Palo Alto Networks

Azure Active/Passive Guide

Matt McLimans, Public Cloud Consultant Engineer

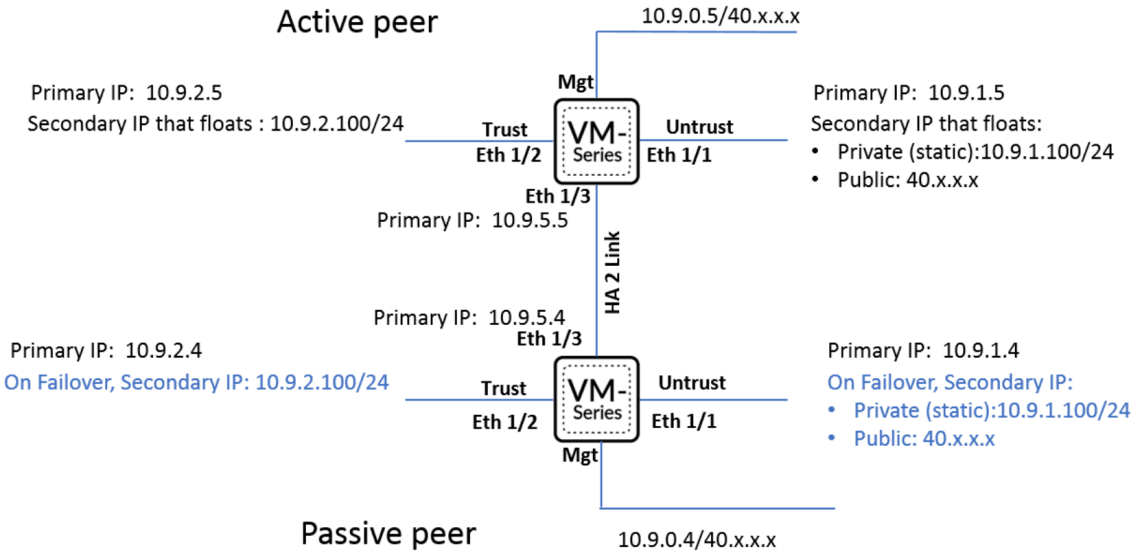
SUPPORT POLICY

This is released under an as-is, best effort, support policy. These scripts should be seen as community supported and Palo Alto Networks will contribute our expertise as and when possible. We do not provide technical support or help in using or troubleshooting the components of the project through our normal support options such as Palo Alto Networks support teams, or ASC (Authorized Support Centers) partners and backline support options. The underlying product used (the VM-Series firewall) by the scripts or templates are still supported, but the support is only for the product functionality and not for help in deploying or using the template or script itself. Unless explicitly tagged, all projects or work posted in our GitHub repository (at https://github.com/PaloAltoNetworks) or sites other than our official Downloads page on https://support.paloaltonetworks.com are provided under the best effort policy.

DEPLOYMENT OVERVIEW

- This is a deployment guide 2xVM-Series firewalls in an Active/Passive pair.

- This deployment aims to replicate the architecture in: Set up Active/Passive HA on Azure.



STEP 1. LAUNCH TEMPLATE

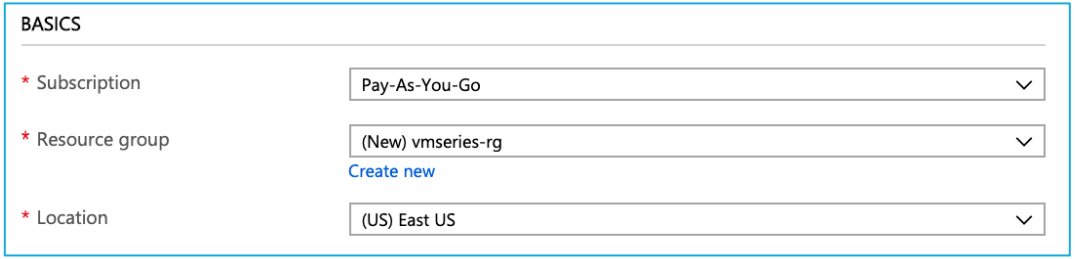
1. Launch the ARM Template

   https://github.com/wwce/azure-arm/tree/master/Azure-CommonDeployments/v1/2fw_3nic_avset_active_passive

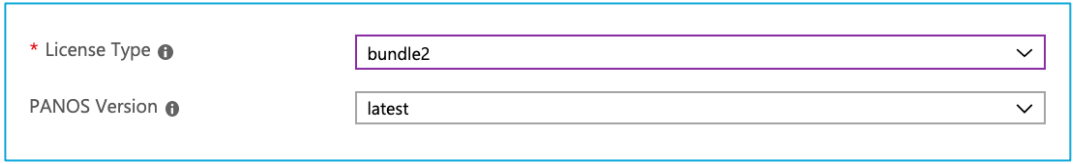
2. Download active-fw-config.xml & passive-fw-config.xml. The firewall configurations are configured to reflect the default parameter settings.

STEP 2. USER REQUIRED PARAMETERS

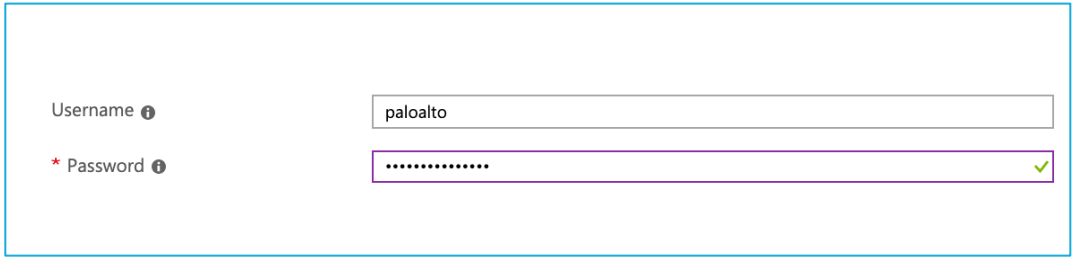
Resource Group: Create a new Resource Group
All resources deployed in template will belong to Resource Group selected.



License Type: Select BYOL / Bundle1 / Bundle2

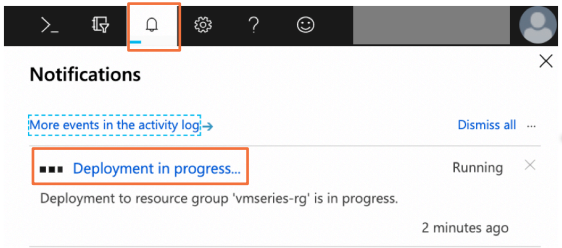


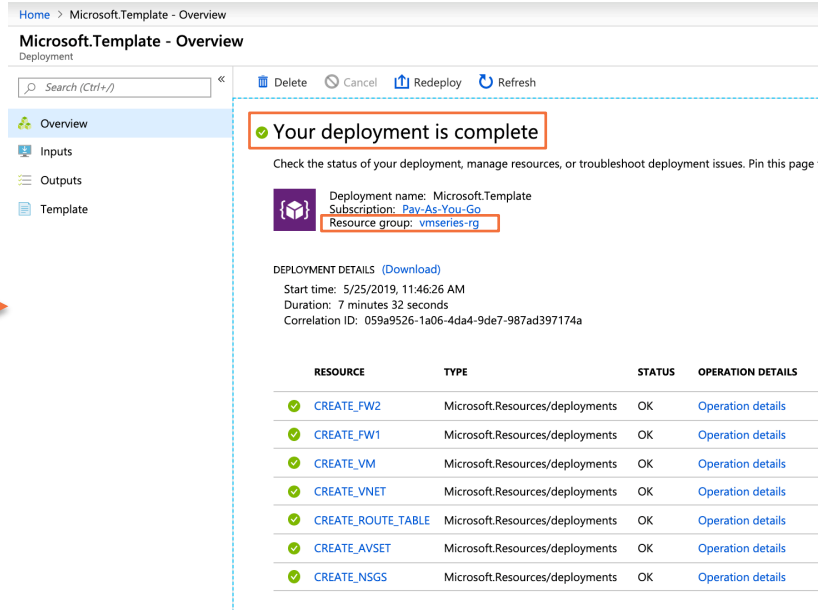
Username: Enter username (do not use admin or root)
Password: Enter password.



STEP 3. VERIFY DEPLOYMENT & OPEN RESOURCE GROUP

- Once the deployment completes, open the Resource Group.

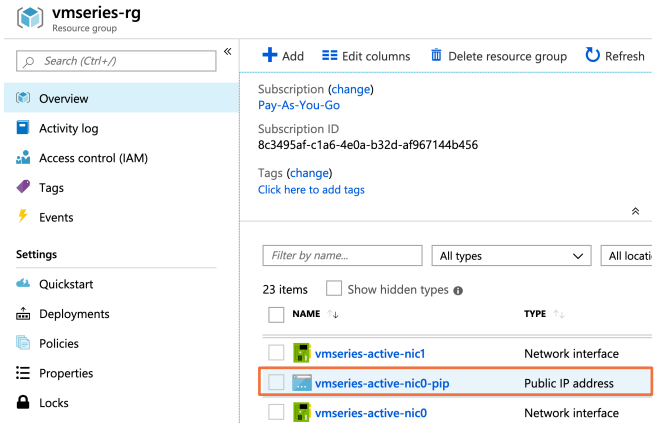




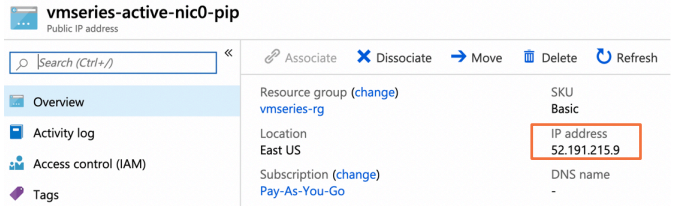
CONFIGURE
ACTIVE FIREWALL

STEP 4. ACCESS ACTIVE FW GUI

1. Resource Group → Overview → **vmseries-active-nic0-pip**



2. Copy public IP Address



3. Paste into URL https://<*public_ip*>
   Login with username & password from **Step 2**

STEP 5. IMPORT & LOAD CONFIGURATION

Device → Setup → Operations

→ **Import named configuration snapshot**

→ select **active-fw-config.xml**

→ **Load named configuration snapshot**

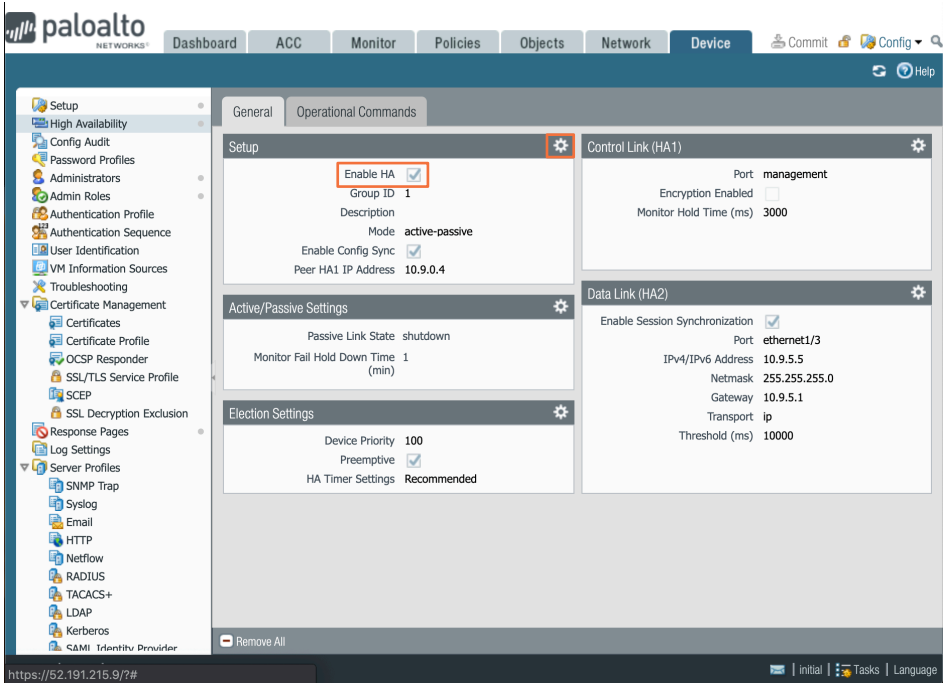
→select **active-fw-config.xml**

STEP 6. ENABLE HA

Device → High Availability

→ General→ Setup

→Check on **Enable HA**



CREATE AZURE SERVICE PRINCIPAL (skip if you already have one)

Please see: - Application and service principal objects in Azure Active Directory
- Create an Azure service principal with Azure CLI

1. Log into Azure CLI

```
> az login
```

2. Create service principal

```
> az ad sp create-for-rbac --name vmseries-HA
  {
    "appId": "17c******-****-****-****-********061",        ← Client ID
    "displayName": "vmseries-HA",
    "name": "http://vmseries-HA",
    "password": "*a36*****-****-****-****-********97b",    ← Client Secret
    "tenant": "52f*****-****-****-****-********b28"        ← Tenant ID
  }
```

3. Verify role

```
> az role assignment list --assignee 17c******-****-****-****-********061
  [
    {
      "canDelegate": null,
      "id": "/subscriptions/<subscription_id>/providers/Microsoft.Authorization/roleAssignments/<redacted>",
      "name": "<redacted>",
      "principalId": "<redacted>",
      "principalName": "http://vmseries-HA",
      "roleDefinitionId": "<redacted>",
      "roleDefinitionName": "Contributor",  ← Valid role
      "scope": "<redacted>",
      "type": "Microsoft.Authorization/roleAssignments"
    }
  ]
```


STEP 7. CONFIGURE AZURE HA PLUGIN

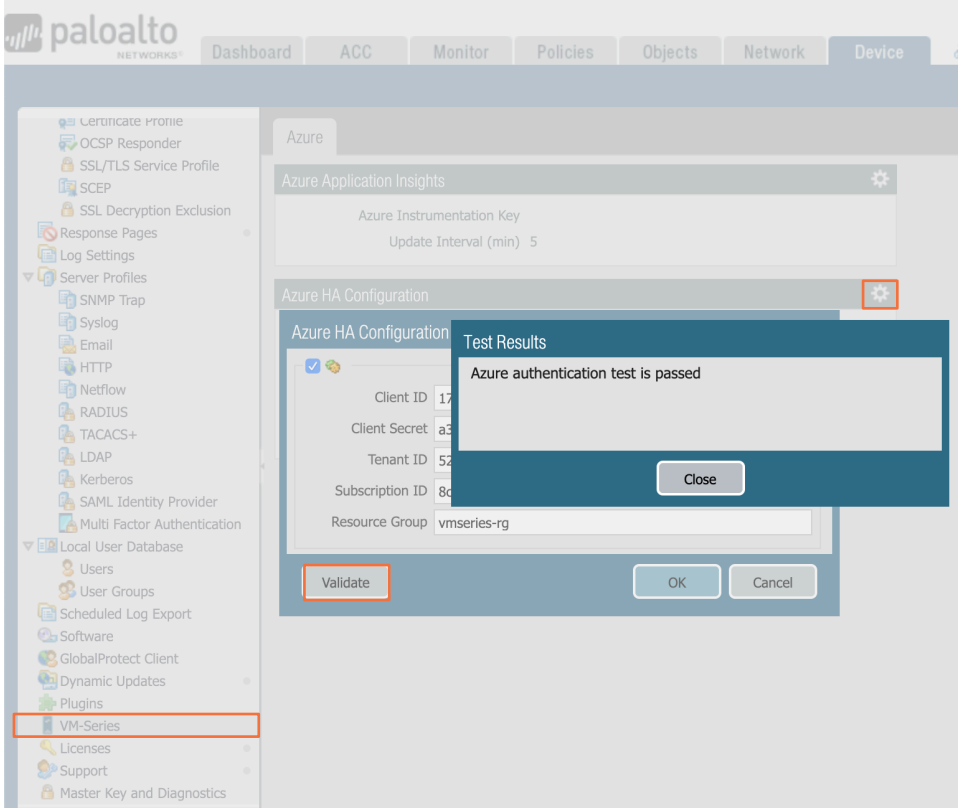
1. Device → VM-Series → Azure HA Configuration
   → Enter your Azure service principal parameters

2. Click Validate to test plugin authentication.

COMMIT CHANGES

The imported configuration has a default username & password

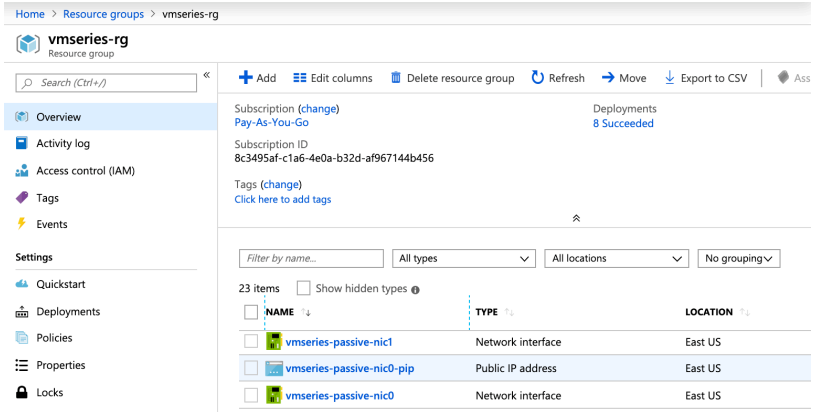
UN:paloalto / **PW:**PanPassword123**!**



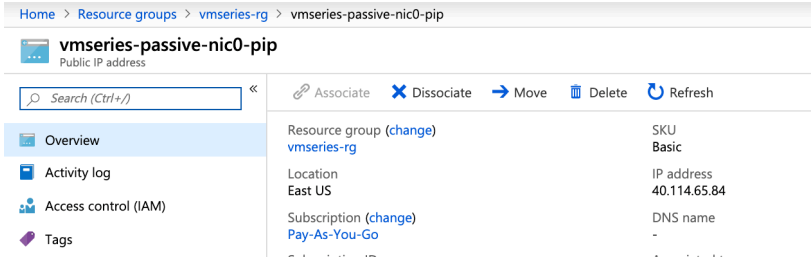
CONFIGURE PASSIVE FIREWALL

STEP 8. ACCESS PASSIVE FW GUI

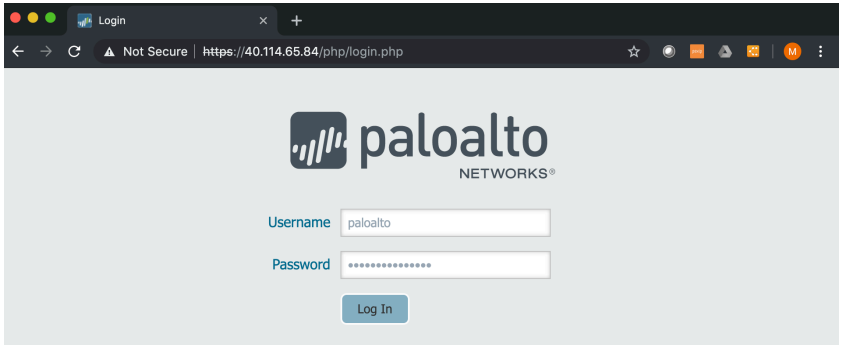
1. Overview → **vmseries-passive-nic0-pip**



2. Copy public IP Address



3. Paste into URL https://<*public_ip*>
   Login with username & password from **Step 2**



STEP 9. IMPORT & LOAD CONFIGURATION

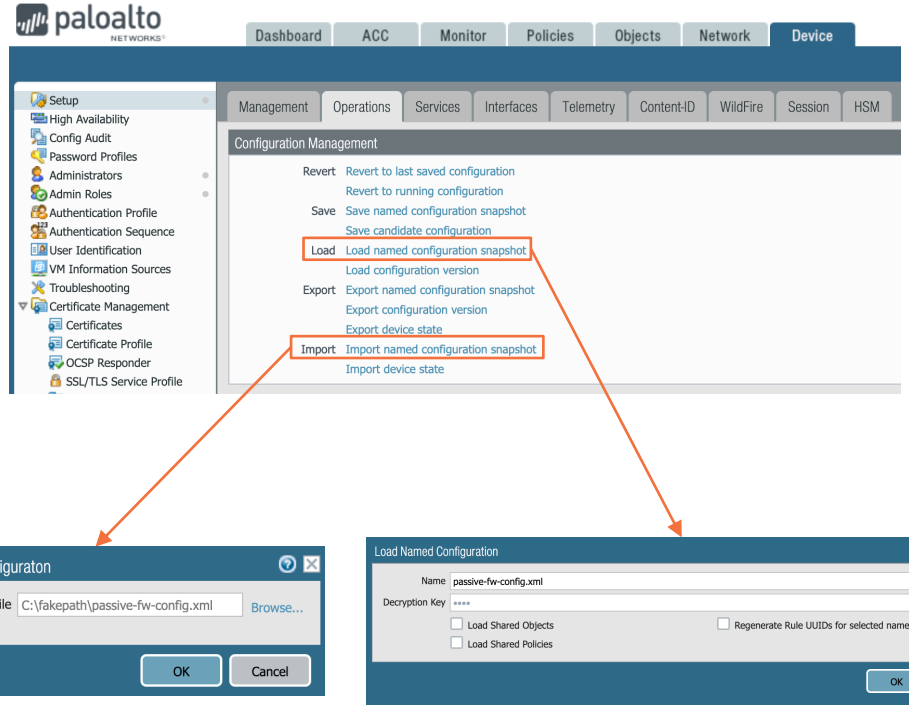
Device → Setup → Operations

→ **Import named configuration snapshot**

→ select **passive-fw-config.xml**

→ **Load named configuration snapshot**

→select **passive-fw-config.xml**



COMMIT CHANGES

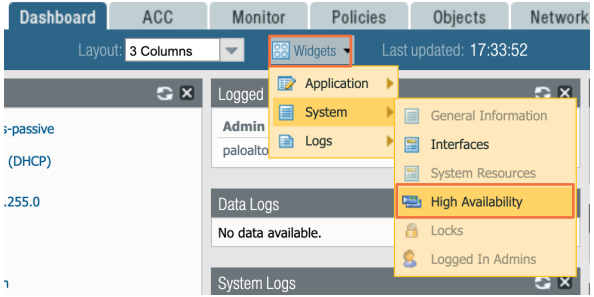
The imported configuration has a default username & password

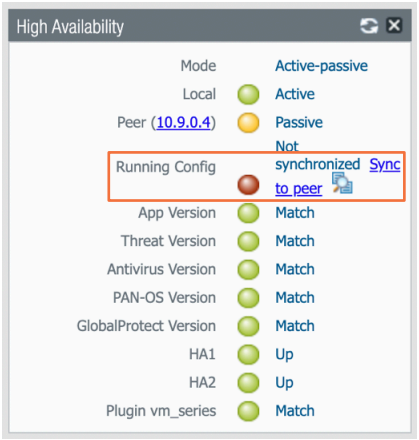
UN:paloalto **/ PW:**PanPassword123**!**

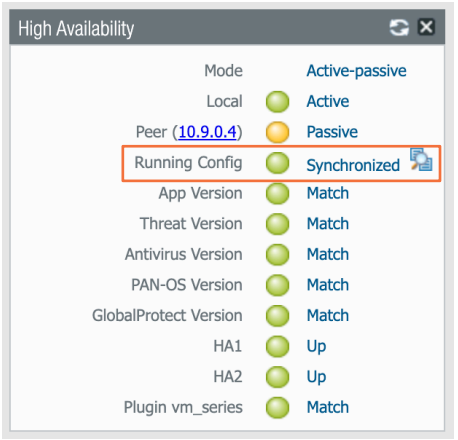
STEP 10. SYNC ACTIVE FW WITH PASSIVE FW

1. On both firewalls, enable the High Availability Widget
   Dashboard → Widgets
   → System → High Availability

2. On the **Active firewall**, click Sync to peer.



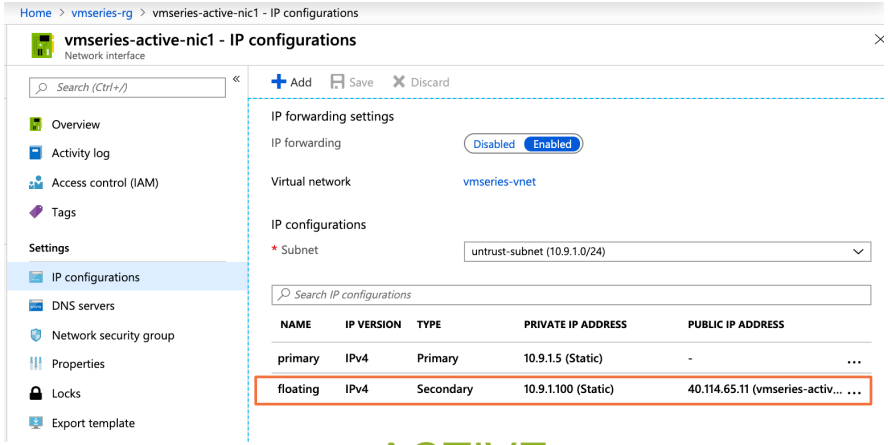




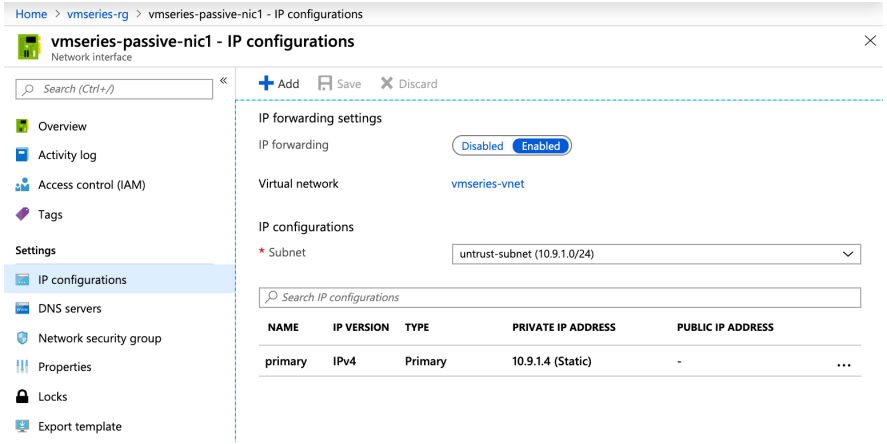
TEST FAILOVER

VERIFY UNTRUST FLOATING IP ON ACTIVE FW

1. In the Azure portal, open the IP configurations for vmseries-active-nic1 and vmseries-passive-nic1
2. The floating IP (10.9.1.100) resides on vmseries-active-nic1.



ACTIVE
(before failover)

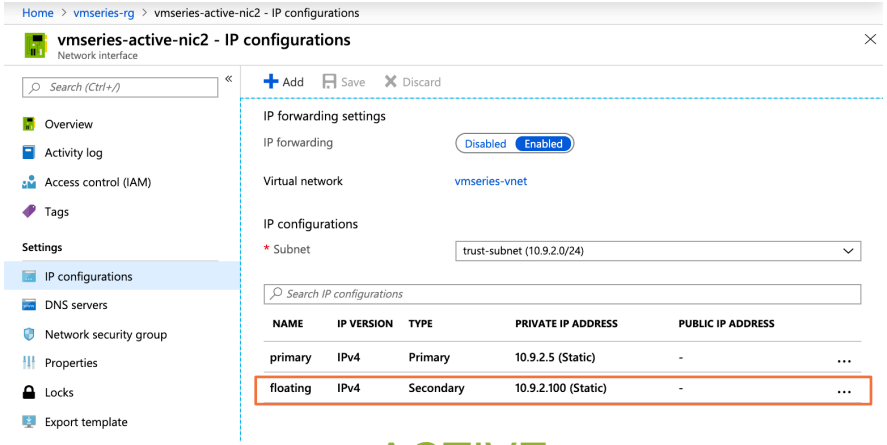


PASSIVE
(before failover)

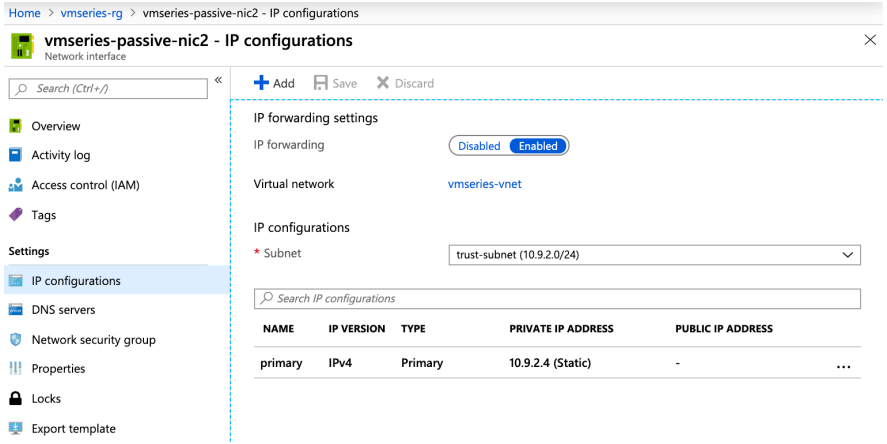
VERIFY TRUST FLOATING IP ON ACTIVE FW

1. In the Azure portal, open the IP configurations for vmseries-active-nic2 and vmseries-passive-nic2

2. The floating IP (10.9.2.100) resides on vmseries-active-nic2.



ACTIVE
(before failover)



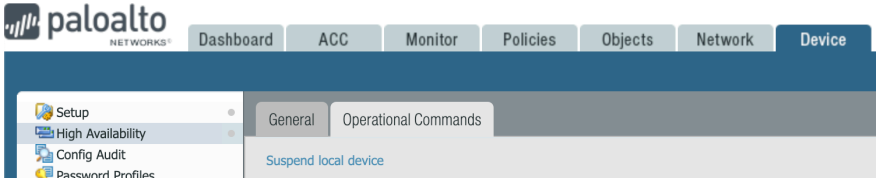
PASSIVE
(before failover)

INITIATE A FAILOVER

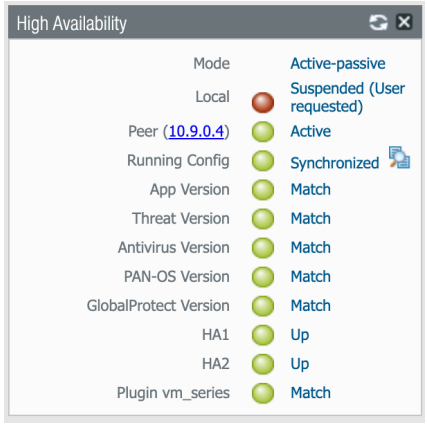
1. On the **Active firewall**, go to:

   Device → High Availability → Operational Commands

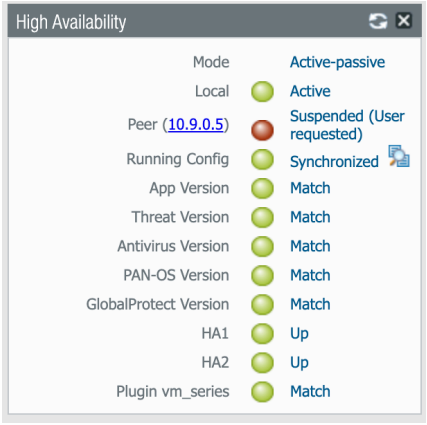
   → click Suspend local device



2. View the High Availability widget. The passive firewall should now be Active.



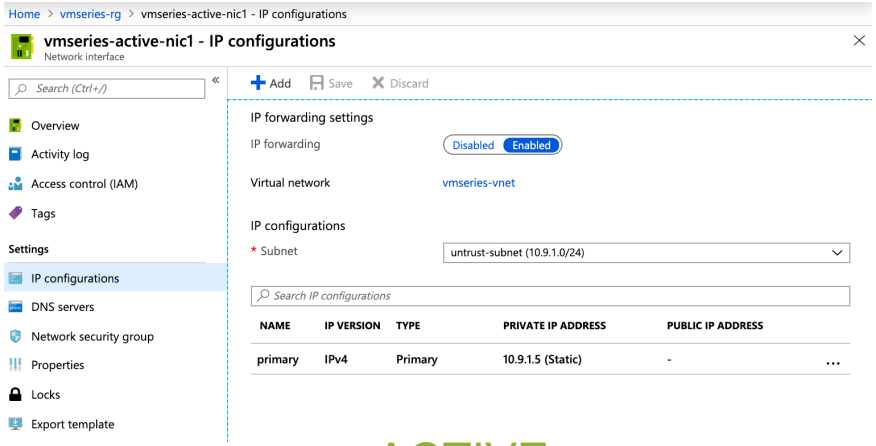
ACTIVE
(after failover)



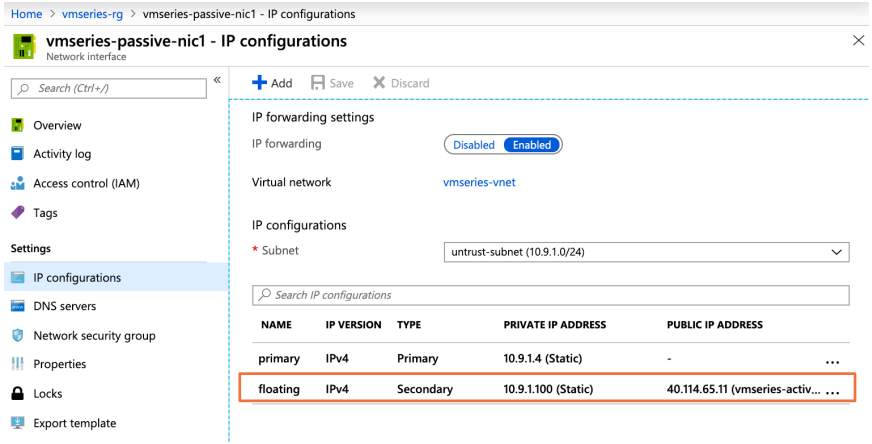
PASSIVE
(after failover)

VERIFY UNTRUST FLOATING IP MOVE TO PASSIVE FW

1. In the Azure portal, open the IP configurations for vmseries-active-nic1 and vmseries-passive-nic1
2. The floating IP (10.9.1.100) should now belong to vmseries-passive-nic1



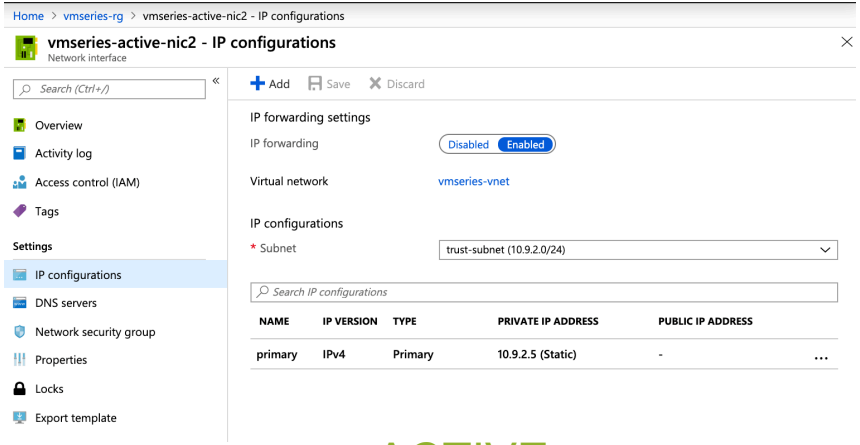
ACTIVE
(after failover)



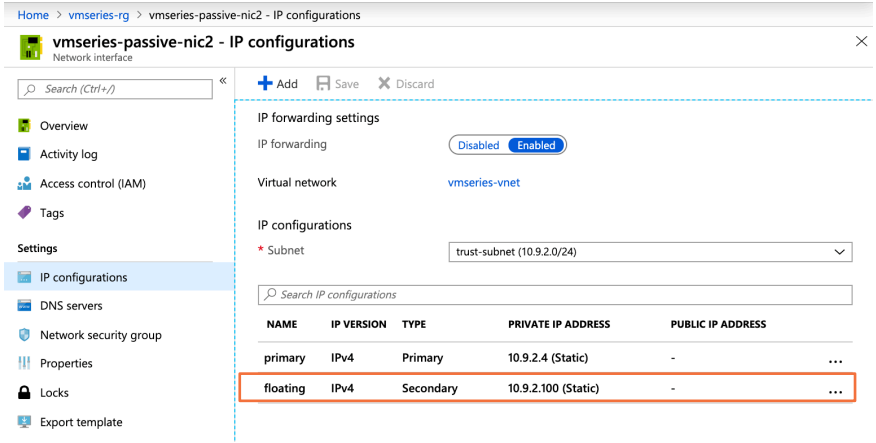
PASSIVE
(after failover)

VERIFY TRUST FLOATING IP MOVE TO PASSIVE FW

1. In the Azure portal, open the IP configurations for vmseries-active-nic2 and vmseries-passive-nic2
2. The floating IP (10.9.2.100) should now belong to vmseries-passive-nic2



ACTIVE
(after failover)



PASSIVE
(after failover)

