OpenShift Networking

What's New in 4.8?

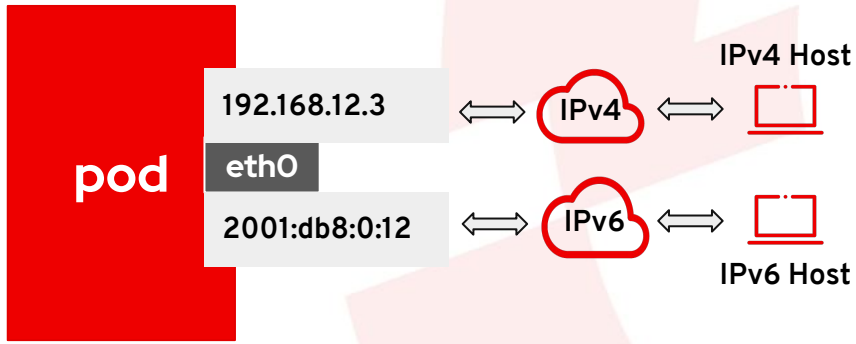
Marc Curry
Consulting Product Manager, OpenShift
Cloud Platform BU
2021-07-20

Topics

- IPv6
- New router configuration settings
- Netflow support for tracking and monitoring OVS flows
- CoreDNS and HAproxy upgrades
- OVN migration tooling
- SR-IOV NIC support
- Network Policy: audit logging of events
- Network Policy: MACVLAN interfaces

IPv6 Single / Dual Stack Support

- IPv6 single/dual stack is supported in OpenShift 4.8 (k8s 1.21) with OVN.
- **Single Stack**
  - Either an IPv4 or IPv6 address is assigned to the pod interface
- **Dual Stack**
  - Both IPv4 and IPv6 addresses assigned to the interface



- Simple install-time configuration
  - Modify "`install-config.yaml`" to specify IPv6 subnets in addition to IPv4.
- Post-install configuration:
  - Edit "`network.config.openshift.io`" config to add secondary "`(machine|cluster|service)Network`" values, and they will get rolled out correctly.
- Restrictions / Caveats / Notes
  - OVN *only*, no plans to support in openshift-sdn
  - Supported platform at GA: Bare Metal IPI (other platforms TBD)

Ingress / Egress Enhancements

Ingress Router (HAProxy)

HAProxy upgrade to 2.2 LTS:

- Performance
- Security hardening
- Health checks
- Observability, debugging and syslog over TCP
- SSL/TLS capabilities
  - 2048 bit
  - Dynamic SSL certificate storage

HAProxy Customization Enhancements:

- Supported HAProxy configuration parameters
  - ROUTER_USE_PROXY_PROTOCOL
  - ROUTER_BACKEND_PROCESS_ENDPOINTS
  - tune.maxrewrite [default = 8192]
  - tune.bufsize [default = 32768]
- Customizable number of router threads (nbthread)

Ingress / Egress Updates

IP Failover support (keepalived) for OpenShift HA.

Gateway API Developer Preview

- Ingress unifying technology
- Support for Contour as primary Ingress Controller for Gateway API traffic along with HAproxy
- Improved integration with Envoy / Service Mesh

Global Access option for GCP Ingress Internal LB to facilitate communication across cross-region shared VPC deployments.

EgressIP load-balancing enhancement for OpenShiftSDN to spread traffic across cluster nodes

- Removed single node "choke point"
- OVN enhancement in a future version

General Networking Enhancements

Network Observability

Network Observability

- Flows Tracking and Monitoring for Network Analytics
- A supported way to monitor and analyze flow traffic:
  - Monitor traffic in and out the cluster
  - Troubleshoot performance issues
  - Capacity planning
  - Security audits
- Support for enabling audit logging of Network Policy Events for regulatory and security policy compliance.

Hardware Enablement

SR-IOV NIC Support Enhancements

- Mellanox MT28800 Family CX-5 Ex
- Intel Columbiaville E810
- HPE Ethernet 10Gb 2-port 562SFP+ Adaptor

Security

Network Policy Support for MACVLAN interfaces

- Pods exposed externally, bypassing the SDN
- Improves performance/functional capability, but no routing layer in front of it to protect it
- New network policy support to protect traffic

Migration

OpenShift SDN to OVN Kubernetes CNI migration

- Support for all platforms
- IPI and now UPI
- Rollback capability
- Reboot required of all nodes

Security

Audit Logging of Network Policy Events

- Optionally audit Network Policy events (accept / deny)
- Present to built-in logging stack and custom Kibana dashboards
- IDS or post-mortem analysis

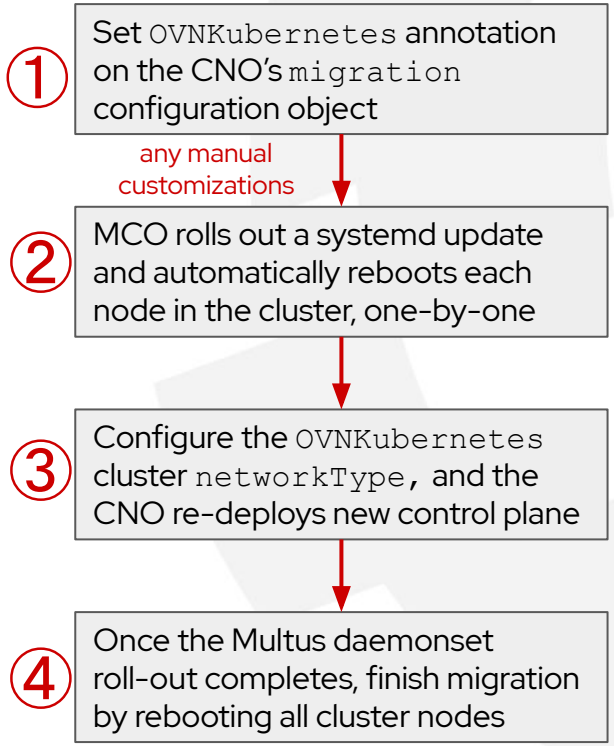
DNS

CoreDNS

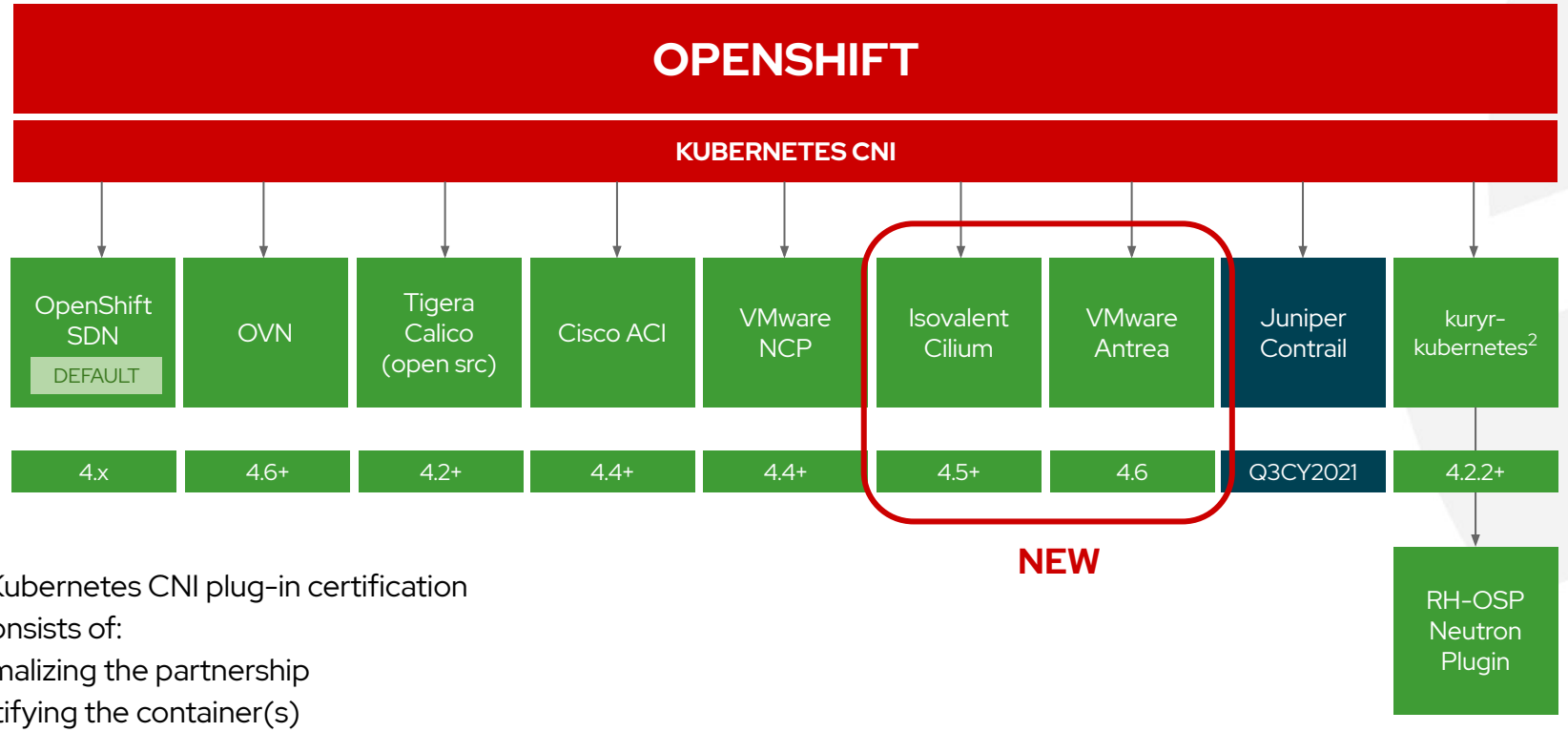
- Update to v1.8.z
- Control openshift-dns Pod Placement

OVN Migration Tooling

- OVN Migration support on all platforms supported by OpenShift.
- OpenShift 4.8 adds support for UPI installation-mode clusters, in addition to IPI.
- During the migration, all the nodes in a cluster need to be rebooted twice which may result in a brief service outage during the migration.
- The serial nature of the first reboot (currently) causes migration time to increase with the size of the cluster.
- The only CNI plugin migrations supported are:
  - openshift-sdn to ovn-kubernetes
  - ovn-kubernetes to openshift-sdn
- In 4.8, ovn-kubernetes switched from local to shared gateway mode, requiring the migration procedure to be split into two distinct phases, split between the Machine Config Operator (MCO) and Cluster Network Operator (CNO).
- Roll-back is supported, with a slightly different procedure.



OpenShift Certified Kubernetes CNI Plugins



3rd-party Kubernetes CNI plug-in certification primarily consists of:

1. Formalizing the partnership
2. Certifying the container(s)
3. Certifying the Operator
4. Successfully passing the same Kubernetes networking conformance tests that OpenShift uses to validate its own SDN

Fully Supported | Tech Preview | Cert In-Progress

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat