IBM Cloud Private v2.1 Network, DNS, PKI Certificates, LDAP

This document focuses on the following infrastructure requirements for ICP:

- Networking
- DNS entries
- PKI certificates
- LDAP configuration

Some of this information is needed to complete the configuration file (`config.yml`) for the ICP installation.

ICP networking

Two networks are declared in the ICP configuration (`config.yaml`).

- The IPv4 cluster network (`network_cidr`) Defaults to `10.1.0.0/16` . (`255.255.0.0`) (65534 IPs)
- The IPv4 service network (`service_cluster_ip_range`) Defaults to `10.0.0.1/24` . (`255.255.255.0`) (254 IPs)

The service network range must not conflict with the cluster network range.

The cluster network and the service network must not conflict with the native network the ICP cluster VMs are using.

The cluster network range is relatively large because every pod gets its own IP address.

It is recommended that all cluster VMs be deployed on the same sub-network.

The `cluster_lb_address` is the "cluster address" used to configure a load balancer that may sit in front of ICP cluster and the master nodes are deployed with multiple NICs. The `cluster_lb_address` gets assigned to the current master node.

The `proxy_lb_address` is the address used to configure a load balancer that may sit in front of the ICP cluster and the proxies are deployed with multiple NICs. The `proxy_lb_address` gets assigned to the currently active proxy.

A distinction is made between a cluster and proxy VIP and a cluster and proxy load balancer address because a VIP moves to a specific machine and is managed by UCARP or `etcd` and a load balancer spreads requests across all of the masters and all of the proxies. (Note that some master components can be clustered while some are singletons.) (TODO - Master load balancing needs more investigation. Clarify how a load balancer spreads requests for some services and not others.)

Firewalls

The ICP installer configures the native OS layer firewall with rules to allow the use of ports needed by the ICP components.

The default ports used by ICP components are listed here: ICP Default Ports

DNS entries

One or more wildcard DNS entries can be used to route requests to the proxy VIP.

Encrypted data/application networks

IPsec can be used for encrypting network traffic on the "data" network among ICP cluster nodes.

When IPsec is to be used all VMs need to be configured with 2 NICs:

- One for management (also may be referred to as the `system` network)
- One for secure networking among the pods (also may be referred to as the `application` or `data` network)

For more details see Encrypting cluster data network traffic with IPsec

By default, the certificates used for mutual authentication among the nodes are generated by the ICP installer and copied to each node. The certificates and keys may also be provided as described in the above reference. (TBD: The KC indicates that they need to be explicitly copied to each node and place in the appropriate places in /etc/ipsec.d/. Does the installer do that work as long as the certs and keys are provided as described below? Need to investigate.)

PKI certificates

The PKI certificates that get used for authentication to the ICP router and the private registry may be provided at installation time. (If they are not provided, the installer creates self-signed certificates.)

At installation time, the certificates and keys are expected to be in `<install_home>/cluster/cfc_certs`.

For step-by-step instructions when using a CA signed certificate see, Specifying your own Certificate Authority (CA) for IBM Cloud Private services

For production deployments in particular, or any deployment where CA signed certificates are used the Certificate Authority domain (`cluster_CA_domain`) must be specified in the `config.yaml` file. The value of `cluster_CA_domain` is a fully qualified domain name (FQDN).

LDAP configuration

The Knowledge Center has a good section of the configuration of LDAP. See Configuring LDAP Connection

With ICP v2.1.0.2 the LDAP used needed at least one group defined in it. This is likely something that will be corrected in later releases.

References

- ICP Knowledge Center: Customizing the cluster with the config.yaml file