

Installation Checklist  
for VMware vRealize Automation 8  
Deployment

WEI  
43 Northwestern Drive  
Salem, NH 03079  
603-893-0900

Table Of Contents

[Table Of Contents 2](#_Toc43985307)

[Installation Requirements 3](#_Toc43985308)

[VMware vRealize Automation - Overview 3](#_Toc43985309)

[VMware Automation Easy Installer Prerequisite Information 4](#_Toc43985310)

[Certificates 7](#_Toc43985311)

[Configuration Process 8](#_Toc43985312)

[Easy Installer Deployment 8](#_Toc43985313)

[Configure vRLCM, vIDM, and vRLCM 9](#_Toc43985314)

[Appendix A – Version Information 13](#_Toc43985315)

[Appendix B – Hardware Requirements 14](#_Toc43985316)

Installation Requirements

VMware vRealize Automation - Overview

This section calls out the required components & infrastructure to complete the installation.  
This is a Simple installation.

| Information | Notes | Enter Value Here |
| --- | --- | --- |
|  | vRealize Automation requires hosts to be identified using their fully qualified domain names (FQDN).  DNS infrastructure is a necessity.  The appliances will have a host name and in most cases an alternative name that is the name on any certificates used.  For example the vRA appliance may be vra1.company.com but the certificate and web address provided to users would be cloud.company.com |  |
| NTP | Appliances have strict time synchronization requirements. If not available, installation will fail and the environment will not operate properly |  |
|  | For production environments certificates are strongly recommended for the three components. An internal Microsoft CA can be used, but it will require a new certificate template to be created. As an important note most older internal CA use SHA-1 which is no longer supported by modern browsers. |  |

Other components to be aware of:

| Information | Notes | Enter Value Here |
| --- | --- | --- |

VMware Automation Easy Installer Prerequisite Information

| Information | Notes | Enter Value Here |
| --- | --- | --- |
| Easy Installer Location | Before beginning, download the VMware vRealize Suite Lifecycle Manager Easy Installer from the My VMWare portal and place it on a machine close to your vCenter. As of this writing, the 8.1 Easy Installer ISO is 11.63 GB, so choose your location wisely. |  |
| Hardware Requirements | Refer to Appendix B and ensure you have sufficient physical resources to host all virtual appliances to be deployed |  |
| vCenter Hostname | Hostname of vCenter vRA will deploy VMs to. |  |
| vCenter Admin Installation Account | vCenter account with admin privileges that the installer will use to deploy products |  |
| vCenter Admin Installation Account Password | Password for above account |  |
| vCenter Admin vRA Service Account | Service with admin privileges in vCenter. vRA will use this account to deploy VMs in vCenter. |  |
| vCenter Admin vRA Service Account Password | Password for above service account |  |
| Management VM Folder | vCenter folder that all management VMs will be placed in |  |
| Management VM Cluster | vCenter cluster that all your management VMs will be placed in |  |
| Management VM Datastore | Datastore or Datastore cluster that all management VMs will be placed in |  |
| vRA VM Folder | Folder in vCenter to place vRA deployed VMs into |  |
| vRA VM Cluster | vSphere cluster that vRA VMs will be deployed to |  |
| Management Subnet Network Information | Subnet info for hosting all management infrastructure (vRA appliance, vIDM, and vRLCM)   * CIDR * Subnet Mask * Gateway * Domain Name * DNS1 * DNS2 * vCenter Port Group | --  --  --  --  --  --  -- |
| Time Sync | Will the appliance sync to an ESXi host or will it use an NTP server?  If NTP Server, what is its info? |  |
| Time Zone |  | America/New\_York |
| Local Admin Username | Username of the local administrator created during the installation process, used for initial configuration of the product and will be the default admin account in the “System Domain” for all deployed products | admin |
| Root Password | Password for all local and “System Domain” accounts on all appliances. Used for SSH access. Account name will always be “root”. |  |
| vRealize Lifecycle Manager Appliance IP and Hostname | IP and FQDN of Lifecycle Manager |  |
| vRealize Identify Manager Appliance IP and Hostname | IP and FQDN of vIDM |  |
| vRealize Automation Appliance IP and Hostname | IP and FQDN of vRA |  |
| NSX Manager FQDN | FQDN of NSX-V manager or VIP of NSX-T Management cluster. vRA will connect to this and use it to create networks in blueprints. |  |
| NSX Manager Admin Account | vRA will deploy things in NSX using this account |  |
| NSX Manager Admin Account Password | Password for above account |  |
| AD Group for vRA Admins | Active Directory group that will be given administrative access to vRA |  |
| AD Group for vIDM Admins | Active Directory group that will be given administrative access to vIDM |  |
| AD Group for vRLCM Admins | Active Directory group that will be given administrative access to vRLCM |  |
| Log Insight Server | What is the name of the Log Insight Server, or additional syslog servers? |  |

Certificates

vRLCM comes with a piece of software called “Locker” built in. Locker can act as a Certificate Authority, generate and automatically install certifications, manage credentials, etc. It is assumed that Locker will be used to generate and manage certificates.

| Completed | Notes |
| --- | --- |
|  | USE WEI Generated SSL Certificate Guide to do Certificate prep |

Configuration Process

Please sign off on the completion of the processes.

Easy Installer Deployment

| Completed | Notes |
| --- | --- |
|  | **Task:** Execute Easy Installer  **Purpose:** The Easy Installer comes in the form of an ISO file. You need to extract it and navigate to the correct folder run the installer  **Steps:**  Hopefully you have already downloaded the installer. If so, navigate to wherever you put it. If not, log in to My VMWare, start the download, and go get a cup of coffee.  Mount the ISO as a CD, then navigate to  vrclcm-ui-installer/${yourplatformhere}  within the mount point and execute the installer  At this point, just follow the installer. The installer deploys 3 different VMs in a Small deployment, so the installation will take awhile. A few things to note:   1. Once the installer starts running, it should show you the path to the installer log file location on your machine. You can tail that log to see installer progress. In Powershell, the command would be: Get-Content -Wait ${path\_to\_file} |

Configure vRLCM, vIDM, and vRLCM

| Completed | Notes |
| --- | --- |
|  | **Task:** Add Active Directory to vIDM  **Purpose:** This adds Active Directory as an identity source for vRealize Identity Manager. You need to do this to be able to log in to vRA and other vIDM integrated appliances using your domain account  **Steps:**  Log in to vIDM using the system domain and the default account created using the easy installer (typically admin or configadmin)  If you land on “User Portal” page, click username dropdown in top right and click “Adminstration Console”. Otherwise, skip this step  Click “Identity and Access Management” > “Add Directory” > “Add Active Directory over LDAP”  Fill out appropriate info |
|  | **Task:** Assign Identity Manager administrative roles to an AD Group  **Purpose:** This assigns the appropriate administrative roles within Identity Manager to an Active Directory group so users can log into and administer vIDM with their domain credentials. vIDM admins manage which users and groups get synced into vIDM, and therefore managed who can log in to vIDM integrated products.  **Steps:**  Log in to vIDM using default System Domain admin account (admin@local)  If you land on “User Portal” page, click username dropdown in top right and click “Adminstration Console”. Otherwise, skip this step  Click “Roles”  Click the checkbox next to the “Super Admin” role  Click “Assign” and search for the correct AD group  Click the group when it appears in the dropdown, then click “Save”  Log out and try logging in with a set of domain credentials |
|  | **Task:** Assign Lifecycle Manager administrative roles to an AD Group  **Purpose:** This assigns the appropriate administrative roles within Lifecycle Manager to an Active Directory group so users can log into and administer vRLCM with their domain credentials. vRLCM admins can create certs, deploy production systems to vCenter environments, and do other pretty invasive things. Choose the AD group wisely.  **Steps:**  Log in to vRLCM using default System Domain admin account (admin@local)  Click “Identity and Tenant Management” under “My Services”  Click “User Management” in left side bar  Click “Add User/Group”  Search for the name of your AD group in the search bar, it should pop up if vIDM was connected to AD properly  Click “Next”, select all the roles.  Click “Next”, then submit  Test by logging out and logging back in with a set of domain credentials |
|  | **Task:** Assign Administrative Roles to AD Group in vRA  **Purpose:**  Need to assign administrative roles to Domain Accounts so they can log in, configure and administer the product. You could assign this to an AD group or directly to a Domain Account. Group is a best practice  **Steps:**  Retrieve the “AD Group for vRA Admins” from the prereqs table  Log in to vRA8 appliance using the system domain and account you set up during the easy installer  Click Identity and Access Management tab at the top > Enterprise Groups > Assign Roles  Search for the group you just retrieved  Assign Organization Roles: Organization Owner  Assign Service Roles: For each of the 5 services (Orchestrator, Cloud Assembly, Service Broker, vRA Migration Assessment, and Code stream) choose the “Administrator” role from the dropdown.  Test by logging out and logging back in with a set of domain credentials |
|  | **Task:** Create Cloud Account(s) in vRA  **Purpose:**  To speak with the various IaaS platforms (vCenter, AWS, Azure, etc) you need to provide vRA with a set of appropriately privileged credentials in order to authenticate with and “talk to” those resources. These sets of credentials are called “Cloud Accounts”  **Steps:**  Log in to vRA with your admin domain credentials  From the “Services” tab, click on Cloud Assembly.  Click the “Infrastructure” tab  Click “Cloud Accounts” in the left side bar  Click “+ Add Cloud Account”  Select the appropriate IaaS platfom  Fill out the form with the correct service account and validate the connection. Note that if you click “Create a cloud zone” when selecting the datacenter, a cloud zone will be configured for you that may not have the setup you require.  TODO: Add useful tagging instructions here |
|  | **Task:** Create Cloud Zone(s)  **Purpose:**  To provision to specific vCenter clusters, AWS regions, etc. you need to create Cloud Zones within your Cloud Account that divide up the infrastructure provided by each IaaS platform. For example, you might have “development” and “production” vSphere clusters, and you want certain blueprints to deploy to *only* development, or *only* production. You would need to create a Cloud Zone for each environment to segment your infrastructure first.  **Steps:**  Open Cloud Assembly  Click the “Infrastructure” tab at the top  Click “Cloud Zones” in the left sidebar  Click “+ NEW CLOUD ZONE”  In the “Summary” tab, search for the parent Cloud Account of this Cloud Zone and select it. Give the Cloud Zone a useful name and description. Choose appropriate Placement Policy, for vCenter Clusters “Spread” is recommended so if a host goes down you don’t have major spikes in vMotion traffic.  Under “Capability Tags” enter tagging information that can be used within blueprints to selectively deploy to this infrastructure. For example, the tag “environment:production” would indicate this Cloud Zone is for production infrastructure.  Under the Compute tab, you will see all the clusters currently available in your cloud account. Assign appropriate tags to the clusters you want included in this Cloud Zone, then enter those tags in the Filter field to select them. |
|  | **Task:** Create Project(s)  **Purpose:**  Projects tie users and groups to Cloud Zones, allowing them to provisions resources to subsets of your infrastructure.  **Steps:**  Open Cloud Assembly  Click the “Infrastructure” tab at the top  Click “Projects” in the left sidebar  Click “+ NEW PROJECT”  Under “Summary” tab, give useful name and description.  Under “Users” tab, add Users/Groups to the project. Choose whether you want deployments created by one user to be accessible by all other users in the project.  Under “Provisioning” tab, add all Cloud Zones you want this project to have access to. You can set limits on resource consumption when adding the Cloud Zone.  Define a naming template for VMs in the Template field. You can access variables in the naming scheme with the ${variable\_here} syntax. |
|  | **Task:** Create Flavor Mapping(s)  **Purpose:**  Flavor mappings are custom “T shirt sizes” for resources (i.e small, medium, large) that allow you to map VM hardware (vCPU and memory) configurations from many different IaaS platforms to a single vRA flavor that will be used in blueprints. This abstracts away the details of any given IaaS VM hardware setup and allows you to create cloud agnostic VMs in your blueprints.  **Steps:**  Open Cloud Assembly  Click the “Infrastructure” tab at the top  Click “Flavor Mappings” in the left sidebar  Click “+ FLAVOR MAPPING”  Give the Flavor Mapping a useful name (Ex: wei.small)  Choose the resource configurations and flavors from all your available regions that map to this intended VM size. |
|  | **Task:** Create Image Mapping(s)  **Purpose:**  Image mappings are maps that map images on multiple different IaaS platforms that all serve the same purpose to one abstract “Image mapping” that will be used in your blueprints to make your blueprints cloud agnostic. For example, you have a custom Ubuntu 18.04 template in vCenter, and the same image in Azure and AWS. You create an Image Mapping for Ubuntu 18.04 that maps all those disparate images into one abstract “Image Mapping”, use that in your blueprints, and vRA knows which image to use based on the Image Mapping and the Cloud Account you are deploying to.  **Steps:**  Open Cloud Assembly  Click the “Infrastructure” tab at the top  Expand “Configure” in the left sidebar  Click “Image Mappings” in the left sidebar  Click “+ IMAGE MAPPING”  Give the Image Mapping a useful name (Ex: Ubuntu-18.04-latest)  Add the backing images from each available region.  If your images have cloud-init installed on them, you can add cloud init scripts to each image here to bootstrap/customize your VM from some base image. |
|  | **Task:** Create Network Profiles  **Purpose:**  Network profiles bind vCenter Port Group and vSwitch information to network information (CIDR, DNS, gateway) so that VMs in blueprints can be automatically assigned IP addresses and configured with the proper networking information during deployment. Network profiles also allow you to group networks under a unified “Network Policy”, apply tags across all networks within the policy, configure available load balancers that will be available to VMs, apply Security Groups to all VMs that consume a Network Profile, and manage ranges of IP addresses that should be consumed from a given network.  **Steps:**  Open Cloud Assembly  Click the “Infrastructure” tab at the top  Expand “Configure” in the left sidebar  Click “Network Profiles”  Click “+ New Network Profile”  Search for and select the Cloud Account where the networks that will be grouped within the Network Profile exist.  Assign a useful name and description  If you want every network within the Network Profile to have the same Capability Tags applied, assign them here.  Under the networks tab, click “+ Add Network”  Select all the networks you want to be included in this Network Profile. You can use the search field to filter the list of networks that appear.  Assign any unique Capability Tags you wish to assign to individual networks by selecting the network and click the “Tags” button.  Add Load Balancers and Security Groups similarly. |
|  | **Task:** Create Storage Profiles  **Purpose:**  **Steps:**  Open Cloud Assembly  Click the “Infrastructure” tab at the top  Expand “Configure” in the left sidebar |
|  | **Task:** Add email servers  **Purpose:**  An email server must be configured so users can receive notifications for things like approval policies, maintenance, etc.  **Steps:**  Log in to Service Broker  Select Content and Policies > Notifications > Email Servers  Enter email server info and test the connection |
|  | **Task:** Connect vRA to Log Insight  **Purpose:**  This configures the vRA appliance to send logs to Log Insight. vRA 8 uses the HTTPS API of Log Insight to stream logs, which is different from vRA 7 agent-based setup.  **Steps:**  SSH into the vRA appliance using “root” user and password  Run the following command  vracli vrli set --environment ${ENV\_TAG\_HERE} --insecure ${LOGINSIGHT\_FQDN\_HERE}  --insecure flag is used to accept untrusted certs. Omit that flag if the certificate of the log insight server is trusted by the vRA appliance.  --environment flag is used to tag all log events from this vRA environment with the provided string for easy searching. Highly recommended to set this to something “vra” relevant and easy to remember.  Double check logs are being ingested by logging in to Log Insight.  Go to “Interactive Analytics” page at the top of the vRLI homepage  Add a filter with "host" "contains" "FQDN\_OF\_VRA8\_APPLIANCE\_HERE" to the search. Do not use the "hostname" tag! It contains the name of a Kubernetes container DaemonSet, which ends with a random ID that will be impossible to know ahead of time.  You should see vRA related messages after running the filter |
|  | Log Out |

Appendix A – Version Information

| Date | Contact | Notes |
| --- | --- | --- |
| 2020-03-20 | Kyle Robertson | First draft |

Appendix B – Hardware Requirements

A screenshot of a cell phone

Description automatically generated