



8. Deploy the admin cluster

NetApp Solutions

Dorian Henderson, Kevin Hoke
April 06, 2021

This PDF was generated from https://docs.netapp.com/us-en/netapp-solutions/containers/anthos_task_deploy_the_admin.html on August 18, 2021. Always check docs.netapp.com for the latest.

Table of Contents

8. Deploy the admin cluster 1

8. Deploy the admin cluster

All Kubernetes clusters deployed as a part of the Anthos solution are deployed from the Anthos admin workstation that you just created. A user logs into the admin workstation using SSH, the public key created in a previous step, and the IP address provided at the end of the VM deployment. An admin cluster controls all actions in an Anthos environment. The admin cluster must be deployed first, and then individual user clusters can be deployed for specific workload needs.



There are specific procedures for deploying clusters that use static IP addresses [here](#), and procedures for environments with DHCP can be found [here](#). In this guide, we use the second set of instructions for ease of deployment.

To deploy the admin cluster, complete the following steps:

1. Log into your admin-workstation using the SSH command prompted at the end of the deployment. After successful authentication, you can list the files in the home directory, which are used to create the admin cluster and additional clusters later on. The directory also includes the copied vCenter cert and the access key for Anthos that was created in earlier steps.

```
[user@rhel7 anthos-install]$ ssh -i ~/.ssh/gke-admin-workstation
ubuntu@10.63.172.10

Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1001-gkeop x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
Last login: Fri Jan 29 15:46:35 2021 from 10.249.129.216

ubuntu@gke-admin-200915-151421:~$ ls
admin-cluster.yaml
user-cluster.yaml
vcenter.pem
component-access-key.json
```

2. Use scp to copy the remaining keys for your Anthos account over from the workstation you deployed the admin-workstation from.

```
ubuntu@gke-admin-200915-151421:~$ scp user@rhel7:~/anthos-
install/connect-register-key.json ./
ubuntu@gke-admin-200915-151421:~$ scp user@rhel7:~/anthos-
install/connect-agent-key.json ./
ubuntu@gke-admin-200915-151421:~$ scp user@rhel7:~/anthos-
install/logging-monitoring-key.json ./
```

3. Edit the admin-cluster.yaml file so that it is specific to the deployed environment. The file is very large, so we will address it by sections.

- a. Most of the information is already filled in by default based on the configuration used to deploy the admin-workstation by gkeadm. This first section confirms the information for the version of Anthos being deployed and the vCenter instance it is deployed on. It also allows you to define a local data disk (VMDK) for Kubernetes object data.

```
apiVersion: v1
kind: AdminCluster
# (Required) Absolute path to a GKE bundle on disk
bundlePath: /var/lib/gke/bundles/gke-onprem-vmware-1.6.0-gke.7-
full.tgz
# (Required) vCenter configuration
vCenter:
  address: anthos-vc.cie.netapp.com
  datacenter: NetApp-HCI-Datacenter-01
  cluster: NetApp-HCI-Cluster-01
  resourcePool: Anthos-Resource-Pool
  datastore: VM_Datastore
  # Provide the path to vCenter CA certificate pub key for SSL
  verification
  caCertPath: "/home/ubuntu/vcenter.pem"
  # The credentials to connect to vCenter
  credentials:
    username: administrator@vsphere.local
    password: "vSphereAdminPassword"
  # Provide the name for the persistent disk to be used by the
  deployment (ending
  # in .vmdk). Any directory in the supplied path must be created
  before deployment
  dataDisk: "admin-cluster-disk.vmdk"
```

- b. Fill out the networking section next, and select whether you are using static or DHCP mode. If you are using static addresses, you must create an IP-block file based on the instructions linked to above, and add it to the config file.



If static IPs are used in a deployment, the items under the host configuration are global. This includes static IPs for clusters or those used for SeeSaw load balancers, which are configured later.

```

# (Required) Network configuration
network:
# (Required) Hostconfig for static addresses on Seesaw LB's
hostConfig:
  dnsServers:
    - "10.61.184.251"
    - "10.61.184.252"
  ntpServers:
    - "0.pool.ntp.org"
    - "1.pool.ntp.org"
    - "2.pool.ntp.org"
  searchDomainsForDNS:
    - "cie.netapp.com"
ipMode:
  # (Required) Define what IP mode to use ("dhcp" or "static")
  type: dhcp
  # # (Required when using "static" mode) The absolute or relative
  # path to the yaml file
  # # to use for static IP allocation
  # ipBlockFilePath: ""
  # (Required) The Kubernetes service CIDR range for the cluster.
  # Must not overlap
  # with the pod CIDR range
  serviceCIDR: 10.96.232.0/24
  # (Required) The Kubernetes pod CIDR range for the cluster. Must
  # not overlap with
  # the service CIDR range
  podCIDR: 192.168.0.0/16
vCenter:
  # vSphere network name
  networkName: VM_Network

```

- c. Fill out the load balancer section next. This can vary depending on the type of load balancer being deployed.

Seesaw example:

```

loadBalancer:
  # (Required) The VIPs to use for load balancing
  vips:
    # Used to connect to the Kubernetes API
    controlPlaneVIP: "10.63.172.155"
    # # (Optional) Used for admin cluster addons (needed for multi
    # cluster features). Must
    # # be the same across clusters

```

```
# # addonsVIP: "10.63.172.153"
# (Required) Which load balancer to use "F5BigIP" "Seesaw" or
"ManualLB". Uncomment
# the corresponding field below to provide the detailed spec
kind: Seesaw
# # (Required when using "ManualLB" kind) Specify pre-defined
nodeports
# manualLB:
# # NodePort for ingress service's http (only needed for user
cluster)
# ingressHTTPTNodePort: 0
# # NodePort for ingress service's https (only needed for user
cluster)
# ingressHTTPSNodePort: 0
# # NodePort for control plane service
# controlPlaneNodePort: 30968
# # NodePort for addon service (only needed for admin cluster)
# addonsNodePort: 31405
# # (Required when using "F5BigIP" kind) Specify the already-
existing partition and
# # credentials
# f5BigIP:
# address:
# credentials:
# username:
# password:
# partition:
# # # (Optional) Specify a pool name if using SNAT
# # snatPoolName: ""
# (Required when using "Seesaw" kind) Specify the Seesaw configs
seesaw:
# (Required) The absolute or relative path to the yaml file to use
for IP allocation
# for LB VMs. Must contain one or two IPs.
ipBlockFilePath: "admin-seesaw-block.yaml"
# (Required) The Virtual Router Identifier of VRRP for the Seesaw
group. Must
# be between 1-255 and unique in a VLAN.
vrid: 100
# (Required) The IP announced by the master of Seesaw group
masterIP: "10.63.172.151"
# (Required) The number CPUs per machine
cpus: 1
# (Required) Memory size in MB per machine
memoryMB: 2048
# (Optional) Network that the LB interface of Seesaw runs in
```

```
(default: cluster
#   network)
vCenter:
#   vSphere network name
networkName: VM_Network
#   (Optional) Run two LB VMs to achieve high availability
(default: false)
enableHA: false
```

- d. For a SeeSaw load balancer, you must create an additional external file to supply the static IP information for the load balancer. Create the file `admin-seesaw-block.yaml`, which was referenced in this configuration section.

```
blocks:
- netmask: "255.255.255.0"
  gateway: "10.63.172.1"
  ips:
  - ip: "10.63.172.152"
    hostname: "admin-seesaw-vm"
```

F5 BigIP Example:

```
# (Required) Load balancer configuration
loadBalancer:
# (Required) The VIPs to use for load balancing
vips:
# Used to connect to the Kubernetes API
controlPlaneVIP: "10.63.172.155"
# # (Optional) Used for admin cluster addons (needed for multi
cluster features). Must
# # be the same across clusters
# # addonsVIP: "10.63.172.153"
# (Required) Which load balancer to use "F5BigIP" "Seesaw" or
"ManualLB". Uncomment
# the corresponding field below to provide the detailed spec
kind: F5BigIP
# # (Required when using "ManualLB" kind) Specify pre-defined
nodeports
# manualLB:
# # NodePort for ingress service's http (only needed for user
cluster)
#   ingressHTTPTNodePort: 0
# # NodePort for ingress service's https (only needed for user
cluster)
#   ingressHTTPSNodePort: 0
```

```

# # NodePort for control plane service
# controlPlaneNodePort: 30968
# # NodePort for addon service (only needed for admin cluster)
# addonsNodePort: 31405
# # (Required when using "F5BigIP" kind) Specify the already-
existing partition and
# # credentials
f5BigIP:
  address: "172.21.224.21"
  credentials:
    username: "admin"
    password: "admin-password"
  partition: "Admin-Cluster"
# # # (Optional) Specify a pool name if using SNAT
# # snatPoolName: ""
# (Required when using "Seesaw" kind) Specify the Seesaw configs
# seesaw:
# (Required) The absolute or relative path to the yaml file to
use for IP allocation
# for LB VMs. Must contain one or two IPs.
# ipBlockFilePath: ""
# (Required) The Virtual Router Identifier of VRRP for the Seesaw
group. Must
# be between 1-255 and unique in a VLAN.
# vrid: 0
# (Required) The IP announced by the master of Seesaw group
# masterIP: ""
# (Required) The number CPUs per machine
# cpus: 4
# (Required) Memory size in MB per machine
# memoryMB: 8192
# (Optional) Network that the LB interface of Seesaw runs in
(default: cluster
# network)
# vCenter:
# vSphere network name
# networkName: VM_Network
# (Optional) Run two LB VMs to achieve high availability
(default: false)
# enableHA: false

```

- e. The last section of the admin config file contains additional options that can be tuned to fit the specific deployment environment. These include enabling anti-affinity groups if Anthos is being deployed on less than three ESXi servers. You can also configure proxies, private docker registries, and the connections to Stackdriver and Google Cloud for auditing.


```

antiAffinityGroups:
  # Set to false to disable DRS rule creation
  enabled: false
# (Optional) Specify the proxy configuration
proxy:
  # The URL of the proxy
  url: ""
  # The domains and IP addresses excluded from proxying
  noProxy: ""
# # (Optional) Use a private Docker registry to host GKE images
# privateRegistry:
#   # Do not include the scheme with your registry address
#   address: ""
#   credentials:
#     username: ""
#     password: ""
#   # The absolute or relative path to the CA certificate for this
#   registry
#   caCertPath: ""
# (Required): The absolute or relative path to the GCP service
# account key for pulling
# GKE images
gcrKeyPath: "/home/ubuntu/component-access-key.json"
# (Optional) Specify which GCP project to connect your logs and
# metrics to
stackdriver:
  projectID: "anthos-dev"
  # A GCP region where you would like to store logs and metrics for
  # this cluster.
  clusterLocation: "us-east1"
  enableVPC: false
  # The absolute or relative path to the key file for a GCP service
  # account used to
  # send logs and metrics from the cluster
  serviceAccountKeyPath: "/home/ubuntu/logging-monitoring-key.json"
# # (Optional) Configure kubernetes apiserver audit logging
# cloudAuditLogging:
#   projectid: ""
#   # A GCP region where you would like to store audit logs for this
#   cluster.
#   clusterlocation: ""
#   # The absolute or relative path to the key file for a GCP service
#   account used to
#   # send audit logs from the cluster
#   serviceaccountkeypath: ""

```



The deployment detailed in this document is a minimum configuration for validation that requires the disabling of anti-affinity rules. NetApp recommends leaving this option set to true in production deployments.



By default, Anthos on VMware uses a pre-existing, Google-owned container image registry that requires no additional setup. If you choose to use a private Docker registry for deployment, then you must configure that registry separately based on instructions found [here](#). This step is beyond the scope of this deployment guide.

4. When edits to the `admin-cluster.yaml` file are complete, be sure to check for proper syntax and spacing.

```
ubuntu@gke-admin-200915-151421:~$ gkectl check-config --config admin-  
cluster.yaml
```

5. After the configuration check has passed and any identified issues have been remedied, you can then stage the deployment of the cluster. Since we have already checked the validation of the config file, we can skip those steps by passing the `--skip-validation-all` flag.

```
ubuntu@gke-admin-200915-151421:~$ gkectl prepare --config admin-  
cluster.yaml --skip-validation-all
```

6. If you are using a SeeSaw load balancer, you must create one before deploying the cluster itself (otherwise skip this step).

```
ubuntu@gke-admin-200915-151421:~$ gkectl create loadbalancer --config  
admin-cluster.yaml
```

7. You can now stand up the admin cluster. This is done with the `gkectl create admin` command, which can use the `--skip-validation-all` flag to speed up deployment.

```
ubuntu@gke-admin-200915-151421:~$ gkectl create admin --config admin-  
cluster.yaml --skip-validation-all
```

8. When the cluster is deployed, it creates the `kubeconfig` file in the local directory. This file can be used to check the status of the cluster using `kubectl` or run diagnostics with `gkectl`.

```
ubuntu@gke-admin-ws-200915-151421:~ $ kubectl get nodes --kubeconfig
kubeconfig
```

NAME	STATUS	ROLES	AGE
gke-admin-master-gkvm	Ready	master	5m
v1.18.6-gke.6600			
gke-admin-node-84b77ff5c7-6zg59	Ready	<none>	5m
v1.18.6-gke.6600			
gke-admin-node-84b77ff5c7-8jdmz	Ready	<none>	5m
v1.18.6-gke.6600			

```
ubuntu@gke-admin-ws-200915-151421:~$ gkectl diagnose cluster --
kubeconfig kubeconfig
```

Diagnosing admin cluster "gke-admin-gkvm"...- Validation Category:
Admin Cluster VCenter

Checking Credentials...SUCCESS

Checking Version...SUCCESS

Checking Datacenter...SUCCESS

Checking Datastore...SUCCESS

Checking Resource pool...SUCCESS

Checking Folder...SUCCESS

Checking Network...SUCCESS- Validation Category: Admin Cluster

Checking cluster object...SUCCESS

Checking machine deployment...SUCCESS

Checking machineset...SUCCESS

Checking machine objects...SUCCESS

Checking kube-system pods...SUCCESS

Checking storage...SUCCESS

Checking resource...System pods on UserMaster cpu resource request
report: total 1754m nodeCount 2 min 877m max 877m avg 877m tracked
amount in bundle 4000m

System pods on AdminNode cpu resource request report: total 2769m
nodeCount 2 min 1252m max 1517m avg 1384m tracked amount in bundle 4000m

System pods on AdminMaster cpu resource request report: total 923m
nodeCount 1 min 923m max 923m avg 923m tracked amount in bundle 4000m

System pods on UserMaster memory resource request report: total
4524461824 nodeCount 2 min 2262230912 max 2262230912 avg 2262230912
tracked amount in bundle 8192Mi

System pods on AdminNode memory resource request report: total 6876Mi
nodeCount 2 min 2174Mi max 4702Mi avg 3438Mi tracked amount in bundle
16384Mi

System pods on AdminMaster memory resource request report: total 465Mi
nodeCount 1 min 465Mi max 465Mi avg 465Mi tracked amount in bundle
16384Mi

SUCCESS

Cluster is healthy.

Next: Deploy user clusters.

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.