IBM Cloud Private Cloud Foundry - VMware, Network, DNS, PKI Certificates and LDAP Considerations

This document focuses on the following infrastructure considerations for an IBM Cloud Private v2.1 Cloud Foundry deployment:

- VMware
- Networking
- DNS entries
- PKI certificates
- LDAP configuration

NOTE: In this document IBM Cloud Private is referred to as ICP. IBM Cloud Private Cloud Foundry is often simply referred to as Cloud Foundry or CF.

NOTE: As the name implies IBM Cloud Private Cloud Foundry is packaged with IBM Cloud Private. However, Cloud Foundry is a completely distinct deployment and a completely distinct operational environment from an ICP deployment. (An ICP deployment provides a Kubernetes and Docker based managed cluster.)

NOTE: The December 2018 release of ICP Cloud Foundry will be using Cloud Foundry version 253. The Cloud Foundry documentation from cloudfoundry.org for version 253 can be used for ICP Cloud Foundry.

VMware considerations

This section describes recommendations about how to structure the VMware environment into which Cloud Foundry is to be deployed.

Recommendation: Each CF deployment should have its own VMware resource pool.

Recommendation: It is not a requirement that CF deployments to use a dedicated vCenter cluster but it is recommended. Create a separate VMware cluster dedicated to the CF deployment. Using a dedicated cluster for CF ensures complete isolation from other guests and environments deployed on the same VMware host systems. The user assigned to the CF deployment has admin access to the vCenter cluster that is dedicated to CF. Restrict access for that user to only the CF cluster. (The CF admin user does need read access to the vCenter

in order to monitor the status of tasks particularly during the CF installation.)

Cloud Foundry VMware resource requirements

The VMware system requirements for a single "enterprise" deployment of Cloud Foundry are described in the KC section VMware Size requirements for IBM Cloud Private Cloud Foundry enterprise installation

The CF infrastructure requirements for a Director, Cloud Foundry and Diego Management subtotal is:

Deployment	VMs	vCPU	Memory (GB)	Storage (GB)
CF infrastructure	29	94	252	2,000

The "standard" cell VM sizing is as follows:

vCPU	Memory (GB)	Storage (GB)
4	32	377

The number of cells to be deployed is needed to calculate the total resource requirements for a given CF deployment.

Horizontal application scaling

Horizontal application scaling for an application is achieved by specifying the number of instances for a given application using the `cf scale` command. See the CF documentation Scaling Horizontally.

NOTE: Application auto-scaling is not supported in the current release of ICP Cloud Foundry nor will it be supported in the December release.

High availability

The current release of IBM Cloud Private Cloud Foundry does not account for VM placement spread amongst available hypervisor hosts (ESXi hosts).

(TBD: The recommended HA deployment is multiple clusters. Need to get details. Is the CF HA topology similar to Bluemix Local HA topology? 3 clusters, each cluster with 3 hosts)

(TBD: What about HA for the singleton instances of the CF infrastructure?)

Networking considerations

A given Cloud Foundry deployment only needs a single VLAN. Separating VLANs for environment and applications is not necessary.

The number of IPs needed on the CF VLAN is at least 40. (It is common to assign a /24 network to a CF deployment. A /24 network allows for 254 usable IP addresses.)

Domain naming

Requirement: A Cloud Foundry deployment must have a minimum of two domain names specified in the CF configuration yaml file, one for environment and API support hosts (`bluemix_env_domain`) and one for application hosts (`bluemix_app_domain`). See the section below on DNS entries for more details.

Custom application domains can be added once the initial CF deployment has completed. (See the CF documentation on the `cf create-domain` command.) The custom application domains must be directed to a load balancer fronting the CF instance. TLS certificates for the custom application domains must be installed at the load balancer and the TLS connections are terminated at the load balancer. Traffic from the load balancer is routed to router/0 and router/1 in the CF instance.

DNS entries

The DNS configuration for Cloud Foundry is described in the Knowledge Center (KC) section, Configure Domain Name Service resolution IBM Cloud Private Cloud Foundry

Two DNS domains are defined: one for CF environment/infrastructure and one for applications. An A-record wild-card entry is created for each domain, e.g., `*.env.cf.myco.com` and `*.apps.cf.myco.com` . The IP address of the ha_proxy or a load balancer in front of the CF deployment is used as the IP address value of the DNS entry.

If a given DNS may have entries for more than one CF deployment, then the DNS names will obviously need to have some part of the name that differentiates among the CF deployments,

e.g., cfqa, cfprod.

Production CF deployments usually use a load balancer in front of the CF deployment rather than the ha_proxy.

When using a load balancer, the IP addresses of the router/0 and router/1 jobs need to be registered with the load balancer.

The `bosch vms` command can be used to get a list of VMs and their jobs. Find the router/0 and router/1 jobs in the command output and note their IP addresses.

The wildcard DNS entries are necessary in order to deploy CF buildpacks using `create_buildpacks.sh`.

If the original CF deployment uses values in the CF configuration yaml for the `bluemix_env_domain` and `bluemix_apps_domain` that are not the actual DNS entries, then update the CF configuration yaml with the actual DNS entries. The PKI certificates also need to be recreated with the wildcard host names that reflect the wildcard DNS entries. The base64 encodings of the certificates and keys need to pasted into the CF configuration yaml. Then the `launch_deployment.sh` script needs to be rerun.

Additional application domains may be added using the `cf create-domain` command line. When additional domains are created, an external load balancer needs to be used to terminate the TLS connections for the additional domains. The external load balancer then routes to the CF router/0 and router/1. (The ha_proxy is only capable of terminating TLS for the original env and apps domains.)

PKI certificates

The minimum certificate requirements for CF are described in the KC section, Providing certificates for IBM Cloud Private Cloud Foundry

The above documentation describes the use of `openssl` to create certificates in order to proceed with the CF installation.

Two wildcard certificates are needed, one for the environment/infrastructure domain and one for the application domain, e.g., `*.env.cf.myco.com` and `*.apps.cf.myco.com`.

Certificates are needed in order to do the CF deployment.

Certificates may be replaced after the CF deployment. When certificates are replaced, the

`launch_deployment.sh` needs to be run again. (After the first successful completion of `launch_deployment.sh` subsequent runs complete in about 45 minutes.)

LDAP configuration

LDAP authentication needs to be configured as part of the CF installation. A separate "custom" yaml file is included that defines the LDAP directory configuration.

The initial CF deployment does not need to include an LDAP configuration. However, at the point it is decided to include LDAP, the CF configuration yaml file needs to be updated; an LDAP configuration yaml file needs to be provided; and the `launch_deployment.sh` script needs to be run again. (After the initial CF deployment, subsequent runs of `launch_deployment.sh` take about 45 minutes.)

Links to KC sections for Cloud Foundry authentication are provided here: Configure authentication for IBM Cloud Private Cloud Foundry

LDAP configuration specifically is documented here: Configuring LDAP authentication for IBM Cloud Private Cloud Foundry