

Panorama on AWS

DEPLOYMENT GUIDE

JUNE 2020



Table of Contents

Preface	1
Purpose of This Guide	3
Objectives	3
Audience	3
Related Documentation	4
Deployment Overview	5
Deployment Considerations	5
Design Model	6
On-Premises Panorama with Dedicated Log Collectors in the Cloud	7
Panorama Management in AWS with Cortex Data Lake	7
Panorama Management and Log Collection in AWS	8
Panorama Device Administration	9
Panorama Operational Considerations	11
Assumptions and Prerequisites	12
Deployment Details for Panorama on AWS Infrastructure	13
Configuring the VPC, Subnet, and Services	13
Deploying a Panorama Server on AWS	19
Deployment Details for Panorama System and Services	26
Updating Panorama System and Activating Services	26
Next Steps: Configuring Network Templates and Policies	35

Preface

GUIDE TYPES

Overview guides provide high-level introductions to technologies or concepts.

Reference architecture guides provide an architectural overview for using Palo Alto Networks® technologies to provide visibility, control, and protection to applications built in a specific environment. These guides are required reading prior to using their companion deployment guides.

Deployment guides provide decision criteria for deployment scenarios, as well as procedures for combining Palo Alto Networks technologies with third-party technologies in an integrated design.

DOCUMENT CONVENTIONS



Notes provide additional information.



Cautions warn about possible data loss, hardware damage, or compromise of security.

Blue text indicates a configuration variable for which you need to substitute the correct value for your environment.

In the IP box, enter **10.5.0.4/24**, and then click **OK**.

Bold text denotes:

- Command-line commands.

show device-group branch-offices

- User-interface elements.

In the **Interface Type** list, choose **Layer 3**.

- Navigational paths.

Navigate to **Network > Virtual Routers**.

- A value to be entered.

Enter the password **admin**.

Italic text denotes the introduction of important terminology.

An *external dynamic list* is a file hosted on an external web server so that the firewall can import objects.

Highlighted text denotes emphasis.

Total valid entries: **755**

ABOUT PROCEDURES

These guides sometimes describe other companies' products. Although steps and screen-shots were up-to-date at the time of publication, those companies might have since changed their user interface, processes, or requirements.

GETTING THE LATEST VERSION OF GUIDES

We continually update reference architecture and deployment guides. You can access the latest version of this and all guides at this location:

<https://www.paloaltonetworks.com/referencearchitectures>

WHAT'S NEW IN THIS RELEASE

Palo Alto Networks made the following changes since the last version of this guide:

- Changed the version of Panorama™ PAN-OS® to version 9.1.2
- Changed the version of the Cloud Services plugin to version 1.6.0
- Modified the deployment so that Panorama is in a dedicated Management Project
- Moved the details on how to configure Panorama device groups, templates, and template stacks to the AWS Single VPC and AWS Transit Gateway Deployment Guides
- Changed phrasing, terminology, and diagrams for clarity

Purpose of This Guide

This guide provides deployment information for the Palo Alto Networks Panorama centralized management system for the Palo Alto Networks family of next-generation firewalls on Amazon Web Services (AWS) public cloud.

This guide:

- Provides architectural guidance and deployment details for using the Panorama management system, deployed on AWS, to provide a single location from which you can create network configurations and security policies that enable visibility, control, and protection to your applications built in the AWS public cloud.
- Requires that you first read the [Securing Applications in AWS: Reference Architecture Guide](#). The reference architecture guide provides design insight and guidance necessary for your organization to plan linkage of pertinent features with the next-generation firewall in a resilient design, and then how to manage the environment with Panorama.
- Provides deployment details for the Panorama management system.

OBJECTIVES

Completing the procedures in this guide, you are able to successfully deploy a Palo Alto Networks Panorama management system on the AWS environment. You also enable the following functionality:

- Centralized management point for the firewalls on the AWS public cloud, and if desired, managing firewalls in other parts of your organization's network.
- Resilient design with primary and secondary Panorama systems each deployed in a separate AWS Availability Zone.
- Centralized logging with Cortex™ Data Lake, which also enables cloud-delivered security analytics.

AUDIENCE

This guide is written for technical readers, including system architects and design engineers, who want to deploy Palo Alto Networks Panorama within a public cloud datacenter infrastructure. It assumes the reader is familiar with the basic concepts of applications, networking, virtualization, security, and high availability, as well as a basic understanding of network architectures.

To be successful, you must have a working knowledge of networking and policy in PAN-OS.

RELATED DOCUMENTATION

The following documents support this guide:

- [Securing Applications in AWS: Reference Architecture Guide](#)—Presents a detailed discussion of the available design considerations and options for securing data and applications in the AWS public cloud infrastructure.
- [Securing Applications in AWS Single VPC: Deployment Guide](#)—Details the deployment of the Single Virtual Private Cloud (VPC) design model, which is well-suited for initial deployments and proof of concepts of Palo Alto Networks VM-Series firewalls on AWS. This guide describes deploying VM-Series firewalls to provide visibility and protection for the VPC's inbound and outbound traffic.
- [Securing Applications in AWS Transit Gateway: Deployment Guide](#)—Details the deployment of the Transit Gateway design model. This model provides a hub-and-spoke design for centralized and scalable firewall services for resilient inbound, outbound, and east-west traffic flows. This guide describes deploying the VM-Series firewalls to provide protection and visibility for traffic flowing through the transit gateway.

Deployment Overview

The [Securing Applications in AWS: Reference Architecture Guide](#) describes AWS concepts that provide a cloud-based infrastructure as a service and how the Palo Alto Networks VM-Series firewalls can complement and enhance the security of applications and workloads in the cloud. The design models presented in that guide provide visibility and control over traffic to the applications in AWS, outbound to on-premises or internet services and east-west flows internal to the AWS.

To reduce the time required to manage multiple devices, maintain consistency of configurations, and deploy security policy changes rapidly, Palo Alto Networks Panorama central management is included in the design. Panorama enables you to manage all the key features of the Palo Alto Networks next-generation firewalls using a model that provides central oversight and local control. You can deploy Panorama as either a hardware appliance or virtual appliance on-premise. You can also deploy it as a virtual appliance in the public cloud.

DEPLOYMENT CONSIDERATIONS

Before deploying Panorama, consider the following factors:

- **Where to deploy the Panorama management system(s)**—Many organizations have an existing on-premises Panorama system that is managing the firewalls in data centers and perhaps remote sites. They can use this Panorama system to manage the firewalls in the cloud, providing that there is a robust encrypted transport to the cloud firewalls. Panorama deployed in the cloud benefits from being inside of the provider's robust network and reduces charges for data that needs to go to/from the cloud for managing the environment. Depending on size and scale projections, you may choose to deploy Panorama systems in both locations and interconnect the systems. This guide focuses on a cloud deployment of Panorama.
- **Where to deploy logging**—Transporting log data from a number of firewalls in the cloud can be an expensive operation due to the cost of transport. You can deploy dedicated logging inside of the cloud deployment even Panorama is not in the cloud. Alternatively, moving to Cortex Data Lake offers more than just a storage location option for your firewall logs; it also provides visibility for a host of network forensics tools.
- **Resilience and availability**—What are the management requirements for availability? You can deploy Panorama as a single instance or a high availability (HA) pair operating in a primary/secondary role to reduce downtime and data loss in the event of a failure. Panorama HA instances can operate in different availability zones for enhanced availability. This guide demonstrates a high availability deployment.
- **System Access**—IP access to the Panorama system is required to deploy and operate Panorama. You should use network tools like access control lists (ACLs) and security grouping to limit the IP addresses that can access Panorama management to those required by your organization. You can pare the application ports allowed to connect to Panorama to those required for central management operation.

Design Model

The best method for ensuring up-to-date firewall configuration is to use Panorama for the central management of firewall policies. Panorama simplifies consistent policy configuration across multiple independent firewalls through its device group and template stack capabilities. When multiple firewalls are part of the same device group, they receive a common ruleset. Because Panorama enables you to control all of your firewalls—whether they are on-premises or in the public cloud or whether they are a physical or virtual appliance—device groups also provide configuration hierarchy. With device group hierarchy, lower-level groups include the policies of the higher-level groups. Configuration hierarchy allows you to configure consistent rulesets that apply to all firewalls, as well as consistent rulesets that apply to specific firewall deployment locations such as the public cloud.

As bootstrapped firewalls deploy, they can also automatically pull configuration information from Panorama. VM-Series firewalls use a VM authorization key and a Panorama IP address in the bootstrap package to authenticate and register to Panorama on its initial boot. You must generate the VM authorization key in Panorama before creating the bootstrap package. If you provide a device group and template in the basic configuration file of the bootstrap package, Panorama can assign the firewall to the appropriate device group and template so that the relevant rulesets are applied. You can manage the device in Panorama going forward.

You can deploy Panorama in your on-premises data center or in a public cloud environment such as AWS. When deployed in your on-premises data center, Panorama can manage all the PA-Series and VM-Series firewalls in your organization. If you want a dedicated instance of Panorama to manage the VM-Series firewalls deployed on AWS, deploy Panorama on AWS.

When you have an existing Panorama deployment on-premises for firewalls in your data center and internet edge, you can use it to manage the VM-Series firewalls in AWS. Beyond management, you need to consider your firewall log collection and retention. Log collection, storage, and analysis is an important cybersecurity best practice that organizations perform to correlate potential threats and prevent successful cyber breaches. Panorama allows you to separate firewall management from log collection, if necessary.

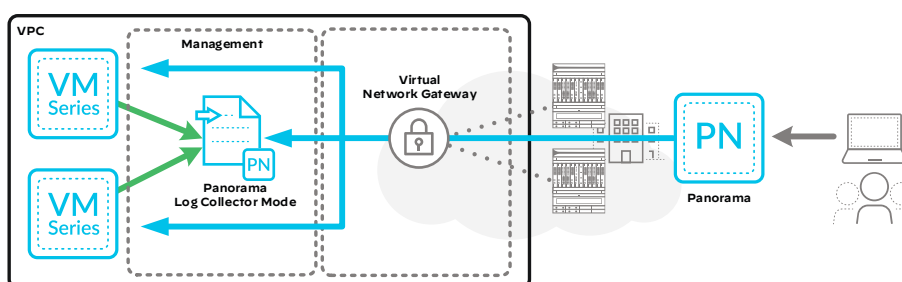
The following three deployment mode options are available for Panorama:

- **Log Collector mode**—One or more log collectors collect and manage logs from the managed devices. This mode assumes that another deployment of Panorama is operating in Management-Only mode.
- **Management-Only mode**—Panorama manages configurations for the managed devices but does not collect or manage logs.
- **Panorama mode**—Panorama controls both policy and log management functions for all the managed devices.

ON-PREMISES PANORAMA WITH DEDICATED LOG COLLECTORS IN THE CLOUD

Sending logging data back to the on-premises Panorama can be inefficient, costly, and pose data privacy and residency issues in some regions. An alternative to sending the logging data back to your on-premises Panorama is to deploy Panorama-dedicated log collectors on AWS and use the on-premises Panorama for management. Deploying a dedicated log collector on AWS reduces the amount of logging data that leaves the cloud but still allows your on-premises Panorama to manage the VM-Series firewalls in AWS and have full visibility to the logs as needed.

Figure 1 Panorama Log Collector mode in AWS

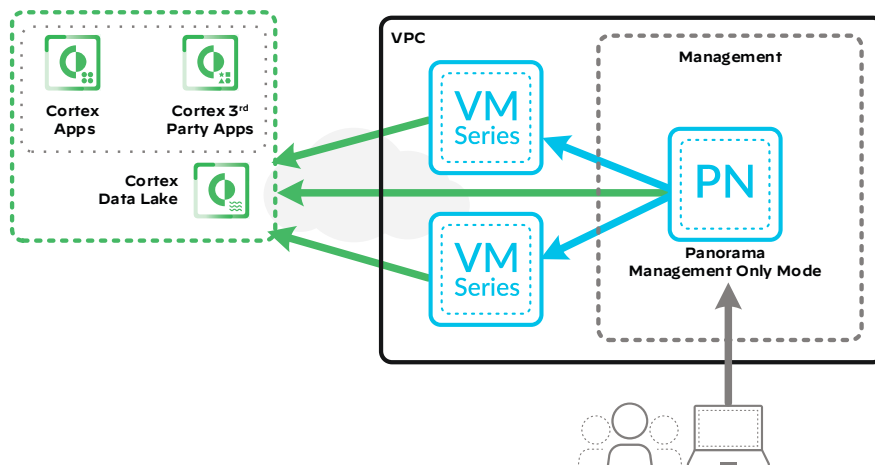


PANORAMA MANAGEMENT IN AWS WITH CORTEX DATA LAKE

There are two design options when deploying Panorama management on AWS. First, you can use Panorama for management only and use Palo Alto Networks Cortex Data Lake to store the logs generated by the VM-Series firewalls. *Cortex Data Lake* is a cloud-based log collector service that provides resilient storage and fast search capabilities for large amounts of logging data. Cortex Data Lake emulates a traditional log collector. The VM-Series firewalls encrypt the logs and then send them to Cortex Data Lake over TLS/SSL connections. Cortex Data Lake allows you to scale your logging storage as your AWS deployment scales because Cortex bases licensing on storage capacity and not the number of devices sending log data.

The benefit of using Cortex Data Lake goes well beyond scale and convenience when tied into the Palo Alto Networks Cortex AI-based continuous security platform. Cortex is a scalable ecosystem of security applications that can apply advanced analytics in concert with Palo Alto Networks enforcement points to prevent the most advanced attacks. Palo Alto Networks analytics applications, such as Cortex XDR and AutoFocus™, as well as third-party analytics applications that you choose, use Cortex Data Lake as the primary data repository for all of Palo Alto Networks offerings.

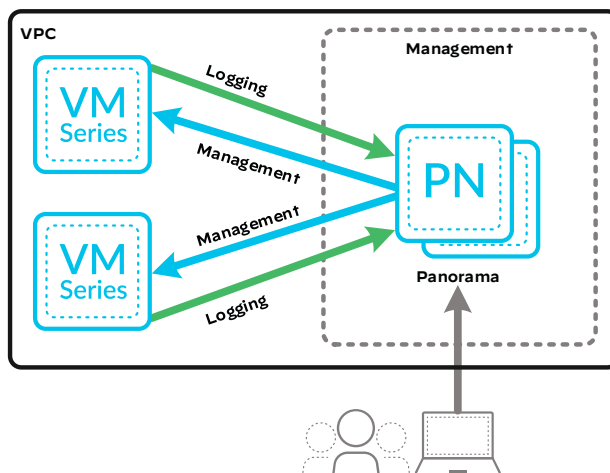
Figure 2 Panorama management and Cortex Data Lake



PANORAMA MANAGEMENT AND LOG COLLECTION IN AWS

Second, you can use Panorama for both management and log collection. You can deploy the management and log collection functionality as a shared virtual appliance or on dedicated virtual appliances. For smaller deployments, you can deploy Panorama and the log collector as a single virtual appliance. For larger deployments, a dedicated log collector per region allows traffic to stay within the region and reduce outbound data transfers.

Figure 3 Panorama management and log collection in AWS



Panorama is available as a virtual appliance for deployment on AWS and supports Management-Only mode, Panorama mode, and Log Collector mode with the system requirements defined in Table 1. Panorama on AWS is only available with a BYOL licensing model.

Table 1 Panorama virtual appliance on AWS

	Management-Only	Panorama	Log Collector
Minimum system requirements	16 CPUs 32GB memory 81GB system disk	16 CPUs 32GB memory 2TB to 24TB log storage capacity	16 CPUs 32GB memory 2TB to 24TB log storage capacity

PANORAMA DEVICE ADMINISTRATION

The time it takes to deploy changes across 10s or 100s of firewalls can be costly in the number of employees required, as well as the delay projects experience while employees wait for the process to complete. In addition to time, errors can increase when network and security engineers program changes firewall-by-firewall. Panorama provides several tools for centralized administration that can reduce time and errors for your firewall management operation.

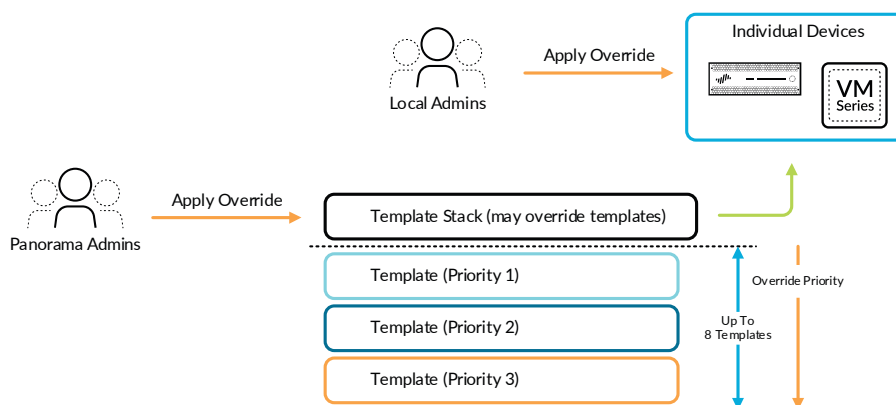
Templates/Template Stacks

Panorama manages common device and network configuration through templates. You can use templates to manage configuration centrally and then push the changes to all managed firewalls. This approach avoids making the same individual firewall change repeatedly across many devices. Templates are grouped within a template stack, and the stack is applied to selected firewalls.

You can define common building blocks for device and network configuration within a template. These building blocks are logically combined by adding them to a template stack. If there are no overlapping parameters, then the stack reflects the combination of all the individual templates. If there is overlap, then the settings from the highest priority template take precedence. You may override the template settings at the stack level. A local administrator may also perform overrides directly on an individual device if necessary.

Firewall-specific settings such as IP addresses must be unique per-device. Instead of using overrides, these settings may be managed using variables within templates. Panorama manages the variable assignments at deployment time, either on a per-device basis through manual assignment or in bulk by importing a spreadsheet with the settings for multiple devices.

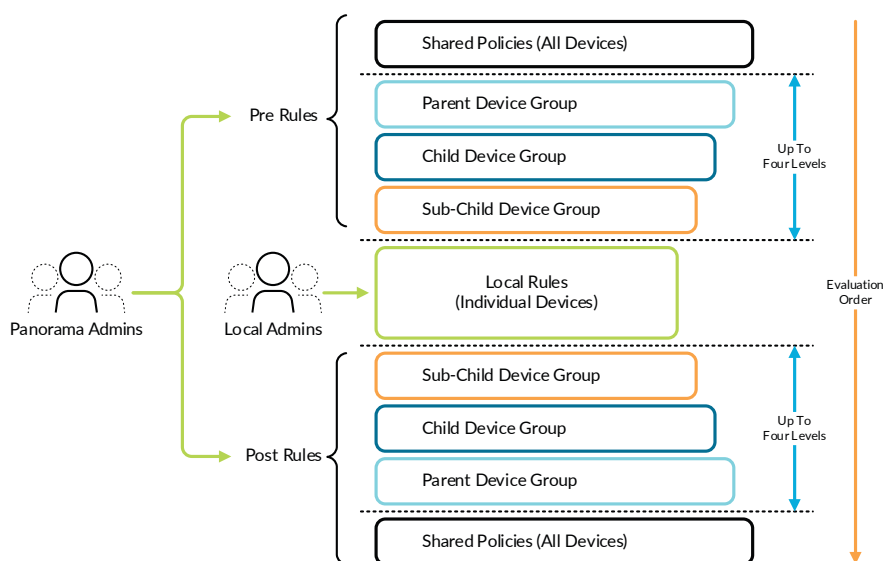
Figure 4 Panorama template stack and templates



Hierarchical Device Groups

Panorama manages common policies and objects through hierarchical device groups. You use multi-level device groups to centrally manage the policies across all deployment locations with common requirements. For example, device groups may be determined geographically, such as Europe and North America. Also, each device group can have a functional sub-device group (for example, perimeter or data center).

Figure 5 Panorama device groups and policy evaluation



You can define shared policies for central control while granting your local firewall administrator the autonomy to make specific local adjustments. At the device group level, you can create common policies that are defined as the first set of rules (pre-rules) and the last set of rules (post-rules) to be evaluated against match criteria. You can view pre- and post-rules on a managed firewall, but they can only be edited in Panorama in the context of the defined administrative roles. You can edit local device rules (those between pre- and post-rules) by either your local firewall administrator or by a Panorama administrator who has switched to a local firewall context. In addition, you can reference shared objects defined by a Panorama administrator in locally managed device rules.

Role-based administration delegates feature-level access, including availability of data (enabled, read-only, or disabled and hidden from view), to different members of your staff. You can give specific individuals access to tasks that are pertinent to their job while making other tasks either hidden or read-only.

As your deployment grows in size, you can make sure updates are sent to downstream boxes in an organized manner. For instance, you may prefer to centrally qualify a software update before it is delivered via Panorama to all production firewalls at once. Using Panorama, you can centrally manage the update process for software updates, content application updates, antivirus signatures, threat signatures, URL-filtering database, and licenses.

Panorama can also integrate with your IT workflow applications. When a log is generated on the next-generation firewall, Panorama can trigger actions and initiate workflows through HTTP-based APIs. Selective log forwarding allows you to define the criteria to automate a workflow or an action.

PANORAMA OPERATIONAL CONSIDERATIONS

Panorama on AWS Licensing

Panorama on AWS is available in a bring your own license (BYOL) and is composed of a license that you purchase from a channel partner. Panorama on AWS supports all deployment modes (Panorama, Log Collector, and Management Only), and shares the same processes and functionality as the M-Series hardware appliances. When using BYOL, you license Panorama like a traditionally deployed appliance, registering it on the Palo Alto Customer Support web site prior to implementation. After the Panorama instance is initialized and accessible, you must apply a licensed serial number for operation. After you apply the serial number to the device, the device registers with the Palo Alto Networks support portal and obtains information about its capacity and subscriptions.

System Access Control

When running the Panorama management system on AWS, you should use AWS security groups and network ACLs to restrict Panorama to management communications to needed ports and IP address ranges. Panorama should have dedicated public IP access so that you can always reach the firewalls in the transit using private IP addressing within the VPC, and you should use security groups to restrict outside access to Panorama to only those ranges in use by your organization to manage the firewalls. If you are not using Panorama, you need public IP addresses on the Transit firewall management interfaces or a jump host in the VPC.

Assumptions and Prerequisites

AWS:

- This design uses two Elastic IP (EIP) addresses. Ensure that you have available EIP addresses in the AWS region into which you will deploy.
- You will deploy one or two AWS instances for Panorama.
- This deployment was tested predominantly in the US West (Oregon) region, although deploying this design should be possible in any AWS region.

Palo Alto Networks Panorama:

- The tested PAN-OS version in this guide is 9.1.2.
- Panorama is implemented in Management-Only mode.
- Cortex Data Lake is provisioned for logging.
- The Cloud services plugin for Panorama tested was version 1.6.0.

Palo Alto Networks licensing:

- Your organization has licenses for Panorama primary and secondary (if used) servers. Panorama in AWS requires BYOL at this time.
- Cortex Data Lake requires a license with sufficient storage for your expected retention period. Cortex Data Lake requires an authentication code and a Panorama system associated to the service. This guide uses a Cortex Data Lake hosted in the Americas region.

Deployment Details for Panorama on AWS Infrastructure

Although an account may have existing AWS VPCs where you plan to deploy your Panorama VM, this section describes some settings specific for Panorama VM deployment.

The first set of procedures sets up an AWS VPC for Panorama operation:

- When deploying Panorama VM in high availability (HA) mode, you need two availability zones, one for each Panorama instance.
- The Panorama console is accessible from outside of the AWS VPC and uses a public IP per instance and an Internet Gateway (IGW).
- Route tables for Panorama need to be programmed for internet access, typically via an IGW.

Follow all sections, or review the necessary sections, in the following procedure to program your VPC settings for correct operation to support Panorama VM.

The second set of procedures deploys the Panorama system as a VM on AWS and prepares the instance for IP communications.



Automation

If you do not want to manually complete the steps outlined in this guide, an alternate deployment method that uses automation to provision and configure the cloud infrastructure and Palo Alto Networks components is available at https://www.github.com/paloaltonetworks/reference_architecture_automation.

Procedures

Configuring the VPC, Subnet, and Services

- 1.1 Create the VPC
- 1.2 Create IP Subnets
- 1.3 Create a VPC Internet Gateway
- 1.4 Create the VPC Route Tables
- 1.5 Create VPC Security Groups

All resources in this guide were created and tested in the AWS US West (Oregon) region. You should change to the AWS region most suitable for your deployment. In this procedure group, you create the VPC, subnets, and security groups to support the instances.

1.1 Create the VPC

In this procedure, you create a VPC named Management.

Step 1: Sign in to the console at <https://console.aws.amazon.com>, and then from the list at the top of the page, choose **US West (Oregon)** region.

Step 2: Navigate to **Services > Networking & Content Delivery > VPC**.

Step 3: In **Virtual Private Cloud > Your VPCs**, click **Create VPC**.

Step 4: In the **Name tag** box, enter **Management**.

Step 5: In the **IPv4 CIDR block** box, enter the IP address and mask **10.255.0.0/16**.

Step 6: Click **Create**, and then click **Close**.

Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an IPv6 CIDR block with the VPC.

Name tag ⓘ

IPv4 CIDR block* ⓘ

IPv6 CIDR block ☒ No IPv6 CIDR Block ⓘ
☐ Amazon provided IPv6 CIDR block
☐ IPv6 CIDR owned by me

Tenancy ⓘ

* Required Cancel **Create**

Next, you enable the assignment of public DNS hostnames for the virtual machines (*instances*) that you create in your VPC. If you do not enable DNS hostnames, you may or may not be assigned a public DNS hostname depending on the DNS attributes of your VPC and if your instance has a public IP address.

Step 7: In the **VPC Dashboard**, select **Management**, click the **Actions** list, and then choose **Edit DNS Hostnames**.

Step 8: For **DNS hostnames**, select **Enable**.

Step 9: Click **Save**, and then click **Close**.

1.2 Create IP Subnets

The initial IPv4 IP address block should be broken up into subnets. Only IP address space in the configured CIDR space(s) can be assigned to a subnet.

Table 2 IP subnets

Subnet name	Availability zone	IPv4 CIDR block
Management-2a	us-west-2a	10.255.0.0/24
Management-2b	us-west-2b	10.255.1.0/24

Step 1: On the VPC dashboard, navigate to **Virtual Private Cloud > Subnets**.

Step 2: At the top of the pane, click **Create subnet**.

Step 3: In the **Name tag** box, enter **Management-2a**.

Step 4: In the **VPC** list, choose **Management**.



Note

When selecting a VPC, the VPC list shows both the VPC name and the VPC-ID number. Once you select a VPC, the VPC list only shows the VPC-ID number in the resulting display.

Step 5: In the **Availability Zone** list, choose **us-west-2a**.

Step 6: In the **IPv4 CIDR block** box, enter **10.255.0.0/24**.

Step 7: Click **Create**, and then click **Close**.

Subnets > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag:

VPC*:

Availability Zone:

VPC CIDRs	CIDR	Status	Status Reason
	10.255.0.0/16	associated	

IPv4 CIDR block*:

* Required

[Cancel](#) [Create](#)

Step 8: If you are deploying Panorama in a HA pair, repeat this procedure for the second subnet in Table 2.

13 Create a VPC Internet Gateway

Create an Internet Gateway (IGW) for external IP connectivity and attach it to the VPC. The IGW allows Panorama to communicate to the internet and reach the Palo Alto Networks licensing and update servers, as well as allows administrators to reach Panorama across the internet.

Step 1: On the VPC dashboard, navigate to **Virtual Private Cloud > Internet Gateways**.

Step 2: Click **Create internet gateway**, and in the **Name tag** box, enter **Management IGW**.

Step 3: Click **Create**, and then click **Close**.

It takes a few minutes for the IGW to initialize.

Step 4: In the **Internet Gateways** list, choose **Management IGW**.

Step 5: In the **Actions** list, choose **Attach to VPC**.

Step 6: In the **VPC** list, choose **Management**, and then click **Attach**.

1.4 Create the VPC Route Tables

Route tables enable you to assign connectivity, such as internet gateways and default gateways, to specific groups of instances. Recall that all instances in the VPC can natively connect to any other instance in the assigned VPC CIDR IP address block. A route table cannot change this behavior. There is a main route table created by default for a VPC, and any subnets that are not assigned to a user-defined route table are assigned to the VPC's main route table. By default, the main route table routes only to the VPC CIDR IP address block. Route tables can control any IP subnet connectivity outside of the VPC CIDR IP address block.



Note

Each route table has a route entry for the VPC CIDR block of IP addresses. This entry is pre-programmed into every VPC route table.

Step 1: On the VPC dashboard, navigate to **Virtual Private Cloud > Route Tables**.

Step 2: At the top of the pane, click **Create route table**.

Step 3: In the **Name** tag box, enter **Management**.

Step 4: In the **VPC** list, choose **Management**.

Step 5: Click **Create**, and then click **Close**.

Step 6: With only **Management** selected in the top pane, click the **Routes** tab on the bottom pane, and then click **Edit routes**.

The screenshot shows the AWS VPC console interface. At the top, there is a search bar and a filter dropdown. Below this is a table listing route tables. The 'Management' route table is selected. Below the table, the 'Routes' tab is active, showing a list of routes. The 'Edit routes' button is visible. The route list shows a single route with the destination '10.255.0.0/16', target 'local', status 'active', and 'Propagated' set to 'No'.

Name	Route Table ID	Explicit subnet association	Edge associations	Main
	rtb-01de8072a5250d3c0	-	-	Yes
Management	rtb-09f61d7e47a2aefc5	-	-	No

Route Table: rtb-09f61d7e47a2aefc5

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.255.0.0/16	local	active	No

Step 7: Click **Add route**, and then in the **Destination** box, enter **0.0.0.0/0**.

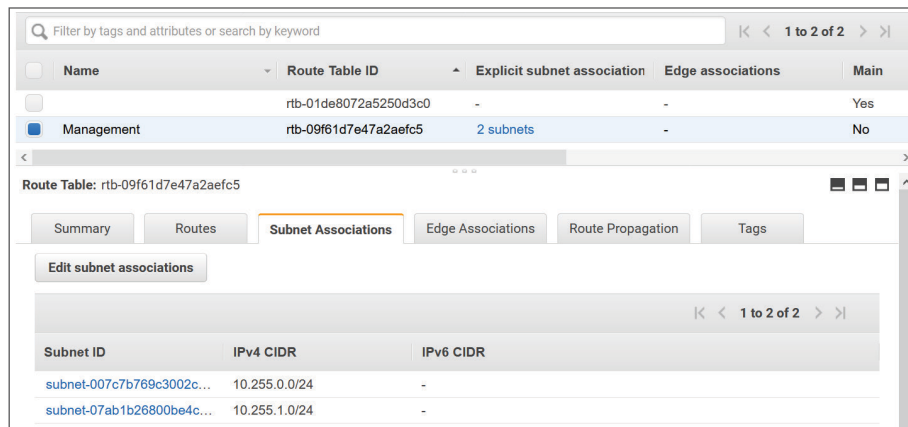
Step 8: Click in the **Target** box, and then choose the **Management IGW** internet gateway.

Step 9: Click **Save routes**, and then click **Close**.

Step 10: On the Subnet Associations tab, click **Edit Subnet Associations**.

Step 11: Choose **Management-2a**.

Step 12: If you are deploying Panorama as a HA pair, choose **Management-2b**, and then click **Save**.



1.5 Create VPC Security Groups

When you create an AWS Elastic Compute Cloud (EC2) compute instance to run an application, you must assign the instance to a new or existing security group (SG). Security groups provide a Layer 4 stateful firewall for control of the source/destination IP addresses and ports that are permitted to or from the instances associated. Security groups are applied to an instance's network interface. You can associate up to five security groups with a network interface. By default, the security groups do not allow inbound traffic. The default outbound behavior allows all traffic. However, you can customize this for your operations.

This procedure creates a Panorama SG that allows inbound traffic necessary for Panorama operation. Depending on your firewall settings, you might require more or fewer ports configured. For more information, see [Palo Alto Networks PAN-OS 9.1 Reference: Port Number Usage](#).

Table 3 Panorama SG—inbound rules

Type	Source IP address
SSH	Your IP
HTTPS	Your IP
All traffic	10.255.0.0/16

Step 1: On the EC2 Compute dashboard, navigate to **NETWORK & SECURITY > Security Groups**, and then click **Create Security Group**.

Step 2: In the **Security group name** box, enter **Panorama**.

Step 3: In the **Description** box, enter **Inbound filtering for Panorama**.

Step 4: In the **VPC** list, choose **Management**.

Step 5: On the **Inbound rules** pane, click **Add Rule**.

Step 6: In the **Type** list, choose **SSH**.

Step 7: In the **Source type** list, choose **My IP**.

Step 8: Repeat Step 5 – Step 7 for the remaining rules in Table 3.

Step 9: Click **Create Security Group**.

Procedures

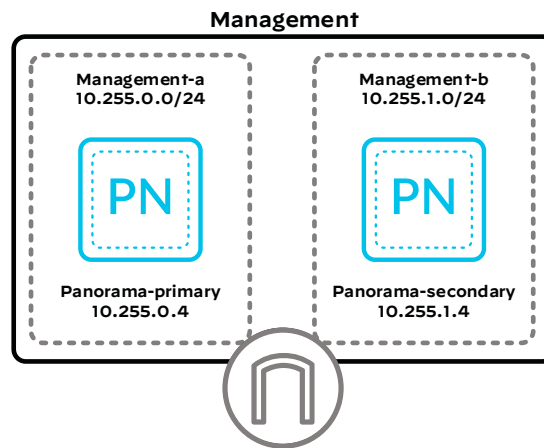
Deploying a Panorama Server on AWS

- 2.1 Create a Panorama Instance
- 2.2 Label the Primary Interfaces for the VM-Series Instance
- 2.3 Create EIP Addresses for the Panorama Instances
- 2.4 Configure the Admin Login for Browser Access

In these procedures, you deploy Panorama in Management-Only mode and connect it to Cortex Data Lake. Panorama defaults to Management-Only mode when it detects that there is not enough log storage capacity to run in Panorama mode.

You need a BYOL license for the primary Panorama server and another for the optional secondary Panorama server.

Figure 6 Panorama on AWS deployment



2.1 Create a Panorama Instance

Table 4 Panorama deployment parameters

System name	Subnet	Management IP address
Panorama-primary	Management-2a	10.255.0.4
Panorama-secondary	Management-2b	10.255.1.4

Step 1: On the EC2 Compute dashboard, navigate to **INSTANCES > Instances**.

Step 2: In the **Launch Instance** list, choose **Launch Instance**.

Step 3: In the **Choose AMI** workflow, click the **AWS Marketplace** tab.

Step 4: In the search box, enter **Palo Alto Networks**, and then press **ENTER**.

Step 5: Click **Select** for the **Palo Alto Networks Panorama** instance.

Step 6: Read the Palo Alto Networks Panorama information message, and then click **Continue**.

Next, you choose the instance sizing. Review the [Setup Prerequisites for the Panorama Virtual Appliance](#) for resource requirements.

Step 7: In the Choose Instance Type window, scroll down and choose an instance type that meets Panorama's requirements, and then click **NEXT: Configure Instance Details**.

This screen configures the networking details for the instance.

Step 8: In the Number of instances box, enter **1**.

Step 9: In the Network list, choose **Management**.

Step 10: In the Subnet list, choose **Management-2a**.

Step 11: For Enable termination protection, select **Protect against accidental termination**.

Step 12: Expand **Network Interfaces**, in the **Primary IP** box for **eth0**, enter **10.255.0.4**.

Number of instances 1 Launch into Auto Scaling Group

Purchasing option ☐ Request Spot instances

Network vpc-0e9f3a93b2cb033d3 | Management Create new VPC
No default VPC found. Create a new default VPC.

Subnet subnet-007c7b769c3002c4d | Management-2a | us-west-1 Create new subnet
251 IP Addresses available

Auto-assign Public IP Use subnet setting (Disable)

Placement group ☐ Add instance to placement group

Capacity Reservation Open Create new Capacity Reservation

IAM role None Create new IAM role

CPU options ☐ Specify CPU options

Shutdown behavior Stop

Enable termination protection ☒ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring
Additional charges apply.

EBS-optimized instance ☒ Launch as EBS-optimized instance

Tenancy Shared - Run a shared hardware instance
Additional charges may apply when launching Dedicated instances.

Elastic Inference ☐ Add an Elastic Inference accelerator
Additional charges apply.

T2/T3 Unlimited ☒ Enable
Additional charges may apply

File systems Add file system Create new file system

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-007c7b76	10.255.0.4	Add IP	Add IP

Step 13: Click **Next: Add Storage**. The AMI template for VM-Series adds storage for the instance.

Step 14: Click **Next: Add Tags**. This procedure does not require tags.

Step 15: Click **Next: Configure Security Group**.

Step 16: For **Assign a security group**, select **Select an existing security group**.

Step 17: Select the **Panorama** security group, and then click **Review and Launch**. Ensure that only the **Panorama** security group is selected.

Step 18: Review all selections, and then click **Launch**.

Next, you create a new key pair for the deployment if you don't already have one. If you have an existing key pair, select the existing key pair and skip to Step 22.

Step 19: In the Select an existing key pair or create a new pair dialog box, choose **Create a new key pair**.

Step 20: In the **Key pair name** box, enter key pair name **paloaltonetworks-deployment**.

Step 21: Click **Download Key Pair**. This downloads a file with a .pem file extension to your machine. Store this file in a convenient and safe place. You need this to create an SSH connection to the instance.



Caution

Be sure to store the private key file in a safe place. Anyone with the private key file can access the instances created with it. If you lose the file, you must create new instances in order to get a new private key file.

Step 22: Click **Launch instances**, and then click **View Instances**.

Step 23: In the Instances pane, hover your cursor over the **Name** field. A pencil image appears. Click the pencil.

Step 24: In the **Name** box, enter **Panorama-primary**, and then select the checkmark.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
Panorama-a	i-010ad6d05a2bd26...	t2.xlarge	us-west-2a	running	2/2 checks ...	None

Step 25: If you are deploying Panorama as a HA pair, repeat this procedure to create the secondary Panorama instance using the parameters from Table 4. In Step 19, use the existing key pair that you created or used in that step.

2.2 Label the Primary Interfaces for the VM-Series Instance

Before assigning EIP addresses to the firewall's management interface, you assign names to the interfaces. This makes it easier to assign EIP addresses.

Step 1: On the EC2 Compute dashboard, navigate to **NETWORK & SECURITY > Network Interfaces**.

Step 2: Scroll to the right of the window, locate the Primary Private column, and then select the private IP address for **Panorama-primary** management interface: **10.255.0.4**.

Step 3: In the Network Interfaces pane, in the **10.255.0.4** row, hover your mouse pointer over the **Name** field. A pencil image appears. Click the pencil.

Step 4: In the network interface **Name** box, enter **Panorama-primary-mgmt**, and then click the checkmark.

Next, if you are deploying Panorama as a HA pair, assign the name for **Panorama-secondary** management interface.

Step 5: Scroll to the right of the window, locate the Primary Private column, and then select the private IP address for **Panorama-secondary** management interface, **10.255.1.4**.

Step 6: In the Network Interfaces pane, in the **10.255.1.4** row, hover your mouse pointer over the **Name** field. A pencil image appears. Click the pencil.

Step 7: In the network interface **Name** box, enter **Panorama-secondary-mgmt**, and then click the checkmark.

2.3 Create EIP Addresses for the Panorama Instances

In this procedure, you create EIP addresses and associate them to Panorama's management interface.

Table 5 EIP addresses for the VM-Series firewalls

EIP and ENI name	Private IP address
Panorama-primary-mgmt	10.255.0.4
Panorama-secondary-mgmt	10.255.1.4

Step 1: On the VPC dashboard, navigate to **Virtual Private Cloud > Elastic IPs**.

Step 2: Click **Allocate Elastic IP address**, and then click **Allocate**.

Step 3: In the **Actions** list, choose **View Details**.

Step 4: Click **Manage Tags**.

Step 5: In the **Key** box, enter **Name**.

Step 6: In the **Value** box, enter **Panorama-primary-mgmt**, and then click **Save**.

Next, you assign the EIP to the Panorama.

Step 7: Click **Associate Elastic IP address**.

Step 8: In **Resource type**, select **Network Interface**.

Step 9: In the **Network Interface** list, choose **Panorama-primary-mgmt**.



Note

The names displayed are the Elastic Network Interface (ENI) names you entered in Procedure 2.2. You can see the ENI name in the list, but you can't see the ENI number in the field until after you choose the ENI name.

Step 10: In the **Private IP** list, choose **10.255.0.4**, and then click **Associate**.

Step 11: If you are deploying Panorama as a HA pair, repeat this procedure for the secondary Panorama in Table 5.

2.4 Configure the Admin Login for Browser Access

Before you login to the VM-Series web interface, you need to set an admin user password. The initial admin password setup must be done via an SSH connection to a CLI shell on the instance.

To connect to your instances, you need to set up your SSH connection to use the key pair created in Procedure 2.1.

Step 1: Use the instructions found in the Amazon Elastic Cloud User Guide for Linux Instances under [Connect to your Linux Instance](#) to set up your system to use a SSH connection to access the instance.

Step 2: On the EC2 Compute dashboard, navigate to **INSTANCES > Instances**.

Step 3: Select the **Panorama-primary** instance, and then in the lower pane, copy the **Public DNS (IPv4)** address.



The next step uses the SSH tool that was set up in Step 1, the key pair, and the Public DNS address.

**Note**

You might not be able to connect to Panorama through SSH until it is fully operational. Panorama can take 30 minutes or more to become operational. If you are prompted for a password, Panorama is most likely not operational yet.

Step 4: Use the admin username to open an SSH session to the FQDN for **Panorama-primary**. For example: `ssh -i paloaltonetworks-deployment.pem admin@ec2-44-230-175-147.us-west-2.compute.amazonaws.com`.

Step 5: If your console shows a security alert that the authenticity of the host can't be established, enter **YES** to continue connecting.

Step 6: At the CLI prompt, set a strong admin password, and then commit the changes.

```
admin@PA-VM> configure
admin@PA-VM# set mgt-config users admin password
Enter password :
Confirm password :
admin@PA-VM# commit
Commit job 2 is in progress. Use Ctrl+C to return to command prompt
.....100%
Configuration committed successfully
admin@PA-VM#
```

Step 7: When the commit is complete, use your browser to connect to the firewall's web interface (Example: `https://ec2-44-230-175-147.us-west-2.compute.amazonaws.com`).

Step 8: Accept the browser certificate warning.

Step 9: Log in to Panorama, using **admin** for the username and the password that you just configured.

Step 10: Log out of the SSH session.

Step 11: If you are deploying Panorama as a HA pair, repeat this procedure for the second Panorama instance.

Deployment Details for Panorama System and Services

Procedures

Updating Panorama System and Activating Services

- 3.1 License Panorama
- 3.2 Configure Panorama for High Availability
- 3.3 Activate Cortex Data Lake
- 3.4 Install the Cloud Service Plugin
- 3.5 Configure Cortex Data Lake with Firewall Logging Storage Space

Panorama is now running; however, it is unlicensed and is running in the default configuration. Based on the disk size provisioned for the Panorama virtual machine, the system is running in Management-Only mode.

3.1 License Panorama

This procedure assumes that you have a valid serial number for your Panorama devices and that registration on the customer support portal (<https://support.paloaltonetworks.com>) is complete.

Step 1: Log in to the web interface of the primary Panorama server.

Step 2: Accept the browser certificate warning.

Step 3: On the **There are no device groups** dialog box, click **OK**.

Step 4: On the **Retrieve Panorama License** dialog box, click **OK**.

Step 5: On the **Retrieve Panorama License** dialog box, click **Complete Manually**.

Step 6: On the **Offline Licensing Information** dialog box, click **OK**.

Step 7: In **Panorama > Setup > Management > General Settings**, click the gear icon.

Step 8: In the **Hostname** box, enter **Panorama-primary**.

Step 9: In the **Time Zone** list, choose the appropriate time zone (Example: [US/Pacific](#)).

Step 10: In the **Serial Number** box, enter the serial number found in the customer support portal, and then click **OK**.



Note

When you license a Panorama system, you use the serial number assigned to your account for that system. The serial number can be found in the Palo Alto Networks customer support portal.

General Settings

Hostname: Panorama-primary

Domain:

Login Banner:

☐ Force Admins to Acknowledge Login Banner

SSL/TLS Service Profile: None

Time Zone: US/Pacific

Locale: en

Date: 2020/05/30

Time: 22:23:43

Latitude:

Longitude:

☐ Automatically Acquire Commit Lock

Serial Number: XXXXXXXXXXXX

URL Filtering Database: paloaltonetworks

☐ GTP Security

☐ SCTP Security

OK Cancel

Step 11: In **Panorama > Setup > Services**, click the gear icon.

Step 12: In the **Primary DNS Server** box, enter **169.254.169.253**. This address is the DNS address for AWS.

Step 13: In the **Secondary DNS Server** box, enter **8.8.8.8**.

Step 14: On the **NTP** tab, in the **Primary NTP Server** section, in the **NTP Server Address** box, enter **0.pool.ntp.org**.

Step 15: In the Secondary NTP Server section, in the **NTP Server Address** box, enter 1.pool.ntp.org, and then click **OK**.

Services	
Update Server	updates.paloaltonetworks.com
Verify Update Server Identity	<input checked="" type="checkbox"/>
Primary DNS Server	169.254.169.253
Secondary DNS Server	8.8.8.8
Minimum FQDN Refresh Time (sec)	1800
FQDN Stale Entry Timeout (min)	
Proxy Server	
Primary NTP Server Address	0.pool.ntp.org
Primary NTP Server Authentication Type	None
Secondary NTP Server Address	1.pool.ntp.org
Secondary NTP Server Authentication Type	None

Step 16: On the **Commit** menu, select **Commit to Panorama**, and then click **Commit**.

Step 17: In **Panorama > Licenses**, click **Retrieve license keys from license server**.

Step 18: Verify in the status pane that **Device Management License** is active and has the correct device count.

Device Management License	
Date Issued	May 30, 2020
Date Expires	Never
Description	VM Panorama license to manage up to 25 devices

Step 19: If you are deploying Panorama as a HA pair, repeat this procedure on the secondary Panorama server. In Step 8, enter the name of the secondary Panorama server, [Panorama-secondary](#). You must have a unique serial number for the secondary Panorama system.

3.2 Configure Panorama for High Availability

Because Panorama supports multiple firewalls, you should configure it for HA operation. This procedure is necessary only to deploy Panorama in a high availability configuration. Panorama supports an HA configuration in which one peer is the active-primary and the other is the passive-secondary. If a failure occurs on the primary peer, it automatically fails over and the secondary peer becomes active.

The Panorama HA peers synchronize the running configuration each time you commit changes on the active Panorama peer. The candidate configuration is synchronized between the peers each time you save the configuration on the active peer or just before a failover occurs.

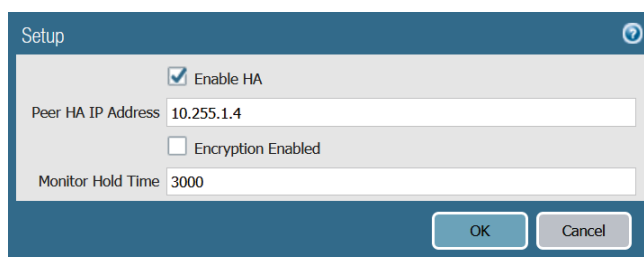
Settings that are common across the pair—such as shared objects and policy rules, device group objects and rules, template configuration, and administrative access configuration—are synchronized between the Panorama HA peers.

Perform Step 1 – Step 6 on the primary Panorama server.

Step 1: In **Panorama > High Availability > Setup**, click the gear icon.

Step 2: Select **Enable HA**.

Step 3: In the **Peer HA IP Address** box, enter **10.255.1.4**, and then click **OK**.

A screenshot of the 'Setup' dialog box in the Palo Alto Networks Panorama interface. The dialog has a title bar with 'Setup' and a help icon. Inside, there are three sections: the first has a checked checkbox for 'Enable HA'; the second has a text field for 'Peer HA IP Address' containing '10.255.1.4' and an unchecked checkbox for 'Encryption Enabled'; the third has a text field for 'Monitor Hold Time' containing '3000'. At the bottom right are 'OK' and 'Cancel' buttons.

Step 4: In **Panorama > High Availability > Election Settings**, click the gear icon.

Step 5: In the **Priority** list, choose **primary**, and then click **OK**.

Step 6: On the **Commit** menu, select **Commit to Panorama**, and then click **Commit**.

Perform steps 7-12 on the secondary Panorama server.

Step 7: In **Panorama > High Availability>Setup**, click the **Edit** cog.

Step 8: Select **Enable HA**.

Step 9: In the **Peer HA IP Address** box, enter **10.255.0.4**, and then click **OK**.

Step 10: In **Panorama > High Availability > Election Settings**, click the **Edit** cog.

Step 11: In the **Priority** list, choose **secondary**, and then click **OK**.

Step 12: On the **Commit** menu, select **Commit to Panorama**, and then click **Commit**.

Step 13: On the primary Panorama server, in **Dashboard > Widgets > System**, click **High Availability** to enable the **High Availability** dashboard widget. This adds a dashboard pane that displays the status of the Panorama peers.

Step 14: Repeat Step 13 on the secondary Panorama server.

Step 15: On the primary Panorama server, in **Dashboard > High Availability**, click **Sync to peer**.

Step 16: Click **Yes** to accept the **Overwrite Peer Configuration** warning and proceed with the synchronization.

Figure 7 Primary Panorama HA status

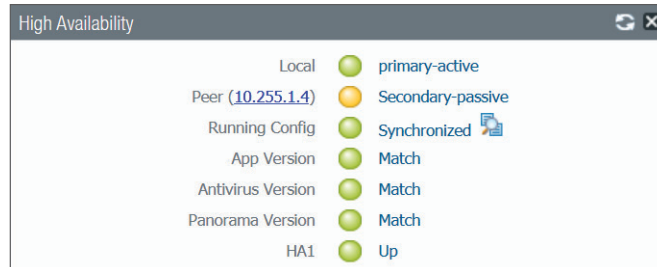
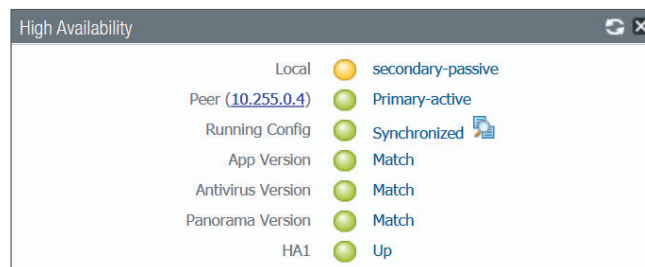


Figure 8 Secondary Panorama HA status



3.3 Activate Cortex Data Lake

Cortex Data Lake requires an authorization code that is used to activate the service. This procedure also assumes that you have a valid serial number for your Panorama device(s) and that registration on the customer support portal is complete.

The Cortex Data Lake instance is associated with the serial number of the primary Panorama server. This procedure is not repeated for the secondary Panorama server.

Step 1: Log in to the Customer Support Portal at <https://support.paloaltonetworks.com>.

Step 2: Select **Assets > Cloud Services**.

Step 3: Click **Activate Cloud Services Auth-Code**.

Step 4: In the Cloud Services window, in the **Authorization Code** box, enter the authorization code (example: **I11223345**), and then press Tab key to advance. The **Panorama** and **Logging Region** boxes appear.

Step 5: In the Cloud Services window, in the **Logging Region** list, choose the value that corresponds to your region (Example: **Americas**).

Step 6: In the Cloud Services window, in the **Panorama** list, choose the value that corresponds to the serial number assigned to your primary Panorama server.

Step 7: Select the checkbox to acknowledge the warning. You perform this update later, in Procedure 3.5.

Step 8: Accept the EULA by clicking on **Agree and Submit**.

Step 9: If you are deploying Panorama as a HA pair, repeat this procedure for the secondary Panorama server and use its serial number in Step 6.

3.4 Install the Cloud Service Plugin

If you are running Panorama in high availability mode, perform this procedure on the primary Panorama server first. Then you repeat this procedure for the secondary Panorama server.

Step 1: In **Panorama > Plugins**, click **Check Now**.

Step 2: For **cloud __services-1.6.0**, in the Action column, click **Download**.

Step 3: After the download is completed, click **Close**.

Step 4: After the status in the **Available** column changes to a checkmark, in the Action column, click **Install**.

Step 5: On the dialog box that indicates a successful installation, click **OK**.

Step 6: In **Panorama > Licenses**, click **Retrieve license keys from server**.

Step 7: Verify that you have a Cortex Data Lake license.

Cortex Data Lake	
Date Issued	May 30, 2020
Date Expires	May 19, 2021
Description	Cloud Service
Log Storage TB	1

Step 8: Open another browser window and navigate to the customer support portal (<https://support.paloaltonetworks.com>). Complete Step 9 through Step 11 in the customer support portal.

Step 9: In Assets > Cloud Services, click **Generate OTP**.

Step 10: In the Generate Cloud Services One Time Password window, in the **Panorama** list, choose the serial number for the primary Panorama server, and then click **Generate OTP**.

Generate One Time Password

Device Type: Generate OTP for Panorama

The OTP provides users the password to input into the Cloud Services. This is a required step to enable secure use of the cloud services. This password is only valid for 10 minutes. If the time has expired before you have use this password, please generate a new password.

Select OTP Type: Logging Service

Panorama : - Panorama Select -

Generate OTP

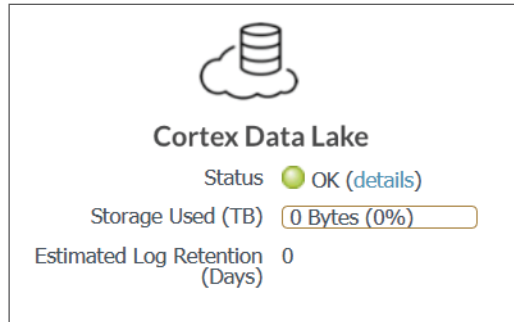
Close

Step 11: In the Generate Cloud Services One Time Password window, click **Copy to Clipboard**.

Step 12: On the primary Panorama server, navigate to **Panorama > Cloud Services > Status**, and then click **Verify**. If you are configuring the secondary Panorama server, verify on [Panorama-secondary](#).

Step 13: In the **One-Time Password** box, paste the OTP that was generated from the Customer Support Portal, and then click **OK**.

Step 14: In **Panorama > Cloud Service > Status**, verify the status. It might take a minute for the verification to complete.

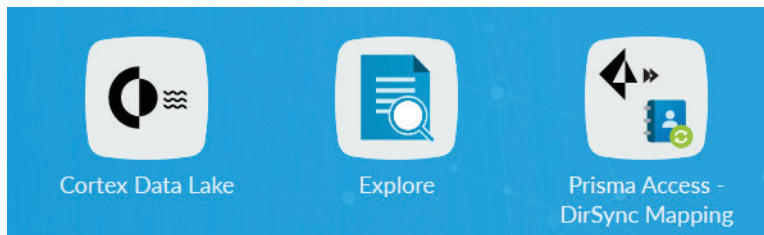


Step 15: If you are deploying Panorama as a HA pair, repeat this procedure for the secondary Panorama server. In step 10, you must generate a new OTP, this time for the secondary Panorama server serial number.

3.5 Configure Cortex Data Lake with Firewall Logging Storage Space

In Procedure 3.3, you acknowledged a warning that you must allocate storage space for firewall logs, or they will be purged from Cortex Data Lake. This procedure provisions storage space for firewall logs.

Step 1: Navigate to <https://apps.paloaltonetworks.com/>, log in, and then click **Cortex Data Lake**.

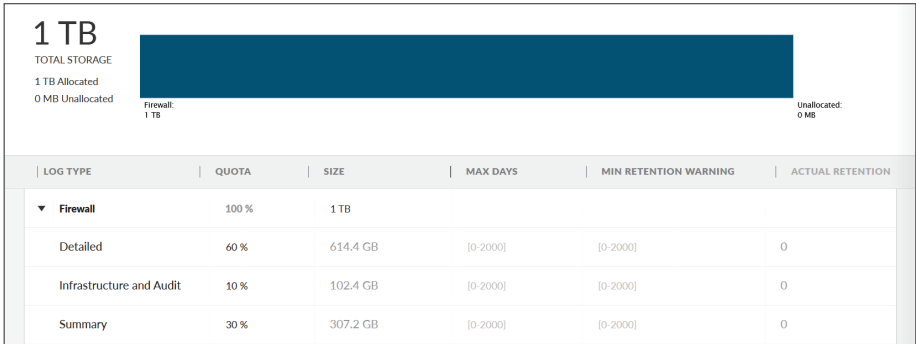


Step 2: If you have multiple Cortex Data Lake instances and Panorama systems, select the appropriate instance from the list.

Step 3: In the navigation pane, click **Configuration**.

Step 4: In the Firewall Log Type **Size** box, enter **1 TB**, and then click **Apply**.

This Firewall Log Type size is an example value. You are provisioning a portion of the total storage space for firewall logs. For storage sizing, see this [Knowledge Base Article](#).



Next Steps: Configuring Network Templates and Policies

Now that your Panorama system(s) are operational, you are ready to build firewall configuration templates on Panorama. You use hierarchical device groups and templates and template stacks to organize configurations that Panorama pushes to VM-Series or PA-Series firewalls.

- **Hierarchical device groups**—Panorama manages common policies and objects through hierarchical device groups. You use multi-level device groups to centrally manage the policies across all deployment locations with common requirements.
- **Templates and template stacks**—Panorama manages common device and network configuration through templates. You can use templates to manage configuration centrally and then push the changes to all managed firewalls. This approach allows you to avoid making the same individual firewall change repeatedly across many devices. To make things easier, you can stack templates and use them as building blocks for device and network configuration.

This reference architecture provides two deployment guides that contain the details for configuring device groups, templates, and template stacks specific to the design models covered in those guides. For more information, see the following guides:

- [Securing Applications in AWS Single VPC: Deployment Guide](#)
- [Securing Applications in AWS Transit Gateway: Deployment Guide](#)



You can use the [feedback form](#) to send comments about this guide.

HEADQUARTERS

Palo Alto Networks	Phone: +1 (408) 753-4000
3000 Tannery Way	Sales: +1 (866) 320-4788
Santa Clara, CA 95054, USA	Fax: +1 (408) 753-4001
http://www.paloaltonetworks.com	info@paloaltonetworks.com

© 2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <http://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. Palo Alto Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.