QuickStart: Mirantis Container Cloud on VMWare vSphere

version latest

Contents

©2021, Mirantis Inc.

Copyright notice

2021 Mirantis, Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. No part of this publication may be reproduced in any written, electronic, recording, or photocopying form without written permission of Mirantis, Inc.

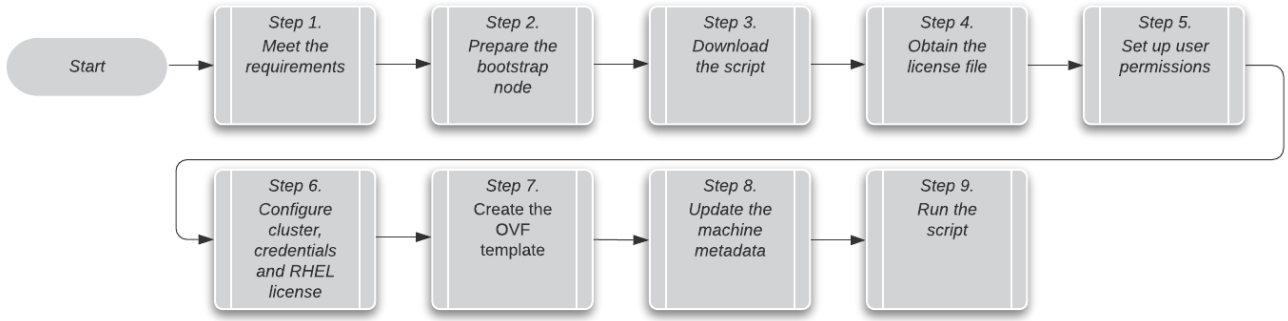
Mirantis, Inc. reserves the right to modify the content of this document at any time without prior notice. Functionality described in the document may not be available at the moment. The document contains the latest information at the time of publication.

Mirantis, Inc. and the Mirantis Logo are trademarks of Mirantis, Inc. and/or its affiliates in the United States an other countries. Third party trademarks, service marks, and names mentioned in this document are the properties of their respective owners.

Introduction

Using this QuickStart tutorial, you can deploy a Mirantis Container Cloud VMWare vSphere-based management cluster containing 3 control plane nodes. This cluster will run the public API and the web UI. Using the Container Cloud web UI, you can deploy managed clusters that run Mirantis Kubernetes Engine.

The following diagram illustrates the deployment overview of a Container Cloud vSphere-based management cluster:



©2021, Mirantis Inc.

Before you begin

Before you start the cluster deployment, verify that your system meets the following minimum hardware and software requirements for a vSphere-based management cluster:

Note

For the bootstrap node, you can use any local machine running Ubuntu 18.04 with the following resources:

- 2 vCPUs
- 4 GB of RAM
- 5 GB of available storage

Minimum hardware requirements for a management cluster

Resource	Requirement
# of hypervisors	1
# of nodes	3 (HA)
# of vCPUs	24 (8 vCPUs per node)
RAM in GB	48 (16 per node)
Storage in GB	360 (120 per node) that must be shared to the hypervisor
RHEL license	1 RHEL license for Virtual Datacenters per hypervisor
Obligatory vSphere capabilities	DRS, Shared datastore
IP subnet size	Minimum 20 IPs: • 1 for load balancing • 3 for nodes • 6 for Container Cloud services • 5 for StackLight services • 5 auxiliary IPs for basic verification testing

Minimum software requirements for a management cluster

Software	Version
Operating system distribution	Ubuntu 18.04, RHEL 7.8

©2021, Mirantis Inc.

VMWare vSphere	7.0 or 6.7
Docker	Current version available for Ubuntu 18.04

©2021, Mirantis Inc.

Prepare the bootstrap node

1. Log in to any personal computer or VM running Ubuntu 18.04 that you will be using as the bootstrap node.
2. If you use a newly created VM, run:

   ```
   sudo apt-get update
   ```

3. Install the current Docker version available for Ubuntu 18.04:

   ```
   sudo apt install docker.io
   ```

4. Grant your USER access to the Docker daemon:

   ```
   sudo usermod -aG docker $USER
   ```

5. Log off and log in again to the bootstrap node to apply the changes.
6. Verify that Docker is configured correctly and has access to Container Cloud CDN. For example:

   ```
   docker run --rm alpine sh -c "apk add --no-cache curl; \
   curl https://binary.mirantis.com"
   ```

   The system output must not contain error records.

©2021, Mirantis Inc.

Download the bootstrap script

1. On the bootstrap node, download and run the Container Cloud bootstrap script:

```
wget https://binary.mirantis.com/releases/get_container_cloud.sh
chmod 0755 get_container_cloud.sh
./get_container_cloud.sh
```

2. Change the directory to the kaas-bootstrap folder created by the script.

©2021, Mirantis Inc.

Obtain the Mirantis license

1. Create a user account at mirantis.com.
2. Log in to your account and download the mirantis.lic license file.
3. Save the license file as mirantis.lic under the kaas-bootstrap directory on the bootstrap node.

©2021, Mirantis Inc.

Prepare the deployment user setup and permissions

1. Log in to the vCenter Server Web Console.
2. Create a virt-who user with at least read-only access to all objects in the vCenter Data Center.

   The virt-who service on RHEL machines will be provided with the virt-who user credentials to properly manage RHEL subscriptions.

   For details on how to create the virt-who user, refer to the official RedHat Customer Portal documentation.
3. Create the cluster-api and storage users with the following sets of privileges:

Privileges set for the cluster-api user

General privileges	Virtual machine privileges
Content library	Change configuration
Datastore	Interaction
Distributed switch	Inventory
Folder	Provisioning
Global	Snapshot management
Host local operations	vSphere replication
Network	
Resource	
Scheduled task	
Sessions	
Storage views	
Tasks	

Privileges set for the storage user

General privileges	Virtual machine privileges
Cloud Native Storage	Change configuration
Content library	Inventory
Datastore	
Folder	
Host configuration	
Host local operations	

©2021, Mirantis Inc.

Host profile	
Profile-driven storage	
Resource	
Scheduled task	
Storage views	

Configure the cluster and vSphere credentials

1. Change the directory to the kaas-bootstrap folder created by the get_container_cloud.sh script.
2. Prepare your RHEL license and deployment templates:
    1. Fill out templates/vsphere/rhellicenses.yaml.template using one of the following set of parameters for RHEL machines subscription:
        - The user name and password of your RedHat Customer Portal account associated with your RHEL license for Virtual Datacenters.

          Optionally, provide the subscription allocation pools to use for the RHEL subscriptions activation. If not needed, remove the poolIDs field for subscription-manager to automatically select the licenses for machines.

          For example:

          ```
          spec:
            username: <username>
            password:
              value: <password>
            poolIDs:
            - <pool1>
            - <pool2>
          ```

        - Available since 2.6.0 The activation key and organization ID associated with your RedHat account with RHEL license for Virtual Datacenters. The activation key can be created by the organization administrator on RedHat Customer Portal.

          If you use the RedHat Satellite server for management of your RHEL infrastructure, you can provide a pre-generated activation key from that server. In this case, also provide the URL to the RedHat Satellite RPM for installation of the CA certificate that belongs to that server.

          For example:

          ```
          spec:
            activationKey:
              value: <activation key>
            orgID: "<organization ID>"
            rpmUrl: <rpm url>
          ```

> Caution!
>
> Provide only one set of parameters. Mixing of parameters from different activation methods will cause deployment failure.

2. Modify templates/vsphere/vsphere-config.yaml.template:

vSphere configuration data

Parameter	Description
SET_VSPHERE_SERVER	IP address or FQDN of the vCenter Server.
SET_VSPHERE_SERVER_PORT	Port of the vCenter Server. For example, port: "8443". Leave empty to use 443 by default.
SET_VSPHERE_DATACENTER	vSphere data center name.
SET_VSPHERE_SERVER_INSECURE	Flag that controls validation of the vSphere Server certificate. Must be true or false.
SET_VSPHERE_CAPI_PROVIDER_USERNAME	vSphere Cluster API provider user name that you added when preparing the deployment user setup and permissions.
SET_VSPHERE_CAPI_PROVIDER_PASSWORD	vSphere Cluster API provider user password.
SET_VSPHERE_CLOUD_PROVIDER_USERNAME	vSphere Cloud Provider deployment user name that you added when preparing the deployment user setup and permissions.
SET_VSPHERE_CLOUD_PROVIDER_PASSWORD	vSphere Cloud Provider deployment user password.

3. Modify the templates/vsphere/cluster.yaml.template parameters to fit your deployment. For example, add the corresponding values for cidrBlocks in the spec::clusterNetwork::services section.

Required parameters

Parameter	Description
SET_LB_HOST	IP address from the provided vSphere network for load balancer (Keepalived).
SET_VSPHERE_METALLB_RANGE	MetalLB range of IP addresses that can be assigned to load balancers for Kubernetes Services.
SET_VSPHERE_DATASTORE	Name of the vSphere datastore. You can use different datastores for vSphere Cluster API and vSphere Cloud Provider.
SET_VSPHERE_MACHINES_FOLDER	Path to a folder where the cluster machines metadata will be stored.

SET_VSPHERE_NETWORK_PATH	Path to a network for cluster machines.
SET_VSPHERE_RESOURCE_POOL_PATH	Path to a resource pool in which VMs will be created.

> Note
>
> The passwordSalt and passwordHash values for the IAM roles are automatically re-generated during the IAM configuration.

4. Starting from Container Cloud 2.6.0, if a vSphere network has no DHCP server, provide the following additional parameters for a proper network setup on machines using embedded IP address management (IPAM) in templates/vsphere/cluster.yaml.template:

vSphere configuration data

Parameter	Description
ipamEnabled	Enables IPAM. Set to true for networks without DHCP.
SET_VSPHERE_NETWORK_CIDR	CIDR of the provided vSphere network. For example, 10.20.0.0/16.
SET_VSPHERE_NETWORK_GATEWAY	Gateway of the provided vSphere network.
SET_VSPHERE_CIDR_INCLUDE_RANGES	Optional. IP range for the cluster machines. Specify the range of the provided CIDR. For example, 10.20.0.100-10.20.0.200.
SET_VSPHERE_CIDR_EXCLUDE_RANGES	Optional. IP ranges to be excluded from being assigned to the cluster machines. The MetalLB range and SET_LB_HOST should not intersect with the addresses for IPAM. For example, 10.20.0.150-10.20.0.170.
SET_VSPHERE_NETWORK_NAMESERVERS	List of nameservers for the provided vSphere network.

3. In bootstrap.env, add the following environment variables:

> Note
>
> For the Keycloak and IAM services variables, assign IP addresses from the end of the provided MetalLB range. For example, if the MetalLB range is 10.20.0.30-10.20.0.50, select 10.20.0.48 and 10.20.0.49 as IPs for KeyCloak and IAM.

vSphere environment data

Parameter	Description
KAAS_VSPHERE_ENABLED	Set to true. Enables the vSphere provider deployment in Container Cloud.
KEYCLOAK_FLOATING_IP	IP address for Keycloak from the end of the MetalLB range.
IAM_FLOATING_IP	IP address for IAM from the end of the MetalLB range.

©2021, Mirantis Inc.

Prepare the OVF template

1. Download the RHEL 7.8 DVD ISO from the RedHat Customer Portal.
2. Change the directory to the kaas-bootstrap folder.
3. Export the following variables:
    1. The virt-who user name and password
    2. The path to the RHEL 7.8 DVD ISO file
    3. The vSphere cluster name

   For example:

```
export KAAS_VSPHERE_ENABLED=true
export VSPHERE_RO_USER=virt-who-user
export VSPHERE_RO_PASSWORD=virt-who-user-password
export VSPHERE_PACKER_ISO_FILE=$(pwd)/rhel-7.8.dvd.iso
export VSPHERE_CLUSTER_NAME=vsphere-cluster-name
```

4. Prepare the OVF template:

```
./bootstrap.sh vsphere_template
```

5. In templates/vsphere/machines.yaml.template:
    - Define SET_VSPHERE_TEMPLATE_PATH prepared in the previous step.
    - Modify other parameters as required.

```
spec:
  providerSpec:
    value:
      apiVersion: vsphere.cluster.k8s.io/v1alpha1
      kind: VsphereMachineProviderSpec
      rhelLicense: kaas-mgmt-rhel-license
      network:
        devices:
        - dhcp4: true
          dhcp6: false
      template: <SET_VSPHERE_TEMPLATE_PATH>
```

> Note
>
> The <rhel-license-name> value is the RHEL license name defined in rhellicenses.yaml.tempalte, defaults to kaas-mgmt-rhel-license.

Finalize the bootstrap

1. On the bootstrap node, run the bootstrap script:

   ```
   ./bootstrap.sh all
   ```

2. When the bootstrap is complete, collect and save the following management cluster details in a secure location:

   - The kubeconfig file located in the same directory as the bootstrap script. This file contains the admin credentials for the management cluster.
   - The private ssh_key for access to the management cluster nodes that is located in the same directory as the bootstrap script.
   - The URL and credentials for the Container Cloud web UI. The system outputs these details when the bootstrap completes.
   - The StackLight endpoints. For details, see Operations Guide: Access StackLight web UIs.
   - The Keycloak URL that the system outputs when the bootstrap completes. The admin password for Keycloak is located in kaas-bootstrap/passwords.yml along with other IAM passwords.

   > Note
   >
   > When the bootstrap is complete, the bootstrap cluster resources are freed up.

What’s next

Using your newly deployed management cluster, you can:

- Deploy an additional vSphere-based regional cluster to operate managed clusters of several configurations within a single Container Cloud deployment in parallel.

  You can also extend your cluster with more options, for example:

  - Configure an external identity provider for IAM
  - Attach an existing Mirantis Kubernetes Engine cluster
- Create and operate managed clusters. Before that, verify that your planned cluster meets the requirements for managed clusters.

For details about all Container Cloud features, refer to the full set of Container Cloud documentation.

©2021, Mirantis Inc.