

VMware vCloud® Architecture Toolkit™
for Service Providers

Architecting a VMware vRealize® Business™ Solution for VMware Cloud Providers™

Version 2.8
August 2017

Daniel Borenstein





© 2017 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. This product is covered by one or more patents listed at <http://www.vmware.com/download/patents.html>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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



Contents

- Introduction 7**
 - 1.1 Document Purpose 7
 - 1.2 Glossary of Terms..... 7
- Technology Mapping..... 9**
 - 2.1 vRealize Business Overview..... 9
- Deployment Model Considerations 10**
 - 3.1 Conceptual Overview 10
 - 3.2 Deployment Models 11
- Design Considerations..... 13**
 - 4.1 Architectural Overview 13
- vRealize Business Standard Use Cases for VMware Cloud Provider Program 17**
 - 5.1 Usage Metering and Costing 17
 - 5.2 Public Cloud Cost Comparison 17
- Availability..... 17**
- Manageability..... 18**
 - 7.1 Management Guidelines 18
 - 7.2 Log Files..... 18
 - 7.3 Database Status..... 18
 - 7.4 Data Collection..... 18
- Performance and Scalability 19**
 - 8.1 Scalability Considerations 19
- Recoverability 19**
- Security..... 20**
 - 10.1 Root Password..... 20
 - 10.2 Password Expiry 21
 - 10.3 Secure Shell, Administrative Accounts, and Console Access 21
 - 10.4 Time Sourcing and Synchronization 22
 - 10.5 Log Forwarding – Syslog-ng and Auditd..... 22
 - 10.6 Boot Loader (GRUB) Password..... 24
 - 10.7 Firewall Requirements 24
- Integration..... 26**



Architecting a VMware vRealize Business Solution for
VMware Cloud Providers

| | | |
|--|---|-----------|
| 11.1 | VMware vSphere..... | 26 |
| 11.2 | VMware vCloud Director for Service Providers | 26 |
| 11.3 | VMware vRealize Automation..... | 26 |
| 11.4 | Public Clouds | 27 |
| 11.5 | VMware vRealize Operations Manager | 27 |
| 11.6 | VMware vRealize Business Advanced and Enterprise..... | 27 |
| Operational Considerations..... | | 28 |
| 12.1 | Update the Reference Database for vRealize Business Standard..... | 28 |
| 12.2 | Calculating Depreciation of Server Hardware Cost | 28 |
| 12.3 | View and Update System Status | 29 |
| 12.4 | Data Collection..... | 29 |
| 12.5 | Updating vRealize Business Standard | 30 |
| References | | 31 |
| 13.1 | vRealize Business Standard | 31 |
| 13.2 | VMware Hardened Virtual Appliances | 31 |
| 13.3 | vSphere Fault Tolerance..... | 31 |



List of Figures

| | |
|--|----|
| Figure 1. vRealize Business Standard Conceptual Design | 9 |
| Figure 2. vRealize Business Standard in Context..... | 10 |
| Figure 3. VMware Cloud Provider – Metering Customer Resource Usage | 11 |
| Figure 4. Hybrid Cloud Cost Management Solution for Enterprises..... | 11 |
| Figure 5. Logical Architecture | 14 |

List of Tables

| | |
|---|----|
| Table 1. Glossary of Terms..... | 7 |
| Table 2. Virtual Appliance Requirements..... | 14 |
| Table 3. vRealize Business Standard Currencies..... | 16 |
| Table 4. Data Collection..... | 18 |
| Table 5. vRealize Business Standard Communication Ports | 24 |
| Table 6. Depreciation Methods | 28 |
| Table 7. Task Execution Intervals..... | 29 |





Introduction

VMware Cloud Providers™ who want to offer cloud services to their customers need a mechanism to meter and manage the costs associated with offering such services. VMware vRealize® Business Standard delivers these capabilities to service providers and enterprises.

vRealize Business Standard provides transparency and control over the costs and quality of IT services offered by a VMware Cloud Provider. It helps service provider organizations shift from a technology orientation to a service broker orientation, delivering a portfolio of IT services that align with the needs of business stakeholders. vRealize Business Standard provides the management capabilities necessary to manage the business aspects of today's emerging hybrid cloud environments and allows IT transformation enabling cloud service providers to reduce capital and operating expenses while improving service delivery performance.

1.1 Document Purpose

This document is intended to help the cloud service provider design a cloud business management solution based on vRealize Business Standard. It focuses on key design considerations a cloud service provider needs to consider when designing and implementing vRealize Business Standard to meet cloud business management requirements.

This is not meant as a replacement for product documentation, but to be used a supplementary component when planning a VMware Cloud Provider Program cloud implementation.

1.2 Glossary of Terms

Table 1. Glossary of Terms

| Term | Description |
|-------|------------------------------------|
| API | Application Programming Interface |
| CPU | Central Processing Unit |
| CSV | Comma Separated Values |
| FT | VMware Fault Tolerance |
| FTP | File Transfer Protocol |
| GB | Gigabyte |
| GRUB | Grand Unified Bootloader |
| HA | High Availability |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| IaaS | Infrastructure as a Service |
| JPA | Java Persistence API |
| NIC | Network Interface Card |



| Term | Description |
|-----------------------|--|
| NTP | Network Time Protocol |
| OS | Operating System |
| SP | Service Provider |
| SRG | Security Requirements Guide |
| SRM | EMC Storage Resource Management |
| SSH | Secure Shell |
| STIG | Security Technical Implementation Guide |
| TCP | Transport Control Protocol |
| URL | Uniform Resource Locator |
| VAMI | VMware Administration and Management Interface |
| VMware vSphere® vApp™ | Virtual Appliance |
| vCPU | Virtual Central Processing Unit |
| VDC | Virtual Data Center |
| VM | Virtual Machine |
| WAN | Wide Area Network |



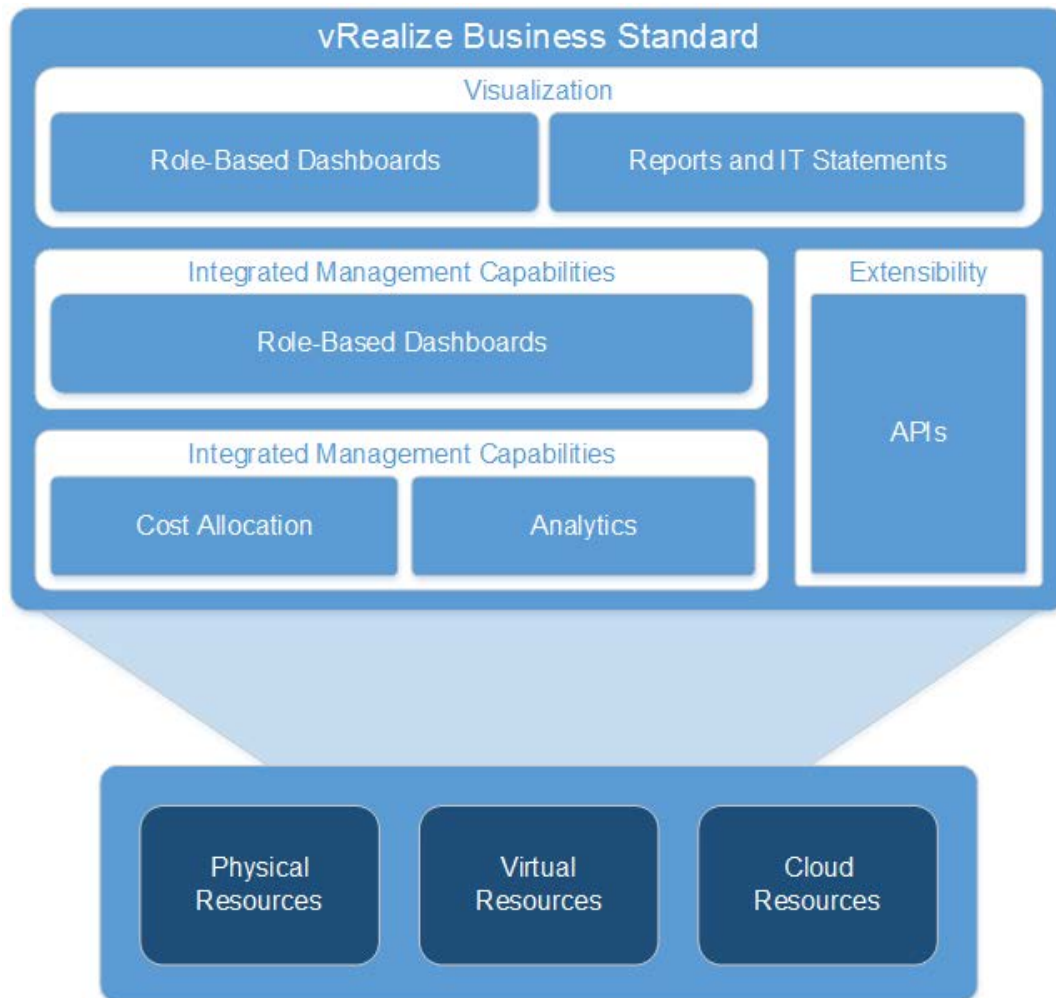
Technology Mapping

For a private, public, or hybrid cloud, the provider must offer appropriate metering services that support customer charges based on utilization. Billing system requirements must be factored into the design so that vRealize Business Standard can provide appropriate data to enable the provider to bill their customers accurately based on the required schedule.

2.1 vRealize Business Overview

vRealize Business Standard provides metering and cost management for private and public clouds. It puts a price on underlying infrastructure and resources, enabling service providers to make informed pricing decisions and extract billing data to charge their customers.

Figure 1. vRealize Business Standard Conceptual Design





Deployment Model Considerations

Multiple deployment models are available when deploying a vCloud, depending on the manner in which resources are provided and who consumes them. These are:

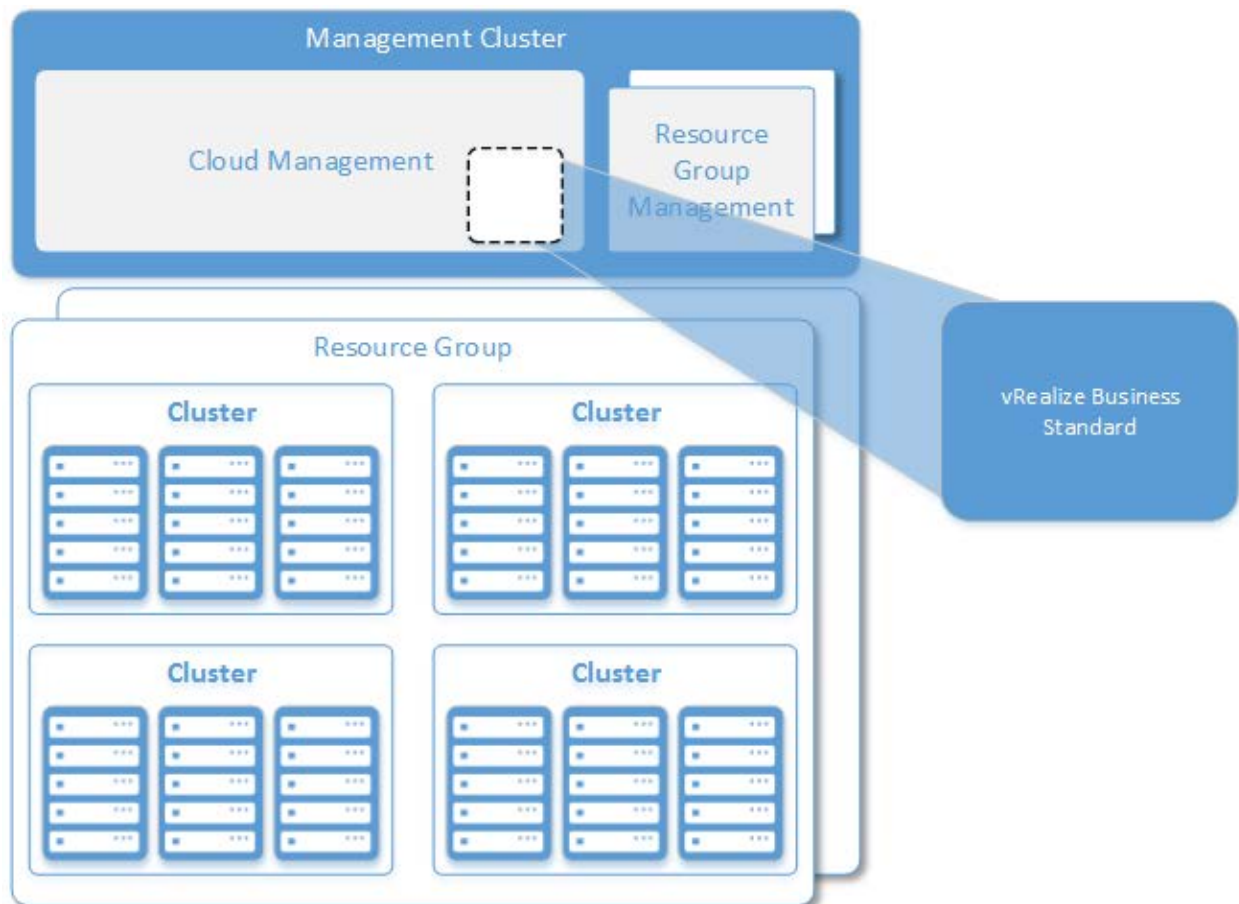
- Private cloud – Cloud infrastructure operated exclusively for an organization. Can be managed by the organization or a third party. The infrastructure can be located on-premises or off-premises.
- Public cloud – Cloud infrastructure made available to the public or to a large industry group and owned by an organization that sells cloud services.
- 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.

3.1 Conceptual Overview

Cloud business management is an important factor in any cloud design, regardless of the deployment model. Both private and public cloud designs require cost management components to put a price on resources and provide cost visibility of private and public cloud resources.

The following figure shows where the cloud business management component is located relative to a vCloud management cluster.

Figure 2. vRealize Business Standard in Context





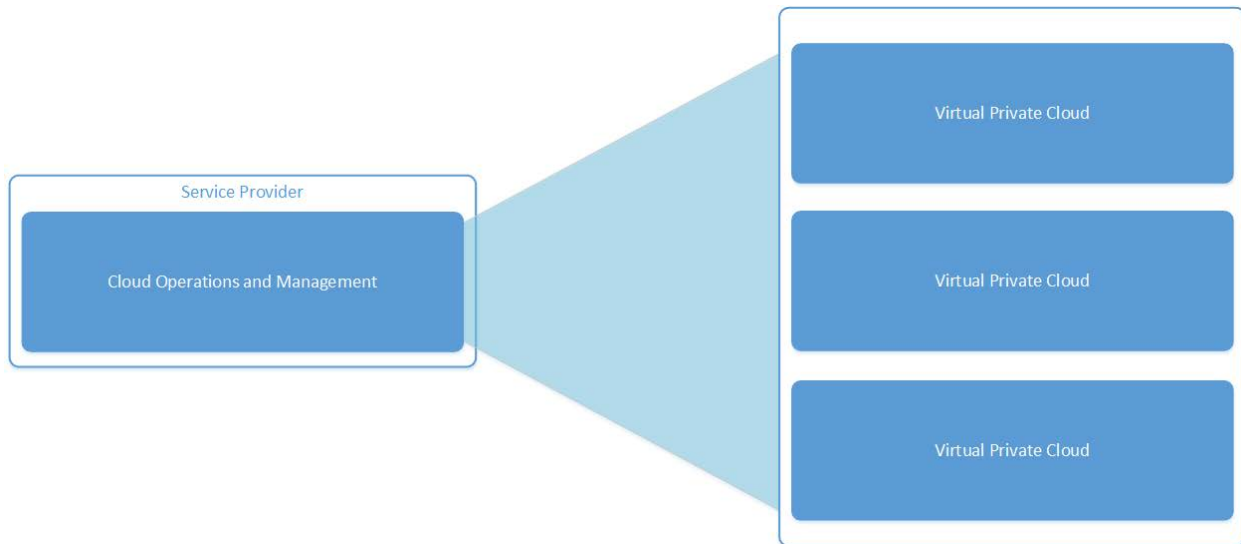
3.2 Deployment Models

The primary vRealize Business Standard deployment mode for a VMware Cloud Provider is to meter customer resource usage.

A service provider may need to meter VMware vCloud Director® for Service Providers organization virtual data centers, a hosted VMware vSphere environment (private hosted cloud), or a combination of both.

The following figure shows an example of the deployment model.

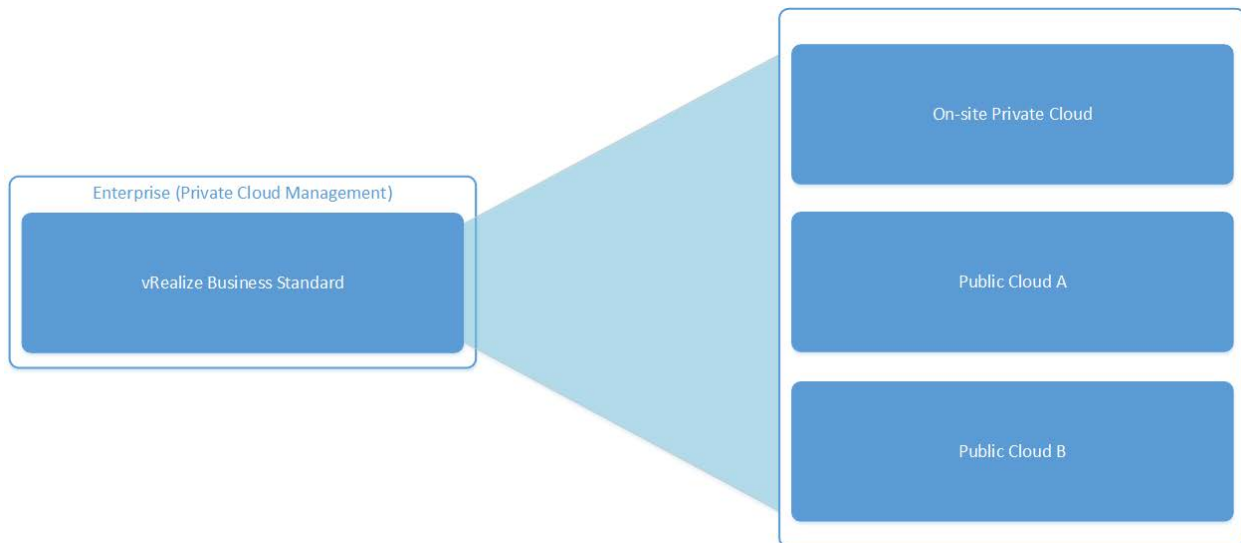
Figure 3. VMware Cloud Provider – Metering Customer Resource Usage



Service provider customers, particularly those using VMware vRealize Automation™ also require a cost management solution to show or charge for the use of cloud resources. An enterprise customer may need to meter an on-premises or off-premises private cloud as well as public cloud resources.

The following figure shows vRealize Business Standard deployed in an enterprise private cloud and providing cost management functions for both private and public cloud resource consumption.

Figure 4. Hybrid Cloud Cost Management Solution for Enterprises





Design Considerations

- vRealize Business must be integrated with a vRealize Automation standalone appliance for basic user interface functionality, but can also be fully integrated with the Infrastructure as a Service (IaaS) component of vRealize Automation.
- To obtain the best performance results, deploy the vRealize Business Standard appliance on the same network as VMware vCenter Server®.
- If possible, do not deploy vRealize Business Standard over a WAN as excessive latency may impact performance.
- Include vRealize Business Standard in both private and public cloud designs to manage business, metering, and cost management functions.
- Deploy vRealize Business Management within a management cluster.



Design Considerations

4.1 Architectural Overview

vRealize Business Standard is deployed as a virtual appliance, encapsulating a VMware virtual machine. Its architecture is comprised of three main components—server, data collector, and reference database. The user interface is provided by the vRealize Automation appliance, and user authentication/authorization is provided by VMware vCenter® Single Sign-On™.

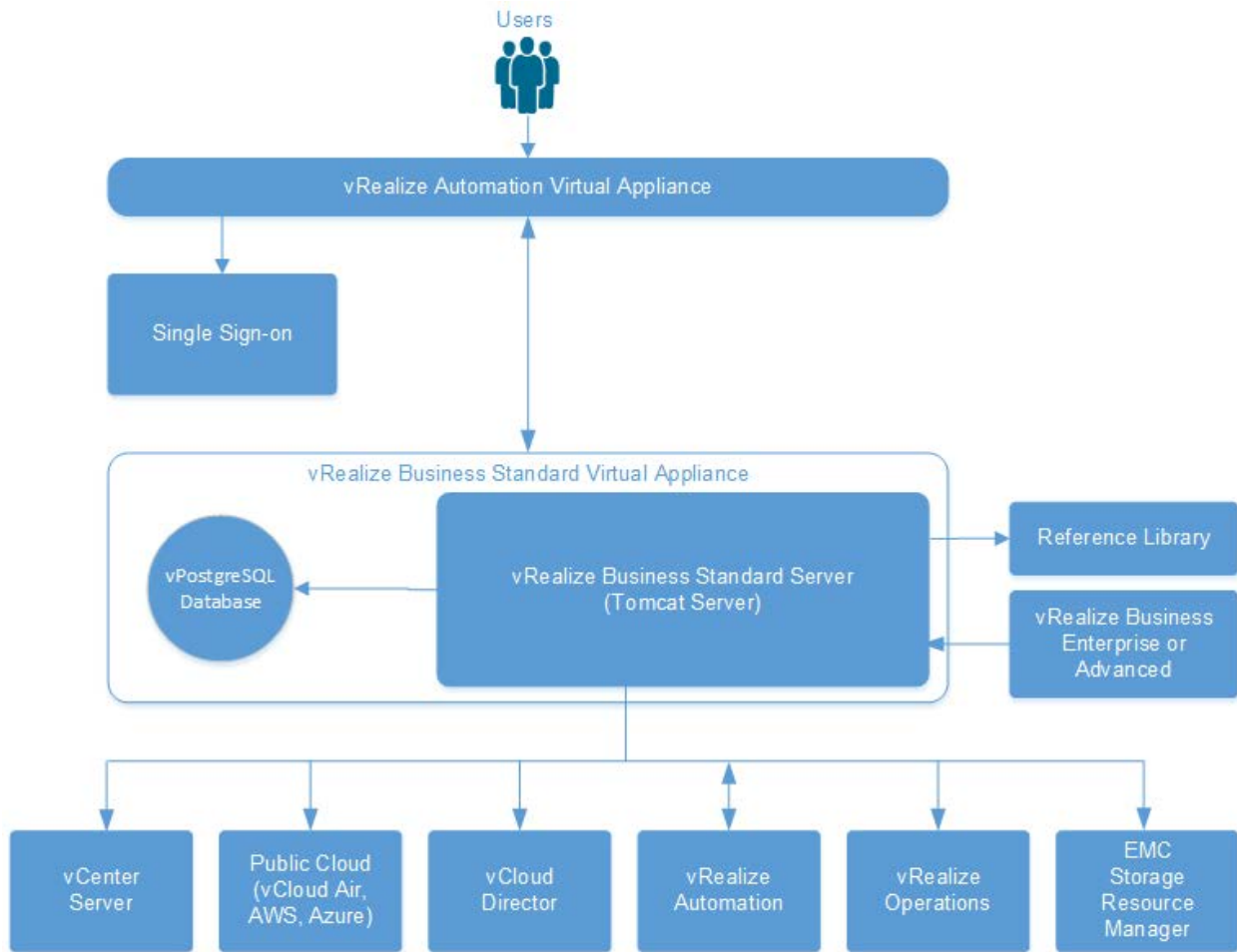
vRealize Business Standard integrates with the following products to provide cost management, analysis, and comparison functions:

- vCenter Server
- vCloud Director
- vRealize Automation
- VMware vRealize Operations Manager™
- Public clouds:
 - VMware vCloud Air™
 - Microsoft Azure
 - Amazon Web Services



The following figure illustrates the interaction between these components.

Figure 5. Logical Architecture



Design Considerations

For optimal performance, deploy vRealize Business Standard on the same network as the infrastructure to be metered (vCenter Server or vCloud Director).

4.1.1 Hardware Requirements

The following table lists hardware requirements for vRealize Business Standard.

Table 2. Virtual Appliance Requirements

| Attribute | Specification |
|----------------------------|---------------|
| vRealize Business Standard | Version 6.1 |
| Physical or virtual system | Virtual |
| Number of CPUs | 2 |
| Processor type | VMware vCPU |



| Attribute | Specification |
|------------------------------------|---------------|
| Memory | 4 GB |
| Number of NICs and ports | 1/1 |
| Number of disks and disk sizes | 50 GB |
| Operating system | vApp |
| Max number of vCenter Server nodes | 4 |
| Max number of VMs | 20,000 |

4.1.2 vRealize Business Server

The vRealize Business server is based on a Tomcat Server instance, communicating through the Java Persistence API (JPA) and the Hibernate framework to a VMware vFabric® Postgres database over a JDBC connection.

The data collector populates the local vFabric Postgres database with infrastructure events and usage statistics from vCenter Server. The vRealize Business server then consumes the collected data from the vFabric Postgres database.

The vRealize Business server uses the Quartz job scheduler to schedule hourly, daily, and monthly collection jobs. Quartz jobs collect the following data:

- Endpoint inventory
- Utilization
- Cost formula
- Reference library updates

Costs are then calculated and updated based on this data.

4.1.3 Reference Library Database

The Reference Library Database holds known configurations and default costs for each of the supported cost drivers. References are updated periodically, and the latest data set is downloaded (as a compressed and encrypted file) for import into vRealize Business Standard. References can also be updated manually by the user.



4.1.4 Currency Considerations

The system currency is specified during the first startup of vRealize Business Standard. The system currency can be set only during the initial startup. Available currencies are specified in the following table.

Table 3. vRealize Business Standard Currencies

| Currency | Abbreviation |
|---------------------|--------------|
| Australian Dollar | AUD |
| Canadian Dollar | CAD |
| China Yuan Renminbi | CNY |
| Euro | EUR |
| British Pound | GBP |
| Hong Kong Dollar | HKD |
| Indonesia Rupiah | IDR |
| Israeli Shekel | ILS |
| Indian Rupee | INR |
| Japanese Yen | JPY |
| Korean (South) Won | KRW |
| Malaysia Ringgit | MYR |
| Norway Krone | NOK |
| New Zealand Dollar | NZD |
| Russia Rouble | RUB |
| Sweden Krona | SEK |
| Singapore Dollar | SGD |
| Turkey Lira | TRY |
| Taiwan New Dollar | TWD |
| US Dollar | USD |
| South Africa Rand | ZAR |

Design Considerations

Select the appropriate currency to use for billing and cost drivers.



vRealize Business Standard Use Cases for VMware Cloud Provider Program

The primary use case that vRealize Business Standard addresses for VMware Cloud Providers is to meter customer resource usage to facilitate billing. Additionally, the following use cases are also addressed:

- Public cloud cost comparison
- Public cloud usage metering and costing
- Scenario planning and forecasting

vRealize Business Standard addresses all of these use cases.

5.1 Usage Metering and Costing

Setting a price for resources and then metering those resources is how service providers bring in revenue and as such is a business critical function. Both allocation and usage based metering and billing are required.

A service provider can also broker public cloud services from other service providers and provide value-added services. These services must also be metered and billed for.

5.2 Public Cloud Cost Comparison

Cloud service providers need to maintain an awareness of what their partners or competitors are charging in order to stay competitive in the marketplace.

Integration with other public cloud service providers to have at-a-glance visibility of current industry pricing enables service providers to make informed decisions on pricing.

Availability

vRealize Business Standard can be protected by VMware vSphere High Availability, providing up to 99.9 percent of availability.

VMware vSphere Fault Tolerance can be used to protect the vRealize Business Standard appliance if it is running on vSphere 6 and meets hardware and network latency prerequisites.

Design Considerations

- Use vSphere HA to protect against host hardware failure. VMware recommends always enabling vSphere HA on vSphere clusters.
- Consider using vSphere Fault Tolerance to protect vRealize Business Standard.



Manageability

vRealize Business Standard is provided as a virtual appliance to simplify management and monitoring operations.

7.1 Management Guidelines

The vRealize Business Standard appliance can be managed through the web-based Virtual Appliance User Interface (VAMI). The interface can be accessed by opening the following URL in a Web browser:

`https://<vRealize Business Standard IP or hostname>:5480`

vRealize Business Standard must be registered with the vRealize Automation virtual appliance. Users can access vRealize Business Standard through the **Business Management** tab of vRealize Automation and must be assigned the Business Management Administrator role.

7.2 Log Files

Log file information is important if vRealize Business Standard requires troubleshooting. The following log files contain important troubleshooting information:

```
/usr/local/tcserver/vfabric-tc-server-standard/itbm-server/logs/itfm.log
```

```
/usr/local/tcserver/vfabric-tc-server-standard/itbm-server/logs/catalina.out
```

If a VMware vRealize Log Insight™ instance is deployed in the environment, these logs can be forwarded there for centralized analysis and troubleshooting.

Design Considerations

Consider forwarding logs to a centralized syslog collector such as vRealize Log Insight.

7.3 Database Status

The status of the embedded vFabric Postgres database can be obtained using the following command:

```
root> su - postgres -c "/opt/vmware/vpostgres/current/bin/pg_ctl status -D  
"/opt/vmware/vpostgres/current/data"
```

The output is similar to the following:

```
pg_ctl: server is running (PID: 2880)  
/opt/vmware/vpostgres/9.2/bin/postgres "-D"  
"/opt/vmware/vpostgres/current/data"
```

7.4 Data Collection

Data collection is performed on the vRealize Business Standard components listed in the following table.

Table 4. Data Collection

| Item | Data Type | Data Collection Frequency |
|----------------------------|-----------|------------------------------------|
| Compute Resource (vSphere) | Inventory | Immediately after Inventory Update |
| Cost Calculation | Costs | Default: Daily |
| vRealize Automation | Status | Default: Daily |



Performance and Scalability

8.1 Scalability Considerations

vRealize Business Standard requires a minimum of 50 GB of disk space, 4 GB memory, and 2 vCPU. vRealize Business Standard allows scaling up to four vCenter Server instances and 20,000 virtual machines.

Recoverability

vRealize Business Standard can be backed up and recovered using traditional virtual machine backup solutions, such as VMware vSphere Data Protection™ or VMware Data Recovery.

It is possible to perform file and database level backups of vRealize Business Standard. However, this will increase the complexity of both the backup configuration and restore process. VMware recommends backing up the entire virtual appliance at an image level.

When backing up the vRealize Business Standard database, follow the native PostgreSQL backup and restore procedures documented at <http://www.postgresql.org/docs/9.2/static/backup.html>.

Design Considerations

Plan to back up the entire vRealize Business Standard virtual appliance.



Security

The virtual appliance method of deployment for VMware data center products provides customers with the ability to rapidly deploy and configure infrastructure components.

VMware has standardized the security profile of VMware produced virtual appliances to a technical standard that meets or exceeds current high governance compliance requirements found in various vertical market segments. See the *Hardened Virtual Appliance Operations Guide* for further details: <http://www.vmware.com/files/pdf/techpaper/VMWare-Hardened-Appliance-Operations-Guide.pdf>.

The following sections cover the technical requirements of the OS SRG STIG standard that are not embedded in the vRealize Business Standard virtual appliance.

10.1 Root Password

Most hardened appliances allow the modification of the root password during initial setup, or are pre-installed with the root password set to “vmware”. VMware highly recommends changing the root password for both complexity and cryptographic hashing to meet STIG compliance.

The vRealize Business Standard root password can be changed through the VAMI or at the command line.

The root user bypasses the `pam_cracklib` module password complexity check (found in `/etc/pam.d/common-password`). Manually verify that the root password meets the password complexity requirements of your organization.

All hardened appliances enable `enforce_for_root` for the `pw_history` module (found in `/etc/pam.d/common-password`). The last five passwords are remembered by default, preventing those passwords from being reused.

Design Considerations

Choose a root password of sufficient length and complexity, using numbers, upper and lower case letters, and non-alphanumeric characters. Random password generators offer a simple way to create passwords based on desired complexity properties.



10.2 Password Expiry

To meet the compliance standard of the STIG, set user accounts to expire after 60 days, and service accounts to expire after 365 days.

As part of an organization's compliance policies, implement a procedure so that administrators do not forget to change their passwords within the active period. If the root account expires, there is no method in the appliance to re-instate the root password. It is imperative that site-specific policies are implemented to prevent administrative and root passwords from expiration.

Design Considerations

- Consider setting password expiry if compliance with the STIG is required, or if policy dictates it.
- Configure the root password not to expire. However, if it does expire, it can be reset by booting the appliance into single user mode.
- If administrators must log in to a command shell on the appliance, they must do so with a user-specific account that is set to expire after the required period.

10.3 Secure Shell, Administrative Accounts, and Console Access

For remote connections, all hardened appliances include the Secure Shell (SSH). Because many appliances do not include default user accounts, the root account might still be able to directly log in through SSH.

To meet the compliance standards for nonrepudiation, the SSH server on all hardened appliances comes preconfigured with the "AllowGroups wheel" entry to restrict SSH access to the secondary group wheel.

Note For separation of duties, the "AllowGroups wheel" entry can be modified in `/etc/ssh/sshd_config` to use another group (such as `sshd`). The wheel group is enabled with the `pam_wheel` module for superuser access, so members of the wheel group are allowed to `su -` to root (password for root is required).

Group separation provides a method for users to SSH to the appliance, but not have the ability to `su` to root. For proper appliance functionality, do not remove or modify other entries in the AllowGroups field. Any change will require a restart of the SSH daemon.

Prior to removing root SSH access, create the local administrative accounts that can both use SSH and/or are members of the secondary wheel group.

Direct root login to SSH is removed by modifying the `/etc/ssh/sshd_config` file, setting the `PermitRootLogin` to `no`, and restarting `sshd`.

Restrict SSH access with the proper entries to limit access. All VMware virtual appliances include the `tcp_wrappers` package to allow TCP supported daemons to control the network subnets that can access the libwrapped daemons.

By default, the `/etc/hosts.allow` file contains a generic entry to allow all access to the secure shell:

```
sshd: ALL : ALLOW
```

VMware recommends that this entry be changed for production environments to include only the localhost entries and the management network subnet for secure operations, such as:

```
sshd: 127.0.0.1 : ALLOW
```

```
sshd: [::1] : ALLOW
```

```
sshd: 10.0.0. : ALLOW
```

This example will allow all localhost connections and connections made by clients on the 10.0.0.0 subnet.



By default, the hardened appliances allow direct login to root through the console. After administrative accounts have been created for non-repudiation and tested for wheel access (`su - root`), direct root logins can be disabled by editing the `/etc/securetty` file as root and replacing the entry

```
tty1
```

with

```
console
```

Design Considerations

Consider implementing the following if compliance with the STIG is required, or policy dictates it:

- Create user-specific administrative accounts for users that need to log in to a command shell.
- Remove ability for the root user to log in through SSH or the appliance console.
- Use `tcp_wrappers` to limit SSH connections to hosts on the management network.

10.4 Time Sourcing and Synchronization

Accurate and consistent time synchronization is essential across virtual infrastructure components to gather accurate and useful data.

Consistent time synchronization across monitored infrastructure eases the task of reconciling, collating, debugging, and the tracing of log information between related devices. Time synchronization is also important for transactional applications where timestamps must be recorded accurately.

The vRealize Business Standard appliance includes two mechanisms for time synchronization: VMware Tools™ and the Network Time Protocol (NTP) service. VMware Tools uses the time of the VMware ESXi™ host the appliance is running on for time synchronization. NTP synchronizes time against a precise time source, usually synchronizing itself with an atomic clock.

VMware recommends that virtual appliances use NTP to synchronize for time-sensitive environments. The hardened vRealize Business Standard appliance allows time to be configured with the VAMI user interface.

Design Considerations

- Configure all devices in an environment to use NTP to synchronize their time against the same time sources.
- Configure devices to use a minimum of two NTP servers for time synchronization in case one is unavailable.

10.5 Log Forwarding – Syslog-ng and Auditd

The vRealize Business Standard appliance includes both comprehensive system and audit logging to support high governance compliance.

10.5.1 Syslog

To enable forwarding of system logs, modify the configuration file of the syslog server to specify the protocol, IP address, and port of the central log server (such as vRealize Log Insight). The syslog configuration file is located in `/etc/syslog-ng/syslog-ng.conf`. The following two lines are pre-populated:

```
#destination logserver { udp("10.10.10.10" port(514)); };  
#log { source(src); destination(logserver); };
```



Uncomment the two lines, and modify the fields. In this example, using TCP as the transport, 10.10.10.10 as the IP of the central syslog server, and port 514 as the syslog central server port, the entry would be:

```
destination logserver { tcp("10.10.10.10" port(514)); };  
log { source(src); destination(logserver); };
```

Restart the syslog-ng service as root to incorporate the change.

Configure firewalls to allow access to the port specified for the syslog destination log server.

Design Considerations

Forward syslog messages to a centralized syslog collector such as vRealize Log Insight.

10.5.2 Auditd

The vRealize Business Standard appliance uses the audispd service to forward all audit logs to the syslog-ng service. The configuration file is located in `/etc/audisp/plugins.d/syslog.conf`. Forwarding can be enabled by editing the syslog server configuration file and setting the following parameter:

```
active=yes
```

Restart the auditd service as root to incorporate the change.

When using the high governance audit rules, there is an increase in the amount of logging traffic that might warrant reconfiguration of both the `q_depth` and the `priority_boost` of the audit dispatcher daemon. The configuration file is located in `/etc/audisp/audispd.conf`. The following configuration file parameters must be set:

```
q_depth = 80 (recommendation for high governance audit logs is at least 1,280)  
priority_boost = 4 (recommendation for high governance audit logs is at least 8)
```

Restart the auditd service as root to incorporate the change.

When using the high governance audit rules, there is an increase in the size of log files. To decrease the number of stored logs on the hardened appliances (this assumes log forwarding has been configured), customers can tune the number of daily log files stored by modifying the rotation number. All log rotation configurations are stored in `/etc/logrotate.d`.

To control the number of stored daily log files for syslog, edit the `/etc/logrotate.d/syslog` file as root. Modify all of the “rotate 15” entries to the number of days to store local logs. The recommended number of days for centralized log services is at least 7.

To control the number of stored daily log files for the audit daemon, edit the `/etc/logrotate.d/audit` file as root. Modify the “rotate 15” entry to the number of days to store local audit logs. The recommended number of days for centralized audit log services is at least 7.

Design Considerations

Configure auditd to forward messages to syslog-ng, which can in turn forward them to a centralized syslog collector such as vRealize Log Insight.



10.6 Boot Loader (GRUB) Password

The vRealize Business Standard appliance has the ability to protect the appliance with a password for modification of the default boot settings. GRUB boot loader settings can be viewed and modified in the following configuration file:

```
/boot/grub/menu.lst
```

To change or add a password for GRUB, run the following procedure as root:

1. Open a command shell session and start a GRUB shell by entering the command `grub`. The grub shell will appear.
2. Run the `md5crypt` command to create the hashed password. After the password is entered, this command returns a hash.
3. Copy the password and enter the `quit` command to exit the GRUB shell.
4. Edit `/boot/grub/menu.lst` and add the following entry, where `<md5hash>` is the hash copied to the clipboard:

```
password --md5 <md5hash>
```

5. Save the file and exit.

Design Considerations

- Consider setting a password on the GRUB boot loader so that the vRealize Business Standard appliance cannot be tampered with from the console.
- Store the boot loader password in a secure place as recovering access is a complex process.

10.7 Firewall Requirements

The vRealize Business Standard virtual appliance requires the ports listed in the following table to be configured where firewalls separate connectivity.

Table 5. vRealize Business Standard Communication Ports

| Source | Destination | Port | Protocol | Service Description |
|--------------------------------------|--------------------------------------|-------|----------|-------------------------------|
| Admin workstation | vRealize Automation appliance | 443 | TCP | User Web access |
| vRealize Automation appliance | vRealize Business Standard appliance | 443 | TCP | vRealize Automation appliance |
| vRealize Business Standard appliance | vCenter Server | 443 | TCP | vCenter Server |
| vRealize Business Standard appliance | vCenter Single Sign-On | 7444 | TCP | vCenter Single Sign-On |
| vRealize Business Standard appliance | vCenter Inventory Services | 10443 | TCP | vCenter Inventory Services |
| vRealize Business Standard appliance | vCloud Air | 443 | TCP | vCloud Air |



| Source | Destination | Port | Protocol | Service Description |
|--------------------------------------|--------------------------------------|------|----------|--|
| Admin workstation | vRealize Business Standard appliance | 22 | TCP | Management (SSH) |
| vRealize Business Standard appliance | vrb-hub.vmware.com | 443 | TCP | Reference database |
| vRealize Business Standard appliance | saasftp.digitalfuel.com | 22 | TCP | Reference database |
| Admin workstation | vRealize Business Standard appliance | 5480 | TCP | Virtual Appliance Management Infrastructure (VAMI) |



Integration

vRealize Business Standard integrates with the following endpoints, enabling cloud business management functionality:

- VMware vSphere
- VMware vCloud Director for Service Providers
- VMware vRealize Automation
- Public Cloud
- VMware vRealize Operations Manager™
- vRealize Business Advanced and Enterprise

11.1 VMware vSphere

vRealize Business Standard integrates with vCenter Server to retrieve the following:

- Inventory
- Virtual machine configuration
- Physical and virtual infrastructure configuration
- Allocation and utilization metrics

This information is used in conjunction with cost drivers to calculate the cost of vSphere virtual machines.

11.2 VMware vCloud Director for Service Providers

vRealize Business Standard allows organizational constructs to be viewed from vCloud Director. vRealize Business Standard supports the following vCloud Director for Service Provider constructs:

- Organization
- Organization virtual data center (VDC)
- vApps
- Virtual machines

These constructs are used in conjunction with vSphere utilization metrics to calculate the virtual machine and infrastructure costs in a vCloud Director for Service Providers context.

11.3 VMware vRealize Automation

vRealize Business Standard is accessed through the vRealize Automation web interface. It is located under the **Business Management** tab.

vRealize Business Standard uses the same vCenter Single Sign-On service as vRealize Automation for authentication and authorization. The vRealize Automation Infrastructure as a Service (IaaS) cost profiles are automatically updated by vRealize Business Standard based on cost driver values, streamlining the process of costing virtual machine blueprints.

The vRealize Automation Infrastructure as a Service (IaaS) is not a hard requirement, and the vRealize Automation virtual appliance can be used solely to provide access to vRealize Business Standard.



11.4 Public Clouds

vRealize Business Standard can be configured to connect to public clouds to retrieve pricing and utilization data. vRealize Business Standard can generate public cloud usage reports as well as provide cost comparisons for future workloads.

vRealize Business Standard can provide users with an overview of how investments are being spread across public cloud providers such as Amazon Web Services (AWS) and Microsoft Azure, and provides detailed analysis of the costs of AWS and Microsoft Azure.

11.5 VMware vRealize Operations Manager

In an environment where VMware vRealize Operations Manager 6.x is installed, vRealize Business Standard can retrieve the expected CPU and memory utilization for each cluster or standalone ESXi host from vRealize Operations Manager.

Otherwise, expected CPU and memory utilization can be set per host by using the system-defined value, (computed by using historical averages), user-defined global value, or by user-defined value at each cluster level. Expected CPU and memory utilization is used to calculate virtual machine cost allocation.

11.6 VMware vRealize Business Advanced and Enterprise

vRealize Business Standard APIs enable third-party systems to extract inventory, utilization and configuration data in CSV format.

VMware vRealize Business Advanced and VMware vRealize Business Enterprise can use these APIs to collect private and public cloud information, which can be used in cost modeling and reports.



Operational Considerations

12.1 Update the Reference Database for vRealize Business Standard

The reference database can be updated to have the most current version of the reference library. The reference database can be updated manually or by running the auto-update feature. The reference database supplies values for cost calculations.

Updating the reference database requires the following ports to be open:

- Port 443, which connects to <https://vrb-hub.vmware.com>
- Port 22, which connects to SaasFTP.digitalfuel.com

If the auto update process fails to run on port 22 (FTP), the process starts on port 443 (HTTPS).

12.2 Calculating Depreciation of Server Hardware Cost

vRealize Business Standard calculates the yearly depreciation values of server hardware costs and then divides the value by 12 to arrive at the monthly depreciation. vRealize Business Standard uses the salvage value of zero dollars.

$$\text{depreciable cost} == \text{original cost}$$

vRealize Business Standard uses the maximum value between yearly depreciation of declining balance with the multiplied depreciation rate and yearly depreciation of a straight line over five years.

$$\text{Yearly depreciation} = \text{Max}(\text{yearly depreciation of double-declining balance method}, \text{yearly depreciation of straight line method})$$

This is the yearly depreciation of double-declining balance method and yearly depreciation of straight-line method.

Table 6. Depreciation Methods

| Method | Calculation |
|--------------------------|---|
| Double-declining balance | Depreciation rate = 2 / number of depreciation years Yearly depreciation: In every year, except the last year of depreciation: Yearly depreciation = (original cost – accumulated depreciation) * depreciation rate In the last year of depreciation: Yearly depreciation = original cost – accumulated depreciation |
| Straight-line method | Yearly depreciation = (original cost – accumulated depreciation) / number of depreciation years |

The depreciation period can be set to three or five years.



12.3 View and Update System Status

The status of critical internal business processes can be viewed to understand the overall system health. The system processes run periodically to verify that inventory and cost data are always up-to-date.

The data collector connects to vCenter Server instances to collect inventory data and usage statistics. After collecting inventory data and usage statistics, vRealize Business Standard displays the timestamp of the last executed job in local time.

The following table provides information about the frequency or interval of each job in vCenter Server data collection.

Table 7. Task Execution Intervals

| Task/Job | Frequency/Interval |
|-----------------------------|---------------------------------------|
| Inventory | Immediately after an inventory update |
| Tags | Every 10 minutes |
| vRealize Operations Manager | Every 30 minutes |
| Storage | Every 12 hours |
| Usage Statistics | Every 24 hours |

12.4 Data Collection

In addition to vSphere, vRealize Business Standard collects configuration and usage data from a number of data sources. The data collectors used to gather this data are detailed in this section.

12.4.1 vCloud Director

vRealize Business Standard connects to vCloud Director to collect data about consumers of virtual machines by organization and organization virtual data center.

vCloud Director connection information appears only after connecting vCloud Director to vRealize Business Standard.

12.4.2 EMC VIPR SRM

The storage collector connects to EMC VIPR SRM server instances and collects data and usage details. After completing the collection process, the details and related timestamp are displayed in vRealize Business Standard.

Cost calculation involves the steps for computing base rates, allocated costs, cost for each virtual machine, classification of virtual machines under Consumers List in Consumption Analysis, and pre-generation of reports. Cost calculation occurs daily, but the process can also be run manually.

12.4.3 vRealize Automation

The vRealize Automation connector collects data about consumers of virtual machines (as blueprints), provisioning groups and tenants from the IaaS component of vRealize Automation, if IaaS is configured.

vRealize Automation connection information appears only after configuring the IaaS component of vRealize Automation.



12.4.4 Amazon Web Services

The public cloud connector connects to listed accounts in AWS to collect inventory and usage data. Public cloud connection information appears only after configuring an AWS account.

12.5 Updating vRealize Business Standard

The vRealize Business Standard administration interface includes a central page where updates to the product software can be installed and managed. vRealize Business Standard can be updated automatically or manually.

Software updates can be downloaded from <https://my.vmware.com/> using an entitled account. Always read the release notes for the update process specific to that release, and for any implications, prerequisites and management pack support before performing a software update.

Updates require vRealize Business Standard to be temporarily taken offline while the update is performed.



References

13.1 vRealize Business Standard

For more information, see *VMware vRealize Business Standard Documentation* (<https://www.vmware.com/support/pubs/vrealize-business-standard-pubs.html>). The information is arranged by topic and includes installation, administration, and user guide topics in the following documents:

- *vRealize Business Standard Release Notes*
- *vRealize Business Standard Installation and Administration Guide*
- *vRealize Business Standard User's Guide*

13.2 VMware Hardened Virtual Appliances

See the *Hardened Virtual Appliance Operations Guide* white paper regarding hardening VMware virtual appliances (referenced in the security section of this document) (<http://www.vmware.com/files/pdf/techpaper/VMWare-Hardened-Appliance-Operations-Guide.pdf>).

13.3 vSphere Fault Tolerance

Requirements and procedures for configuring vSphere Fault Tolerance can be found in the *VMware vSphere 6 Documentation* (<https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html>).