Deploy the Firewall Management Center Virtual on OCI

Oracle Cloud Infrastructure (OCI) is a public cloud computing service that enables you to run your applications in a highly available, hosted environment offered by Oracle. OCI provides real-time elasticity for enterprise applications by combining Oracle's autonomous services, integrated security, and serverless compute.

You can deploy the Firewall Management Center Virtual on OCI.

Overview

The Firewall Management Center Virtual runs the same software as physical Firewall Management Center to deliver proven security functionality in a virtual form factor. The Firewall Management Center Virtual can be deployed in the public OCI. It can then be configured to manage virtual and physical devices.

OCI Compute Shapes

A shape is a template that determines the number of CPUs, amount of memory, and other resources that are allocated to an instance. The Firewall Management Center Virtual support the following OCI shape types:

Table 1: Supported Compute Shapes for Firewall Management Center Virtual

OCI Shape	Supported Firewall Management Center Virtualversion	Attributes	
		oCPUs	RAM (GB)
Intel VM.StandardB1.4	7.3.0 and later	4	48
Intel VM.Standard2.4	7.1.0 and later	4	60
Intel VM.Standard3.Flex	7.3.0 and later	4	64

OCI Shape	Supported Firewall Management Center Virtualversion	Attributes	
		oCPUs	RAM (GB)
Intel VM.Optimized3.Flex	7.3.0 and later	4	56
AMD VM.Standard.E4.Flex	7.3.0 and later	4	32

Recommendations for using the OCI Compute shapes supported by Firewall Management Center Virtual version 7.3 and later.

- OCI marketplace image version **7.3.0-69-v3** and later are compatible only with the OCI compute shapes of Firewall Management Center Virtual 7.3 and later.
- You can use the OCI compute shapes supported by Firewall Management Center Virtual 7.3 and later only for new deployments.
- OCI compute shapes version **7.3.0-69-v3** and later are not compatible with upgrading VMs that are deployed with Firewall Management Center Virtual using the OCI compute shape versions earlier to Firewall Management Center Virtual 7.3.

Table 2: Supported Compute Shapes for Firewall Management Center Virtual 300 (FMCv300) on Version 7.1.0 and Later

OCI Shape	Attributes	
	oCPUs	RAM (GB)
VM.Standard2.16	16	240 GB SSD storage: 2000 GB

Note Supported shape types may change without notice.

- In OCI, 1 oCPU is equal to 2 vCPU.
- The Firewall Management Center Virtual requires 1 interface.

You create an account on OCI, launch a compute instance using the Firewall Management Center Virtual offering on the Oracle Cloud Marketplace, and choose an OCI shape.

Prerequisites

- Create an OCI account at https://www.oracle.com/cloud/.
- A Cisco Smart Account. You can create one at Cisco Software Central (https://software.cisco.com/).
  - Configure all license entitlements for the security services from the Firewall Management Center.
  - See “Licensing the System” in the Firewall Management Center Configuration Guide for more information about how to manage licenses.

- Interface requirements:
  - Management interface — One used to connect the Firewall Threat Defense device to the Firewall Management Center.
- Communications paths:
  - Public IP for administrative access to the Firewall Management Center Virtual.
- For the Firewall Management Center Virtual and System compatibility, see Cisco Secure Firewall Threat Defense Compatibility Guide.

Guidelines and Limitations

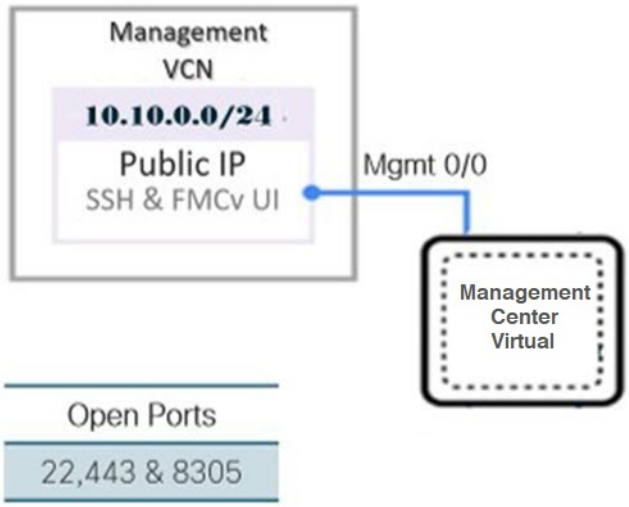
Supported Features

- Deployment in the OCI Virtual Cloud Network (VCN)
- Maximum of 8 vCPUs per instance
- Routed mode (default)
- Licensing – Only BYOL is supported
- IPv6
- **Firewall Management Center Virtual 300 (FMCv300) for OCI**—A new scaled Firewall Management Center Virtual image is available on the OCI platform that supports managing up to 300 devices and has higher disk capacity (7.1.0+).
- Firewall Management Center Virtual high availability (HA) is supported

Sample Network Topology

The following figure illustrates the typical topology for the Firewall Management Center Virtual with 1 subnet configured in OCI.

Figure 1: Topology Example for the Firewall Management Center Virtual Deployment on OCI



Deploy the Firewall Management Center Virtual

Configure the Virtual Cloud Network (VCN)

You configure the Virtual Cloud Network (VCN) for your Firewall Management Center Virtual deployment.

Before you begin

Note After you select a service from the navigation menu, the menu on the left includes the compartments list. Compartments help you organize resources to make it easier to control access to them. Your root compartment is created for you by Oracle when your tenancy is provisioned. An administrator can create more compartments in the root compartment and then add the access rules to control which users can see and take action in them. See the Oracle document "Managing Compartments" for more information.

Procedure

Step 1 Log into OCI and choose your region.

OCI is divided into multiple regions that are isolated from each other. The region is displayed in the upper right corner of your screen. Resources in one region do not appear in another region. Check periodically to make sure you are in the intended region.

Step 2 Choose **Networking** > **Virtual Cloud Networks** and click **Create VCN**.

Step 3 Enter a descriptive **Name** for your VCN, for example *FMCv-Management*.

Step 4 Enter a **CIDR block** for your VCN.

Step 5 Click **Create VCN**.

What to do next

You can continue with the following procedures to complete the Management VCN.

Create the Network Security Group

A network security group consists of a set of vNICs and a set of security rules that apply to the vNICs.

Procedure

Step 1 Choose **Networking** > **Virtual Cloud Networks** > **Virtual Cloud Network Details** > **Network Security Groups**, and click **Create Network Security Group**.

Step 2 Enter a descriptive **Name** for your Network Security Group, for example *FMCv-Mgmt-Allow-22-443-8305*.

Step 3 Click **Next**.

Step 4 Add your security rules:

a) Add a rule to allow TCP port 22 for SSH access.
b) Add a rule to allow TCP port 443 for HTTPS access.
c) Add a rule to allow TCP port 8305.

The device Firewall Management Center Virtual can be managed via the Firewall Management Center Virtual, which requires port 8305 to be opened for HTTPS connections. You need port 443 to access the Firewall Management Center itself.

Step 5 Click **Create**.

Create the Internet Gateway

An Internet gateway is required to make your management subnet publicly accessible.

Procedure

Step 1 Choose **Networking** > **Virtual Cloud Networks** > **Virtual Cloud Network Details** > **Internet Gateways**, and click **Create Internet Gateway**.

Step 2 Enter a descriptive **Name** for your Internet gateway, for example *FMCv-IG*.

Step 3 Click **Create Internet Gateway**.

Step 4 Add the route to the Internet Gateway:

a) Choose **Networking** > **Virtual Cloud Networks** > **Virtual Cloud Network Details** > **Route Tables**.
b) Click on the link for your default route table to add route rules.
c) Click **Add Route Rules**.
d) From the **Target Type** drop-down, select **Internet Gateway**.
e) Enter the Destination CIDR Block, for example 0.0.0.0/0.

f) From the **Target Internet Gateway** drop-down, select the gateway you created.
g) Click **Add Route Rules**.

Create the Subnet

Each VCN will have one subnet, at a minimum. You'll create a Management subnet for the Management VCN.

Procedure

Step 1 Choose **Networking** > **Virtual Cloud Networks** > **Virtual Cloud Network Details** > **Subnets**, and click **Create Subnet**.
Step 2 Enter a descriptive **Name** for your subnet, for example *Management*.
Step 3 Select a **Subnet Type** (leave the recommended default of **Regional**).
Step 4 Enter a **CIDR Block**, for example 10.10.0.0/24. The internal (non-public) IP address for the subnet is taken from this CIDR block.
Step 5 Select one of the route tables you created previously from the **Route Table** drop-down.
Step 6 Select the **Subnet Access** for your subnet.

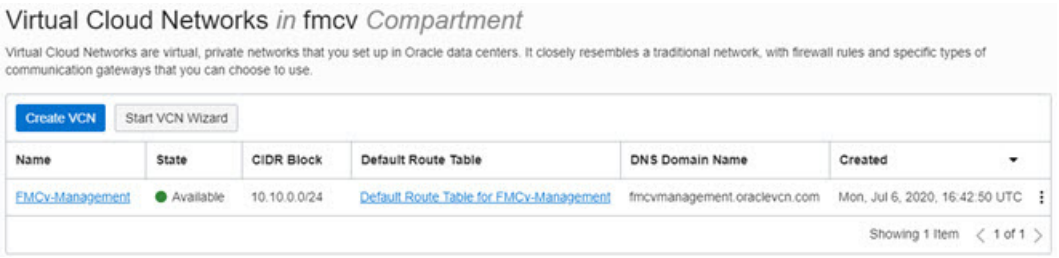
For the Management subnet, this must be **Public Subnet**.

Step 7 Select the **DHCP Option**.
Step 8 Select a **Security List** that you created previously.
Step 9 Click **Create Subnet**.

What to do next

After you configure your Management VCN you are ready to launch the Firewall Management Center Virtual. See the following figure for an example of the Firewall Management Center Virtual VCN configuration.

Figure 2: Firewall Management Center Virtual Virtual Cloud Network



Create the Firewall Management Center Virtual Instance on OCI

You deploy the Firewall Management Center Virtual on OCI via a Compute instance using the Firewall Management Center Virtual - BYOL offering on the Oracle Cloud Marketplace. You select the most appropriate machine shape based on characteristics such as the number of CPUs, amount of memory, and network resources.

Procedure

Step 1 Log into the OCI portal.

The region is displayed in the upper right corner of your screen. Make sure you are in the intended region.

Step 2 Choose **Marketplace** > **Applications**.

Step 3 Search Marketplace for “Firewall Management Center Virtual” and choose the offering.

Step 4 Review the Terms and Conditions, and check the **I have reviewed and accept the Oracle Terms of Use and the Partner terms and conditions.**check box.

Step 5 Click **Launch Instance**.

Step 6 Enter a descriptive **Name** for your instance, for example *Cisco-FMCv*.

Step 7 Click **Change Shape** and select the shape with the number of CPUs, amount of RAM, and number of interfaces required for the Firewall Management Center Virtual, for example VM.Standard2.4 (see OCI Compute Shapes, on page 1).

Step 8 From the **Virtual Cloud Network** drop-down, choose the Management VCN.

Step 9 From the **Subnet** drop-down, choose the Management subnet if it's not autopopulated.

Step 10 Check **Use Network Security Groups to Control Traffic** and choose the security group you configured for the Management VCN.

Step 11 Click the **Assign a Public Ip Address** radio button.

Step 12 Under **Add SSH keys**, click the **Paste Public Keys** radio button and paste the SSH key.

Linux-based instances use an SSH key pair instead of a password to authenticate remote users. A key pair consists of a private key and public key. You keep the private key on your computer and provide the public key when you create an instance. See Managing Key Pairs on Linux Instances for guidelines.

Step 13 Click the **Show Advanced Options** link to expand the options.

Step 14 Under **Initialization Script**, click the **Paste Cloud-Init Script** radio button to provide the day0 configuration for the Firewall Management Center Virtual. The day0 configuration is applied during the firstboot of the Firewall Management Center Virtual.

The following example shows a sample day0 configuration you can copy and paste in the **Cloud-Init Script** field:

```
{
"AdminPassword": "myPassword@123456",
"Hostname": "cisco-fmcv"
}
```

Step 15 Click **Create**.

What to do next

Monitor the Firewall Management Center Virtual instance, which shows the state as Provisioning after you click the **Create** button. It’s important to monitor the status. Look for the Firewall Management Center Virtual instance to go from Provisioning to Running state, which indicates the Firewall Management Center Virtual boot is complete.

Access the Firewall Management Center Virtual Instance on OCI

You can connect to a running instance by using a Secure Shell (SSH) connection.

- Most UNIX-style systems include an SSH client by default.
- Windows 10 and Windows Server 2019 systems should include the OpenSSH client, which you'll need if you created your instance using the SSH keys generated by Oracle Cloud Infrastructure.
- For other Windows versions you can download PuTTY, the free SSH client from http://www.putty.org.

Prerequisites

You'll need the following information to connect to the instance:

- The public IP address of the instance. You can get the address from the Instance Details page in the Console. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**. Then, select your instance. Alternatively, you can use the Core Services API ListVnicAttachments and GetVnic operations.
- The username and password of your instance.
- The full path to the private key portion of the SSH key pair that you used when you launched the instance.

  For more information about key pairs, see Managing Key Pairs on Linux Instances.

Note If you choose not to add a Day0 configuration, you can log in to the Firewall Management Center Virtual instance using the default credentials (admin/Admin123).

You are prompted to set the password on the first login attempt.

Connect to the Firewall Management Center Virtual Instance Using PuTTY

To connect to the Firewall Management Center Virtual instance from a Windows system using PuTTY:

Procedure

Step 1 Open PuTTY.

Step 2 In the **Category** pane, select **Session** and enter the following:

- **Host Name (or IP address):**

  `<username>@<public-ip-address>`

  Where:

  `<username>` is the username for the Firewall Management Center Virtual instance.

<public-ip-address> is your instance public IP address that you retrieved from the Console.

- **Port:** 22
- **Connection type:** SSH

Step 3 In the **Category** pane, expand **Window**, and then select **Translation**.

Step 4 In the **Remote character set** drop-down list, select **UTF-8**.

The default locale setting on Linux-based instances is UTF-8, and this configures PuTTY to use the same locale.

Step 5 In the **Category** pane, expand **Connection**, expand **SSH**, and then click **Auth**.

Step 6 Click **Browse**, and then select your private key.

Step 7 Click **Open** to start the session.

If this is your first time connecting to the instance, you might see a message that the server's host key is not cached in the registry. Click **Yes** to continue the connection.

Connect to the Firewall Management Center Virtual Instance Using SSH

To connect to the Firewall Management Center Virtual instance from a Unix-style system, log in to the instance using SSH.

Procedure

Step 1 Use the following command to set the file permissions so that only you can read the file:

```
$ chmod 400 <private_key>
```

Where:

<private_key> is the full path and name of the file that contains the private key associated with the instance you want to access.

Step 2 Use the following SSH command to access the instance:

```
$ ssh -i <private_key> <username>@<public-ip-address>
```

<private_key> is the full path and name of the file that contains the private key associated with the instance you want to access.

<username> is the username for the Firewall Management Center Virtual instance.

<public-ip-address> is your instance IP address that you retrieved from the console.

Connect to the Firewall Management Center Virtual Instance Using OpenSSH

To connect to the Firewall Management Center Virtual instance from a Windows system, log in to the instance using OpenSSH.

Procedure

Step 1 If this is the first time you are using this key pair, you must set the file permissions so that only you can read the file.

Do the following:

a) In Windows Explorer, navigate to the private key file, right-click the file, and then click **Properties**.
b) On the **Security** tab, click **Advanced**.
c) Ensure that the **Owner** is your user account.
d) Click **Disable Inheritance**, and then select **Convert inherited permissions into explicit permissions on this object**.
e) Select each permission entry that is not your user account and click **Remove**.
f) Ensure that the access permission for your user account is **Full control**.
g) Save your changes.

Step 2 To connect to the instance, open Windows PowerShell and run the following command:

```
$ ssh -i <private_key> <username>@<public-ip-address>
```

Where:

`<private_key>` is the full path and name of the file that contains the private key associated with the instance you want to access.

`<username>` is the username for the Firewall Management Center Virtual instance.

`<public-ip-address>` is your instance IP address that you retrieved from the Console.