HPE OneSphere
Your hybrid cloud manager is here
**Contents**

- Executive summary ......................................................... 3
- HPE OneSphere core functionalities .................................. 4
  - The hybrid cloud management service .......................... 4
  - The cloud platforms .................................................... 5
- Understanding HPE OneSphere at a deeper level ............. 6
- HPE OneSphere requirements .......................................... 8
  - Networking for on-premises virtualized environments .... 8
  - Hybrid licensing requirements ..................................... 9
- Connecting cloud platforms to HPE OneSphere .............. 10
  - VMware-based private cloud provider ......................... 10
  - KVM-based private cloud provider ............................... 13
  - Amazon Web Services public cloud provider ................. 14
  - Microsoft Azure public cloud provider ......................... 17
  - Kubernetes in underlying IaaS cloud platforms ........... 18
- Controlling multiple cloud resources access through Projects ............................................................................ 20
  - AWS Compliance ....................................................... 21
- Hybrid service catalog management ................................ 24
  - Catalog curation .......................................................... 25
- Deploying workloads across multiple cloud platforms .. 26
  - Deploying services on private and public IaaS clouds .. 26
  - Deploying containerized applications ......................... 28
- IT operations .................................................................... 29
- Business control and analytics ....................................... 30
  - Insights Dashboards .................................................... 30
  - Insights Reports .......................................................... 32
- How is cost information calculated? ............................... 33
- About HPE OneSphere API ............................................ 33
- Summary ........................................................................ 34
- Resources ........................................................................ 34
Executive summary

By 2020, Gartner predicts that multi-cloud, which includes hybrid cloud, will become the standard as medium to large enterprises have begun moving suitable workloads to public and private clouds. This introduces new challenges for IT organizations in how they manage their cloud environments. Enterprises are seeking a unified management experience as they begin to implement their cloud strategies.

HPE OneSphere is a new approach to hybrid cloud, delivering a comprehensive, end-to-end, software-as-a-service (SaaS) solution with hybrid cloud management as a service. With HPE OneSphere, you will have flexibility to compose and operate virtualized and containerized workloads across on-premises private cloud platforms and public cloud platforms from a single unified user interface and common API.

HPE OneSphere is designed to simplify the hybrid cloud operations and provide a "low-ops" experience with Hewlett Packard Enterprise managing all back end operations. HPE OneSphere gives you, the IT operations manager, a single point of management for organizing hybrid cloud resources and users into projects. This helps you to control the resources that are delivered to users as a service from private and public cloud providers while monitoring the resources availability, performance, utilization, and usage cost of each cloud platform provider.

HPE OneSphere is architected to accelerate application delivery and deployment on containers, virtualized environments, and bare metal servers, thereby optimizing the right mix of on- and off-premise resources. Developers get fast access to their projects with a rich library of applications and service templates that facilitate quick OS and application deployments across your hybrid cloud platforms.

HPE OneSphere is engineered with dashboard reports providing IT and line of business executives with analytics across the entire hybrid cloud estate for near-real-time utilization, health, and cost insights. This enables greater visibility and control of your on-premises and public cloud costs while helping you to manage deployments and optimize cloud usage.

This technical white paper describes the technical features of the HPE OneSphere solution and provides insights into how the solution operates to deliver a true hybrid cloud management solution.

HPE OneSphere provides unified management of your cloud and cloud-like resources hosted in your hybrid cloud environments. For the purpose of this document, hybrid cloud refers to a mix of traditional on-premises IT, private cloud, and public cloud platforms. Hybrid cloud refers to a mix of private and public clouds while multi-cloud refers to more than one cloud platform.

---

1 If you are a Gartner seat holder, you may view the full Gartner 2018 planning guide for cloud computing: gartner.com/document/3810365
HPE OneSphere core functionalities

HPE OneSphere is a hybrid cloud management platform delivered as a managed service via a SaaS platform hosted in the public cloud. Figure 1 shows the different functional components of the solution dedicated to each HPE OneSphere customer. This architectural view represents HPE's long-term vision of the services and deployment options for HPE OneSphere. The solution consists of two distinct component groups; the hybrid cloud “Management as a Service” group used for managing cloud deployments and, below that, the cloud platforms that are running the different workloads and applications.

![Diagram of HPE OneSphere functional view](image)

**Figure 1. HPE OneSphere long-term functional view**

The hybrid cloud management service

When an HPE customer signs up for an HPE OneSphere account, a dedicated SaaS-based management service environment created, hosted and centrally managed by HPE for that customer. Each customer's cloud-hosted management service runs in isolation from every other customer's management service, so no two customers will ever share the same components. These components provide the management plane functions needed to manage and operate multiple cloud environments across private and public clouds. They include the following functional capabilities that enable on-demand resource provisioning across the managed multiple clouds.

- A single and unified hybrid cloud portal (console) is used by IT operations for managing the cloud platform resources, users, projects, and service catalog registries. This portal is also used for monitoring the utilization of resources and their associated health status. It is used by cloud service consumers, such as developers, to deploy workloads across private and public clouds. It is used by IT operations and lines of business executives to get visibility on cost insights and analytics as well as show back information.
- A REST Application Programming Interface (API) that offers programmatic access to the hybrid cloud management service.
- Extensive communication and security standards to securely deploy, operate, and manage a customer's cloud infrastructure.
- The ability for the hybrid cloud administrator to organize hybrid cloud resources, users, and multi-tenancy into projects to control the resources that are available for a users' consumption.
- A service catalog of curated service and application image templates, containers, and helm charts, plus deployed instances. This provides business users and developers the resources needed to run efficiently in the hybrid cloud environment.
- Centralized runtime tasks such as management, control, monitoring, and metering functions that run across a customer's managed private and public cloud platforms.
• Cloud platforms lifecycle management (LCM) services orchestrate and simplify deployment and operations of the cloud platforms across the entire hybrid cloud estate.

• Cloud analytics that provides IT executives and business leaders with visibility into on-premises and public cloud utilization and usage costs, thereby enabling them with the information they need to control cloud costs.

The cloud platforms
The management service components provide a hybrid cloud management layer that delivers insight and control of resources and orchestrates the deployment of workloads across multiple private and public cloud platforms. The cloud platforms are:

• On-premises resources running on HPE hardware and non-HPE hardware. HPE OneSphere is a hybrid cloud management solution that optimizes what customers already have in their data centers. In the context of HPE OneSphere, this approach is defined as “brownfield” where the offering manages the virtual resources running on the existing on-premises virtualized infrastructures connected to HPE OneSphere management service. These virtualized infrastructures, when connected to HPE OneSphere, enable on-premises equipment to be composed into a variety of modern private cloud stacks. They are infrastructure as a service (IaaS) delivered on virtualized environments (VMware and KVM) and Kubernetes-based containers as a service (CaaS) delivered on VMware-based virtualized environments from HPE OneSphere.

• Public cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) for IaaS and CaaS capabilities delivered to users as a service from HPE OneSphere.

Note
HPE OneSphere currently supports Microsoft Azure IaaS through ARM templates deployment, AWS-based IaaS through CloudFormation template deployments and Kubernetes-based CaaS as well as cloud analytics functionalities for AWS and Microsoft Azure public cloud accounts connected to HPE OneSphere. Support of Infrastructure as a Service Google Cloud Platform is being considered for a future release.

2 Kubernetes is a leading container orchestration framework. It is an open-source platform for automating deployment, scaling, and management of containerized applications. More information about Kubernetes can be found at [kubernetes.io/docs/concepts/overview/what-is-kubernetes/](https://kubernetes.io/docs/concepts/overview/what-is-kubernetes/)
Understanding HPE OneSphere at a deeper level

The previous section depicted a high-level understanding of the components that make up HPE OneSphere and their functions. Let’s dive into the technical details. Figure 2 outlines the HPE OneSphere architecture, its underlying components, and their relationships. It also illustrates how it delivers a hybrid cloud management solution for IaaS and CaaS environments across on-premises virtualized resources, AWS public cloud, and Kubernetes clusters.

Figure 2. HPE OneSphere technical architecture

Note
For Microsoft Azure service provider, there is no zone relationship, and the deployment of the workloads will be performed using the Azure Resource Manager (ARM) templates. The discovery is using Azure services is different from AWS; however, OneSphere provides the same ratings, compliance capability, and projects to deploy the Azure workloads.

The SaaS-based management service tier is the backbone of HPE OneSphere. The management service tier is a set of scalable and highly available services and tools running in containers. HPE OneSphere is built on a modern architecture using the leading open-source container orchestration framework, Kubernetes, as the base technology to deliver the hybrid cloud management service functions described in the previous section. The management service is operated and managed by HPE. It provides a centralized method for deploying and managing a customer’s private and public cloud platforms.
As shown in Figure 2, the SaaS-based management service is divided into **zones**. Zones are target cloud platforms where resources are made available to users to deploy services. A zone consists of a control plane in the management service tier and the compute, network, and storage resources in the on- or off-premises cloud platforms tier. Each cloud platform connected to the SaaS-based management service has its own control plane deployed in the hosted management service. HPE OneSphere monitors, troubleshoots, and upgrades them. The control plane provides the functions to control as well as manage resources and workloads deployed in a particular zone.

HPE OneSphere uses services and functionality as leveraged in OpenStack®, a popular open-source standard for IaaS, as the underlying technology to control and manage pools of compute, storage, and networking of on- and off-premises resources. Each zone dictates a set of OpenStack service endpoints for compute, networking, and storage that are independent from the other zones. All the zones in the customer's management service share one identity management service (OpenStack Keystone) that provides consistent access control across multiple cloud platforms.

For an AWS public cloud service provider, a zone is bound to an AWS availability zone (AZ). For an AWS public cloud platform, the control plane services provide the ability to integrate the core OpenStack projects such as Nova (compute), Glance (image), Neutron (network), and Cinder (persistent block storage) services with the customer's AWS public cloud accounts. This allows HPE OneSphere to orchestrate the deployment of users' virtual computing instances to Amazon Elastic Compute Cloud (EC2) and persistent block storage volumes attachment to EC2 instances using public cloud provider APIs.

For an on-premises KVM-based private cloud platform, a zone is bound to a set of KVM servers. Host agents running on each Linux® KVM server enables the KVM server to act as an OpenStack compute node for on-demand resource provisioning. The control plane in the management service tier utilizes the agents to communicate with the KVM server to install software that is required by a compute node such as the image library (Glance) service, persistent block storage (Cinder) service for data volume attachment to virtual machine instances, and novncproxy for virtual machine instance console access. The host agents also discovers and manages resources deployed on that server (network configuration, storage capacity, virtual machines) over a bidirectional secure communication channel initiated by the host agents.

For an on-premises VMware-based private cloud platform, a zone is bound to a VMware vCenter® environment which can manage one or more VMware ESXi™ clusters. A key component that enables HPE OneSphere to integrate with VMware-based on-premises resources is the **HPE OneSphere VMware Gateway Appliance (VGA)**. This appliance is a Linux virtual machine (VM), deployed as an open virtual appliance (OVA), by HPE OneSphere on a designated VMware vsphere® cluster in the VMware vCenter environment. The VGA transforms the VMware-based infrastructure into a self-service private cloud platform for on-demand resource provisioning. The HPE OneSphere VGA:

- Is configured per customer management service account and designed to HPE security standards. It is stamped with a customer's specific self-signed certificate. See the document “HPE OneSphere Security” for more context.
- Serves as the connection point between the HPE OneSphere management service's hosted control plane and the VMware vsphere vCenter environment. It establishes a secure internet communication channel and eliminates the need for VPN or other private communication channels between the control plane and the on-premises vCenter environment. The host agent installed in the VGA initiates a bidirectional secure TLS channel to HPE OneSphere management service using outbound HTTPS connections.
- Acts as an OpenStack compute service (Nova) “proxy” that maps OpenStack Nova service requests issued from HPE OneSphere into an equivalent that VMware vsphere vCenter Server can interpret. This, in turn, schedules wherein the vCenter infrastructure the users' VM instances should be deployed.
- Runs the OpenStack block storage Cinder volume service enabling HPE OneSphere users to create persistent block storage data volumes and attach them to VM instances using OpenStack CLI commands (OpenStack client).
- Is the OpenStack Image service (Glance) endpoints API, which allows VMware templates to be imported as service images in the HPE OneSphere service catalog.
- Acts as the nova-novncproxy endpoint for VM instance console access.
- Enables discovery of all the resources running on the private cloud platform including running VMs, VMware templates, network configuration, and storage capacity.
- Runs the metrics and health collection agent that continually sends metrics and health data to the management service (via the Monasca API) for calculation of utilization, performance, and availability of the resources in the private cloud platform. It also monitors information and statistics flow from the VGA to the HPE OneSphere management service.
The Kubernetes zone, which provides the CaaS to users, is a special case. The zone is positioned as a subset of underlying IaaS public or private cloud platforms that are connected to the SaaS-based management service. The IaaS cloud platforms are either on-premises VMware-based virtualized environments or AWS public cloud, or both. The Kubernetes cluster infrastructure (master nodes and worker nodes) are deployed on virtual machines in IaaS cloud platforms. Host agents are installed on each node so the HPE OneSphere management service controls all aspects of deployment, configuration, health monitoring, and upgrade of the Kubernetes components through a secure TLS communication channel. The host agents initiate a bidirectional secure TLS channel to HPE OneSphere management service using outbound HTTPS connection. In addition, the agents continually send utilization metrics and health data to the management service.

**HPE OneSphere requirements**

HPE OneSphere allows customers to connect to their existing on-premises virtualized environments and their public cloud provider accounts to enable workload deployments and a unified view of resource utilization and costs across all clouds platforms. For information about supported public cloud provider account types, as well as hardware and software requirements for existing on-premises virtualized environments, please refer to the HPE OneSphere support matrix documentation available at [hpe.com/onesphere/supportmatrix](http://hpe.com/onesphere/supportmatrix).

**Networking for on-premises virtualized environments**

Figure 3 depicts the logical network infrastructure recommended by HPE to prepare existing (brownfield) on-premises environments hosting VMware vSphere or KVM servers so they are ready for connection to HPE OneSphere. It is a best practice to segregate network traffic on separate network segments (VLANs). However, depending on a customers’ networking and security requirements, along with other configuration considerations, the network topology design may be different and some network traffic may be combined into one network segment or network trunk.
Table 1. Networking for on-premises virtualized private cloud platforms

<table>
<thead>
<tr>
<th>Network name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC management</td>
<td>The customer data center management network. Typically, it connects data center infrastructure services such as DNS, NTP and DHCP services.</td>
</tr>
<tr>
<td>ESXi host management</td>
<td>Network segment that carries ESXi cluster management traffic. It must have connectivity to VMware vCenter Server®.</td>
</tr>
<tr>
<td>HPE OneSphere management</td>
<td>Network carries HPE OneSphere management traffic. It must have outbound HTTPS connectivity to HPE OneSphere management service through the internet, with or without a proxy server, on the standard HTTPS port 443. It must also have connectivity to vCenter Server. This is the network segment into which you connect the KVM servers and the HPE OneSphere VMware Gateway Appliance.</td>
</tr>
<tr>
<td>Tenant networks (external)</td>
<td>Tenant's VM networks. There could be one or more tenant networks to carry VM instances traffic. Networks should have connectivity to and from the outside to make tenant's VM instances reachable from outside (internet/intranet). IP Address Management (IPAM) can be customer's DHCP service or provided by HPE OneSphere.</td>
</tr>
<tr>
<td>Tenant networks (private)</td>
<td>Tenant's VM networks. There could be one or more tenant networks to carry VM instances traffic. The VM networks are private. Network traffic is not routed outside the private segment. IPAM can be customer's DHCP service or provided by HPE OneSphere.</td>
</tr>
<tr>
<td>ESXi cluster services</td>
<td>Network segments that carry ESXi cluster services traffic for vMotion, or vSAN (if vSAN is implemented).</td>
</tr>
<tr>
<td>Storage (Front side)</td>
<td>Client-facing network that carries traffic between storage client (the KVM Servers) and Ceph Storage service.3</td>
</tr>
<tr>
<td>Storage (Back side)</td>
<td>Network segment that carries Ceph storage back-end traffic such as data replication between Ceph storage nodes.</td>
</tr>
<tr>
<td>HW management network</td>
<td>Hardware management network for HPE Synergy infrastructure, it carries HPE Synergy Composer (HPE OneView) traffic.</td>
</tr>
<tr>
<td>OS deployment</td>
<td>For HPE Synergy infrastructure, this is the Image Streamer OS deployment network that carries OS deployment traffic.</td>
</tr>
</tbody>
</table>

Hybrid licensing requirements

As a SaaS-based solution, HPE OneSphere is licensed via a 1-year, 3-year, or 5-year subscription model and offered as a 4-hybrid license unit (HLU) or 12-HLU license bundle. The hybrid licensing model addresses both on-premises and public cloud resource management with conversion between physical and virtual CPUs entitlements.

As shown in Figure 4, the basic HLU allows HPE OneSphere to manage 2 physical CPUs (2 sockets) on-premises or up to 20 virtual CPUs in the public cloud, with a conversion ratio of 1 physical CPU for 10 virtual CPUs.

![Figure 4. HPE OneSphere hybrid licensing entitlement](image-url)

3 HPE OneSphere integrates with Ceph storage solution powered by SUSE Enterprise Storage to provide persistent data volumes to KVM workloads. This enables customers to deploy enterprise class KVM applications in the HPE OneSphere private cloud. For more information about the Ceph storage solution, please refer to HPE OneSphere support Matrix documentation available at [hpe.com/onesphere/supportmatrix](http://hpe.com/onesphere/supportmatrix).
For example, the customer can start with a 4-HLU bundle for a 1-year subscription. That entitlement grants the customer eight physical CPUs for up to four on-premises servers with dual processors each or 80 virtual CPUs on the public cloud. Any combination of physical CPUs and virtual CPUs remains compliant with the entitlement as long as the maximum number of simultaneously managed physical CPUs on-premises and virtual CPUs on public cloud do not exceed the total entitlement quantity. Later, if needed, the customer can purchase additional HLUs with 1-HLU increments. When the subscription period is over, the customer will need to purchase new HLUs in order to renew their subscription. Each HLU license includes as well 24x7 foundation support licensing for reactive and monitoring support of the HPE OneSphere SaaS portal through HPE Pointnext Cloud CoE operations team.

Connecting cloud platforms to HPE OneSphere

In order to deliver a true hybrid cloud management solution of self-service infrastructures to users and enable on-demand resource provisioning across on- and off-premises resources, you must first connect private and public cloud providers to HPE OneSphere. Connectivity for each of the OneSphere supported zone types is covered in the following sub-sections for VMware, KVM, AWS, Azure, and Kubernetes.

VMware-based private cloud provider

HPE OneSphere has some requirements for working with VMware vSphere environment. You need a VMware vCenter Server and the vCenter user account to authenticate with HPE OneSphere.

Note

HPE OneSphere does not require vCenter root access permission to operate the vCenter environment. For further information about the minimum VMware vCenter access rights required to connect existing VMware vCenter environment to HPE OneSphere, refer to the HPE OneSphere Support Matrix available at hpe.com/OneSphere/supportmatrix.

The VMware vCenter Server can manage one or more VMware ESXi clusters with Distributed Resource Scheduler (DRS) enabled with the fully automated option and networking topology as described in the previous section. In order to provide high-availability of the VGA, VMware vSphere HA is recommended for the designated vSphere cluster that hosts VGA. The clusters must be configured with sufficient CPU, memory, and shared storage capacity to host the VM workloads that are anticipated to be deployed by users. All ESXi cluster hosts must have the Virtual Network Computing (VNC) server port (gdbserver) enabled in the ESXi security profile firewall for VM console access via the VNC protocol and the ESXi hosts system clock should be synchronized. Finally, you also need one or more VMware vSphere templates to act as images for the HPE OneSphere service catalog, although you can create the VMware templates later.

Note

A VMware ESXi Enterprise Plus license is required to meet OneSphere requirements for DRS and VMware vSphere® Distributed Switch™ (vDS) enablement.

HPE OneSphere makes integration of the existing on-premises vCenter environment very simple, in a matter of minutes. The integration steps that transform existing VMware-based environment into a private cloud platform, are depicted in Figure 5.
First, log in to HPE OneSphere portal using credentials with administrator role (Figure 6).

Then, select Providers from the main dashboard and select the Private Zones option to add a private cloud platform from an existing virtualized environment (Figure 7).
You are then prompted to download the **HPE OneSphere CONNECT** app for your preferred OS flavor (Windows® or MAC) on your workstation. HPE OneSphere CONNECT app automates the deployment of the VGA in the vCenter environment and its integration with your HPE OneSphere account.

Start the HPE OneSphere CONNECT app wizard on your workstation and after you specify the HPE OneSphere account URL and administrator credentials, just follow the wizard steps (Figure 8), which will guide you throughout the process to connect existing virtualized environment. You will first specify where your existing infrastructure is located by defining a region name, a zone name, as well as the zone type (vCenter or KVM). A region typically represents a data center location in which the on-premises infrastructures reside. A zone represents a virtualized environment in the data center. You can pick a dot in the world map where your region is located.

For a VMware-based private zone, you will then enter your VMware vSphere information such as the vCenter credentials, the vSphere cluster where the VGA will live, the VGA name, the network where the VGA will be deployed, as well as the vDS data network available for users’ VM deployments. You will then specify the VGA networking settings (DHCP or static IP address assignment), and proxy information if the internet access is through a proxy.

**Important note**

Network connectivity is required between the VMware vCenter Server and the Windows or MAC workstation where the HPE OneSphere CONNECT app is launched. The workstation must also have internet connectivity over HTTPS protocol. The vCenter credentials specified in the app wizard are used to deploy the VGA OVA in vCenter environment. They are also used by the VGA to communicate with the vCenter Server.
The HPE OneSphere CONNECT App will then deploy the VGA on the designated VMware vSphere cluster in your vCenter environment and establish the secure connection between the VGA and your HPE OneSphere account (Figure 9).

Once the VGA is deployed and connected to your HPE OneSphere account, existing VMs running on the ESXi cluster, as well as the network port groups on the selected dvSwitch-based Data Network and datastores associated with the cluster are discovered automatically and become part of the HPE OneSphere managed private cloud platform. VMware templates located on managed datastores are discovered and their metadata information is imported as service images as part of the HPE OneSphere catalog. HPE OneSphere checks for new VMware templates periodically and any new templates are automatically added to the service catalog.

Once this is done, the result is a working private cloud platform managed by HPE OneSphere and available to users for self-service access. Additionally, if your vCenter Server manages multiple vSphere clusters, you have the ability, through the HPE OneSphere portal, to choose exactly which ESXi cluster(s) you wish to be used as compute resources by HPE OneSphere. You also have the option to expose VM deployment networks from the dvSwitch-based Data network to specific projects or to all projects and to configure how IP addresses are assigned to VM instances being deployed by either using the infrastructure DHCP service in your data center or using a static range of IP addresses defined in HPE OneSphere.

**Note**
The minimum ESXi cluster virtual hardware requirements for the HPE OneSphere VMware Gateway Appliance are as follows:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum required CPU</td>
<td>4</td>
</tr>
<tr>
<td>Minimum required RAM</td>
<td>16 GB</td>
</tr>
<tr>
<td>Minimum required HD</td>
<td>40 GB</td>
</tr>
<tr>
<td>Download directory space</td>
<td>600 MB</td>
</tr>
</tbody>
</table>

**KVM-based private cloud provider**

Your VMware private cloud platform can be extended beyond VMware virtual machine based workload deployments to include Kubernetes container workloads and services that utilize a single catalog to deploy Kubernetes container based applications and other micro-services to your on-premises VMware environment. With this solution, if desired, you can provision a private infrastructure to support and deploy a load balanced Kubernetes environment, with added separation provided by a virtualized VMware private cloud. HPE OneSphere efficiently configures an existing VMware private cloud instance to support load balanced Kubernetes deployments through the OneSphere catalog. This functionality is available through the HPE OneSphere simple to use UI and APIs that provides administrators and developers the ease of deployments expected from any modern platform.
**Notes**

The Kubernetes cluster is deployed with one master node and two worker nodes by default. When a Kubernetes cluster is deployed, a zone with the same name as the Kubernetes cluster is created in the private cloud region. External load balancer capabilities are built into the Kubernetes clusters that are deployed to the private cloud. Details of the created cluster are available in the HPE OneSphere Project.

To deploy a private (not internet accessible) Docker image or Helm chart to the Kubernetes cluster, ensure that a trusted root certificate is added to the server. For details, please refer to the "Creating an Ubuntu 16.04 virtual machine image with cloud-init in a VMware vSphere" section of the HPE OneSphere online documentation available at hpeonesphere.com/docs/article/managing-images-and-templates.

Connecting existing on-premises Linux KVM server to HPE OneSphere follows the same integration steps as VMware-based environment depicted in Figure 5. As with VMware-based private cloud, HPE OneSphere CONNECT app is also used to connect your KVM server with HPE OneSphere in a KVM zone.

HPE OneSphere CONNECT app downloads a script from the HPE OneSphere management service tier. It then runs the script on the KVM server that installs host agents on the KVM server and configures it as OpenStack KVM compute node with the hypervisor role.

A KVM zone can contain one or more KVM servers, each with different roles. All KVM servers in a zone will have the hypervisor (compute) role enabling them to start hosting virtual machines deployed from HPE OneSphere. At least one KVM server in the zone should also have the Image Library role enabled. The server with the Image Library role serves virtual machine images to other KVM hosts in the zone using the OpenStack Glance image library service. Multiple KVM hosts running the image library service and attached to a shared storage back end such as an NFS share can improve image availability and balance the load among all the image library hosts.

Furthermore, the block Storage (Cinder) service can be enabled for KVM zones to provide persistent storage volumes that can be attached, using standard OpenStack CLI commands, to enterprise class production workloads. HPE OneSphere integrates with SUSE Enterprise Storage solution which supports Ceph to host Cinder volumes. With this configuration, you choose one KVM server in the zone to assume the Block Storage (Cinder volume) Service role and you configure all KVM servers in the zone as Ceph clients.

**Note**

For further information about KVM server integration with HPE OneSphere, KVM server roles, configuring high availability of Image Library service and integrating Ceph enterprise storage solution such as SUSE Enterprise Storage with HPE OneSphere, please refer to the HPE OneSphere online documentation available at hpeonesphere.com/docs/.

**Amazon Web Services public cloud provider**

In order to connect your AWS public cloud provider account to HPE OneSphere, the following prerequisites must first be fulfilled:

- You must sign up for an AWS account for your organization if you do not already have one.
- If you have multiple AWS accounts in your organization and want to track the combined costs of all AWS accounts in your organization, you must set up an AWS organization. In this case, one account will become the **Master** account, and the other accounts will be the **Member** (also known as linked or managed) accounts.
- You must create an Amazon **S3 bucket** in your AWS (Master or Standalone) account for cost data repository.
- You must turn on monthly detailed billing reports with resources and tags in Amazon billing services preferences for AWS to deliver these reports to the S3 bucket you created for your Master or standalone account. When you turn on billing reports, an Amazon S3 bucket policy is generated by AWS billing services. The bucket policy needs to be applied to your S3 bucket permissions. This policy grants AWS billing and cost management system principal permission to deliver reports to your Amazon S3 cost bucket. AWS delivers the cost and usage report files (estimated bill several times per day, and final bill at the conclusion of each billing period) to Amazon S3 bucket where HPE OneSphere can collect the billing information programmatically.
- You must create an AWS Identity and Access Management (IAM) user identity with programmatic access for your AWS accounts (Master, Member, or standalone). This IAM user identity is used by HPE OneSphere to sign programmatic AWS API requests using that IAM user identity’s access keys (access key ID and secret access key).
- The IAM user identity used by HPE OneSphere must be capable of getting billing data from the S3 bucket, listing member accounts in the AWS organization, deploying and managing VM instances, and deploying and managing Kubernetes clusters through programmatic calls. The HPE policies with these requirements are available for download in Configuring Amazon Web Services accounts in the HPE OneSphere documentation.
• You should also prepare one or more Amazon Elastic Compute Cloud (EC2) private AMI images in your AWS accounts (Master, Member, or standalone) in your preferred deployment AWS regions.

• Finally, if you plan to deliver containers to your users as a service running on AWS, you need a DNS domain name and hosted DNS zone in Amazon Route 53 that you can dedicate to the Kubernetes clusters.

**Note**
For detailed instructions for configuring your AWS account and permissions for the S3 bucket, the policies for the IAM user identity for Payer/Master, Member, and standalone accounts, refer to the HPE OneSphere documentation.

HPE OneSphere makes connecting with your AWS public cloud provider very simple and the connection is complete in a matter of minutes. You first connect HPE OneSphere to your public cloud billing account in order for HPE OneSphere to collect billing and cost metrics for either your standalone account or Master account for a consolidated set of member AWS public accounts. You then establish AWS public cloud provider accounts with AWS Regions enabled in HPE OneSphere. The integration steps are depicted in the Figure 10.

**Figure 10.** Steps to connect an AWS public cloud provider account to HPE OneSphere

First, log in to HPE OneSphere portal using credentials with administrator role and create a project that will be associated with your public billing cloud account. Select **Settings** from the main dashboard, then select **Public Billing Accounts** (Figure 11) option to connect HPE OneSphere to your billing account (Master account or Standalone account). Enter the AWS IAM user identity access key, secret access key, as well as the S3 bucket name for the cost data and a project name. Clicking the link ‘**How do I find this information?**’ will display the detailed information on how to configure AWS accounts.
If you are connecting an AWS Master account and want to connect AWS member accounts as public cloud resource providers, you can add each member account individually to predefined projects. You will have to provide the access key information for each AWS Member account selected. Each Member account will appear as an individual provider. You then select the AWS regions you want to make available (Figure 12) for cloud resources deployment. All AWS availability zones in the selected regions are then automatically enabled as zones in HPE OneSphere.

**Figure 11.** Connecting AWS public cloud provider account to HPE OneSphere

**Figure 12.** AWS regions selection

**Note**
In the context of a public cloud service provider such as AWS, a region is defined by AWS cloud provider. A region is an Amazon data center location. Each region contains multiple distinct locations called availability zones (AZs). Within the HPE OneSphere data model, a zone maps one-to-one to an AZ. An HPE OneSphere region and a zone allow users to launch CloudFormation template deployments from the AWS regions and AWS AZs associated with your AWS account(s). These deployments will then belong to the project assigned to a specific AWS account provider.

Once this is done, the result is a working public cloud platform managed by HPE OneSphere and available to users for self-service access.
Microsoft Azure public cloud provider

HPE OneSphere can retrieve usage, cost, and performance data from Microsoft Azure public cloud platform and can deploy Azure Resource Manager (ARM) templates. Like AWS, HPE OneSphere makes the connection of Microsoft Azure public cloud accounts very simple.

You first need to connect your Microsoft Enterprise Agreement (EA) account as the Azure public billing account for HPE OneSphere to collect billing information and display cost data in HPE OneSphere. The EA account consolidates billing data for all the Microsoft Azure subscriptions associated to the EA account. You will need to gather your Microsoft EA enrollment secret access key, enrollment account number and Active Directory name to add the EA account to HPE OneSphere. This information will allow HPE OneSphere to authenticate access to the Microsoft Azure APIs.

After you add the public billing account for your Microsoft EA account, you can add one or more Azure subscriptions as Azure public provider accounts that you associate to predefined projects. This allows HPE OneSphere to collect Azure subscription-level usage and cost data for those subscriptions associated to the registered Microsoft EA account. Connecting Microsoft Azure subscriptions as public account provider to HPE OneSphere enables users to deploy Azure resources through ARM templates from the HPE OneSphere service catalog.

HPE OneSphere allows you to deploy an application to Microsoft Azure using an ARM template registered in the HPE OneSphere catalog. ARM templates are JSON files that define resources, including virtual machines that you need to deploy for your solution. There are prerequisites in order to deploy ARM Templates. As an Administrator you must:

1. Add a project for use with ARM Templates
2. Added an Azure Public Billing account
3. Added an Azure public account
4. Registered a catalog of Azure ARM Templates

Once the prerequisites are in order you can select Azure ARM Templates as a type in the HPE OneSphere Catalog (Figure 13).

![Figure 13. Azure ARM Template services in catalog](image)

Using the ARM catalog you can deploy an Azure ARM template (Figure 14).
Figure 14. Deploying an Azure ARM Template

Kubernetes in underlying IaaS cloud platforms

CaaS is delivered to users in underlying IaaS cloud platforms (AWS public cloud and VMware-based private cloud) connected to HPE OneSphere.

This section describes how an administrator provisions a Kubernetes cloud platform on managed AWS public cloud provider account. A similar process is used to deploy a Kubernetes cloud platform on a managed VMware private cloud. Information specific to VMware was described in the previous VMware connection section.

Once AWS public cloud provider account is added to HPE OneSphere, a user can create a highly available Kubernetes cluster on a selected AWS region, from a Kubernetes cluster image template available in the HPE OneSphere service catalog (Figure 15).
For AWS, the Kubernetes cluster is composed of at least three master nodes, but only one is required for VMware. To deploy a highly available Kubernetes cluster, you specify a Kubernetes cluster name, a project which is associated with the AWS provider, the AWS region and the AWS Availability Zone on which to deploy the cluster, the K8 cluster & worker nodes flavor profile, and a domain name for serving Kubernetes API and service requests. Optionally, you can specify the number of Kubernetes worker nodes\(^4\) to deploy. You also specify a SSH public key to be injected into the EC2 VM instances as they are being deployed in AWS.

\(^4\) A Kubernetes worker node runs the containerized applications in Kubernetes Pods. Pods are scheduled, orchestrated, and monitored by Kubernetes master node(s). A typical HA cluster is designed with multi-master nodes and multi-worker nodes. For non-production environment, you may want to run a cluster without any worker node. In this case, Pods will be scheduled to run on the master nodes.
HPE OneSphere simplifies the process of setting up high-availability multi-master Kubernetes cluster on the AWS region and Availability Zone on which you want to deploy the Kubernetes cluster. HPE OneSphere:

- Automates the deployment of all the underlying VMs (Kubernetes master and worker nodes) in your AWS account.
- Installs the host agents on the VMs, so HPE OneSphere controls all aspects of the management of the Kubernetes cluster such as:
  - The installation of all required Kubernetes services on the three master nodes and worker nodes
  - The orchestration of the formation of the Kubernetes cluster
  - The monitoring of the Kubernetes cluster components
  - The upgrade of the Kubernetes components
  - The scalability of the number of worker nodes in the Kubernetes cluster

Once this is done, you have a new cloud platform that appears as a zone type of Kubernetes in HPE OneSphere and as a deployment in the selected project. The Kubernetes cloud platform is then available to users for deployment of containerized applications. You have just established, in a matter of minutes, a Kubernetes-based CaaS offering that can be delivered to application developers as a service.

**Controlling multiple cloud resources access through Projects**

The hybrid cloud administrator organizes multiple cloud resources and users into Projects. Think of HPE OneSphere Project as a way to control access to hybrid cloud resources through a project’s membership and role-based security (also known as role-based access control [RBAC]). Projects are HPE OneSphere objects that typically represent a department, a business unit, a collaborative project, or a program in your enterprise. For example, the development of a new application or a marketing campaign.

Projects allow administrator to control the multiple cloud resources that are available for a user’s consumption. Global roles are implemented, such as administrator, consumer, project-creator, and analyst. Users with the “consumer” role are always working in the context of projects. Consumers have membership to one or more projects and they are granted permissions through project-specific roles such as project owner and project member. An administrator manages the cloud platforms exposure to projects by controlling cloud platforms that can be used by a given project. In addition, an administrator also controls project access to a private cloud platforms’ networks.

**Note**

A private cloud platform is exposed to all projects whereas a public cloud platform provider can only have one project assigned. However, multiple public cloud provider accounts can be added to HPE OneSphere, each belonging to a different project. This design allows a better control of public cloud service usage and restricts access to designated consumers. Private cloud platforms can be assigned to one or more specific projects.

The administrator and a user with the role of “project creator” can create projects and add user membership (Figure 16) in any project. An administrator or the project creator can then assign the “project owner” role to a consumer in order to delegate the management of the project and its memberships.

A project’s owner can then grant access to other consumers and the resources assigned to the project by adding them to the project with the “project member” role. A consumer with the “project member” role will be able to create and manage the lifecycle of the deployments in that project.

**Note**

Ability to define and manage resources quotas (operational limits) and cost budgets (spend limits) for projects is being considered for a future release.
AWS Compliance

When an AWS master account is added to your project, AWS compliance reporting is automatically enabled as shown in Figure 17. The AWS compliance check is based on a subset of Cloud Technology Partners (CTP)\(^5\) Best Practices and Center for Internet Security (CIS)\(^6\) Benchmarks framework for AWS. Compliance checks are run against all AWS member accounts in the project to provide continuous reporting and analytics so you can prove to the business that you have the right controls and transparency in place to run your applications on AWS. CTP Continuous Compliance provides a single source of truth across Governance, Risk, and Compliance (GRC) to enable real-time monitoring and remediation recommendations. This allows you to be ready for audits at any time while reducing your cost and risk exposure.

\(^5\) Cloud Technology Partners is a Hewlett Packard Enterprise company and the premier cloud services and Software Company for enterprises moving to AWS, Google, Microsoft, and other leading cloud platforms. For additional information, please see [cloudtp.com/partners/amazon-web-services](http://cloudtp.com/partners/amazon-web-services).

\(^6\) Center for Internet Security is a non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyberattacks. CIS controls and benchmarks are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. For additional information, please see [cissecurity.org/cis-benchmarks](http://cissecurity.org/cis-benchmarks).
By default, the compliance check is run against five benchmarks with details available by selecting the AWS Compliance link that will take you to the Project AWS Compliance report shown in Figure 18. The five default benchmarks are:

- RDS volumes should be encrypted: validates that the Relational Database Service “StorageEncrypted” field is set to “true”
- RDS instances should not be publicly accessible: validates that the Relational Database Service “PublicAccessible” field is not set to “true”
- EBS volumes should be encrypted: validates that the Elastic Block Store volumes “Encryption” field is set to “true”
- CloudTrail should be enabled in all regions: validates that the CloudTrail resource “IsMultiRegionTrail” field is set to “true”
- The Root account should not be used: validates that the root user account has not been used in the past 90 days

You will receive guidance on how to resolve any compliance check failures along with the ability to run the compliance checks on demand.
In the right column of the Project AWS Compliance report is a “Get in Control” link that will take you to a CTP demo request page as seen in Figure 19. CTP consultants can customize your OneSphere compliance reporting to match the requirements of your business, including the addition of graphical content for a quick visual indication of compliance trends.

Figure 19. Cloud Technology Partners demo request form
Hybrid service catalog management

HPE OneSphere provides a service catalog of public and private catalog repositories for enterprise consumers and developers, giving them access to what they need to get their application development work done more quickly. From the service catalog, you can provision cloud resources from service catalog items. You can leverage open-source application images from third-party catalogs such as AWS CloudFormation (CF)\(^7\) repository, Azure Resource Manager (ARM)\(^8\) Templates repository, Kubernetes Helm Chart\(^9\) repository, and Docker Hub\(^{10}\) repository to quickly build new products and solutions.

**Note**

Templates are not “downloaded” or “stored” in OneSphere, they are only referenced through their metadata as resources for deployment via OneSphere. They are listed as items in the OneSphere Services Catalog.

Third-party catalog sources are managed from the **Catalog Registry** from **Settings** menu (Figure 20) in the HPE OneSphere portal. A cloud administrator can add a new private or public repository by providing a name for the repository, specifying the target URL, the catalog type, and any required credentials. These registries will provide the containerized application images for application deployments to cloud platforms.

The metadata from VM templates, both VMware-based and KVM-based, appears automatically in the HPE OneSphere Service Catalog as service images after you connect on-premises virtualized environments to HPE OneSphere.

**Note**

A catalog registry can be exposed to all projects or no projects. The ability to curate catalog service into custom catalog groups and assign catalog group access to specific projects is discussed below.

---

7 An AWS CloudFormation (CF) template may be as simple as single VM instance (AWS Service), or it may include a combination of VMs, Container Services, and other AWS services (DNS, load balancing, databases, firewalls, etc.) in order to deploy a full application stack (AWS App Frameworks). CF templates are easily modifiable as they are declared in JSON format. For more information about CF templates, please refer to [github.com/awslabs/aws-cloudformation-templates](https://github.com/awslabs/aws-cloudformation-templates).

8 Azure Resource Manager (ARM) templates are available to HPE OneSphere administrators with an Azure account. They can configure the ARM template repositories as part of the Azure Provider configuration, such as the Azure QuickStart Templates GitHub repository which offers users access to the publicly defined templates. ARM templates are easily modifiable as they are declared in JSON format. For more information about ARM templates, please refer to [github.com/Azure/azure-quickstart-templates](https://github.com/Azure/azure-quickstart-templates).

9 Helm is a Kubernetes-based package installer. It is a tool for managing Kubernetes charts. Charts are curated application definitions for Kubernetes Helm. Charts contain all of the resource definitions necessary to run an application inside of a Kubernetes cluster. Charts can be published on public or private Helm charts repositories. For more information about Helm, please refer to [docs.helm.sh](https://docs.helm.sh).

10 Docker Hub is a cloud-based repository of open-source Docker containers images. Docker Hub provides public and private repository. For more information about Docker Hub, please refer to [hub.docker.com](https://hub.docker.com/).
Catalog curation

HPE OneSphere allows administrators to create a catalog service group that can be associated to specific projects. This allows an administrator to control the catalog items that consumers can deploy.\(^{11}\)

Figure 21. Catalog Service Groups

Once your catalog registries have been added, go to Catalog and click Service Groups. From the actions drop-down menu, select Crate Service Group. Enter a name, expose to the needed projects and click Done.

Figure 22. Catalog Services

Catalog Services can be added to a catalog service group. These services will be visible and can be deployed by consumer members of the projects that are associated with the catalog service group.

Figure 23. Adding Services to a Service Group

\(^{11}\) For more information on catalog curation and management, see the HPE OneSphere Docs page.
When a Service Group has been created, you can then add services to it. While still in the Catalog screen click Services, select the services you want to add to the Service Group (The green square border around the service is highlighted when it is selected). See Figure 23. Once all the services are selected, choose Add to Service Group from the Actions menu. Select the correct Service Group or Groups and click Add.

**Deploying workloads across multiple cloud platforms**

Once you have connected multiple cloud platforms to HPE OneSphere, organized users authority to utilize available cloud resources and catalog registries, users can start deploying workloads on their cloud platforms.

From the Catalog menu in the portal UI (Figure 21), consumers can search for specific named items, filter by Service Type (for example, Virtual Machine or Container) or by Catalog Type, and select a Service (a VM image template or an application image) they want to use.

![Figure 24. Searching filtering catalog items per Catalog Type or Service Type](image)

Then, they create a **deployment** (that is, an instance) of that service image in a particular project that they are member and in a cloud platform (a zone) that hosts the corresponding image service.

**Note**

Some services may be constrained to a specific cloud platform (zone). Services that are VM images can only be deployed into the cloud platform that hosts the corresponding VM image template. A service that is a containerized Docker or Helm chart application image can be deployed into any cloud platform that is a Kubernetes cluster with access to a Docker or Helm registry that can provide the containerized application image.

**Deploying services on private and public IaaS clouds**

Figure 22 illustrates deployments of virtual machine instances in a VMware-based cloud platform and an AWS public cloud platform connected to HPE OneSphere. Once the user has selected a VM image in the catalog, the user specifies a name for the service, and a VM profile that defines the size of compute resources (virtual CPU, memory, and storage) that support the service being provisioned.

For a service instance deployed on the private cloud platform, the user must specify a tenant network segment into which user wants to connect the VM instance. If the VM image template has been built with the cloud-init12 package installed, an SSH public key pair can be specified and/or a cloud-init user data scripts can be used to customize the VM instance with a default locale, a hostname, a password, and other details while it is being provisioned.

12 cloud-init is a standard for customizing Linux cloud instances on private and public clouds. More information about cloud-init can be found at [cloud-init.io](http://cloud-init.io). Cloudbase-Init for Windows instances on private and public clouds is also available. Visit [cloudbase.it](http://cloudbase.it) for further information.
For a service instance deployed on the AWS public cloud, distribution of Linux in Amazon EC2 supports cloud-init. The user must launch the deployment with either an SSH public key or a cloud-init custom script that allows SSH connection with traditional user name/password credentials. In addition, the user can specify the kind of inbound traffic (protocol ports) and source IP addresses that can reach the VM instance being deployed in the public cloud. The user can also assign a floating (public) IP address to the VM instance to make it reachable from the internet. When an instance is deployed, the user can create persistent block storage volumes and connect them to their VM instances from HPE OneSphere.

For a service instance deployed on the Azure public cloud, ARM templates declare the objects that are required in any specific deployment within the Azure Cloud environment, including the Azure region into which the resource group will be deployed. ARM templates allow the specification of dependencies in the deployment of cloud services within Azure. The security key configuration for deploying new Resource Groups must be available either at the Azure subscription configuration or to be captured during the ARM template deployment.

OneSphere provides the User with the status of the template deployment, including if the template is in the process of deployment (several cloud platform services may need to be launched and configured during the deployment), if the template has successfully deployed, or if there was a problem and the deployment failed. Any state changes and error messages available from the cloud platform regarding the template deployment should be logged within the OneSphere logging service and reported to the user when appropriate.

Figure 25. VM instance deployment in VMware-based private cloud platform and VM instance deployment in AWS cloud platform
Deploying containerized applications

A consumer, typically a developer, will have the ability to deploy containerized applications from the service catalog. Figure 26 shows the deployment wizard for a WordPress application in a Kubernetes zone named K8sCluster. HPE OneSphere will create the required Kubernetes elements in the Kubernetes cluster for the application such as the PODs, the deployments, and the services.

![Figure 26. Deploying a containerized application from HPE OneSphere](image)

The developer can also obtain the kubeconfig file from HPE OneSphere portal (Figure 27) and connect to the Kubernetes Cluster using the Kubectl command line. Kubectl is Kubernetes command line utility that can run on Linux and Windows workstation. The utility allows a developer to interact with the Kubernetes Cluster via the Kubectl command line interface and performs action such as the control of Kubernetes cluster nodes and applications elements (PODs, deployments, and services).

![Figure 27. Downloading the kubeconfig file from HPE OneSphere portal](image)
IT operations

When managing multiple cloud environments, IT administrators need to understand and manage the utilization of cloud resources. HPE OneSphere provides centralized operations for monitoring and reporting of resource availability, performance, and utilization for multiple cloud accounts.

The consolidated IT resource utilization, availability, and performance metrics for a cloud provider type (e.g., all AWS accounts) is shown in Figure 28. This report is accessible from the Providers menu in the HPE OneSphere portal. Since different metrics are used for different cloud providers, it does not make sense to mix providers into a single report.

The Utilization, Availability, and Performance charts show a score from 0 to 1000, where 1000 is a perfect score. Scores are computed hourly from a set of metrics such as CPU, memory, storage, network, VM utilization, network errors, disk I/O latency, queue length, node status, and network status.

![Resource Utilization, Availability, and Performance metrics](image)

**Figure 28.** Resource Utilization, Availability, and Performance metrics

Click the icon to get information about the metrics used and weighting used to compute the scores. Note that the metrics and weighting vary for different cloud platform providers as is shown in the Figure 29 images.

![Metrics and weighting used for AWS, Azure, and VMware-based cloud providers](image)

**Figure 29.** Metrics and weighting used for AWS, Azure, and VMware-based cloud providers, respectively
- **Availability** score is a measure of health over time. For private cloud, it is computed from the proportion of time that the on-premises hosts are available for use. For public cloud providers, it is computed from the proportion of time that VM instances are available.

- **Utilization** score is a measure of how much cloud resources are utilized. The score is computed from raw consumption metrics (CPU, memory, and storage utilization for private cloud providers and CPU utilization for VM instances running in public cloud providers). It is measured against a target utilization rate of 75%. A high score means you are using a large percentage of available resources.

- **Performance** score gives user some idea of how well a cloud entity is performing. It is computed from performance metrics that measure network congestion and overall network performance for private cloud, and I/O operations performance for public cloud providers.

- The **Overall** score is computed from the weighted scores of Availability (50%), Utilization (30%), and Performance (20%) scores.

---

**Note**

HPE OneSphere currently supports performance and utilization reporting for public cloud providers and VMware-based private cloud providers. Support for performance and utilization reporting for KVM-based private cloud providers is being considered for a future release.

---

**Business control and analytics**

Cost management is often a challenge for organizations using multiple cloud environments. Cost management starts with achieving spend visibility across cloud infrastructures. HPE OneSphere offers native tools to create accurate estimates of cloud spend, as well as track and monitor consumption.

When managing a multiple cloud environments, IT organizations, IT executives, and business leaders want to compare spending in public and private clouds in order to optimize cloud utilization. Therefore, they need to understand and manage the costs associated with the services and resources across the entire hybrid cloud estate. HPE OneSphere provides them with near-real-time cloud cost, consumption, and utilization insights and analytics across their hybrid cloud estate.

HPE OneSphere allows you to collect data on costs associated with your public and private provider accounts and display the aggregated data in an interactive dashboard or as downloadable reports. Both the dashboard view and the reports option allow you to configure data from multiple categories, including provider type, account information, region, date range, and more. Currently, HPE OneSphere only shows costs/rates in U.S. Dollars.

For Amazon Web Services (AWS), the cost includes all payer accounts that you connected to HPE OneSphere as Public Billing Accounts, plus any member accounts associated with those payer accounts in AWS. Cost information for these member accounts will appear whether or not you have connected those member accounts to HPE OneSphere.

For Microsoft Azure, the cost includes all enterprise accounts that you connected to HPE OneSphere as Public Billing Accounts, plus any subscription accounts connected to those enterprise accounts in Azure. Cost information for these subscription accounts will appear whether or not you have connected those subscription accounts to HPE OneSphere.

For private cloud providers, the cost represents actual usage costs for the vCPU, memory, and disk usage rates defined per private cloud provider/zone.

---

**Note**

Only HPE OneSphere Administrators and Analysts have permission to access cost analytics information. HPE OneSphere users with the Project Creator and Consumer roles will not see Insights on their main menu. However, Consumer's will still be able to see the costs associated with the projects they are assigned.

---

**Insights Dashboards**

When you first click Insights, the System Default Dashboards view is displayed as shown in Figure 27. This dashboard presents the total cost for the time period shown and the main chart displays the total amount spent during that period. The total spent over the previous same period of time is presented below the current period expenditure followed by a percent change and actual dollar change. The drop-down allows you to quickly select a time period or you can specify a custom period.
The System Default Dashboard view cannot be edited or deleted. You can add one or more custom dashboard views. Any custom dashboard view you add can be edited or deleted. Custom dashboard views have a unique name and contain the date range and filter set you specify. By selecting “Save Changes”, the custom dashboard view you create will be saved, “published”, to the dashboard collection of reports available for you to scroll through.

Quick View Filters, below the chart area, take the total cost for the time frame you selected and break it down across different categories. Each category is further broken down by each item in that category, such as costs per day, per account, and per provider. You can organize how information in each category is displayed by clicking on an individual item in a category. If you want to see how much money was spent from one account and how much of that was spent per day in the date range you selected, click on the account you want to analyze and the information in the other categories will automatically be filtered to reflect that selection.

Report Views, in the next section, gives you quick access to on-demand tabular reports that you can customize and download.

Figure 30. Insights Dashboard
Insights Reports

As a Global Analyst or Administrator, you can access the Reports screen by clicking on the greyed out Reports link in the banner at the top of the default Insights screen. The first time you access the Reports screen, there will be no available reports. You can add and configure reports as shown in Figure 30.

Reports run against the cost data that HPE OneSphere collects from your public and private cloud providers. Reports are tabular and highly customizable. You decide what columns to include in your report, how to organize those columns, and how to filter the data to include only what you need in the report. For example, you might want to see all costs, grouped by account, but only for a particular region. You can also pivot your data by column, much like you can in Microsoft Excel. Plus, reports can be downloaded to a CSV file or exported to Excel.

Reports can be adjusted to show different data depending on different conditions, such as different date ranges, different columns, and so on. As long as these changes are not saved, your report will revert to its previous state once you navigate away from the page. By selecting “Save Changes”, the modified report will be added, “published”, to your collection of reports.

Note

Some queries will fail to return any results at all if the report you configured requested too much data for the system to process. Also, to protect your browser from overload, HPE OneSphere Insights limits a report to displaying up to 10,000 rows of data. If your report exceeds 10,000 rows, viewers may not be able to access some rows. There is no way to control which rows will be displayed and which will be left off.
How is cost information calculated?

Public cloud platforms
The total cost is based on public provider’s cost (billing) information. It includes month-to-date cost data of all resources deployed in public cloud providers for all the organization’s accounts connected to HPE OneSphere. For example, for an AWS provider, the total cost is the AWS billing information collected by HPE OneSphere via the customer-provided credentials. It includes cost data of all resources deployed in AWS for your accounts, including those services and resources deployed from outside HPE OneSphere. The accounts can be the Standalone accounts and the Master accounts with their consolidated set of member accounts that have been enabled in HPE OneSphere as well as those member accounts that have not been enabled in HPE OneSphere. For Microsoft Azure, the total cost is the Microsoft EA billing information for all resources and services deployed in all the Azure subscriptions associated to that Microsoft EA account.

The managed cost is the month-to-date usage cost of all cloud resources and services deployed in public cloud accounts. It includes usage cost data of cloud resources deployed on managed provider accounts connected to HPE OneSphere. For AWS, these are the Standalone accounts, Master accounts and their consolidated set of member accounts which are enabled in HPE OneSphere. For Azure, it is the month-to-date cost of all resources and services deployed in Azure subscriptions connected to HPE OneSphere.

Private cloud platforms
The total cost and managed costs are based on a fixed cost model. For each private cloud platform connected to HPE OneSphere, you define a customized fixed cost rate and a usage rate. The fixed cost rate typically corresponds to the up-front hardware infrastructure investment. Customized fixed cost rate can also include software, support, and operational costs. The usage rate is the cost per VM/hour including the hourly cost per CPU core and per memory GB, along with a monthly cost of storage per GB.

If you do not provide your own rate values, you can select a default fixed cost rate from a sample HPE hardware configuration from which the usage rate is derived.

The total cost is then the calculated monthly fixed cost value, which is based on the fixed cost rate. The managed cost will be computed using the usage rate values.

Note
HPE OneSphere currently supports VMware-based private cloud costing model. Costing model for KVM-based private cloud is being considered for a future release.

About HPE OneSphere API
In addition to the unified user interface, HPE OneSphere provides a common API that allows organizations to develop innovative applications that integrate with HPE OneSphere. You can programmatically access all the management functions that might be invoked through the HPE OneSphere unified user interface, except for Insights Dashboards and Reports which are planned for a later release.

The API uses modern REST protocols to initiate actions (PUT, GET, POST, DELETE, and PATCH) on objects managed by HPE OneSphere. The API is using JSON as interchange data format and the token-based open standard authentication method, OAuth 2.0, to secure the API calls.

The easiest way to start using the HPE OneSphere API and learn how to structure the REST API calls is to use a REST client such as Postman. To get the authentication token and know how to structure your requests, you will need syntax information found in OneSphere API documentation.

Note
The HPE OneSphere API and data model documentation is available in the HPE OneSphere Documentation Portal at hpeonesphere.com/docs. For further information about the HPE OneSphere API, please refer to the HPE Developer Portal at developer.hpe.com/platform/hpe-onesphere/home.
Summary

HPE OneSphere is a hybrid cloud management platform delivered as a managed service. It unifies the management of on- and off-premises resources and enables seamless deployment, operation, and optimization of hybrid cloud environments and applications. It helps you manage digital services and workloads across the hybrid cloud estate from a single point, delivering the speed and simplicity of a public cloud experience but with more choices, control, and greater cost efficiency.

HPE OneSphere is a platform enabling digital transformation that delivers simplicity, agility, and cost-efficiency. It takes away all the complexity of deploying and operating across multiple clouds. It does that so you can focus on next-generation cloud-native applications development and your own business.

If your company is like most, you want to move fast and keep things simple and streamlined. You want to use your choice of development tools and environments, maintain control, and do it all cost-efficiently. That’s what you get with HPE OneSphere.

Resources

HPE OneSphere
HPE OneSphere Developer Portal
HPE OneSphere Documentation Library
HPE OneSphere Documentation Portal
HPE OneSphere Installation Service
HPE OneSphere Managing Images and Templates
HPE OneSphere Security white paper
HPE OneSphere Support Matrix
Cloud Technology Partners
HPE Composable Infrastructure
HPE Hyperconverged Infrastructure
HPE Synergy

Amazon Web Services documentation
AWS CloudFormation Sample Templates
Center for Internet Security benchmarks
Cloudbase Solutions
cloud-init documentation
Docker Hub
Helm documentation
Kubernetes documentation
Microsoft Azure Resource Manager QuickStart Templates
OpenStack documentation
SUSE Enterprise Storage documentation

Learn more at
hpe.com/onesphere