Auto Scaling the VM-Series Firewall on Google Cloud Platform

docs.paloaltonetworks.com

techDOCS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Last Revised

November 5, 2019

Table of Contents

Auto Scaling the VM-Series Firewall on Google Cloud Platform

The Panorama plugin for Google Cloud Platform (GCP) version 2.0 Beta enables Panorama to manage VM-Series firewalls securing VM monitoring and auto scaling deployments in GCP.

This topic focuses on an auto scaling use case that requires Google shared VPC technology to create a common VPC network composed of a host project containing shared VPC networks and the VM-Series firewalls, and a service project containing a sample application deployment. Palo Alto networks supplies templates to help you deploy the VM-Series firewalls in the host project and deploy the sample application in the service project.

Using Panorama to maintain your GCP managed instance groups has the following benefits:

- BYOL licenses can be used for the VM-Series firewalls.
- Panorama automatically monitors the VM-Series firewall status and automatically deregisters a VM-Series firewall when it is automatically removed.
- With Panorama, you can create application enablement policies that protect and control the network. Using Panorama for centralized policy and firewall management increases operational efficiency in managing and maintaining a distributed network of firewalls.

Auto Scaling Components for Google Cloud Platform

Software Version Requirements

- Panorama—Panorama physical or virtual appliance running version 9.0.4 or later in Panorama mode.

  The Panorama appliance must be able to communicate with the VM-Series firewalls deployed on your GCP shared VPC infrastructure to enable centralized management of the auto scaling VM-Series firewalls. You also require the Panorama plugin for GCP version 2.0 and the VM-Series plugin version 1.0.6 or later.

  The GCP plugin takes care of the interactions required to license, bootstrap and configure the VM-Series firewalls using device groups and template stacks on Panorama, and programs the NAT rules to direct traffic to the firewalls.

  Obtain the Panorama plugin for GCP from the auto scaling beta site (registration required), upload it to Panorama, and install it as described in Install Panorama Plugins.

  You cannot upgrade the GCP plugin from version 1.0 to version 2.0

- VM-Series Firewalls—The PAN-OS version for the auto scaling set of VM-Series firewalls is PAN-OS 8.1.4 or later. The Panorama must be running a PAN-OS version that is the same or later than the managed firewalls.

  The managed firewall require a valid license.
- Templates—Download the templates for deploying the auto scaling VM-Series firewall and the sample application template from GitHub. The zip file contains separate zip files for the firewall and application templates.

  Palo Alto Networks provides the templates to deploy VM-Series firewall instances in the host project so you can secure inbound traffic for a GCP application deployment in the service project. The firewall templates create a Cloud Pub/Sub service that relays information from GCP to the Panorama plugin for GCP. With this infrastructure in place, the plugin can leverage dynamic address groups to apply security policy on inbound traffic routed to services running on GCP, and use autoscale metrics to deploy VM-Series firewalls to meet increased demand for application workload resources or to eliminate firewalls that are no longer needed.

GCP Auto Scaling Prerequisites

The auto scaling deployment on GCP requires a shared VPC with host and service projects that use a common VPC network. In this topology, the host project contains the networks and VM-Series firewalls that secure traffic to your applications, which are deployed in the service project.

Complete the following tasks before you deploy the auto scaling templates.

- Prepare a Host Project
- Configure gcloud SDK
- Prepare a Service Project
- Prepare a VM-Series Bootstrap Package

Prepare a Host Project

You need a host project and a service project to form the shared VPC topology that supports the firewall and application templates. You can create a new host project or prepare an existing project to act as your host.

To set up the Shared VPC an organization admin must grant the host project administrator the Shared VPC Admin role. The Shared VPC Admin can enable a project to act as a host, and grant the Service Project Admin role to the service project administrator. Review the GCP documentation on Administrators and IAM roles.

STEP 1 | In the GCP console, create a GCP project. If you want to use an existing one, go to the next step.

To create a new project, select your organization or **No organization**, click **New Project** and fill in your project information. Note, this is your only chance to **EDIT** the project ID.

STEP 2 | Enable GCP service APIs.

1. Select the host project and from the Navigation menu, select **APIs & Services**.
2. Search for and view each API below. **ENABLE** any APIs that do not display the “API enabled” status.

   - ❑ Cloud Pub/Sub API
   - ❑ Cloud Deployment Manager API
   - ❑ Cloud Storage API
   - ❑ Compute Engine API
   - ❑ Google Compute Engine Instance Group Manager API
   - ❑ Google Compute Engine Instance Group Updater API
   - ❑ Google Compute Engine Instance Groups API
   - ❑ Kubernetes Engine API
   - ❑ Stackdriver API
   - ❑ Stackdriver Logging API
   - ❑ Stackdriver Monitoring API

STEP 3 | Create a service account for deploying the VM-Series firewall, and assign the IAM roles required for auto scaling.

1. In the GCP console select **IAM & Admin** > **Service accounts** and select **+CREATE SERVICE ACCOUNT**.

   Fill in the service account details and **CREATE**.
2. Give the service account permissions to auto scale resources in this project.

   Add the following roles:

   - Compute Engine > Compute Admin
   - Compute Engine > Compute Network User
   - Project > Editor
   - Pub/Sub > Admin

   Continue when you are finished.
3. (Optional) Add email addresses to grant users or administrators access to this service account.
4. Download a JSON file with a private key.

   Click **+CREATE KEY**, select JSON, click **CREATE**, and store the key in a secure location.
5. Click **DONE**.

STEP 4 | Create a service account that a Panorama administrator can use to interact with the host project. You specify this service account and upload its key when you configure auto scaling on the GCP plugin for Panorama.

1. Repeat step 3 but add only the following roles:
    - Compute Engine > Compute Viewer
    - Pub/Sub > Admin
2. Add users, download the private key in JSON form, and store it in a safe location.

Configure gcloud SDK

You will use the command line interface to deploy the firewall template and the application template, and to attach the service project to the host project.

STEP 1 | If you have not done so, install the Google Cloud SDK.

STEP 2 | Verify that you can authenticate with the GCP console.

```
gcloud auth login <your-account-email-address>
```

STEP 3 | Set your project to the host project you just created.

```
gcloud set project <your-autoscale-host-project-name>
```

STEP 4 | Create a configuration for auto scaling.

```
gcloud config configurations create CONFIGURATION_NAME
```

Your new config is automatically activated unless you disable activation.

```
gcloud config list
```

Prepare a Service Project

Create a separate service project, or choose an existing project, for your application.

To learn more about host and service projects in a shared VPC, see the Shared VPC Overview, and review the Administrators and IAM roles. A host project administrator must have the proper role to set up the Shared VPC, make the application project a service project for the host project. See the instructions in Provisioning Shared VPC.

Prepare a VM-Series Bootstrap Package

Set up the storage bucket with the folders required to Bootstrap the VM-Series Firewall on Google Cloud Platform. Later you will configure an `init-cfg.txt` file with firewall template information and upload it to the `/config` folder in your bootstrap package.

Deploy GCP Auto Scaling Templates

You can download the Palo Alto Networks auto scaling templates from https://github.com/PaloAltoNetworks/GCP-AutoScaling. The zip file contains separate zips for firewall and application templates. Each template directory contains many files but you only need to edit the YAML files.

This beta supports greenfield deployments only.

- Firewall templates—The firewall templates create VM-Series firewalls and other resources for a greenfield deployment. It creates new networks and the familiar subnetworks for the VM-Series firewall: management, untrust, and trust. The firewall templates also deploy a Cloud Pub/Sub messaging service to handle communications with your firewall instance group.

  To customize firewall template, edit `vm-series-fw.yaml`.
- Application templates—The application templates provide a sample application. Customize these templates so that your application servers can subscribe to the Pub/Sub service and communicate with your VM-Series firewalls and the GCP plugin on Panorama.

  To customize the application template, edit `app.yaml`.

Prepare the Panorama Plugin

Install the Panorama plugin and create assets to support the auto scaling firewall deployment.

- Review the Software Version Requirements.

- Download the Panorama plugin for GCP version 2.0 from the auto scaling beta site (registration required).

- Upload the plugin to Panorama, and install it as described in Install Panorama Plugins.

- On Panorama create the following resources:
  1. Add any VMs associated with your GCP project as managed devices.
  2. Add Device Groups and assign managed VMs to a single Device Group (a VM can be a member of only one Device Group across all plugins).
  3. Add a template, and a template stack that includes your managed VMs or Device Groups, and commit the changes.
  4. In a template stack create a virtual router.

     Make sure to add the virtual router to the template stack and not to the template. If you do not create the virtual router in the template stack, the static routes that the Inbound firewall template automatically creates will not be added to the virtual router, and your application template may not launch successfully.
  5. In a template, create two interfaces—ethernet1/1(Untrust) and ethernet1/2 (Trust) interfaces. On each interface, **Enable DHCP** and clear **Automatically create default route pointing to default gateway provided by server**.
  6. Assign the interfaces to the virtual router.

Prepare to Deploy the Firewall Templates

The firewall templates include a sample `init-config.txt` file.

Parameter	Value	Comment
type	dhcp-client	
op-command-modes	mgmt-interface-swap	Required in this Beta release.
hostname	<gcp-pa-vm>	Optional name you assigned when you created the host project. Only required if a specific host is necessary, and dhcp-send-hostname is no.
vm-auth-key	<vmauthkey>	A key that Panorama must validate before adding a firewall as a managed device. See Generate the VM Auth Key On Panorama.
panorama-server	<panorama-ip>	The IP address of the Panorama management device you configured in Prepare the Panorama Plugin.
tplname	<tmplstk-name>	The template stack you created in Prepare the Panorama Plugin.
dgname	<dg-name>	The name of the Device Group you created in the Panorama Plugin for GCP.
dns-primary	8.8.8.8	Your primary DNS.
dns-secondary	208.67.222.222	Your secondary DNS.
dhcp-send-hostname	yes	Leave as is.
dhcp-send-client-id	yes	Leave as is.
dhcp-accept-server-hostname	yes	Leave as is.
dhcp-accept-server-domain	yes	Leave as is.

STEP 1 | Edit the values in the **`init-config.txt`** file to customize the file for your environment.

STEP 2 | Upload your edited **`init-config.txt`** file to the **`/config`** folder in your bootstrap package.

STEP 3 | If you are using BYOL, put your **`authcodes`** file in the license folder.

Deploy the Firewall Template

Edit the Firewall template from the host project.

STEP 1 | Edit the `vm-series-fw.yaml` environment variables to reflect your cloud environment.

```
properties:region: us-east1zones: -us-east1-b # Do not modify the lb-type
field. lb-type: nlb cloud-nat: yes  forwarding-rule-port: 80
```

```
#urlPath-namedPort-maps:
    - appName: app1
    bootstrap-bucket: rr-bootstrap-1
    image: vmseries-byol-814
    machine-type: n1-standard-4
     service-account: username-autoscale@gcp-autoscale-
host.iam.gserviceaccount.com
     fw-instance-tag: vm-series-fw
# Possible values for metrics.
#     panSessionActive
#     panSessionUtilization
#     DataPlaneCPUUtilizationPct
#     DataPlanePacketBufferUtilization
#     panSessionUtilization
metric: custom.googleapis.com/VMSeries/panSessionActive
max-size: 2
min-size: 1
target-type: GAUGE
util-target: 100
```

min-size and max-size represent the minimum and maximum number of firewalls in an instance group.

```
# Greenfield deployment
mgmt-network-cidr: 172.22.2.0/24
untrust-network-cidr: 172.22.1.0/24
trust-network-cidr: 172.22.3.0/24
mgmt-network-access-source-range:
- 199.167.54.229/32
- 199.167.52.5/32
mgmt-network-access-ports:
- 22
- 443
```

```
outputs:
- name: trust-network-name
value: $(ref.vm-series-fw.trust-network-name)
- name: trust-subnet-name
value: $(ref.vm-series-fw.trust-subnet-name)
- name: deployment-name
value: $(ref.vm-series-fw.deployment-name)
- name: panorama-pubsub-topic
value: $(ref.panorama-pubsub.vm-series-fw-template-pubsub-topic)
```

STEP 2 | Deploy the firewall template.

```
gcloud deployment-manager deployments create <firewall-template-name>
--config vm-series-fw.yaml --automatic-rollback-on-error
```

Take note of the outputs the CLI prints after the deployment (the subnet names and the Panorama Pub/Sub topic name). You need the output values to configure the Shared VPC.

The Managed Instance Group name as specified in the firewall template needs to be configured in the Panorama plugin for GCP auto scaling definition.

Deploy the Application Template

The Service project adminstrator deploys the Application template from the service project.

STEP 1 | Create a separate application project (service project) to deploy the application.

STEP 2 | Prepare the application template.

```
properties:
  host-project: gcp-autoscale-host
  fw-deployment-name: rr-fw-template-9
  region: us-east1
  zones:
    - us-east1-b
    - us-east1-c
```

STEP 3 | Deploy a new application with the application template and define a label for the named port.

```
gcloud deployment-manager deployments create <your-template>--config
app.yaml --labels named-port=82--automatic-rollback-on-error
```

Configure the Shared VPC

After the firewall template is deployed in the host project, configure the service project that supports your applications. An administrator with Shared VPC credentials performs these tasks from the host project. To understand more about the host project and service projects in the context of shared VPC, see the Shared VPC Overview.

STEP 1 | Create a shared VPC using the Trust VPC created when you deployed the firewall template.

Set up shared VPC for the host (firewall) project:

```
gcloud compute shared-vpc enable HOST_PROJECT_ID
```

STEP 2 | Make the application project a service project for the host project.

- Add the service account email (<project number>@cloudservices.gserviceaccount.com) from Service/application project administrator as a member in host project with below role:
    - Compute Admin
    - Compute Network User
    - Pub/Sub admin
    - Editor (Need to check if this is required)

STEP 3 | Attach the service/application project to the host project.

```
gcloud compute shared-vpc associated-projects add SERVICE_PROJECT_ID --host-
project HOST_PROJECT_ID
```

Additional options are available to share only specific subnets, rather than all subnets in the host project.

Onboard a New Application

For every application you must supply the application name, the named ports, and the path.

Follow these steps to onboard a new application in the service project. The sample template shows app1 as the only application. Here you add app2 and app3.

STEP 1 | Prepare new named port and URL path on HTTP external load balancer.

STEP 2 | Update all instance groups named-ports with an additional service name and port values for app2 and app3.

```
gcloud compute instance-groups set-named-ports
 wli-fw-template2-fw-igm-us-east1-b
--zone us-east1-b --named-ports=app1:80,app2:81,app3:82

gcloud compute instance-groups set-named-ports
 wli-fw-template2-fw-igm-us-east1-c
--zone us-east1-c --named-ports=app1:80,app2:81,app3:82
```

STEP 3 | Create a new http-health-check.

```
gcloud compute backend-services create wli-fw-template2-backend-app3
--protocol="HTTP"
--port-name=app3
--http-health-checks=wli-fw-template2-healthcheck-app3
--load-balancing-scheme="EXTERNAL"
--global
```

STEP 4 | Create a new backend service with the port-name created earlier on the HTTP external load balancer.

```
gcloud compute backend-services create wli-fw-template2-backend-app3
--protocol="HTTP" --port-name=app3
--http-health-checks=wli-fw-template2-healthcheck-app3 --load-balancing-
scheme="EXTERNAL" --global
```

Check to see if it is visible.

```
gcloud compute backend-services list
```

STEP 5 | Edit url-maps and add new path rule.

For example:

```
- paths:
    - /app3
    - /app3/*
    service: https://www.googleapis.com/compute/v1/projects/stellar-
cumulus-95806/global/backendServices/wli-fw-template2-backend-app3
```

```
gcloud compute url-maps edit wli-fw-template2-ext-loadbalancer
```

Known Issues

This plugin supports VM Monitoring and Auto Scaling tasks. Please review the known issues for the Panorama plugin for GCP version 2.0 Beta.

- Auto Scaling
- VM Monitoring
- General

Auto Scaling

Issue ID	Description
PAN-129356	Panorama management server sometimes crashes and restarts when you add a device.
PLUG-2940	When the **Push NAT Rules automatically** is disabled, then the onboarded application is not added to the database and is not displayed in **Panorama** > **Google Cloud Platform** > **Auto Scaling**.

PLUG-2731	When you add a new auto scaling configuration, the plugin creates a new NAT rule and address objects but does not commit the change to the associated Device Group as expected. Although partial commit does not occur, the following message is displayed:
	`Partial changes to commit:`
	`changes to configuration by all administrators`
	`Changes to device-group configuration: (your-configuration)`

PLUG-2692	On Panorama, the GCP plugin gets a message from Pub/Sub, generates the configuration, initializes a commit, then pushes the configuration to the device. Although this process is shown to be successful on Panorama, the shared policy remains out-of-sync for all managed firewalls so the NAT rules aren't pushed. After the initial commit, you must manually push the configuration to your managed firewalls.

VM Monitoring

Issue ID	Description
PLUG-2716	If a monitoring definition cannot retrieve tags, the **Status** column displays **Fail** but there is no related error message. Use the following CLI command to get status information: **`show plugins gcp vm-mon-status`**

Issue ID	Description
PLUG-2650	A GCP service account and its related project can be associated with only one monitoring definition. At this time the Panorama web interface does not prevent you from making multiple monitoring definitions for the same project.
PLUG-2499	You must ensure that a Device Group is a member of only one notify group. Your Panorama can have many plugins installed—for example plugins for AWS, Azure, GCP, and more. If you add a Device Group to multiple notify groups, tags learned by one plugin are overwritten by another.

General

Issue ID	Description
	At this time the GCP plugin for Panorama version 2.0.0 Beta version supports VM Monitoring and Auto Scaling, but does not support Google Kubernetes Engine (GKE). Do not use the GCP Plugin web interface for **Setup** > **GKE Service Account**.
PLUG-2380	The Google Cloud Platform plugin cannot be upgraded from 1.0.0 to 2.0.0.
PLUG-2618	You cannot use the Panorama CLI to configure a GCP service account object. You must use the web interface.
PLUG-2657	A GCP service account credential file can be used only once. At this time the Panorama web interface does not prevent making multiple Panorama service account objects with the same credential.
PLUG-1694	(PAN-OS VMs with PAYG licenses) Your pay-as-you-go (PAYG) license is not retained when you upgrade a PAN-OS 8.1 release to PAN-OS 9.0. To recover your license after an upgrade to 9.0, upgrade the VM-Series plugin to 1.0.2 or later, and reboot the firewall. If you have manually installed the VM-Series plugin on Panorama, ensure that the version is the same or later than the version on your managed devices.

Get Help

The following topics provide information on where to find more about this release and how to request support:

- Related Documentation
- Requesting Support

Related Documentation

Refer to the following documentation on https://docs.paloaltonetworks.com/ or search the documentation for more information on our products:

- **Palo Alto Networks Compatibility Matrix**—Provides compatibility and interoperability information for Palo Alto Networks hardware and software products.
- **Panorama Administrator's Guide**—Provides the basic framework to quickly set up the Panorama™ virtual appliance or an M-Series appliance running version 8.1 or 9.0 for centralized administration of the Palo Alto Networks firewalls.
- **PAN-OS Administrator's Guide**—Provides the concepts and solutions to get the most out of your Palo Alto Networks next-generation firewalls. This includes taking you through the initial configuration and basic set up on your Palo Alto Networks firewalls for PAN-OS 8.1 or 9.0.
- **VM-Series Deployment Guide**—Provides deployment concepts and workflows for setting up, licensing, and managing the VM-Series firewall on public and private cloud platforms.

Requesting Support

To learn about Support programs, to manage your account or devices, or to open a support case, go to https://support.paloaltonetworks.com.

To provide feedback on the documentation, please write to us at: documentation@paloaltonetworks.com.

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

https://www.paloaltonetworks.com/company/contact-support

Palo Alto Networks, Inc.

www.paloaltonetworks.com