.

IMPORTANT: The Private IPs defined for these Network Interfaces must, ultimately, match the IP addresses in your APN Configuration. It may be necessary to define more than one Private IP for the WAN Network Interface if that interface will be associated with more than one WAN Link IP in the APN Configuration. This can be accomplished by defining Secondary Private IPs for the WAN Interface as needed.

26. From the left menu bar of the EC2 Dashboard select **Instances**, highlight the new EC2 Instance, then select **Actions > Networking > Attach Network Interface** to attach *first* the LAN Network Interface and *then* the WAN Network Interface to the EC2 Instance.

IMPORTANT: Attaching MGT, LAN, and WAN in that order attaches to eth0, eth1, and eth2 in the EC2 Instance. This aligns with the mapping inside the Cloud Appliance and will ensure that interfaces are not re-assigned incorrectly in the event of a Cloud Appliance reboot

Create Elastic IPs for the EC2 Instance

27. From the left menu bar of the EC2 Dashboard select **Elastic IPs > Allocate New Address** to create two new Elastic IPs (EIPs)
28. Highlight one EIP and select **Associate Address** to associate the EIP with the MGT interface. Repeat this process to associate the other EIP with the WAN interface.

Elastic IP	Instance	Private IP Address	Scope
54.171.133.120	i-eaa5fb0f (Ireland-CT800)	172.17.82.10	vpc-88cf0aed
54.171.70.113	i-eaa5fb0f (Ireland-CT800)	172.17.83.10	vpc-88cf0aed

Connect to the Cloud Appliance MGT Interface

1. Open a new browser window and navigate to the Elastic IP (EIP) of the MGT Interface (you may need to create a security exception if the security certificate is not recognized).

Note: If the MGT interface cannot be reached, check the following:

- Make sure the EIP is correctly associated with the MGT interface.
- Make sure the EIP responds to ping.
- Make sure the MGT interface Route Table includes an Internet Gateway route (0.0.0.0/0).
- Make sure the MGT interface Security Group allows HTTP/HTTPS/ICMP/SSH.

2. Login to talariuser using ssh to the Cloud Talari Appliance, using the key pair you entered in step #20

Note: This is only applicable if you are running OS 7.0.3 or later.

3. Change the talariuser password (sudo passwd talariuser)

4. Login to the Cloud Talari Appliance web UI with the following credentials:
- **Username** = talariuser
- **Password** = password entered in previous step

Note: User may also login to the Cloud Appliance console using "ssh talariuser@<*mgt-elastic-ip*>," assuming that the key pair for the EC2 Instance has been added to the user's SSH key chain.

Cloud Appliance: CT800/CT800-128 Requirements and Installation Guide

Add the Cloud Appliance to Your Network

Add the Cloud Appliance to your Talari Adaptive Private Network (APN) by adding it as a new Site to your APN Configuration, generating an appliance package (APN Software + APN Configuration) for the Site, and installing the appliance package on the Cloud Talari Appliance. Contact Talari Support if you need assistance (http://www.talari.com/support).

Note: When the Cloud Appliance is added to your APN, a Talari Conduit will be established between the Cloud Appliance and the Network Control Node (NCN). This will allow you to manage the Cloud Appliance via the WAN interface (over the Conduit) instead of via direct connection to the MGT interface.

Note: A Private IP must be defined on the EC2 WAN Network Interface for every WAN Link IP in the APN Configuration. This can be accomplished by defining one or more Secondary Private IPs for the Network Interface as necessary.

Note: EC2 Instance Ethernet interfaces map to Cloud Talari Appliance ports as follows:

- EC2 Instance eth0 --> mgt0 (MGT)
- EC2 Instance eth1 --> port1 (LAN)
- EC2 Instance eth2 --> port2 (WAN)

Configure the Cloud Appliance for Management via the WAN Interface

Once a Talari Conduit has been established between the Cloud Appliance and the NCN (see previous step), the MGT interface can be accessed through the Elastic IP (EIP) of the WAN interface if the route tables are set up correctly. Doing so will allow management traffic to utilize the Talari Conduits and will allow the EIP of the MGT interface to be removed, if the user desires to limit the expense of extra EIPs.

29. From the left menu bar of the VPC Dashboard, select **Routes Tables**, highlight the MGT route table previously defined for the VPC, then select **Routes > Edit** in the edit panel to add routes for management traffic that point to the LAN interface. When complete, select **Save**.
30. Repeat this process for the LAN route table, so that there are routes for management traffic that point to the LAN interface.