



VMware vRealize Automation

Reference Architecture
Version 6.0 or Later

TECHNICAL WHITE PAPER
MARCH 2016
VERSION 1.6





Table of Contents

Overview	4
What's New	4
Initial Deployment Recommendations	4
General Recommendations	4
vRealize Automation	5
Load Balancer Considerations	5
Database Deployment	5
Data Collection Configuration	5
Proxy Agents	5
Distributed Execution Manager Configuration	6
vRealize Orchestrator	6
vRealize Application Services	6
Authentication Setup	6
vRealize Business Standard Edition	6
Load Balancer Considerations	6
Scalability Considerations	7
vRealize Automation	7
Concurrent Provision Scalability	7
Data Collection Scalability	7
Performance Analysis and Tuning	7
Additional Data Collection Scalability Considerations	8
Workflow Processing Scalability	8
Performance Analysis and Tuning	8
vRealize Application Services	9
Adjust Memory Configuration	9
vRealize Business Standard Edition	9
High Availability Considerations	10
vRealize Automation	10
Identity Appliance	10
vCenter Single Sign-On	10
vRealize Automation Appliance	10
Infrastructure Web Server	10
Infrastructure Manager Server	10
Agents	10



Distributed Execution Manager Worker	10
Distributed Execution Manager Orchestrator	10
vRealize Automation Appliance Database Server	11
vRealize Orchestrator	11
vRealize Application Services	11
vRealize Business Standard Edition	11
vRealize Automation Machines.....	12
Deployment Profiles.....	15
Small Deployment	15
Support	15
Requirements	15
Certificates.....	15
Ports.....	16
Diagrams.....	18
Medium Deployment	20
Support	20
Requirements	20
Certificates.....	21
Ports.....	22
Diagrams.....	25
Large Deployment	27
Supports.....	27
Virtual Appliances	27
Windows Server Virtual Machines	27
Load Balancers	28
Certificates.....	28
Ports.....	29
Diagrams.....	32



Overview

This document provides recommendations about deployment topology, hardware specifications, interoperability, and scalability for the following VMware components:

- VMware vRealize Automation (formerly vCloud Automation Center)
- VMware vRealize Application Services (formerly vCloud Automation Center Application Services)
- VMware vRealize Business Standard

For software requirements, installations, and supported platforms, see the documentation for each product.

This document applies to vRealize Automation versions 6.0 and later, with the following exception for 6.2

- Virtual Machine Remote Console has been disabled in 6.2 and requires 6.2.1

The following additional exception applies to version 6.1:

- vRealize Automation Infrastructure servers do not require access to port 5480 on the vRealize Appliance.

The following additional exceptions apply to version 6.0:

- Port 443 of the Infrastructure Web Server must be exposed to the consumers of the product.
- Virtual appliances do not require inbound and outbound communication over port 5672.

What's New

This document includes the following updated content:

- Updated vRealize Automation appliance database server recommendations
- Additional port requirements for Virtual Machine Remote Console (VMRC)
- Additional load balancer recommendations
- Updated diagrams
- Update Proxy Agents section to clarify recommendations around geographical distribution of agents

Initial Deployment Recommendations

This section describes the initial deployment configuration for vRealize Automation, vRealize Application Services, and vRealize Business Standard Edition.

General Recommendations

Keep your VMware vRealize Business Standard Edition, VMware vCenter Server Single-Sign-On, VMware Identity Appliance, and vRealize Automation in the same time zone with their clocks synchronized. Otherwise, data synchronization might be delayed.

vRealize Automation, vRealize Business Standard, VMware vCenter Server Single-Sign-On, VMware Identity Appliance, and vRealize Orchestrator should be installed on the same management cluster. You should provision machines onto a cluster that is separate from the management cluster so that user workload and server workload can be isolated.

You can deploy the vRealize Automation DEM Worker and proxy agents over a WAN, but do not deploy other components of vRealize Automation, vRealize Application Services, or vRealize Business Standard Edition over a WAN because performance might be degraded.

You should use the Identity Appliance only in simple deployments. If High Availability is required, you must use



vCenter Single-Sign-On 5.5 U2 or later, where vCenter Single-Sign-On 5.5 U2c is recommended.

vRealize Automation

The general deployment configuration for vRealize Automation should be considered as a starting point for deployment. After initial testing and deployment to production, you should continue to monitor performance and allocate additional resources if necessary, as described in [Scalability Considerations](#).

Load Balancer Considerations

Use the Least Response Time or round-robin method to balance traffic to the vRealize Automation appliances and infrastructure Web servers. Enable session affinity or the sticky session feature to direct subsequent requests from each unique session to the same Web server in the load balancer pool.

You can use a load balancer to manage failover for the Manager Service, but do not use a load-balancing algorithm because only one Manager Service is active at a time. Do not use session affinity when managing failover with a load balancer.

Use only port 443, the default HTTPS port, when load balancing the vRealize Automation Appliance, Infrastructure Web server, and Infrastructure Manager server together.

Although you can use other load balancers, NSX, F5 BIG-IP hardware and F5 BIG-IP Virtual Edition have been tested and are recommended for use.

For more information on configuring an F5 BIG-IP Load Balancer for use with vRealize Automation: [Configuring VMware® vRealize Automation High Availability Using an F5 Load Balancer](#).

Database Deployment

For production deployments, you should deploy a dedicated database server to host the Microsoft SQL Server (MSSQL) databases. vRealize Automation requires machines that communicate with the database server to be configured to use Microsoft Distributed Transaction Coordinator (MSDTC). By default, MSDTC requires port 135 and ports 1024 through 65535. For more information about changing the default MSDTC ports, see [Configuring Microsoft Distributed Transaction Coordinator \(DTC\) to work through a firewall](#).

For the vRealize Automation appliance database you must use the database server internal to the appliance. For medium and large configurations the appliance database must be clustered. For more information about setting up appliance database replication, see [Configuring internal vPostgres Database Server for replication in VMware vRealize Automation virtual appliance \(KB 2108923\)](#).


NOTE: VMware no longer recommends vRealize Automation appliance database server configurations which use databases external from active vRealize Automation appliances. Examples of external databases include VMware vFabric Postgres, Open-source Postgres, and vRealize Automation appliances as database servers only. Customers who have deployed other configurations are still supported, but any new installation of vRealize Automation 6.x should follow recommendations in the knowledge base article linked above.

Data Collection Configuration

The default data collection settings provide a good starting point for most implementations. After deploying to production, continue to monitor the performance of data collection to determine whether you must make any adjustments.

Proxy Agents

For maximum performance, agents should be deployed in the same data center as the endpoint to which they are associated. Your deployment can have multiple agent servers that are distributed around the globe. You can install additional agents to increase throughput and concurrency.



When agents are installed in the same data center as their associated endpoint, you could see an increase of 200 percent, on average, in data collection performance. The time measured includes only the time spent transferring data between the Proxy Agent and the Manager Service. It does not include the time it takes for the Manager Service to process the data.

For example, you currently deploy the product to a Data Center in Palo Alto and you have vSphere endpoints in Palo Alto, Boston, and London. In this configuration, the vSphere Proxy Agents are deployed in Palo Alto, Boston, and London for their respective endpoints. If instead, you deploy all of the agents in Palo Alto, you could see a 200 percent increase in data collection time for Boston and London.

Distributed Execution Manager Configuration

In general, locate distributed execution managers (DEMs) as close as possible to the Model Manager host. The DEM Orchestrator must have strong network connectivity to the Model Manager at all times. You should have two DEM Orchestrator instances, one for failover, and two DEM Worker instances in your primary data center.

If a DEM Worker instance must execute a location-specific workflow, install the instance in that location.

You must assign skills to the relevant workflows and DEMs so that those workflows are always executed by DEMs in the correct location. For information about assigning skills to workflows and DEMs by using the vRealize Automation Designer console, see the vRealize Automation *Extensibility* documentation. Because this is advanced functionality, you must make sure you design your solution in a way that WAN communication is not required between the executing DEM and any remote services for example, vRealize Orchestrator.

For the best performance, DEMs and agents should be installed on separate machines. For additional guidance about installing vRealize Automation agents, see the vRealize Automation *Installation and Configuration* documentation.

vRealize Orchestrator

In general, use an external vCenter Orchestrator system for each tenant to enforce tenant isolation. All vRealize Orchestrator instances should use SSO Authentication. If SSO Authentication is chosen the vRO Admin – domain and group should be vsphere.local vroadmins.

vRealize Application Services

vRealize Application Services supports a single-instance setup.

To avoid security and performance problems in the vRealize Application Services server, do not add unsupported services or configure the server in any way other than as mentioned in this document and the product documentation. See the vRealize Application Services documentation in the vRealize Automation documentation center.

Do not use vRealize Application Services as the content server. A separate content server or servers with appropriate bandwidth and security features are required. vRealize Application Services hosts only the predefined sample content.

Locate the content server in the same network as the deployments to improve performance when a deployment requires downloading a large file from an external source. Multiple networks can share a content server when the traffic and the data transfer rate are light.

Authentication Setup

When setting up vRealize Application Services, you can use the vCenter Single Sign-On capability to manage users in one place.

vRealize Business Standard Edition

Load Balancer Considerations

For data collection connections, load balancing is not supported. For more information, see [Scalability Considerations](#). In the vRealize Business Standard Edition appliance for UI and API client connections, you can use the vRealize Automation load balancer.



Scalability Considerations

This section describes various performance characteristics of vRealize Automation, vRealize Application Services, and vRealize Business Standard Edition. It provides recommendations for your initial deployment based on anticipated usage and guidance for tuning performance based on actual usage over time.

vRealize Automation

Concurrent Provision Scalability

By default, vRealize Automation processes only two concurrent provisions per endpoint. For information about increasing this limit, see [Configuring Concurrent Machine Provisioning](#).

Data Collection Scalability

The time required for data collection to complete depends on the capacity of the compute resource, the number of machines on the compute resource or endpoint, the current system, and network load, among other variables. The performance scales at a different rate for different types of data collection.

Each type of data collection has a default interval that can be overridden or modified. Infrastructure administrators can manually initiate data collection for infrastructure source endpoints. Fabric administrators can manually initiate data collection for compute resources. The following values are the default intervals for data collection.


Data Collection Type	Default Interval
Inventory	Every 24 hours (daily)
State	Every 15 minutes
Performance	Every 24 hours (daily)

Performance Analysis and Tuning

As the number of resources to be data collected increases, the time required to complete data collection might become longer than the interval between data collections, particularly for state data collection. See the Data Collection page for a compute resource or endpoint to determine whether data collection is completing in time or is being queued. The Last Completed field value might always be “In queue” or “In progress” instead of a timestamp when data collection last completed. If so, you might need to decrease the data collection frequency, that is, increase the interval between data collections.

Alternatively, you can increase the concurrent data collection limit per agent. By default, vRealize Automation limits concurrent data collection activities to two per agent and queues requests that are over this limit. This limitation allows data collection activities to complete quickly and not affect overall performance. You can raise the limit to take advantage of concurrent data collection, but weigh this option against any degradation in overall performance.

If you do increase the configured vRealize Automation per-agent limit, you might want to increase one or more of these execution timeout intervals. For more information about configuring data collection concurrency and timeout intervals, see the vRealize Automation *System Administration* documentation. Data collection is CPU-intensive for the Manager Service. Increasing the processing power of the Manager Service host can decrease the time required for data collection overall.



Data collection for Amazon Elastic Compute Cloud (Amazon EC2) in particular can be CPU intensive, especially if running data collection on multiple regions concurrently and if those regions have not had data collection run on them before. This type of data collection can cause an overall degradation in Web site performance. Decrease the frequency of Amazon EC2 inventory data collection if it is having a noticeable effect on performance.

Additional Data Collection Scalability Considerations

If you expect to use a VMware vSphere cluster that contains a large amount of objects, for example, 3000 or more virtual machines, modify the default value of the ProxyAgentServiceBinding and maxStringContentLength in the **ManagerService.exe.config** file. If this setting is not modified, large inventory data collections might fail.

To modify the default value of the ProxyAgentServiceBinding and maxStringContentLength in the ManagerService.exe.config file:

1. Open the **ManagerService.exe.config** file, typically in C:\Program Files (x86)\VMware\VCAC\Server.
2. Edit the configuration file.
3. Locate the following two lines.

```
<binding name='ProxyAgentServiceBinding'  
maxReceivedMessageSize='13107200'>  
    <readerQuotas maxStringContentLength='13107200' />
```

NOTE: Do not confuse these two lines with the lines that are very similar, but with binding name = "ProvisionServiceBinding".
4. Replace the number values assigned to the maxReceivedMessageSize and maxStringContentLength attributes with a larger value. How much larger depends on how many more objects you expect your VMware vSphere cluster to have in the future. For example, you can increase these numbers by a factor of 10 for testing.
5. Restart the vRealize Automation Manager Service.

Workflow Processing Scalability

The average workflow processing time, from when the DEM Orchestrator starts preprocessing the workflow to when the workflow finishes executing, increases with the number of concurrent workflows. Workflow volume is a function of the amount of vRealize Automation activity, including machine requests and some data collection activities.

Performance Analysis and Tuning

You can use the Distributed Execution Status page to view the total number of workflows that are in progress or pending at any time, and you can use the Workflow History page to determine how long it takes to execute a given workflow.

If you have a large number of pending workflows, or if workflows are taking longer to complete, you should add more DEM Worker instances to pick up the workflows. Each DEM Worker instance can process 15 concurrent workflows. Excess workflows are queued for execution.

Additionally, you can adjust workflow schedules to minimize the number of workflows scheduled to be kicked off at the same time. For example, rather than scheduling all hourly workflows to execute at the top of the hour, you can stagger their execution time so that they do not compete for DEM resources at the same time. For more information about workflows, see the vRealize Automation *Extensibility* documentation.

Some workflows, particularly certain custom workflows, can be very CPU intensive. If the CPU load on the DEM Worker machines is high, consider increasing the processing power of the DEM machine or add more DEM machines to your environment.



vRealize Application Services

vRealize Application Services can scale to over 10,000 managed virtual machines and over 2,000 library items. You can run over 40 concurrent deployments and support over 100 concurrent users.

The performance does not take into account the cloud provider's capacity or other external deployment tools that vRealize Application Services depend on. An application needs a cloud provider to provision a VM and other resources. Overloading a cloud provider might not allow vRealize Application Services to meet the minimum load expectations. Refer to the product documentation for your cloud infrastructure product or external tool for information about how the system can handle a certain load.

Adjust Memory Configuration

You can adjust the available vRealize Application Services server memory by configuring the max heap size.

1. Navigate to the `/home/9arwin/tcserver/bin/setenv.sh` file.
2. Open the file and locate `JVM_OPTS` and change the `Xmx` value.

For example, to increase the max heap size to 3 GB, change the `Xmx` value to `3072m` in the code sample.

```
JVM_OPTS="-Xms256m -Xmx3072m -XX:MaxPermSize=256m"
```

3. Restart the vRealize Application Services server.

```
VMware-darwin-tcserver restart
```

You can also specify a larger initial heap size by changing the `-Xms` value to reserve larger memory. If the load is uncertain, you can reserve a smaller initial memory footprint to conserve the memory for other processes running on the server. If the load is consistent, then you can have an initial large reserve for efficiency.

You can configure heap size values to find the best one for your load. The max heap size of an application server should be at least half of the total memory. The rest of the memory should be left for the Postgres, RabbitMQ, and other system processes.

You do not need to change the `-XX:MaxPermSize` value unless you are trying to troubleshoot a permgen error.

vRealize Business Standard Edition

vRealize Business Standard Edition can scale up to 20,000 virtual machines across four VMware vCenter Server instances. The first synchronization of the inventory data collection takes approximately three hours to synchronize 20,000 virtual machines across three VMware vCenter Server instances. Synchronization of statistics from VMware vCenter Server takes approximately one hour for 20,000 virtual machines. By default, the cost calculation job runs every day and takes approximately two hours for each run for 20,000 virtual machines.

NOTE: In version 1.0, the default configuration of the vRealize Business Standard Edition appliance can support up to 20,000 virtual machines. Increasing the limits of the appliance beyond its default configuration does not increase the number of virtual machines that it can support.



High Availability Considerations

vRealize Automation

Identity Appliance

High availability (HA) and failover protection for the vRealize Automation Identity Appliance are handled outside of vRealize Automation. Use a cluster enabled with VMware vSphere HA to protect the appliance.

vCenter Single Sign-On

You can configure vCenter Single Sign-On in an active-passive mode. To enable failover, you must disable the active node in the load balancer, and enable the passive node. Session information is not persisted across SSO nodes, so some users might see a brief service interruption. For more information about how to configure vCenter Single Sign-On for active-passive mode, see the *Configuring VMware vCenter SSO High Availability for vRealize Automation* technical white paper.

vRealize Automation Appliance

The vRealize Automation Appliance supports active-active high availability. To enable high availability for these appliances, place them under a load balancer. For more information, see the vRealize Automation *Installation and Configuration* documentation.

Infrastructure Web Server

The Infrastructure Web server components all support active-active high availability. To enable high availability for these components, place them under a load balancer.

Infrastructure Manager Server

The Manager Server component supports active-passive high availability. To enable high availability for this component, place two Manager Servers under a load balancer. As two Manager Servers cannot be active at the same time, disable the passive Manager Server in the cluster and stop the Windows service.

If the active Manager Server fails, stop the Windows service (if not already stopped) under the load balancer. Enable the passive Manager Server and restart the Windows service under the load balancer. See the vRealize Automation *Installation and Configuration* documentation for more information.

Agents

Agents support active-active high availability. See the vRealize Automation *System Administration* documentation for information about configuring agents for high availability. You should also check the target service for high availability.

Distributed Execution Manager Worker

DEMs running under the Worker role support active-active high availability. If a DEM Worker instance fails, the DEM Orchestrator detects the failure and cancels any workflows being executed by the DEM Worker instance. When the DEM Worker instance comes back online, it detects that the DEM Orchestrator has canceled the workflows of the instance and stops executing them. To prevent workflows from being canceled prematurely, a DEM Worker instance must be offline for several minutes before its workflows can be canceled.

Distributed Execution Manager Orchestrator

DEMs running under the Orchestrator role support active-active high availability. When a DEM Orchestrator starts, it searches for another running DEM Orchestrator. If none is found, it starts executing as the primary DEM Orchestrator. If it does find another running DEM Orchestrator, it monitors the other primary DEM Orchestrator to detect an outage. If it detects an outage, it takes over as the primary. When the previous primary comes online again, it detects that another DEM Orchestrator has taken over its role as primary and monitors for failure of the primary Orchestrator.



vRealize Automation Appliance Database Server

For the vRealize Automation appliance database you must use the database server internal to the appliance. For medium and large configurations the appliance database must be clustered. This is an active-passive configuration which requires manual failover steps to be executed in order to switch the primary (master) node. For more information about setting up and maintaining appliance database replication, see [Configuring internal vPostgres Database Server for replication in VMware vRealize Automation virtual appliance \(KB 2108923\)](#).

NOTE: VMware no longer recommends vRealize Automation appliance database server configurations which use databases external from active vRealize Automation appliances. For example: VMware vFabric Postgres, Open-source Postgres and vRealize Automation appliances as database servers only. Customers who have deployed other configurations are still supported, but any new installation of vRealize Automation 6.x should follow recommendations in the above mentioned knowledge base article.

You should use a SQL Server Failover Cluster Instance. vRealize Automation does not support AlwaysOn Availability Groups due to use of Microsoft Distributed Transactions Coordinator.

vRealize Orchestrator

vRealize Orchestrator can be configured in an active-active mode behind a load balancer. See the vCenter Orchestrator documentation for more information.

vRealize Application Services

vRealize Application Services 6.1 does not support load balancing for multiple instances.

To reduce the downtime and provide quick recovery from disaster, you can implement some or all of the following strategies.

Select the appropriate resources for the vRealize Application Services load. Do not overload the system. See [vRealize Automation Machines](#) for the recommended load.

- Divide the application deployments to use multiple vRealize Application Services instances. If applications or components are shared, you can use the import and export feature to synchronize the data among instances.
- Take snapshots of the vRealize Application Services Appliance when there is a major change applied to the environment. The snapshot minimizes the downtime and you can recover data if the system fails.
- Use the vSphere HA feature, which restarts a failed VM. See the VMware vSphere product documentation for instructions on how to set up high availability.

vRealize Business Standard Edition

Use the VMware vSphere HA feature for the vRealize Business Standard Edition appliance. To configure the VMware vSphere HA feature on the VMware ESXi host, see the vCenter Server and Host Management documentation.

vRealize Automation Machines

The following table indicates which components to install on each server profile in your deployment, and includes their required and recommended hardware specifications.

Server Role	Description	Components	Required Hardware Specifications	Recommended Hardware Specifications
Identity Appliance	Virtual appliance that provides Single Sign-On (SSO) capabilities for the vRealize Automation environment		CPU: 1 vCPU RAM: 2 GB Disk: 10 GB Network: 1 GB/s	Same as required hardware specifications
vCenter Single Sign-On	vCenter Single Sign-On 5.5 U2 or later		CPU: 2vCPU RAM: 3 GB Disk: 2 GB Network: 1 GB/s	Same as required hardware specifications
vRealize Automation Appliance	Virtual appliance that deploys the vRealize Automation server	vRealize Automation Appliance Services vRealize Automation Appliance Database Server vFabric RabbitMQ	CPU: 2 vCPU RAM: 8 GB Disk: 30 GB Network: 1 GB/s	CPU: 4 vCPU RAM: 16 GB Disk: 30 GB Network: 1 GB/s
Infrastructure Web Server		Web site	CPU: 2 vCPU RAM: 2 GB Disk: 40 GB Network: 1 GB/s	CPU: 2 vCPU RAM: 4 GB Disk: 40 GB Network: 1 GB/s
Infrastructure Manager Server		Manager Service DEM Orchestrator	CPU: 2 vCPU RAM: 2 GB Disk: 40 GB Network: 1 GB/s	CPU: 2 vCPU RAM: 4 GB Disk: 40 GB Network: 1 GB/s
Infrastructure Web/Manager Server		Infrastructure Web/Manager Server	CPU: 2 vCPU RAM: 4 GB Disk: 40 GB Network: 1 GB/s	CPU: 2 vCPU RAM: 8 GB Disk: 40 GB Network: 1 GB/s
Infrastructure DEM Server		(One or more) DEM Workers	CPU: 2 vCPU RAM: 2 GB Disk: 40 GB Network: 1 GB/s Per DEM Worker	CPU: 2 vCPU RAM: 6 GB Disk: 40 GB Network: 1 GB/s Per DEM Worker
Infrastructure Agent Server		(One or more) Proxy Agent	CPU: 2 vCPU RAM: 4 GB Disk: 40 GB	Same as required hardware specifications



Server Role	Description	Components	Required Hardware Specifications	Recommended Hardware Specifications
			Network: 1 GB/s	
MSSQL Database Server		Infrastructure Database	CPU: 2 vCPU RAM: 8 GB Disk: 40 GB Network: 1 GB/s	CPU: 8 vCPU RAM: 16 GB Disk: 80 GB Network: 1 GB/s
vRealize Orchestrator Appliance			CPU: 2vCPU RAM: 3 GB Disk 12 GB Network: 1 GB/s	Same as required hardware specifications
vRealize Application Services Appliance	Small deployment (see Small Deployment)	vRealize Appliance Service services vRealize Application Services Appliance Database Server vFabric RabbitMQ VMware SLES	CPU: 2 vCPU RAM: 4 GB Disk: 16 GB Network: 1 GB/s	Same as required hardware specifications
	Medium deployment (see Medium Deployment)	vRealize Appliance Service services vRealize Application Services Appliance Database Server vFabric RabbitMQ VMware SLES	CPU: 4 vCPU RAM: 8 GB Disk: 30 GB Network: 1 GB/s	Same as required hardware specifications
	Large deployment (see Large Deployment)	vRealize Appliance Service services vRealize Application Services Appliance Database Server vFabric RabbitMQ VMware SLES	CPU: 8 vCPU RAM: 16 GB Disk: 50 GB Network: 1 GB/s	Same as required hardware specifications
vRealize Business Standard Appliance		vRealize Business Standard Appliance services vRealize Business Database Server VMware SLES	CPU: 2 vCPU RAM: 4 GB Disk: 50 GB Network: 1 GB/s	CPU: 2 vCPU RAM: 4 GB Disk: 50 GB Network: 1 GB/s





Deployment Profiles

Small Deployment

Support

- 10,000 managed machines
- 500 catalog items
- 10 concurrent deployments
- 10 concurrent application deployments
 - Each deployment has approximately 3 to 14 VM nodes

Requirements

- Identity Appliance (small-sso.ra.local)
- vRealize Automation Appliance (small-vrva.ra.local)
- Infrastructure core server (small-Infrastructure.ra.local)
 - Configure this server with a minimum of two processors and 8 GB of memory. A smaller configuration can lead to out-of-memory exceptions and timeouts.
- MSSQL Database Server (small-mssql.ra.local)
- vRealize Application Services Appliance: small-appd.ra.local
- vRealize Business Standard Edition appliance (small-itbm.ra.local)

Certificates

The host names that are used in this table are examples only.

Server Role	CN/SAN
vRealize Automation Identity Appliance	CN = small-sso.ra.local
vRealize Automation Appliance (VA)	CN = small-vrva.ra.local
Infrastructure Core Server	CN = small-Infrastructure.ra.local
MSSQL Database Server	NA
vRealize Application Services Server	CN = small-appd-.ra.local
vRealize Business Standard Edition Server	CN = small-itbm.ra.local

Ports

All ports listed are default ports.

Users require access to the following ports.


Server Role	Port
vRealize Automation Identity Appliance	7444
vRealize Automation Appliance	443, *8444
vRealize Application Services Server	8443

*8444 is required for the Virtual Machine Remote Console.

Administrators require access to the following ports, in addition to those ports required by users.

Server Role	Port
vRealize Automation Identity Appliance	5480
vRealize Application Services Server	5480
vRealize Business Standard Server	5480

Server Role	Inbound Ports	Service/System: Outbound Ports
vRealize Automation Identity Appliance	7444 SSH: 22 VAMI: 5480	LDAP: 389 LDAPS: 636
vRealize Automation Appliance	443, 8444 SSH: 22 VAMI: 5480	Identity VA: 7444 VMware ESXi: 902
Infrastructure Core Server	135, 443, 1024-65535*	Identity VA: 7444, vRealize Automation VA: 443, 5480 vSphere Endpoint: 443** MSSQL: 135, 1433, 1024-65535*
MSSQL Database Server	135,1433, 1024-65535*	Infrastructure Core: 135, 1024-65535*
	Do not change or blocked these ports:	
vRealize Application Services Server	8443 HTTPS User Interface connection 8080 HTTP (legacy port; do not use)	Identity VA: 7444 vRealize Automation VA: 443 Infrastructure Core: 443
vFabric, RabbitMQ	5671 AMQP over SSL	
External SSH connection	22	
Content Server	80 HTTP (used to host as is content, agent binary, and CLI binary)	
vRealize Business Standard Edition Server		Identity VA: 7444



Server Role	Inbound Ports	Service/System: Outbound Ports
		vRealize Automation VA: 443 Infrastructure Core: 443
vRealize Business Standard Edition UI connection	443 HTTPS	
External SSH connection	22	
Web console access (VAMI)	5480	

*For information about how to narrow this range, see [Database Deployment](#).

** Infrastructure Core requires access to vSphere Endpoint Port 443 to obtain a ticket for Virtual Machine Remote Console. vRealize Appliance requires access to ESXi host Port 902 to proxy traffic to the consumer.

Diagrams

NOT SHOWN

All Infrastructure systems require access to Port 5480 of all vRealize Appliances for Log Collection (vRA Settings > Cluster > Collect Logs on Virtual Appliance:5480) to function.

For Virtual Machine Remote Console vRealize Appliance requires access to VMware ESXi Port 902, and Infrastructure Core Server requires access to vSphere Endpoint Port 443.

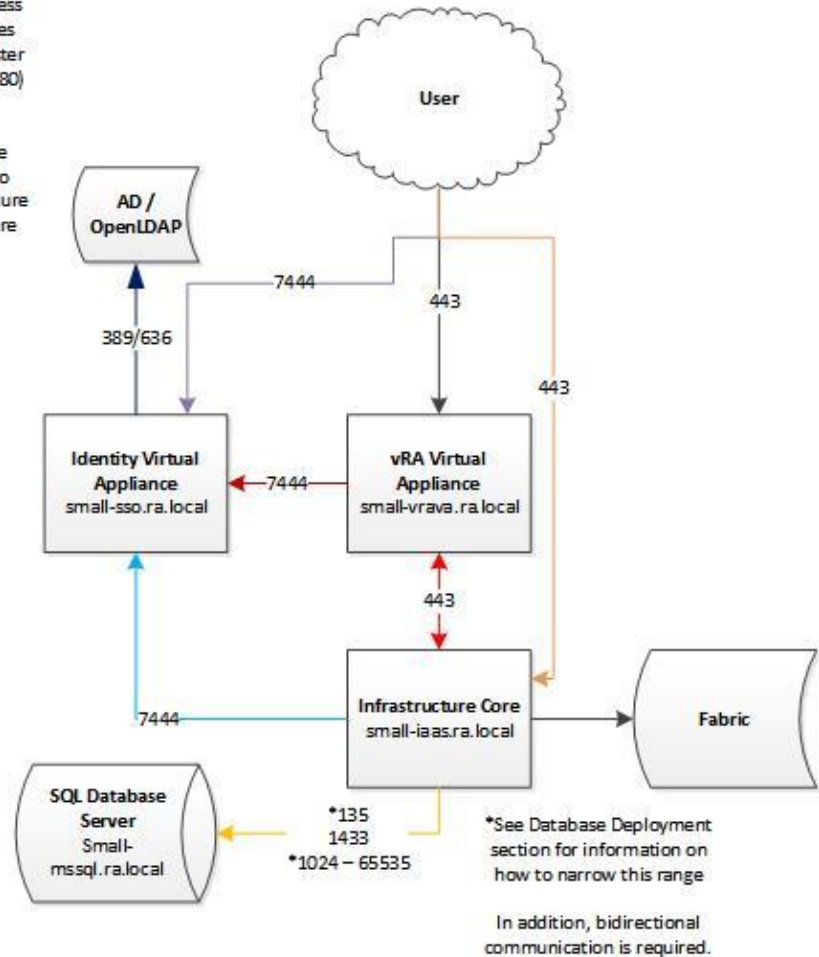


Figure 1. Minimum Footprint for Small Configuration (vRealize Automation)

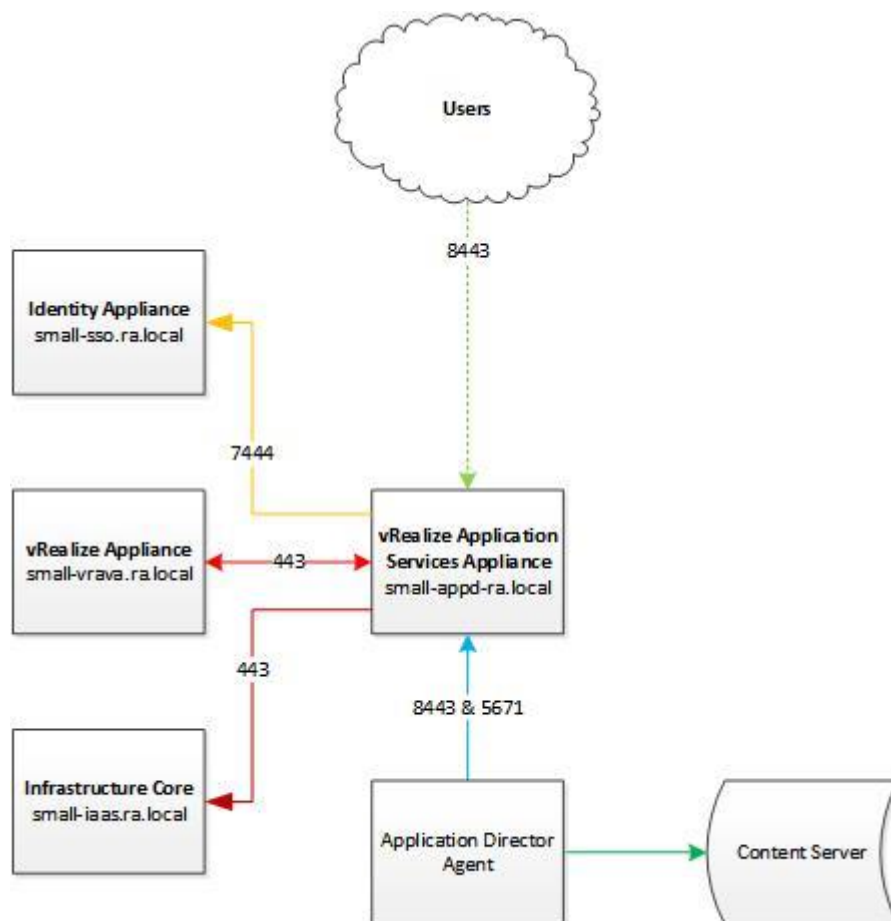


Figure 2. Minimum Footprint for Small Configuration (vRealize Application Services)

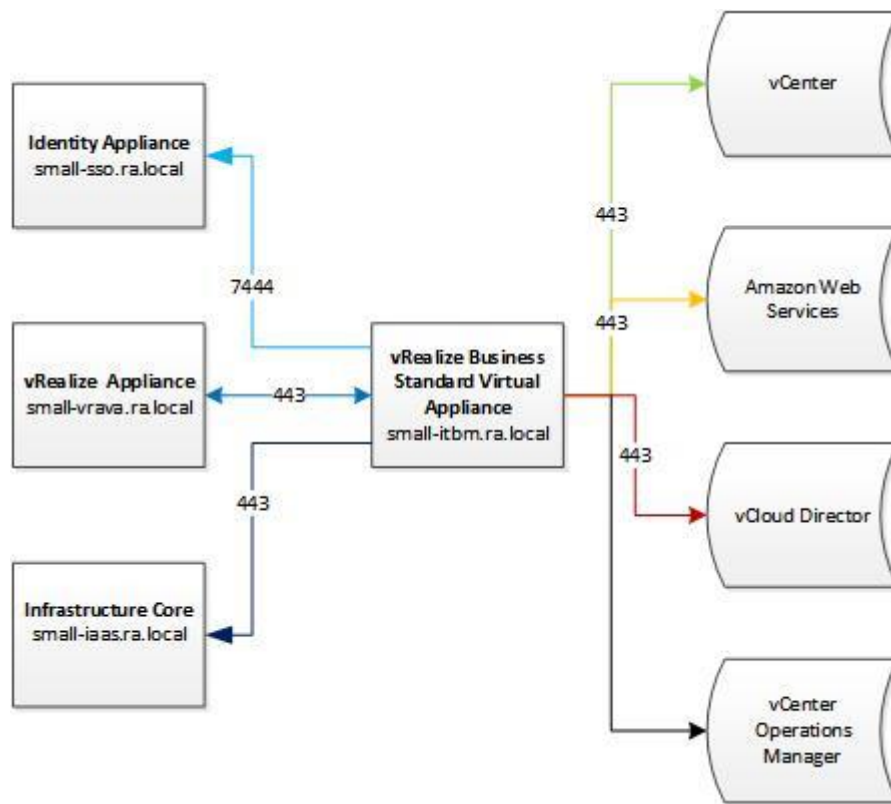


Figure 3. Minimum Footprint for Small Configuration (vRealize Business Standard Edition)

Medium Deployment

Support

- 30,000 managed machines
- 1,000 catalog items
- 50 concurrent deployments
- Up to 20 concurrent deployments
 - Each deployment has approximately 3 to 14 VM nodes

Requirements

Virtual Appliances

- vRealize Automation Appliance 1: med-vrava-1.ra.local
- vRealize Automation Appliance 2: med-vrava-2.ra.local
- vRealize Orchestrator Appliance 1: med-vro-1.ra.local
- vRealize Orchestrator Appliance 2: med-vro-2.ra.local
- vRealize Business Standard Edition appliance: med-itbm.ra.local
- vRealize Application Services appliance: med-appd.ra.local

Windows Server Virtual Machines

- vCenter Single Sign-On Server 1: med-sso-1.ra.local
- vCenter Single Sign-On Server 2: med-sso-2.ra.local

- Infrastructure Web/Manager Server 1 (Active Web/DEM-O, Active Manager): med-webman-1.ra.local
- Infrastructure Web/Manager Server 2 (Active Web/DEM-O, Passive Manager): med-webman-2.ra.local
- Infrastructure DEM Server 1: med-dem-1.ra.local
- Infrastructure DEM Server 2: med-dem-2.ra.local
- Infrastructure Agent Server 1: med-agent-1.ra.local
- Infrastructure Agent Server 2: med-agent-2.ra.local
- Clustered MSSQL Database: med-mssql.ra.local

Load Balancers

- vCenter Single Sign-On Load Balancer: med-sso.ra.local
- vRealize Automation Appliance Load Balancer: med-vrava.ra.local
- vRealize Automation Appliance Database Server Load Balancer: med-app-db.ra.local
- vRealize Orchestrator Load Balancer: med-vrova.ra.local
- Infrastructure Web Load Balancer: med-web.ra.local
- Infrastructure Manager Server Load Balancer: med-manager.ra.local

Certificates

The host names that are used in this table are examples only.

Server Role	CN/SAN
vCenter Single Sign-On Server	SAN contains: med-sso.ra.local med-sso-1.ra.local med-sso-2.ra.local
vRealize Automation Appliance	SAN contains: med-vrava.ra.local med-vrava-1.ra.local med-vrava-2.ra.local
Infrastructure Web/Manager Server	SAN contains: med-web.ra.local med-manager.ra.local med-webman-1.ra.local med-webman-2.ra.local
Infrastructure DEM Server	NA
Infrastructure Agent Server	NA
MSSQL Database Server	NA
vRealize Orchestrator Appliance	CN = med-vro.ra.local
vRealize Application Services Server	CN = med-appd.ra.local
IT Business Management Standard Suite Edition Server	CN = med-itbm.ra.local

Ports

All ports listed are default ports. Users require access to the following ports.

Server Role	Port
vCenter Single Sign-On Load Balancer	7444
vRealize Automation Appliance Load Balancer	443, *8444
vRealize Application Services Server	8443


*8444 is required for Virtual Machine Remote Console.

Administrators require access to the following ports, in addition to those ports required by users.

Server Role	Port
vRealize Automation Appliance VAMI	5480
vRealize Orchestrator Appliance	8281, 8283
vRealize Automation vRealize Application Services Server	5480
vRealize Business Standard Edition Server	5480

The following table shows inter-application communications.


Server Role	Inbound Ports	Service/System: Outbound Ports
vCenter Single Sign-On Server	7444	LDAP: 389 LDAPS: 636 vCenter Single Sign-On: 11711, 11712, 12721
vRealize Automation Appliance	443, 8444, 5432, 5672	vCenter Single Sign-On Load Balancer: 7444 vRealize Automation Appliance (All other): 5432, 5672 vRealize Automation Infrastructure Web Load Balancer: 443 vRealize Automation Appliance Database Server Load Balancer: 5432 vRealize Orchestrator Load Balancer: 8281 ***VMware ESXi: 902
Infrastructure Web/Manager Server	135, 443, 1024-65535*	vCenter Single Sign-On: 7444 vRealize Automation Infrastructure Web Load Balancer: 443 **vRealize Automation Appliance (VA): 5480 ***vSphere Endpoint: 443 MSSQL: 135, 1433, 1024-65535*



Server Role	Inbound Ports	Service/System: Outbound Ports
Infrastructure DEM Server	NA	vCenter Single Sign-On: 7444 vRealize Automation Appliance Load Balancer: 443 vRealize Automation Infrastructure Web Load Balancer: 443 vRealize Automation Infrastructure Manager Load Balancer: 443 **vRealize Automation Appliance (VA): 5480
Infrastructure Agent Server	NA	vRealize Automation Infrastructure Web Load Balancer: 443 vRealize Automation Infrastructure Manager Load Balancer: 443 **vRealize Automation Appliance (VA): 5480
vPostgres	5432	NA
MSSQL Database Server	135, 1433, 1024-65535*	Infrastructure Web/Manager Server: 135, *1024-65535
vRealize Orchestrator Appliance	8281	vCenter Single Sign-On Load Balancer: 7444 MSSQL: 1433
	Do not change or block these ports:	
vRealize Application Services Server	8443 HTTPS User Interface connection 8080 HTTP (legacy port; do not use)	vCenter Single Sign-On: 7444 vRealize Automation Appliance Load Balancer: 443 vRealize Automation Infrastructure Web Load Balancer: 443
vFabric RabbitMQ	5671 AMQP over SSL	
External SSH connection	22	22
Content Server	80 HTTP (used to host OOB content, agent binary, and CLI binary)	
vRealize Business Standard Edition Server		vCenter Single Sign-On: 7444 vRealize Automation Appliance Load Balancer: 443 vRealize Automation Infrastructure Web Load Balancer: 443
vRealize Business Standard Edition UI connection	443 HTTPS	
External SSH connection	22	
Web console access (VAMI)	5480	

*For information about how to narrow this range, see [Database Deployment](#).

**This port is required only for Log Collection functionality (vRealize Automation Settings > Cluster > Collect Logs on Virtual Appliance:5480).



*** Infrastructure Web/Manager requires access to vSphere Endpoint Port 443 in order to obtain a ticket for Virtual Machine Remote Console. vRealize Appliance requires access to ESXi host Port 902 in order to proxy console data to the user.

Load Balancer	Ports Balanced
vCenter Single Sign-On Load Balancer	7444
vRealize Automation Appliance Load Balancer	443, 8444
vRealize Automation Appliance Database Server Load Balancer	5432
vRealize Automation Infrastructure Web Load Balancer	443
vRealize Automation Infrastructure Manager Server Load Balancer	443
vRealize Orchestrator Load Balancer	8281

Diagrams

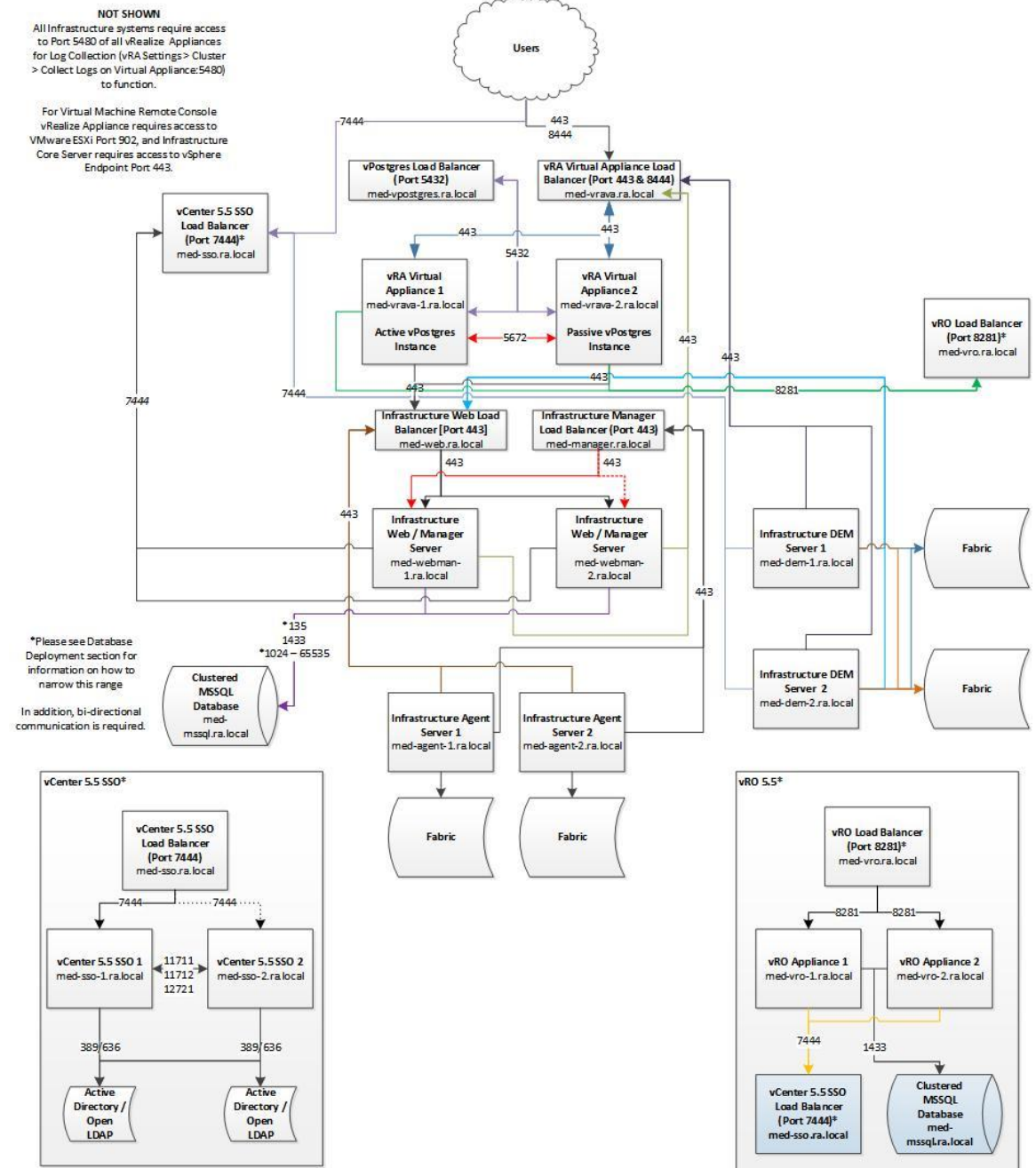


Figure 4. Minimum Footprint for Medium Configuration (vRealize Automation)

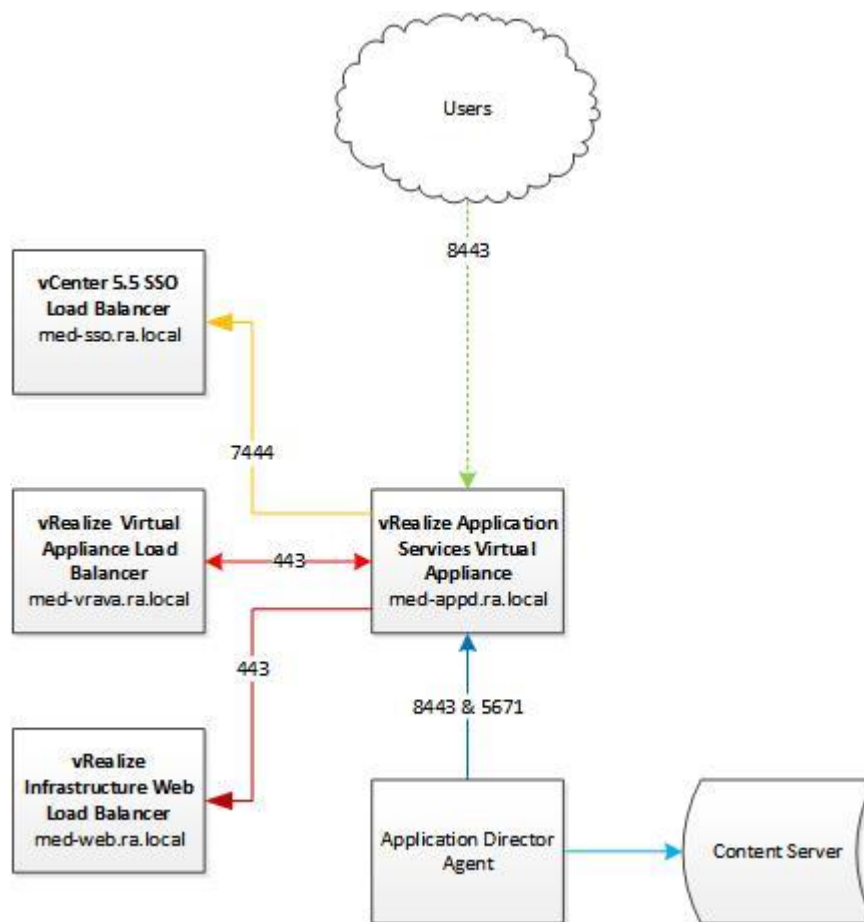


Figure 5. Minimum Footprint for Medium Configuration (vRealize Application Services)

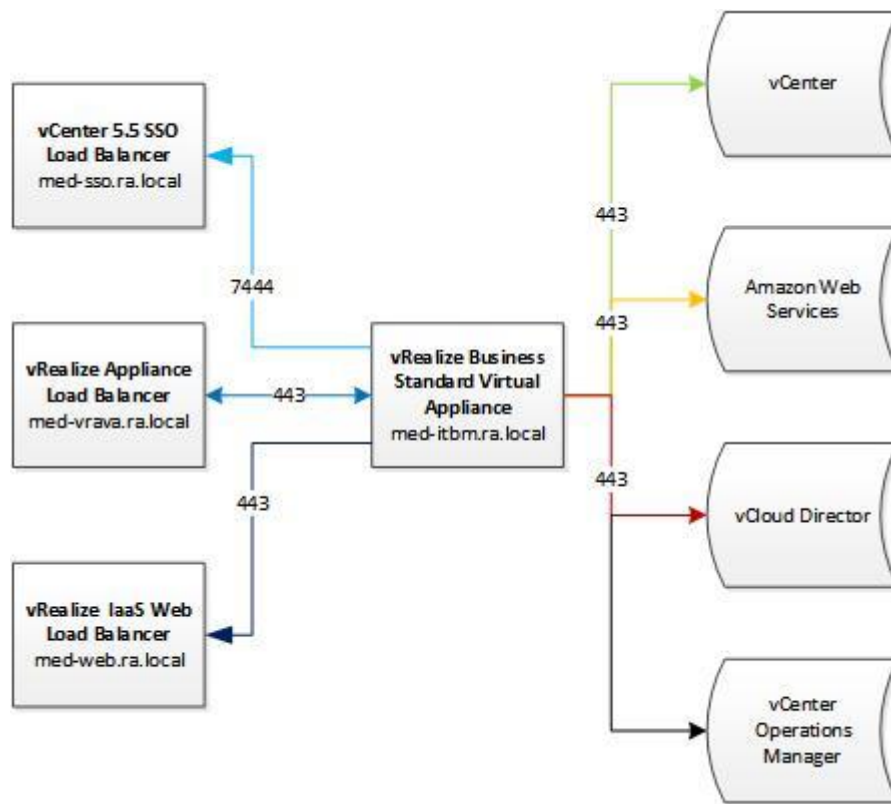


Figure 6. Minimum Footprint for Medium Configuration (vRealize Business Standard Edition)

Large Deployment

Supports

- 50,000 managed machines
- 2,500 catalog items
- 100 concurrent deployments
- Up to 40 concurrent application deployments
 - Each deployment has approximately 3 to 14 VM nodes

Virtual Appliances

- vRealize Automation Appliance 1: lg-vrava-1.ra.local
- vRealize Automation Appliance 2: lg-vrava-2.ra.local
- vRealize Orchestrator appliance 1: lg-vro-1.ra.local
- vRealize Orchestrator appliance 2: lg-vro-2.ra.local
- vRealize Business Standard Edition appliance: lg-itbm.ra.local
- vRealize Application Services Appliance: lg-appd.ra.local

Windows Server Virtual Machines

- vCenter Single Sign-On Server 1: lg-sso-1.ra.local
- vCenter Single Sign-On Server 2: lg-sso-2.ra.local
- Infrastructure Web Server 1: lg-web-1.ra.local

- Infrastructure Web Server 2: lg-web-2.ra.local
- Infrastructure Manager Server 1: lg-manager-1.ra.local
- Infrastructure Manager Server 2: lg-manager-2.ra.local
- Infrastructure DEM Server 1: lg-dem-1.ra.local
- Infrastructure DEM Server 2: lg-dem-2.ra.local
- Infrastructure Agent Server 1: lg-agent-1.ra.local
- Infrastructure Agent Server 2: lg-agent-2.ra.local
- Clustered MSSQL Database Server: lg-mssql.ra.local

Load Balancers

- vCenter Single Sign-On Server Load Balancer: lg-sso.ra.local
- vRealize Automation Appliance Load Balancer: lg-vrava.ra.local
- vRealize Automation Appliance Database Server Load Balancer: lg-app-db.ra.local
- vRealize Orchestrator Load Balancer: lg-vrova.ra.local
- Infrastructure Web Load Balancer: lg-web.ra.local
- Infrastructure Manager Server Load Balancer: lg-manager.ra.local

Certificates

The host names that are used in this table are examples only.

Server Role	CN/SAN
vCenter Single Sign-On Server	SAN contains lg-sso.ra.local lg-sso-1.ra.local lg-sso-2.ra.local
vRealize Automation Appliance	SAN contains lg-vrava.ra.local lg-vrava-1.ra.local lg-vrava-2.ra.local
Infrastructure Web Server	SAN contains lg-web.ra.local lg-manager.ra.local lg-web-1.ra.local lg-web-2.ra.local
Infrastructure DEM Server	NA
Infrastructure Agent Server	NA
MSSQL Database Server	NA
vRealize Orchestrator Appliance	CN = lg-vro.ra.local
vRealize Application Services Appliance	CN = lg-appd.ra.local
vRealize Business Standard Edition appliance	CN = lg-itbm.ra.local



Ports

All ports listed are default ports. Users require access to the following ports.


Server Role	Port
vCenter Single Sign-On Load Balancer	7444
vRealize Automation Appliance Load Balancer	443, *8444
vRealize Application Services Appliance	8443

*Port 8444 is required for Virtual Machine Remote Console.

Administrators require access to the following ports, in addition to those ports required by users.

Server Role	Port
vRealize Automation Appliance	5480
vRealize Application Services Appliance	5480
vRealize Business Standard Edition Appliance	5480

Server Role	Inbound Ports	Service/System: Outbound Ports
vRealize Automation		
vCenter Single Sign-On Server	7444	LDAP: 389 LDAPS: 636 vCenter Single Sign-On: 11711, 11712, 12721
vRealize Automation Appliance	443, 8444, 5432, 5672	vCenter Single Sign-On Load Balancer: 7444 vRealize Automation Appliance : 5432, 5672+ vRealize Automation Infrastructure Web Load Balancer: 443 vRealize Orchestrator Load Balancer: 8281 ***VMware ESXi: 902
Infrastructure Web Server	135, 443, 1024-65535*	vCenter Single Sign-On Load Balancer: 7444 vRealize Automation Appliance Load Balancer: 443 **vRealize Automation Appliance (VA): 5480 ***vSphere Endpoint: 443 MSSQL: 135, 1433, 1024-65535*
Infrastructure Manager Server	135, 443, 1024-65535*	vRealize Automation Infrastructure Web Load Balancer: 443 vRealize Automation Appliance (VA): 5480 MSSQL: 135, 1433, 1024-65535*
Infrastructure DEM Server	NA	vCenter Single Sign-On Load Balancer: 7444 vRealize Automation Appliance Load Balancer: 443



Server Role	Inbound Ports	Service/System: Outbound Ports
		vRealize Automation Infrastructure Web Load Balancer: 443 vRealize Automation Infrastructure Manager Load Balancer: 443 **vRealize Automation Appliance (VA): 5480
Infrastructure Agent Server	NA	vRealize Automation Infrastructure Web Load Balancer: 443 vRealize Automation Infrastructure Manager Load Balancer: 443 **vRealize Automation Appliance (VA): 5480
MSSQL Database Server	135, 1433, 1024-65535*	Infrastructure Web Server: 135,1024-65535* Infrastructure Manager Server: 135, 1024-65535*
	Do not change or block these ports:	
vRealize Application Services Appliance	8443 HTTPS User Interface connection 8080 HTTP (legacy port; do not use)	vCenter Single Sign-ON: 7444 vRealize Automation Appliance Load Balancer: 443 vRealize Automation Infrastructure Web Load Balancer: 443
vFabric RabbitMQ	5671 AMQP over SSL	
External SSH connection	22	
Content Server	80 HTTP (used to host OOB content, agent binary, and CLI binary)	
vRealize Business Standard Edition Appliance		vCenter Single Sign-On: 7444 vRealize Automation Appliance Load Balancer: 443 vRealize Automation Infrastructure Web Load Balancer: 443
vRealize Business Standard Edition UI connection	443 HTTPS	
External SSH connection	22	
Web console access (VAMI)	5480	



Load Balancer	Ports Balanced
vCenter Single Sign-On Load Balancer	7444
vRealize Automation Appliance Load Balancer	443, 8444
vRealize Automation Appliance Database Server Load Balancer	5432
vRealize Automation Infrastructure Web Load Balancer	443
vRealize Automation Infrastructure Manager Server Load Balancer	443
vRealize Orchestrator Load Balancer	8281

* For information about how to narrow this range, see [Database Deployment](#).

**This port is required only for Log Collection functionality (vRealize Settings > Cluster > Collect Logs on Virtual Appliance:5480).

***Infrastructure Web requires access to vSphere Endpoint Port 443 to obtain a ticket for Virtual Machine Remote Console. vRealize Appliance requires access to ESXi host Port 902 to proxy console data to the user.

Diagrams

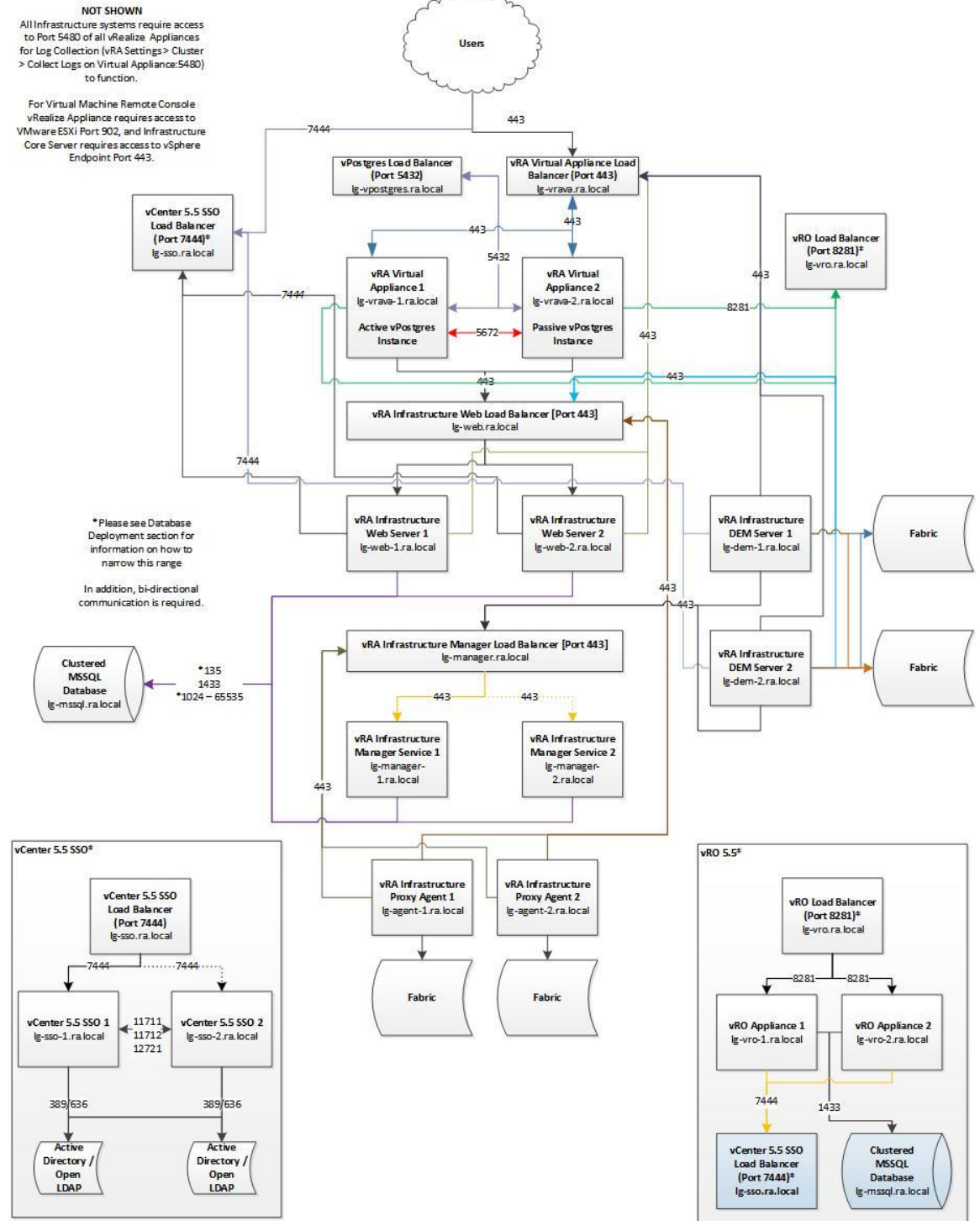


Figure 7. Minimum Footprint for Large Configuration (vRealize Automation)

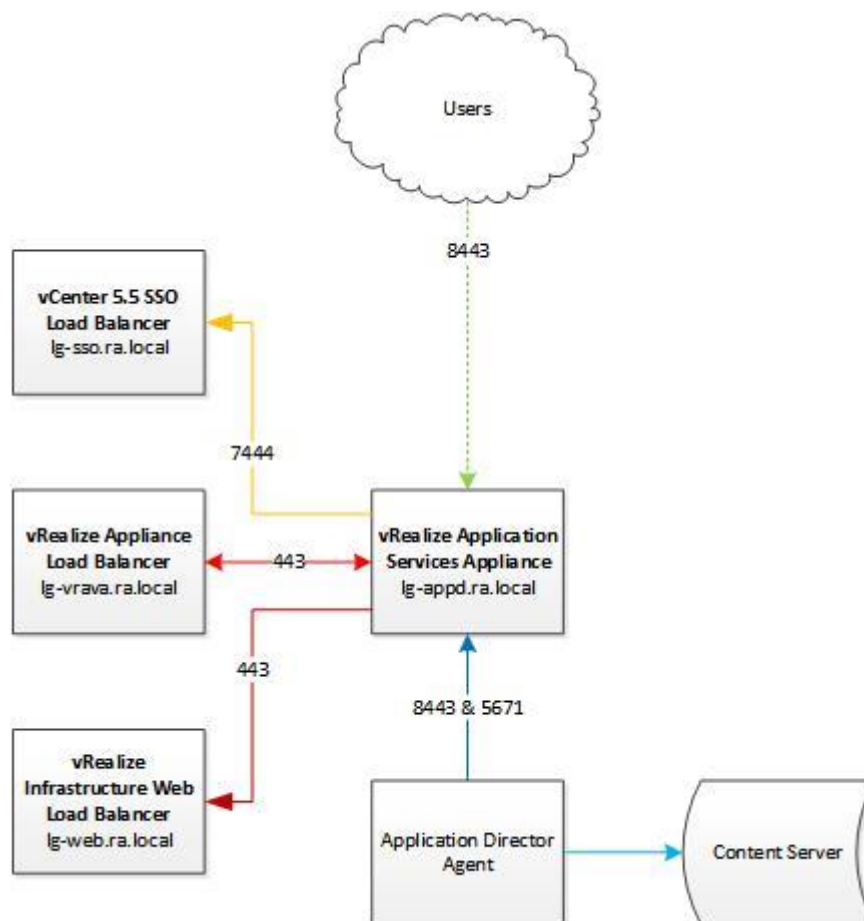


Figure 8. Minimum Footprint for Large Configuration (vRealize Application Services)

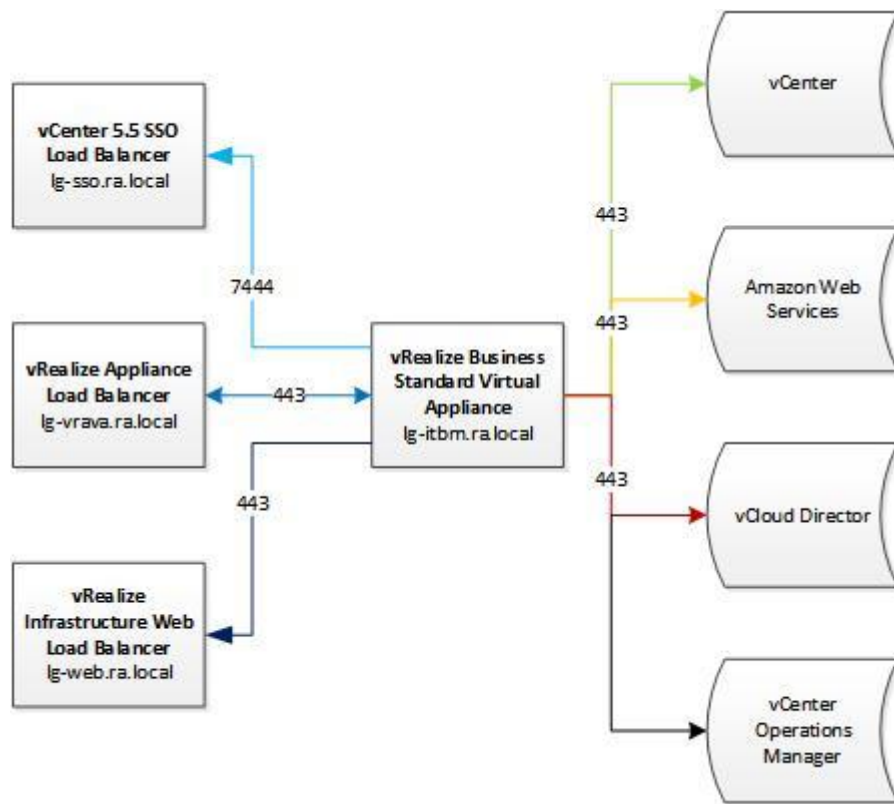


Figure 9. Minimum Footprint for Large Configuration ((vRealize Business Standard Edition)

