VMware vCloud® Architecture Toolkit™
for Service Providers

Multitenant Use of VMware vRealize® Operations™ as a Service

Version 2.9

January 2018

Yves Sandfort

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304
www.vmware.com

Contents

List of Tables

List of Figures

Introduction

1.1 Overview

The VMware Cloud Provider™ Program is an ecosystem of over 4,000 service providers located in more than 100 countries offering VMware based cloud services. Local providers protect data sovereignty while providing a wide range of cloud services and vertical market expertise through specialized compliance and certifications.

VMware vRealize® Operations Manager™ delivers intelligent operations management across the physical, virtual, and cloud infrastructure, enabling the VMware Cloud Provider to efficiently operate a cloud platform and meet required customer service level agreements (SLAs).

vRealize Operations Manager correlates data from applications to storage in a unified easy-to-use management tool that provides control over performance, capacity, and configuration, with predictive analytics driving proactive policy-based automation.

1.2 Document Purpose

This document is intended to help the cloud service provider design an operations management solution for tenants based on vRealize Operations Manager in an “as a service” model. It highlights key design considerations pertinent to the service provider service model, and describes the different deployment models, use cases, and design considerations that VMware Cloud Providers must consider when deploying vRealize Operations Manager for the use of their tenants on their cloud platform.

Note This document is not a replacement for product documentation. Use it as a supplementary resource when planning a VMware Cloud Provider Program implementation.

1.3 List of Acronyms

Table 1. List of Acronyms

Term	Description
API	Application Programming Interface
CA	Certificate Authority
CPU	Central Processing Unit
DRS	Distributed Resource Scheduler
FSDB	File System Database
GB	Gigabyte
HA	High Availability
HIS	Historical Inventory Service
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IOPS	Input Output Operation per Second

Term	Description
LAN	Local area network
LDAP	Lightweight Directory Access Protocol
MB	Megabyte
NA	Not Available / Not Applicable
NOC	Network Operations Center
RBAC	Role-based access control
RC	Remote collector
REST	Representational State Transfer
SAN	Subject Alternative Name (in the context of SSL certificates)
SAN	Storage area network (in the context of shared storage)
SDDC	Software-defined data center
SDK	Software development kit
SDN	software-defined networking
SDS	Software-defined storage
SLA	Service level agreement
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SP	Service provider
SSL	Secure Sockets Layer
UI	User interface
vApp	Virtual appliance
vCPU	Virtual central processing unit
VDC	Virtual data center
VM	Virtual machine
VPC	Virtual private cloud
WAN	Wide area network

Solution Mapping

2.1 vRealize Operations Manager for Service Providers Overview

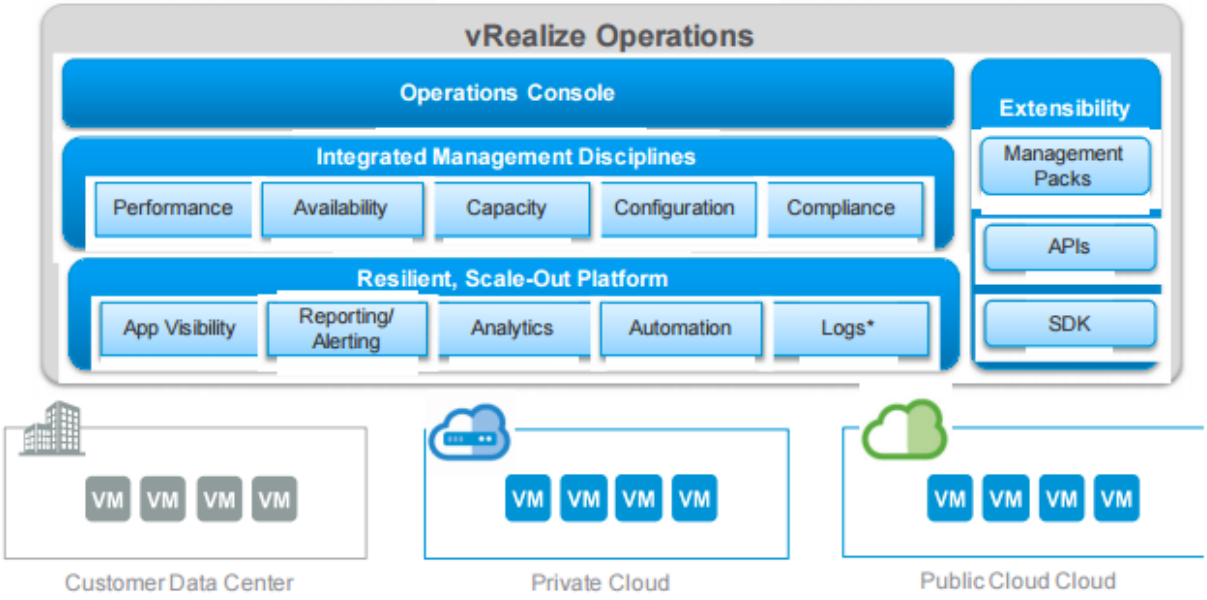
vRealize Operations Manager is a key component of a VMware Cloud Provider Program powered cloud service offering. It provides a simplified yet extensible approach to operations management of the cloud infrastructure. It helps service providers maximize profitability by optimizing efficiency, and differentiates their service offerings by increasing customer satisfaction and delivering to SLAs. vRealize Operations Manager also enables service providers to generate new revenue streams by expanding their footprint to offer VMware vRealize Operations™ as a service to their tenants.

vRealize Operations Manager collects and analyzes information from multiple data sources and uses advanced analytics algorithms to learn and recognize the “normal” behavior of every object it monitors. Through dashboard views and reports, users are able to analyze details so that they can make informed decisions in the following areas:

- Issue resolution and root cause analysis
- Environment health and advanced warning of potential issues
- Capacity management and forecasting

vRealize Operations Manager uses management packs to collect, analyze, and present data from many VMware and third-party data sources, thereby providing a holistic view of a service provider’s cloud infrastructure and tenant-specific workloads.

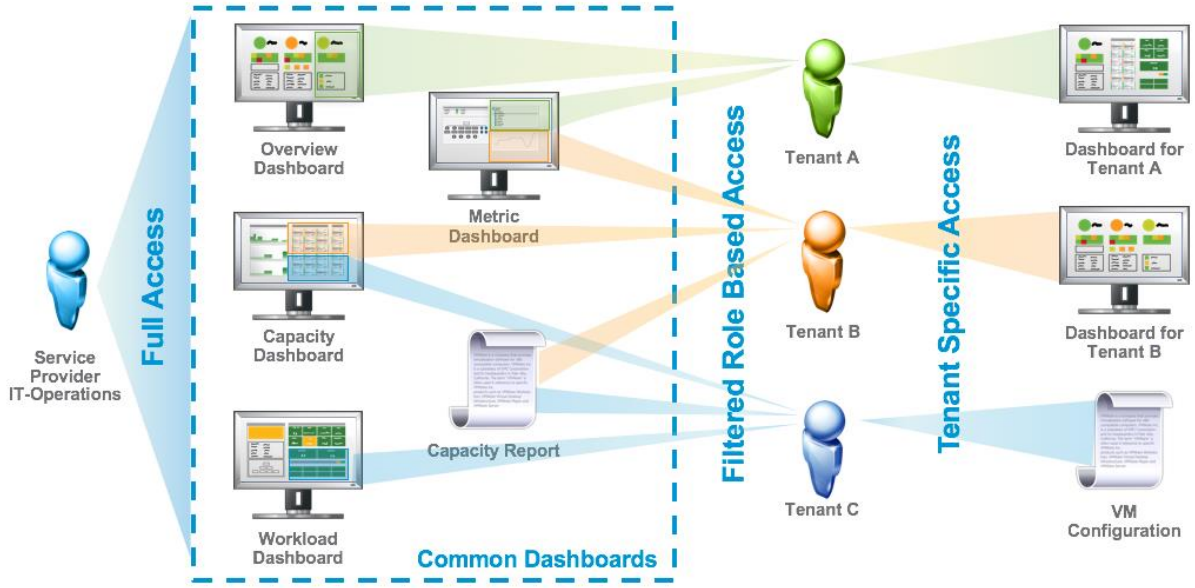
Figure 1. vRealize Operations for the VMware Cloud Provider Program



2.2 Service Provider Use Cases

This section describes some of the use cases relevant to a VMware Cloud Provider when implementing vRealize Operations for tenant consumption. While many service providers use vRealize Operations already to manage their own environment, providing it as a service for tenants is a different approach, especially because vRealize Operations was originally not developed with a direct multitenant layer.

Figure 2. Common and Custom Dashboards Role-Based Access



2.2.1 Tenant Access to vRealize Operations Manager in Shared Environments

A constant challenge from customers that VMware Cloud Providers face is to operate cloud-hosted workloads in a manner similar to local workloads. Part of this is what data to provide and how to enable access to this data as a service. vRealize Operations Manager can be configured in a multitenant way, allowing service providers to customize the level of access and data giving the customer the advantage to use the same tool on premises and in the cloud. Studies show that vRealize Operations Manager users experience 16 percent faster troubleshooting (and it improves to 50 percent if they add VMware vRealize Log Insight™). This additional data insight also lowers operational costs for the service provider because customers are enabled to solve performance problems themselves.

2.2.2 Dedicated Cloud Deployment

Customers operating a dedicated cloud environment with a VMware Cloud Provider can either use a dedicated vRealize Operations Manager deployment to operate their environment or be serviced with a vRealize Operations as a service option as described in the previous use case. A dedicated cloud deployment can also be expanded with remote collectors into the private cloud operated by the customer locally on premises.

2.2.3 Trusted Advisor and Tenant Optimization as a Service

Another use case is to provide optimization as a service leveraging vRealize Operations Manager. In this case, the service provider uses the existing optimization features provided by vRealize Operations Manager to help the customer right-size their virtual machines' workloads to reduce cost and optimize performance while still delivering to the SLAs defined. This could be provided as an additional service for existing customers or be provided as part of a managed services solution.

2.2.4 Internal Use – Optimize the Service Provider Cloud

The final use case demonstrates the value of vRealize Operations for managing and optimizing a cloud infrastructure to get more VMs out of the same hardware, accelerate troubleshooting, deliver to SLAs, and more predictably manage data center growth using capacity planning and modeling. VMware studies show that vRealize Operations can help service providers achieve a 36 percent better consolidation ratio and a 34 percent improvement in hardware utilization.

Conceptual Architecture

When deploying operations and management solutions into a cloud based environment, it is important to validate the different resource/data providers:

- Private cloud – Cloud infrastructure operated exclusively for an organization. Can be managed by the organization or a third party. The infrastructure can be located on premises or off premises. When operated off premises and hosted by a cloud service provider, this is also sometimes referred to as a dedicated private cloud.
- Public cloud – Cloud infrastructure made available to the public or to a large industry group and owned by an organization that sells cloud services. In the majority of the cases, this environment is partly or completely shared between different customers.
- Hybrid cloud – Cloud infrastructure is a composite of two or more cloud instances (private and public) that are unique entities but are also bound together by standardized technology. This is primarily the tenant/customer view as they mix public and private cloud resources.

3.1 Business Drivers

The key business drivers for implementing vRealize Operations as a service depend on the target use case. The multitenancy use cases described in Section 2.2.1, Tenant Access to vRealize Operations Manager in Shared Environments and Section 2.2.2, Dedicated Cloud Deployment primarily focus on generating additional revenue with self-service options. The use case described in Section 2.2.3, Trusted Advisor and Tenant Optimization as a Service focuses more on a managed services environment and the use case described in Section 2.2.4, Internal Use – Optimize the Service Provider Cloud focuses on the internal use approach.

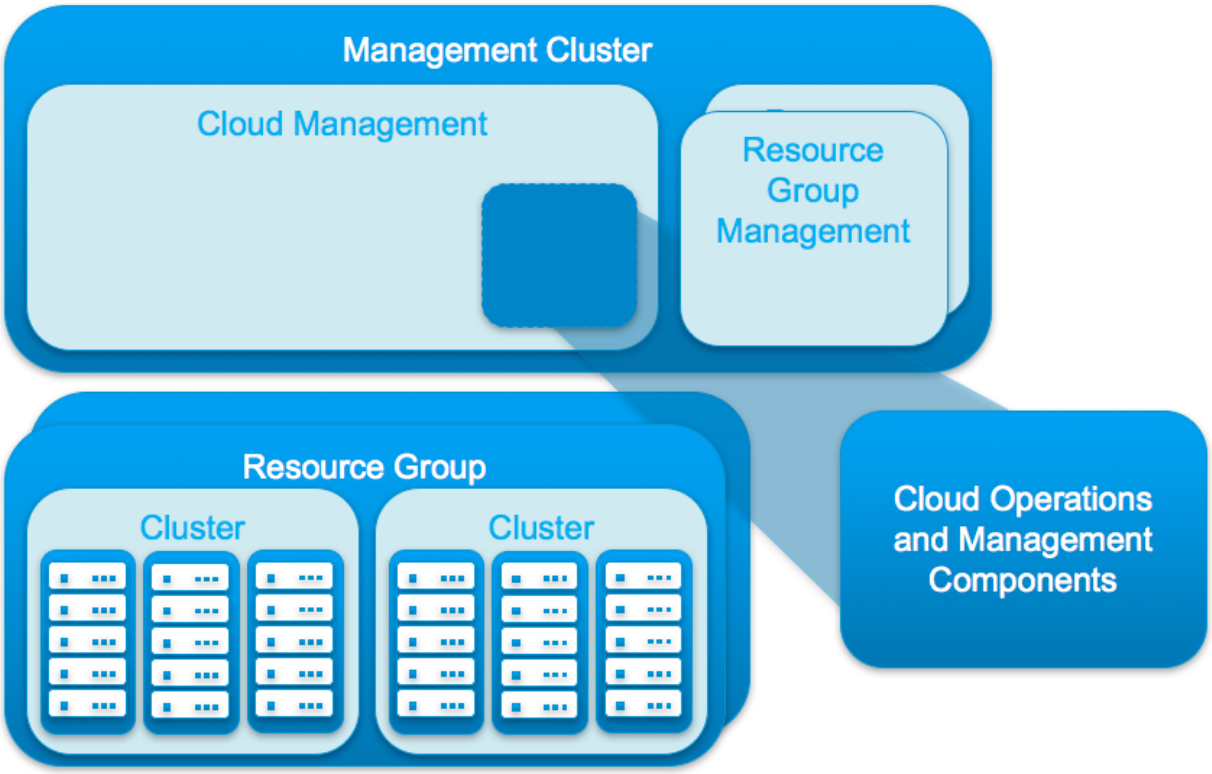
With the multitenancy vRealize Operations as a service approach discussed in the first two use cases, vRealize Operations Manager might also be used by the service provider itself for operations. However, that requires either complete openness with customers/tenants or reduced visibility for the service provider due to some limitations in the policy engine covered later in this document. Additionally, there are security requirements and implications when opening up vRealize Operations to customers and tenants that must be considered.

The third and fourth use cases do not focus on direct customer/tenant access to the vRealize Operations environment and expect the service provider to be the primary user. The business driver for the third use case is additional revenue generation, and for the fourth use case, is cost reduction through faster support and a more efficient data center operation.

3.2 Conceptual Overview

Cloud operations and management is an important factor in any cloud design, regardless of the deployment model. In both private and public cloud designs, incorporate cloud operations and management components to monitor the cloud infrastructure. The following figure shows where cloud operations and management components are located relative to the management cluster.

Figure 3. Cloud Operations and Management in Context



Designing for vRealize Operations as a Service

4.1 vRealize Operations Manager Deployment Models

Depending on the actual use case, different deployment models can be used:

- Shared multitenant environment with tenant and service provider access
- Dedicated environment with tenant access
- Shared and/or dedicated environment with no tenant access

While this document covers the default vRealize Operations Manager deployment for service provider use, this can easily be extended with additional management packs and remote collectors into a widely distributed environments.

4.1.1 Shared Multitenant Environment with Tenant and Service Provider Access

In this scenario, the service provider operates a centralized vRealize Operations Manager instance to collect all data generated by the resource cluster. Both service provider personnel and tenants will access the same instance of vRealize Operations, and data access will be controlled with RBAC. This scenario allows for easy management and deployment.

This approach is especially attractive for service providers who can operate their complete environment within one vRealize Operations Manager environment.

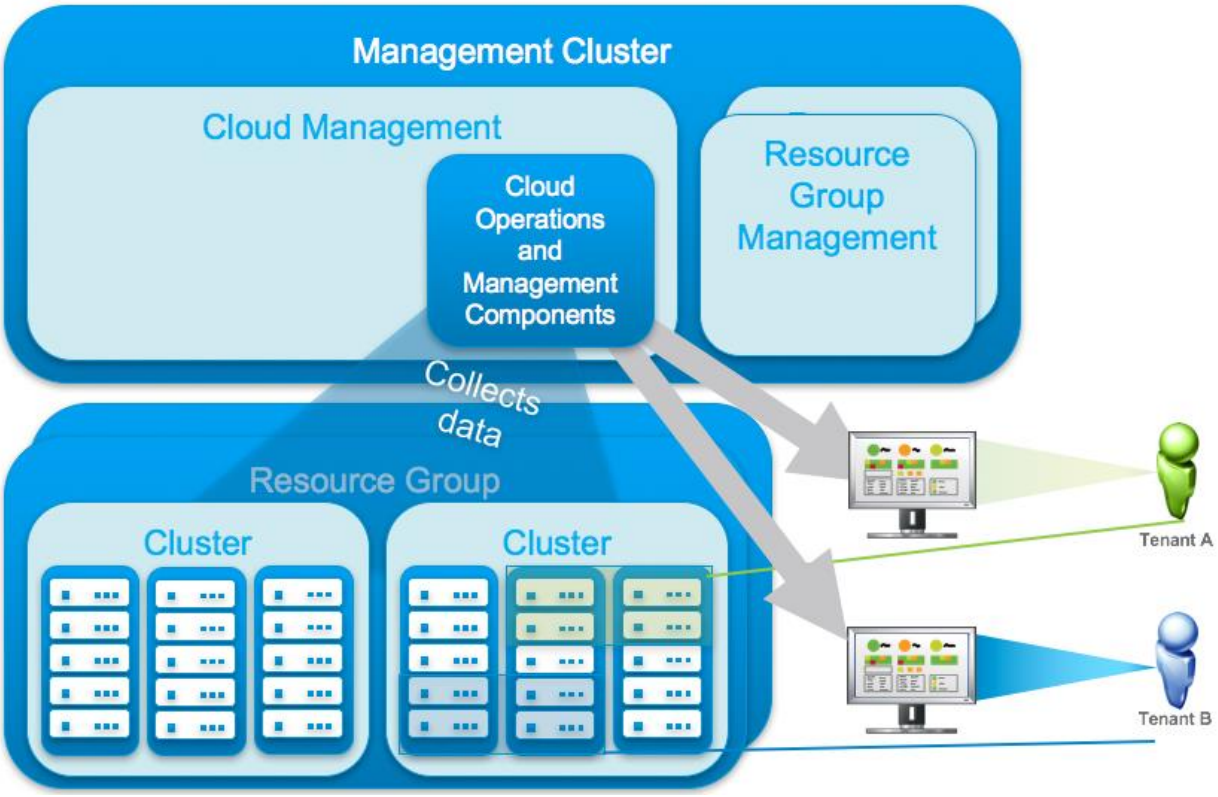
Advantages include the following:

- Easy to deploy and manage
- No additional data/configuration distribution for dashboards, policies, and so on is needed
- Only one instance to maintain (software updates, management packs, and so on)

Disadvantages involve the following:

- Role-based access control requires careful maintenance
- Objects can only be operated under one policy, removing the ability to limit alert visibility for a customer/tenant
- Sizing can become complex and larger environments could be limited by sizing parameters. A possible workaround is to build instances per larger resource group.

Figure 4. Shared Multitenant Environment with Tenant and Service Provider Access



4.1.2 Dedicated Environment with Tenant Access

This scenario is unrelated to the vRealize Operations Manager multitenant use case that this document is focused on. This scenario is included for comparison reasons.

In this scenario, the service provider operates a vRealize Operations Manager instance per dedicated customer. This is usually done when the customer operates its own cluster and vCenter Server within the service provider environment. Access to this environment is primarily focused on the tenant, but might be open for the service provider as well. An extended scenario might be that the service provider also collects data from the customer operated vCenter Server. This approach is commonly used in managed service environments or dedicated public cloud offerings where the customer rents a dedicated hardware stack.

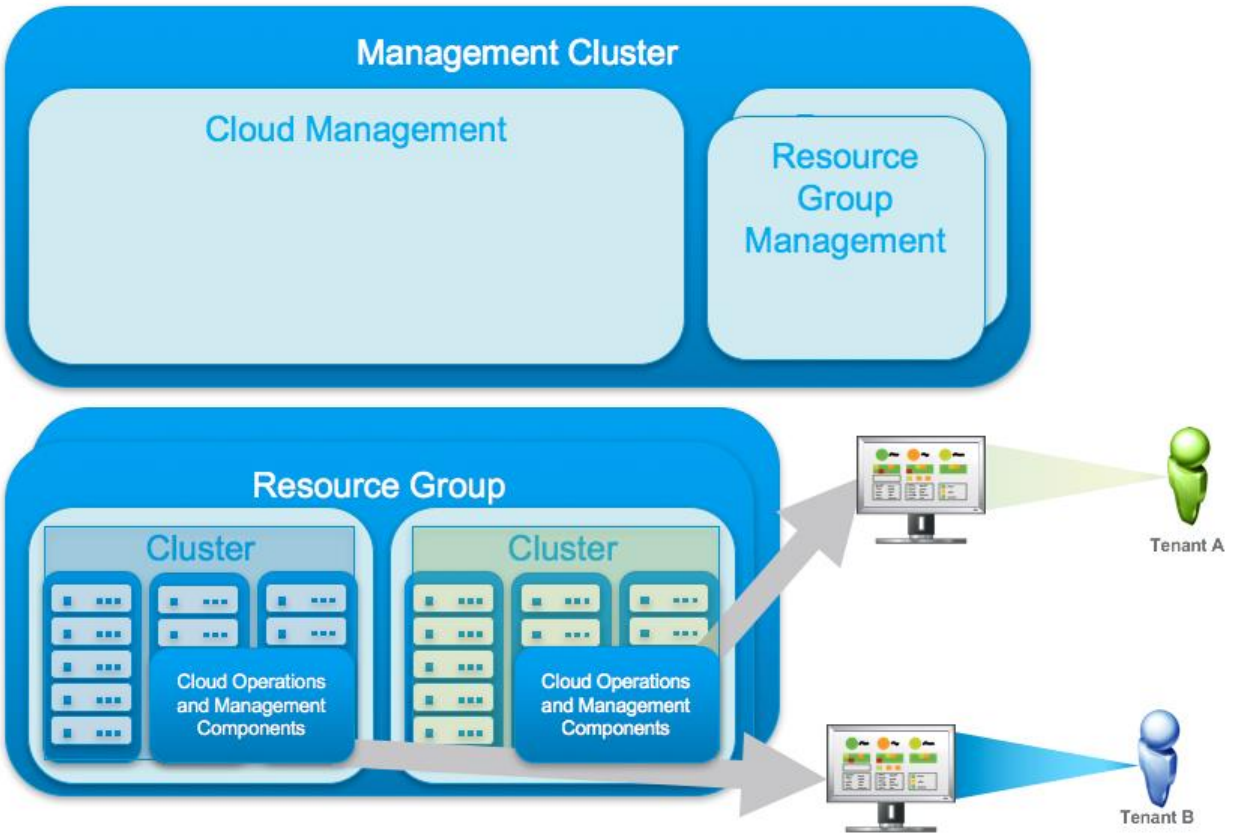
The advantages are as follows:

- Easy to deploy and manage
- Sizing is easy because it can be done per tenant/customer
- Object policies can be customized to be tenant specific

Disadvantages include the following**:**

- Difficult to get a “big picture” when each customer operates on its own
- Currently no data federation available for vRealize Operations
- Service provider must monitor a high number of instances
- Maintenance (upgrades and so on) requires more resources

Figure 5. Dedicated Environment with Tenant Access



4.1.3 Shared and/or Dedicated Environment with No Tenant Access

In this scenario, the service provider operates a centralized vRealize Operations Manager instance to collect all data generated by the resource cluster. The primary difference from the scenario described in Section 4.1.1, Shared Multitenant Environment with Tenant and Service Provider Access is that access is only provided for the service provider. This scenario allows for easy management and deployment.

This approach is often used in managed services environments where the service provider focuses on resource optimization.

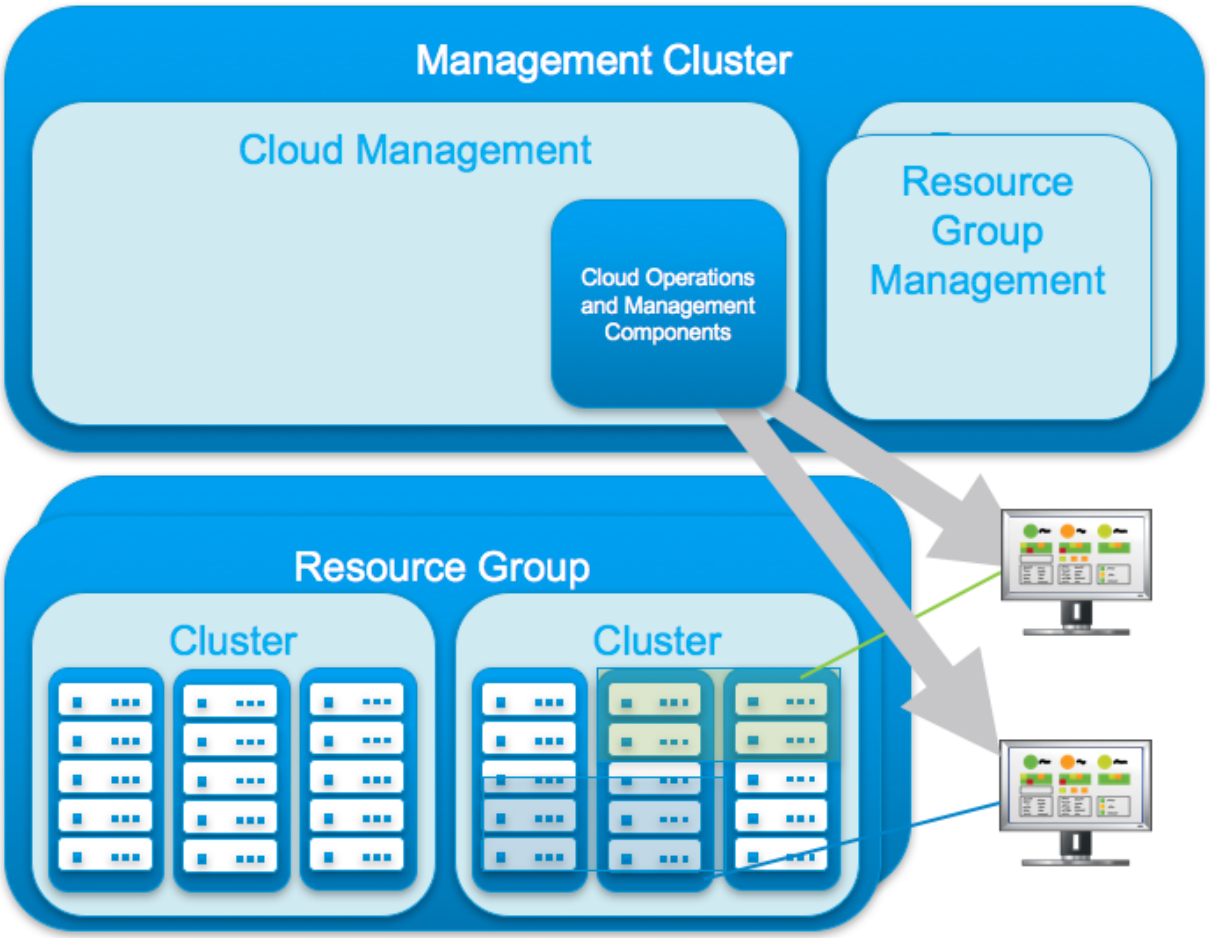
The following advantages apply:

- Easy to deploy and manage
- No additional data/configuration distribution for dashboards, policies, and so on necessary
- Only one instance to maintain (software updates, management packs and so on)
- No complex RBAC necessary

Disadvantages include the following**:**

- Sizing can become complex and larger environments might be limited by sizing parameters. A possible workaround is to build instances per larger resource group.
- No customer/tenant access to vRealize Operations Manager possible.

Figure 6. Shared Multitenant Environment with Tenant and Service Provider Access



4.2 Architectural Overview

vRealize Operations Manager is available in two different deployment models—as a preconfigured virtual appliance (vApp) or as a Windows or Linux installable package.

The vRealize Operations Manager vApp encapsulates a VMware virtual machine. Each instance of vRealize Operations Manager can be configured to perform one of the following roles within the complete vRealize Operations Manager instance/cluster:

- Master node – First node (mandatory) in a cluster or single standalone node.
- Master replica node – An optional node to provide high availability (HA) to the master node.
- Data node – Used to scale out a vRealize Operations Manager cluster.
- Remote collector node – Performs data collection only, and can be used behind firewalls or across limited bandwidth connections.

The following table lists the components that make up a vRealize Operations Manager node.

Table 2. vRealize Operations Manager Logical Node Architecture

Component	Description
Admin / Product UI server	Web application that serves as both the user interface and the administrative interface.
REST API / Collector	Collects data from all the components in the enterprise.
Controller	Handles data movement between the UI, collector, and analytics.
Analytics	Analytics engine performs data correlation, calculation of metrics and super metrics, capacity planing, and alert generations.
Persistence	Performs database operations across all nodes in the solution.
FSDB	File System Database stores the raw metrics in the file system. Each node of a vRealize Operations Manager cluster contains parts of the FSDB for overall persistence.
xDB (HIS)	Historical Inventory Service data is maintained only on the master node and master replica.
Global xDB	Data that needs to be persisted on each master node and/or replica like dashboards, reports, policy settings, alert rules, and super metric formulas, which can not be distributed across the system.

vRealize Operations Manager can be horizontally scaled out to multiple nodes to monitor larger environments and provide high availability. Each vRealize Operations Manager installation can scale to a maximum of eight nodes. There is a minimum of one master node. In a high availability configuration, this is accompanied by a master replica. All other nodes are data nodes. Remote collectors are not counted as cluster nodes.

4.3 Availability and Recoverability

Because vRealize Operations Manager is used to provide end user access, data and access availability as well as recoverability must be considered. One of the biggest challenges with vRealize Operations Manager is the amount of data being created.

vRealize Operations Manager supports high availability (HA) by creating an additional node that is a replica of the vRealize Operations Manager master node. This node type is called a master replica. When present, a master replica can take over the functions of a master node. When a problem occurs with the master node, failover to the replica node is automatic and requires only two to three minutes of vRealize Operations Manager downtime. Data stored on the master node is fully backed up on the replica node. With HA enabled, the cluster can survive the loss of a single data node without losing any data.

4.3.1 Access Layer

The vRealize Operations Manager user interfaces can be accessed from any node. A load balancer can be used to detect if a node is down and forward traffic to surviving nodes.

The following are access layer design considerations:

- Design for HA by having two or more nodes in a cluster configuration with the HA option enabled.
- Use a load balancer to monitor for node failure and forward traffic to surviving nodes.

4.3.2 Clustering for Data and Application Availability

vRealize Operations Manager supports application-level HA. Enabling HA has a penalty in the maximum number of objects and metrics that can be stored. With HA enabled, each piece of data contained on the master node is stored twice, halving the maximum number of supported objects and metrics, and doubling the I/O and disk space requirements. See the table in Section 4.4, Architecture Prerequisites for further details on the maximum amount of objects and metrics in a cluster.

The following are clustering for data and application availability design considerations:

- To enable HA, at least one more data node must be deployed in addition to the master node. If possible when HA is enabled, deploy the replica node within the same cluster and put VMware vSphere Distributed Resource Scheduler™ (DRS) rules in place to keep the replica separate from the master so there is physical redundancy.
- The HA feature of vRealize Operations Manager operates independently of, but complementary to VMware vSphere High Availability.

4.3.3 vRealize Operations Manager Backup

The vRealize Operations Manager vApp can be backed up like any virtual machine. Choose a backup product that uses VMware vSphere Storage APIs - Data Protection. Take the cluster offline during backup and back up all nodes at the same time (or before the cluster is brought back online).

Avoid the recalculation time window at night for backups and verify that your backup is completed before the recalculation takes place.

As a design consideration, use a full, not partial, restore operation, and restore the entire cluster, not individual nodes. If vRealize Operations Manager is configured to use HA, the cluster can withstand the loss of any single node and continue to function.

4.4 Architecture Prerequisites

4.4.1 VMware Software Product Requirements

Required product versions detailed for this document are as follows:

- VMware vSphere 5.5.x
- VMware vCenter Server 5.5.x
- VMware vRealize Operations Manager 6.2.*x*
  - Management Pack for VMware vCloud Director® requires vCloud Director 5.6 or later
  - Management Pack for VMware NSX® requires VMware NSX 6.1 or later

4.4.2 VMware vRealize Operations Manager Sizing

Sizing is always done based on VMware KB article 2146615. Always validate any new deployment against the latest sizing guidelines provided online.

The KB article also provides for a sizing Excel document (advanced tabs) to be used for any sizing. Because the sizing document does not provide for sizing data for all adapters, additional data must be included in the Other Data Sources area of the Excel document. The amount of objects/metrics can be collected from within vRealize Operations Manager.

Because the service provider environment is used to host access for external users, the sizing based on actual system access must be considered as well: The maximum number of concurrent users is achieved on a system configured with the objects and metrics at 50 percent of supported maximums. (For example, 4 large nodes with 20K objects or 7 nodes medium nodes with 17.5K objects.) When the cluster is running with the nodes filled with objects or metrics at maximum levels, the maximum number of concurrent users is 4 users per node. (For example, 16 nodes with 120K objects can support 64 concurrent users.)

Any configuration operating in high availability mode must account for twice the number of nodes. This will not change the maximum amount of 16 nodes.

See the following snapshot for the base figures.

Figure 7. Sizing Guidelines According to VMware KB 2146615

Characteristics/ Node Size	Extra Small	Small	Medium	Large	Standard Size Remote Collectors	Large Size Remote Collectors
vCPU	2	4	8	16	2	4
Memory (GB)	8	16	32	48	4	16
Datastore latency	Consistently lower than 10 ms with possible occasional peaks up to 15 ms					
Network latency for data nodes	< 5 ms					
Network latency for remote collectors	< 200 ms					
Network latency between agents and vRealize Operations Manager nodes and remote collectors.	< 20 ms					
vCPU: Physical core ratio for data nodes (*)	1 vCPU to 1 physical core at scale maximums					
IOPS	See the attached Sizing Guidelines worksheet for details.					
Disk Space						
Single-Node Maximum Objects	250	2,400	7,000	12,000	1,500 (****)	12,000 (****)
Single-Node Maximum Collected Metrics (**)	70,000	800,000	2,000,000	3,500,000	600,000	3,500,000
Multi-Node Maximum Objects Per Node (***)	NA	2,000	5,000	10,000	NA	NA
Multi-Node Maximum Collected Metrics Per Node (***)	NA	700,000	1,500,000	2,500,000	NA	NA
Maximum number of End Point Operations Management agents per node	100	300	1200	2500	250	2,000
Maximum Objects for 16-Node Maximum (***)	NA	NA	60,000	120,000	NA	NA
Maximum Metrics for 16-Node Configuration (***)	NA	NA	15,000,000	30,000,000	NA	NA

4.4.3 Client Access

vRealize Operations Manager can be accessed through the user interfaces listed in the following table. Each user interface is used for specific operations in vRealize Operations Manager.

Table 3. vRealize Operations Manager User Interface

Component	Description
Product User Interface	• Primary user: Operations teams, infrastructure administrator, and infrastructure teams • VMware vSphere summary and detailed information • Access to dashboard, metrics, super metrics, and configuration
Admin User Interface	• Primarily used for initial configuration, administration, and upgrades

vRealize Operations Manager user interfaces can be accessed through the following web browsers:

- Google Chrome: Latest and most previous releases
- Mozilla Firefox: Latest and most previous releases
- Safari: Latest release
- Internet Explorer for Windows 10 and 11

The minimum supported resolution is 1024 x 768.

4.4.4 Load Balancing

The vRealize Operations Manager user interfaces can be accessed from any full node. VMware recommends a load balancer for even distribution of the user interface traffic and load. The maximum number of concurrent user connections is 200. This maximum number of concurrent users is achieved on a system configured with the objects and metrics at 50 percent of supported maximums. (For example, 4 large nodes with 20K objects or 7 nodes medium nodes with 17.5K objects.) When the cluster is running with the nodes filled with objects or metrics at maximum levels, the maximum number of concurrent users is 4 users per node. (For example, 16 nodes with 120K objects can support 64 concurrent users.)

The load per user varies depending how many objects the user is permitted to access (in particular, if the user is running views or reports against large sets of metrics over a long time).

As a design consideration, if vRealize Operations Manager is to be configured as a cluster, use an external load balancer to distribute the load across the cluster.

4.4.5 Remote Collectors

VMware recommends deploying remote collectors in either of the following cases:

- If a vRealize Operations Manager cluster must analyze data from remote sites connected by low-bandwidth or high-latency communication links.
- If the infrastructure to be monitored is in a secure zone and protected by a firewall.

Remote collectors can be deployed in one of two resource profiles: standard or large. The configuration for each size is shown in Figure 7. Disk space is not important to a remote collector, because collection data is stored in memory. The virtual disk can be left at the default size (thin provisioning is also acceptable).

As a design consideration, if monitoring targets are in a secure zone or on the opposite end of a WAN link, consider deploying a remote collector to reduce the number of firewall rules required and reduce load on the WAN.

vRealize Operations Manager Management Packs

The out-of-the-box functionality of vRealize Operations Manager can be extended with vRealize Operations management packs. With management packs, other VMware and partner products can be configured as data sources within the vRealize Operations Manager environment.

This section describes the integrations between vRealize Operations Manager and external systems commonly used in private and public cloud deployments. All management packs produced by VMware and partners can be found at the VMware Solution Exchange (https://solutionexchange.vmware.com).

5.1 vRealize Operations Manager and VMware NSX

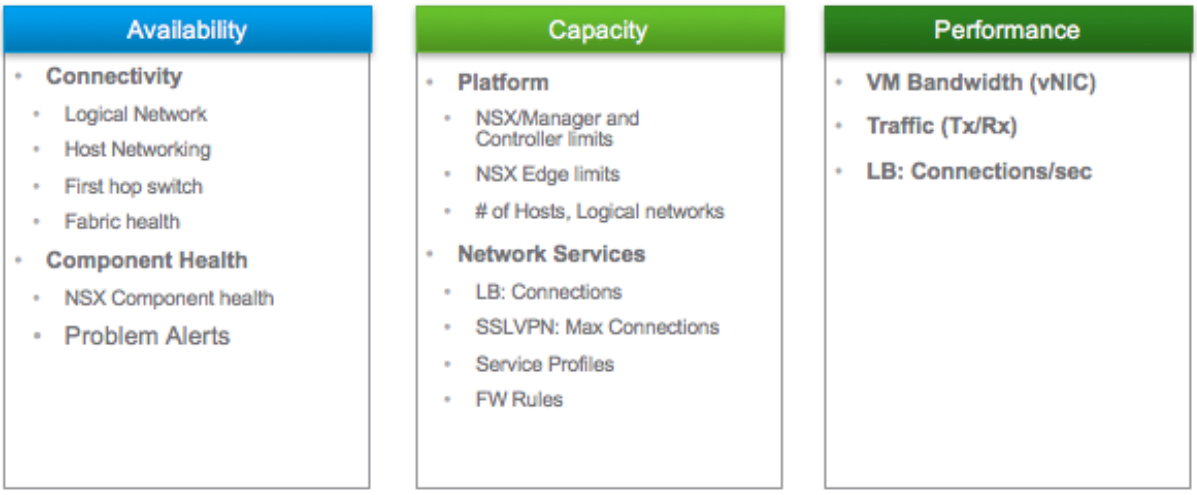
VMware NSX has different use case scenarios in a VMware Cloud Provider environment. The primary focus for the VMware NSX Management Pack is for internal use of the service provider. Exposure to a tenant/customer is not expected.

The VMware NSX Management Pack provides the operations team with a variety of additional information about different problem areas:

- Configuration errors
  - NTP server configuration mismatch across hypervisors and VMware NSX components
  - VLAN, MTU, and teaming configuration issues across physical and virtual switches
  - VM gateway and IP configuration issues
- Failures and capacity issues
  - VMware NSX component failures
  - System events from the VMware NSX components
  - CPU, memory, and network resource utilization above thresholds
- Connectivity issues
  - Failures of physical links of a hypervisor or appliance
  - Failure of communication channels between the VMware NSX components
  - Communication issues across a logical network

The management pack is built on top of the vRealize Operations Manager relationship model and uses analytics and dynamic thresholds to provide better data insights.

Figure 8. vRealize Operations Management Pack Overview



5.2 vRealize Operations Manager and Storage Devices (Including VMware vSAN)

The vRealize Operations Management Pack for Storage Devices provides a complete view of the entire storage topology, including hosts, storage network, and storage array. vRealize Operations Manager can be used to monitor and troubleshoot capacity and performance problems on different components of a storage area network.

This solution provides the following capabilities:

- An end-to-end view of topology, statistics, and events at every affected level of the storage area network
- Isolation of problems caused by elements in the physical storage stack, such as the host bus adapter (HBA), storage switches, or array
- Capture and analysis of information on throughput and latency for the HBA and mount objects
- Capture of throughput on the switch ports.
- Capture of IOPS and queue depth at the HBA and switch ports for read and write components
- Storage device discovery and data collection
- Use of the Common Information Model (CIM) to exchange information with objects managed by the following fabric management systems:
    - Cisco Data Center Network Manager (DCNM)
    - Brocade Network Advisor (BNA)

5.3 vRealize Operations Manager and vCloud Director for Service Providers

The vRealize Operations Management Pack for vCloud Director is an embedded adapter for vRealize Operations Manager. The adapter monitors the health of supported vCloud Director for Service Provider entities and sends early warning smart alerts for monitored provider virtual data center (VDC) resources.

The Management Pack for vCloud Director collects information for provider VDC, organization, organization VDC, and vApp entities from the vCloud Director for Service Providers database and creates the corresponding resources in vRealize Operations Manager.

The Management Pack for vCloud Director maps the vApps that it imports to virtual machine resources that the VMware vCenter Server adapter has already imported and creates resource relationships between the vApps and the virtual machines.

vRealize Operations Manager does not collect performance data from vCloud Director for Service Providers. Instead, the Management Pack for vCloud Director enables vRealize Operations Manager to present health data by mapping vCloud Director for Service Providers entities to vCenter Server objects. The vCenter Server adapter collects performance data for vCenter Server objects.

Figure 9. vRealize Operations Management Pack vCloud Director Overview

vRealize Operations Manager Tenant Customization

6.1 Functional Overview and Limitations of RBAC for Tenant-Based Access

vRealize Operations Manager does not have a native tenant functionality. However, the usage of dynamic groups and role-based access control (RBAC) can be used to create a multitenant like behavior. This section provides an overview of the functions available and the limitations applicable to this approach.

6.1.1 Available Features with RBAC Base Tenant Access in vRealize Operations Manager

Base level feature requirements for service provider usage of vRealize Operations Manager include the following:

- Provide customer access

  Because vRealize Operations Manager provides a web-based user interface, it is easy to provide customer access without needing to distribute an application. Login can be managed through central LDAP and local user accounts.

- Limit object visibility based on RBAC

  While providing access is relatively simple, one of the big challenges is to limit access to only relevant objects for the tenant/customer. vRealize Operations Manager provides dynamic groups and custom group types, which allow you to link all objects and apply permissions for only these groups.

- Group tenant/customer objects

  Often the service provider must group objects by customer to not only have all objects in direct access, but also to operate specific profiles/SLAs on them. Ideally, the same grouping as described in the previous point can be used.

- Customer-specific permissions/features

  Some service providers want to limit functionality based on packaging, such as base monitoring, reporting, capacity management, and so on. Specific roles can be created to allow a customer only the features that are based on the service provider definition.

6.1.2 Limitations with RBAC Base Tenant Access in vRealize Operations

While the majority of requirements can be fulfilled, there are some limitations when using RBAC and dynamic groups to build a multitenant like environment:

- Alert/symptom visibility per user/role/customer

  Alerts and symptoms within vRealize Operations Manager are based on policies. Each object can only hold one policy. For example, while the service provider might be interested to see if a VM is overprovisioned, this information will be visible to the tenant as well. Whatever the alert or symptom raises will always be visible for everyone with access to the object.

- Customer-defined policies

  You can link a customer-based policy to a dynamic group object specific to the customer, but you cannot allow customization of this policy by a tenant/customer, because it is not possible to operate permissions on a per-policy basis.

- Account management by tenant/customer

  All account management and permission control must be performed by the service provider. While a tenant can have different users with different permissions, it is not possible to allow the tenant control/customization.

- Remediation/actions by tenant

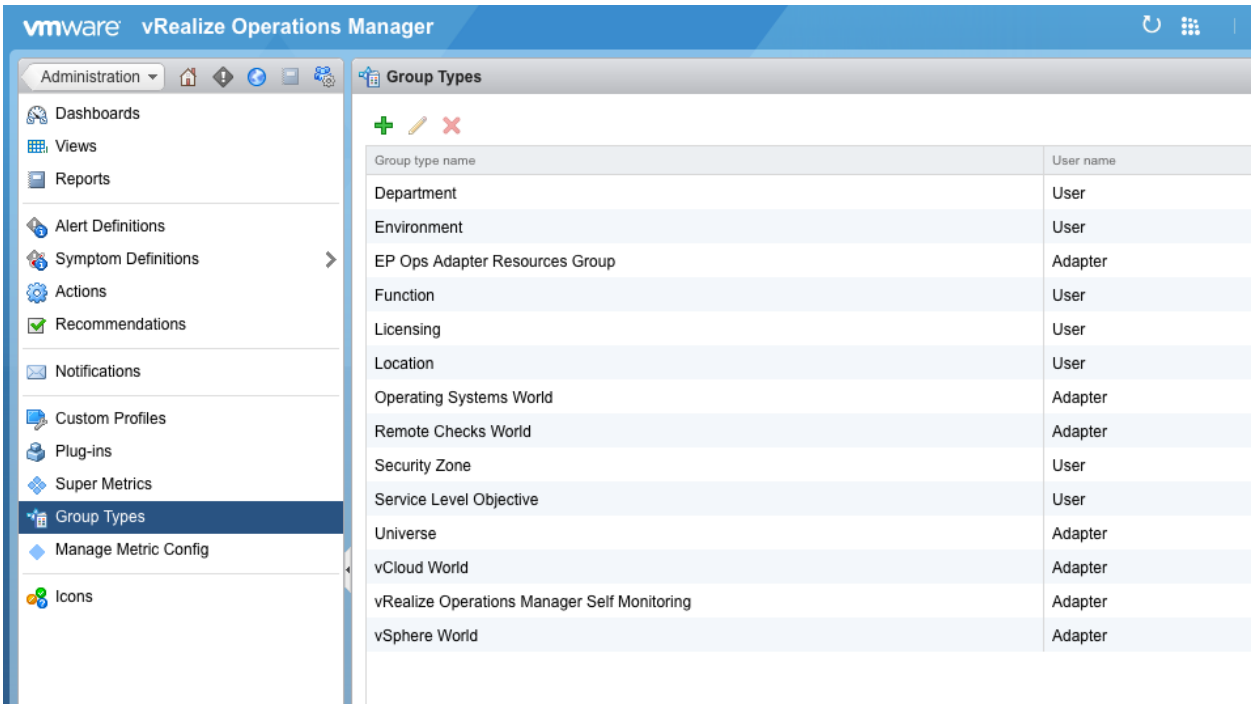
  vRealize Operations Manager provides for remediation actions, which operate under a central account and might be a security risk. Therefore, VMware does not recommend allowing any tenant/customer access to remediation actions.

6.2 Group Type and Custom Group Definition

The first step toward tenant-like role-based access is to create a custom group type. vRealize Operations Manager comes with a variety of prebuilt group types. However, to verify that you do not create an overlap with pre-existing configurations, VMware recommends creating a custom group type.

6.2.1 Custom Group Type

Figure 10. Group Types in vRealize Operations Manager (Content/Group Types)



VMware recommends creating a group type for all tenants. In the following sections, this group type is referred to as “Tenant”.

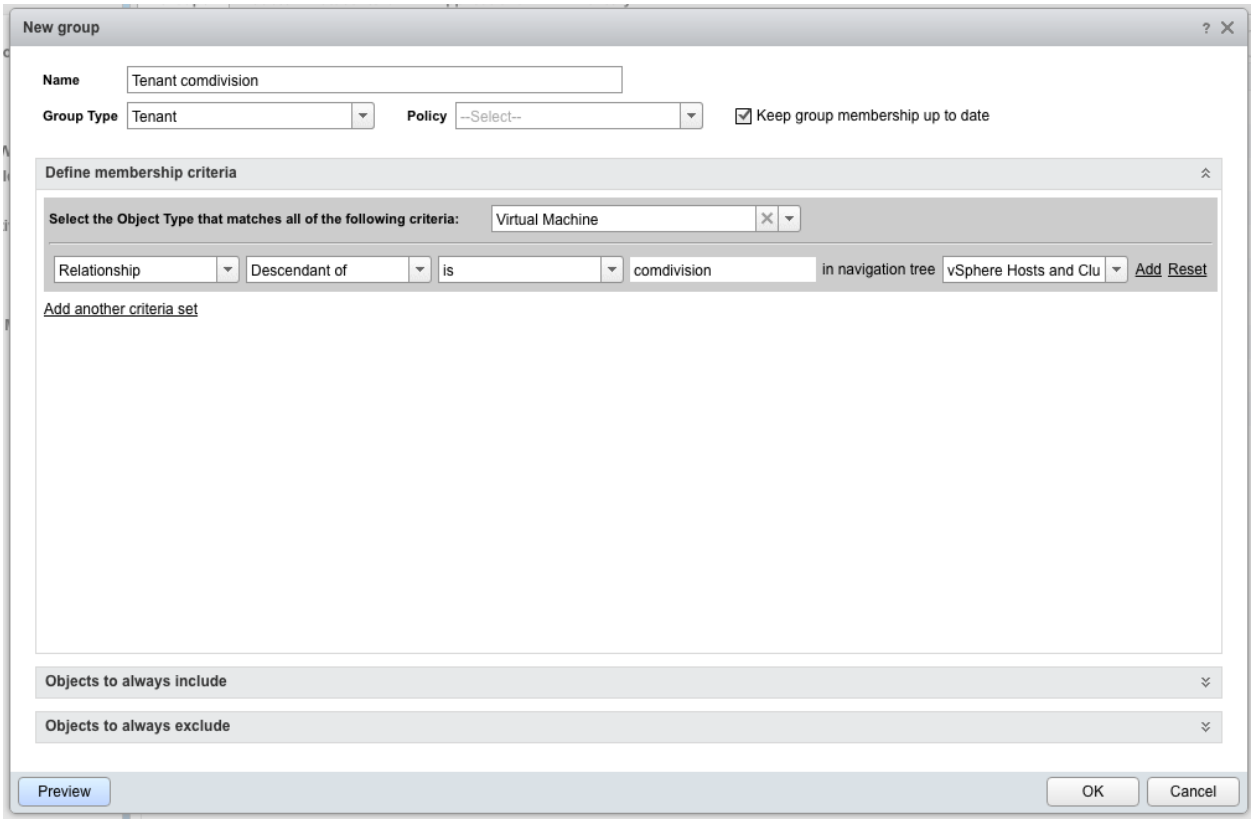
6.2.2 Group Definition (Environment / Custom Groups)

Within the newly created group type, each tenant requires one group. This does not restrict you from creating additional sub-groups within the tenant. One of the advantages within vRealize Operations Manager is that any object can be linked to any number of groups and hierarchies.

A group within vRealize Operations Manager is a container that can hold any number and type of resources:

- Groups can be dynamic or static
- Groups can be assigned to policies
- Groups can be nested

Figure 11. Group Definition for a New Tenant



When you create one group per tenant, use the same prefix for the group name followed by a customer name or ID. As the group type, select what you created in the previous section. A policy can also be linked to the group, but must pre-exist. Select the **Keep group membership up to date** check box.

In this example, only virtual machines are included as the object type. Other object types could be added to the same group if the customer has dedicated resources, such as datastores and so on. The dynamic inclusion is done with a **Relationship** of type **Descendant of** linked to a folder in the vSphere structure. Select the folder from the drop-down which is displayed after a search term is entered.

You can also add static inclusion or exclusions (for example, for service/management VMs).

Use the **Preview** function to validate group membership before the group is saved.

Create the same group structure for each tenant/customer.

6.3 Role-Based Access

6.3.1 Role Definition

In this section, the role definition for a tenant/customer allows each user to log in to vRealize Operations Man/ager and access basic information. Depending on the actual use case, you might need to change the individual permissions assigned to the role within vRealize Operations Manager.

Create a new role in vRealize Operations Manager with the following permissions:

- Administration > Login Interactively
- Administration > View Collector Groups
- Environment > Alerts Management > Cancel
- Environment > Alerts Management > Suspend
- Environment > Alerts Management > View Alerts Page
- Environment > Alerts Management > View Impacted Object Symptoms
- Environment > Alerts Management > View Metric Charts
- Environment > Alerts Management > View Relationships
- Environment > Alerts Management > View Timeline
- Environment > Analysis Views
- Environment > Applications Management > View Application Page
- Environment > Environment Details Pages > Views
- Environment > Environment Page > Map
- Environment > Inventory trees > vCloud Adapter (only if vCloud Director is configured)
- Environment > Inventory trees > VMware Adapter
- Environment > View Dashboard Home Page
- Environment > View Environment Home Page
- Environment > View Recommendations Page
- Environment > View Summary Page

6.3.2 Local User Groups for Dashboard Alignment

vRealize Operations Manager normally leverages an **Everyone** group to allow access to all dashboards. To control access for operations (internal) users and tenant/customer (external) users, you must set up at least two groups within vRealize Operations Manager. If you plan to separate permissions on dashboards even further, you must create more groups.

Within **Administration** -> **Access Control** -> **User Groups** create two groups:

- Group name: Tenant User
  Description: Contains all tenant / customer user
- Group name: Operations User
  Description: Contains all internal / operations user
  You need to assign all users/groups internally to this group to provide dashboard access, because the dashboard access will be removed from the **Everyone** group at a later point.

If you plan to split dashboard permissions further, you can create more groups because access control to dashboards is sorted through local groups.

6.3.3 Access Control – Authentication

vRealize Operations Manager supports different authentication sources:

- Local users

  These are users maintained within vRealize Operations Manager. Password control is done internally. This is the recommended approach when no central LDAP/AD containing all tenant/customer users is available.

- LDAP users

  When available LDAP / Active Directory can be used to allow user access. Note that all LDAP sources will be listed at login. Therefore, VMware does not recommend using a per-tenant LDAP source. Instead, have a service provider-based LDAP source.

- SSO SAML based

  SAML-based authentication can be used in combination with a supported SSO system. It can be used in a service provider environment, but LDAP is easier to maintain in most cases.

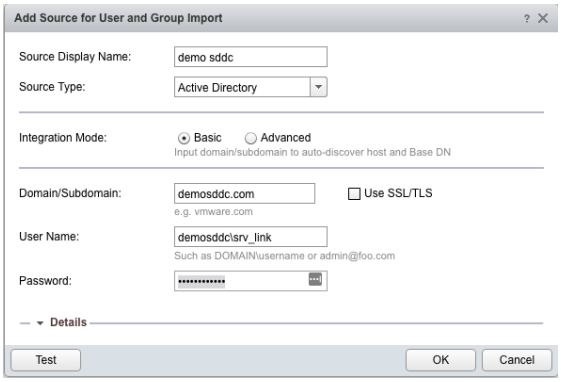
- vCenter Server users

  This refers back to users with access to vCenter Server. They can be delegated access to vRealize Operations Manager objects as well. Note that vCenter Server authentication allows users to interact only with vSphere objects. This is not a suggested approach for tenant users. It can, however, be a reasonable approach for operations users.

6.3.4 Use of an LDAP / Active Directory Source

In the case where an LDAP or Active Directory will be used as an authentication source, the source must be defined first. You can create the definition under **Administration** -> **Authentication Sources** -> **Add**.

Figure 12. Active Directory Authentication Source



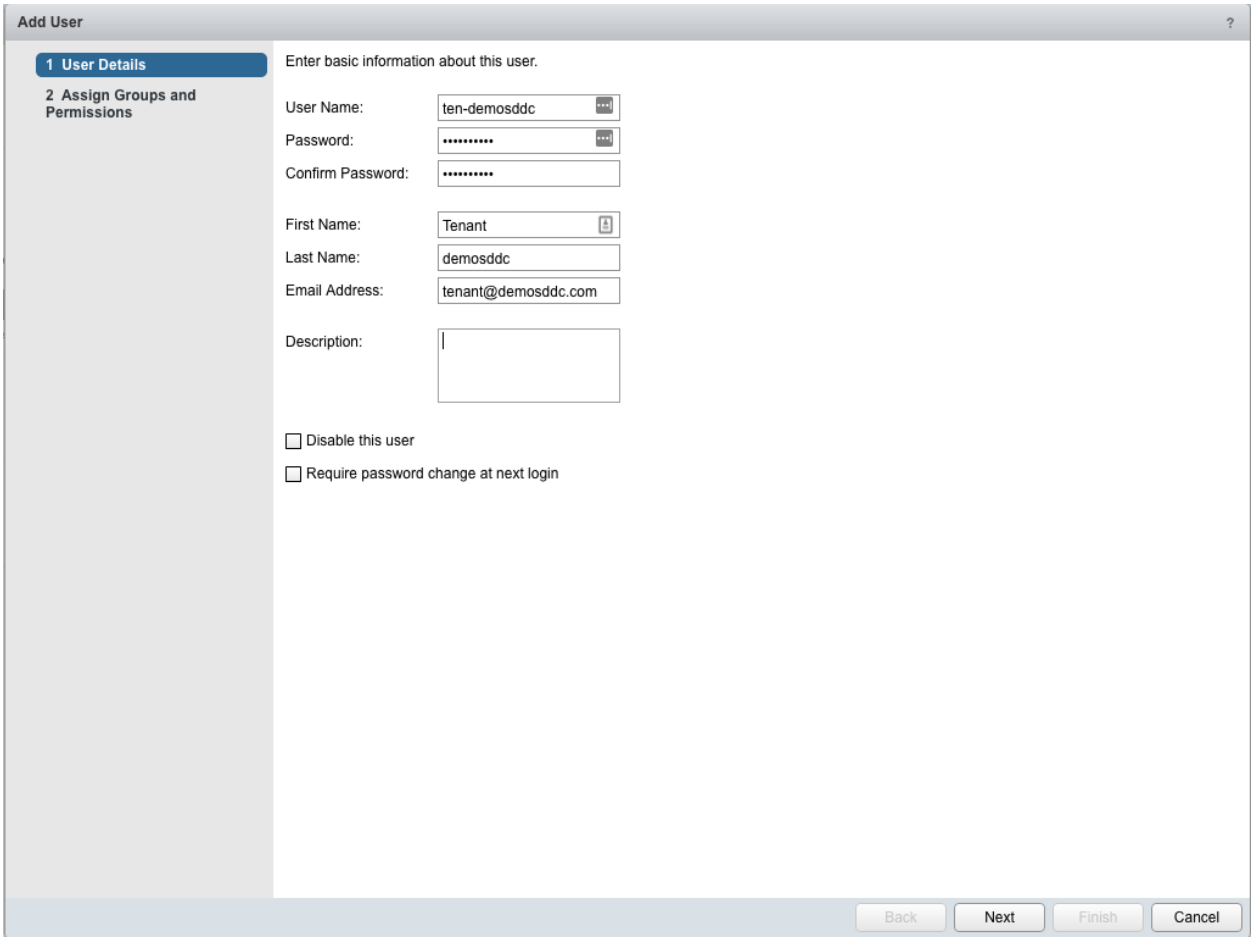
To configure and add authentication sources, see the vRealize Operations Manager documentation.

You will need to import users/groups from LDAP before they can be used within vRealize Operations Manager.

6.3.5 Use of Local Users

If LDAP / Active Directory is not an option, you might want to create local user accounts. The groups and roles must be created beforehand.

Figure 13. Local User Account



Confirm that you link the user to the group and role created previously.

6.3.6 Import of LDAP/Active Directory Users

As an alternative to manual user creation, you can import users from LDAP or Active Directory if the authentication source has already been created. After the search, you must link the user to one of the precreated groups and assign the precreated role.

6.3.7 Control Dashboard Access

While permissions can be set up for functions, the default behavior of vRealize Operations Manager is that every user with dashboard access has access to all dashboards. This is due to the fact that all dashboards are linked to the **Everyone** group.

To change the default dashboard assignment, go to **Content** -> **Dashboards** -> **Actions** -> **Share Dashboards.** Click the **Everyone** group and drag and drop all dashboards to the **Operations User** group. Next, click **Everyone** again, select all dashboards, and click the **Stop Sharing** button to remove all dashboards. The **Everyone** group should show zero dashboards assigned.

Those dashboards you would like to make available for your tenant users can be assigned now by dragging them from the **Operations User** group to the **Tenant User** group.

References

The following documentation provides additional information pertinent to this document and its topics.

Document Title	Link or URL
VMware vCloud Architecture Toolkit for Service Providers	www.vmware.com/solutions/cloud-computing/vcat-sp.html
vCloud Architecture Toolkit (vCAT) Blog	https://blogs.vmware.com/vcat/
VMware vRealize Operations Manager 6.3 Sizing Guidelines	VMware KB article 2146615

Acknowledgements

Parts of this document are based on the *VMware vCloud Architecture Toolkit for Service Providers* chapter, *Architecting a VMware vRealize Operations Management Solution for the VMware Cloud Provider Program* by Daniel Borenstein.

Appendix A: vRealize Operations Port Requirements

Source	Destination	Port	Protocol	Service Description
End-User Workstation	All Cluster Nodes	22	TCP	Enables SSH access to the vRealize Operations Manager vApp
End-User Workstation	All Cluster Nodes	80	TCP	Redirects to port 443
End-User Workstation	All Cluster Nodes	443	TCP	Used to access the vRealize Operations Manager Admin portal and the vRealize Operations Manager product user interface
End-User Workstation	Remote Collector	443	TCP	Remote Collector Admin user interface
vCenter Server	All Cluster Nodes	443, 22	TCP	Used for the collection of metric data
Remote Collector	All Cluster Nodes	443	TCP	Cluster nodes CASA
Remote Collector	All Cluster Nodes	6061, 10000	TCP	GemFire locator and data
Remote Collector	vCenter Server Instances	443, 10443, 8443	TCP	Data collection and access to vCenter Inventory Service
Remote Collector	DNS Servers	53	TCP/UDP	Name resolution
Remote Collector	NTP Servers	123	UDP	Time synchronization
All Cluster Nodes	Remote Collector	443	TCP	Remote collector CASA and Admin user interface
All Cluster Nodes	SMTP	25	TCP	Alert notifications (if port not changed!)
All Cluster Nodes	LDAP	389	TCP	LDAP access (if port not changed or LDAPs in use)
All Cluster Nodes	All Cluster Nodes	*	*	All cluster nodes must be on the same LAN
All Cluster Nodes	VMware NSX Manager™	443	TCP	VMware NSX Management Pack: API Port usage
All Cluster Nodes	SNMP Devices	161	TCP/UDP	VMware NSX Management Pack: SNMP Monitoring

Source	Destination	Port	Protocol	Service Description
All Cluster Nodes	SNMP Devices	161/162	TCP/UDP	Storage Management Pack: Storage and Fabric Monitoring
All Cluster Nodes	vCloud Director Cells	443	TCP	vCloud Director Management Pack: API access