
vRealize Automation Reference Architecture
vRealize Automation Secure Configuration
Installing vRealize Automation
Installation Overview
Preparing for Installation
General Preparation
Accounts and Passwords
Host Names and IP Addresses
vRealize Automation Appliance
IaaS Windows Servers
IaaS Web Server
IaaS Manager Service Host
IaaS SQL Server Host
IaaS Distributed Execution Manager Host
Certificates
Extracting Certificates and Private Keys
Deploying the vRealize Automation Appliance
Installing with the Installation Wizard
ADD TOPIC TO MYLIBRARY
vRealize Automation uses SSL certificates for secure communication among IaaS components and instances of the vRealize Automation appliance. The appliances and the Windows installation machines exchange these certificates to establish a trusted connection. You can obtain certificates from an internal or external certificate authority, or generate self-signed certificates during the deployment process for each component.
For important information about troubleshooting, support, and trust requirements for certificates, see VMware Knowledge Base article 2106583.
Note:
vRealize Automation supports SHA2 certificates. The self-signed certificates generated by the system use SHA-256 With RSA Encryption. You might need to update to SHA2 certificates due to operating system or browser requirements.
You can update or replace certificates after deployment. For example, a certificate may expire or you may choose to use self-signed certificates during your initial deployment, but then obtain certificates from a trusted authority before going live with your vRealize Automation implementation.
Certificate Implementations
Component
Minimal Deployment (non-production)
Distributed Deployment (production-ready)
vRealize Automation Appliance
Generate a self-signed certificate during appliance configuration.
For each appliance cluster, you can use a certificate from an internal or external certificate authority. Multi-use and wildcard certificates are supported.
IaaS Components
During installation, accept the generated self-signed certificates or select certificate suppression.
Obtain a multi-use certificate, such as a Subject Alternative Name (SAN) certificate, from an internal or external certificate authority that your Web client trusts.
No mentioned of wildcard cert