Hewlett Packard
Enterprise

Helion OpenStack Carrier Grade 4.0

RELEASE NOTES

4.0

Helion OpenStack Carrier Grade 4.0

Release Notes

Contents

1

Helion OpenStack Carrier Grade 4.0 Release Overview

Helion OpenStack Carrier Grade 4.0 is a high-performance, high-availability, cloud operating system that enables telecommunications operators to use Commercial-off-the-shelf (COTS) hardware to manage Virtualized Network Functions (VNF) within a carrier grade Network Function Virtualization (NFV) architecture.

Helion OpenStack Carrier Grade 4.0 brings together the flexibility and scalability of the IT cloud, and the high-availability and performance demanded by the Telecommunications industry, into a unique carrier grade, industry-leading solution to deliver a price-performance ratio well above alternative solutions. Helion OpenStack Carrier Grade 4.0 is aligned with the ETSI-NFV architecture

For more information on using Helion OpenStack Carrier Grade 4.0, see the *Helion OpenStack Carrier Grade 4.0 Software Installation Guide* and the *Helion OpenStack Carrier Grade 4.0 Administration Guide*. For information on using the Helion OpenStack Carrier Grade 4.0 Developer API, including API definitions and usage descriptions, see the *Helion OpenStack Carrier Grade 4.0 SDK* in the file **Helion OpenStack Carrier Grade 4.0-SDK.tgz**.

Supported System Configuration

Helion OpenStack Carrier Grade 4.0 has been verified to work using the following system configuration:

- two (2) controllers
- up to eight (8) storage nodes
  - up to eight OSDs per storage node
- up to 100 compute nodes with dual Intel(R) Xeon(R) CPUs

NOTE: For predictable performance, it is recommended to disable hyper-threading in the BIOS of all nodes in the cluster

- up to 1000 virtual machine instances (10 VMs per compute node on average; max 20 VMs per compute node)
- maximum eight vNICs per guest
- The following has been validated for parallel VM launches. For more information, refer to the *Helion OpenStack Carrier Grade 4.0 System Engineering Guidelines*.
  - Up to 80 VMs using local storage over 10 compute nodes.
  - Up to 40 VMs using Cinder volumes backed by the storage node. A single raw cached image used.
  - Up to 10 VMs using Cinder volumes backed by the controller cinder backend.

For information about the minimum system requirements for Helion OpenStack Carrier Grade 4.0, refer to the installation guide for your Helion OpenStack Carrier Grade 4.0 configuration.

Supported Guest OSs

The following Guest OSs are supported by Helion OpenStack Carrier Grade 4.0:

- Wind River Linux 5.0
- Wind River Linux 6.0
- CentOS 6.4
- CentOS 7
- RHEL 6.5
- RHEL 7.2
- OpenSUSE 11.3
- OpenSUSE 12.3
- Ubuntu 14.04

Requirements for specific guest OSs are included in the SDK README files.

Supported SDN Controllers

For demonstration purposes, Helion OpenStack Carrier Grade 4.0 currently supports integration with the OpenDaylight SDN controller running the Beryllium release.

Security Recommendations

- The HTTPS X.509 certificate that Helion OpenStack Carrier Grade 4.0 uses for authentication is not signed by a known authority. For increased security, obtain, install, and use a certificate that has been signed by a certificate authority.

Upgrade Notes

In-service upgrades are supported for Helion OpenStack Carrier Grade 4.0 R2 / 15.12. For more information, refer to the *Helion OpenStack Carrier Grade 4.0 Software Management Guide*.

2

Changes in This Release

This release of Helion OpenStack Carrier Grade 4.0 includes a number of performance enhancements and additions to functionality.

Enhancements

- **Platform**
  - New host OS based on CentOS 7
  - OpenStack up-versioned to Mitaka
  - DPDK up-versioned to DPDK 2.2
  - Support for UEFI boot
    - Improved hardware feature support over traditional BIOS booting
  - Support for Patching Orchestration
  - - Automated installation of patches across the Helion OpenStack Carrier Grade 4.0 system, while migrating VMs or stopping and starting them to maintain hosting service
  - Support for In-Service Patches
    - Depending on patch changes, may be applied to a running system without locking or rebooting hosts
  - Support for in-service software upgrade of Titanium Software from one major release to the next major release
    - Manages upgrades of all platform software: host OS, OS packages, OpenStack and Helion OpenStack Carrier Grade 4.0specific features
    - Executes a rolling upgrade of Titanium Software across all nodes of system
    - Manages API compatibility between nodes at release N and release N+1
    - Deals transparently with database schema changes and database data conversion
    - Live-migrates hosted applications during upgrade for deployed VMs that can support it (otherwise uses cold migration)
  - Support for multi-region OpenStack cloud deployments

    - Support for multi-region Helion OpenStack Carrier Grade 4.0 deployment
    - Support for multi-region mixed 3rd-party or open-source OpenStack cloud and Helion OpenStack Carrier Grade 4.0 deployment
        - Support for extending an existing 3rd-Party or open-source OpenStack cloud using a Secondary Region Helion OpenStack Carrier Grade 4.0 deployment, to leverage Helion OpenStack Carrier Grade 4.0 extensions incrementally in an integrated fashion

- **Increased Scalability**
    - Supports a maximum configuration of up to 100 compute nodes per system
        - 2x controller nodes
        - 8x storage nodes
        - 100x compute nodes
            - Average of 10 VMs per compute node
    - For multi-region configurations, please discuss use cases with Wind River.
- **Security**
    - Support for Remote CLI
        - Support for using Helion OpenStack Carrier Grade 4.0-extended OpenStack CLIs remotely
        - controller SSH login privileges no longer required for CLI access
        - HTTP and HTTPS modes supported
        - Delivered as SDK module with installer script for installation on remote server
    - Improved operator-command audit logging
        - All non-passive operator commands on system are now logged
    - Improved login authentication logging
        - All login attempts (success and failure) are logged, including horizon logins and ssh logins as well as internal local LDAP and internal database login attempts
    - Improved user and password management
        - Temporary lockout of Horizon user after a configurable number of failed login attempts
        - Increased complexity requirements on Linux user passwords (minimum length, at least one number, at least one capital letter, and at least one special character)
        - wrsroot password aging (in addition to already supported non-wrsroot Linux user-password aging)
- **Fault and Performance Management**
    - Merged alarm history and log list in Horizon, CLI and REST API
        - Provides a more usable single list of customer historical events (set/clear customer alarms and customer logs)
    - Horizon global alarm banner
        - Alarm counts visible on every Horizon page
    - Provider Network Topology view

  - Graphically displays host provider network topology
  - Includes alarm information for visualizing and diagnosing issues
- Alarm Suppression
  - Provides ability to suppress notifications for particular Alarm IDs
  - Suppressed alarms are hidden in the Active Alarm and Historical Events lists, and not included in global alarm banner counts
- Remote ELK-based log server support
  - Support for pushing system logs, including expert-level troubleshooting logs, customer logs, and alarms, to an external centralized ELK-based log server
  - Allows leveraging of Elastic ELK Stack Tools for fast and easy analysis of logs, report generation, and so on
  - SDK module provided for simple sample installation of ELK server on a remote server

- **Storage**
  - Support for adding CEPH after installation
  - Support for remote ephemeral storage (Nova storage) using CEPH as the backend
  - Support for up to eight storage nodes
    - Deployed in 1:1 node pairs
    - Up to eight OSDs per node
  - Support for CEPH SSD-backed journals for improved speed; transparent to VMs
    - Uses large, less-expensive, slower SATA or SAS disks as OSDs, and partitions on separate fast SSD disks for journalling and as a small cache
  - Support for Ceph cache tiering for a larger-scale cache solution and enhanced speed improvements; transparent to VMs
    - Uses dedicated pairs of SSD-populated storages nodes as a Ceph cache in front of standard SATA/SAS-populated storage nodes
  - Support for Glance using higher-speed infrastructure network, if present, for improved performance on image operations
  - Support for SWIFT Object Storage services, using Ceph as the backend
- **Networking**
  - AVS support for vhost-user
    - Improved networking performance for VMs with standard virtio NICs using vhost-user, with optional multi-queue support for virtio interfaces
  - Improved distributed scheduling of neutron routers
    - More intelligent scheduling of routers and DHCP agents across compute nodes
    - Improved balancing algorithm and dynamic re-balancing on change to state or number of compute nodes
  - Link Layer Discover Protocol (LLDP) peer discovery and reporting to verify cabling to the next hop device (for example, TOR switch)

  - AVS now supports sending and receiving of LLDP messages on all physical interfaces
  - LLDP information (far-end switch name, far-end switch port, and so on) received by each compute node interface is displayed in Horizon Inventory panels and system CLI
- Automated provider network connectivity tests and alarms to identify provider network connectivity issues between compute nodes
- Support for SDN networking technology
  - See detailed SDN Support section in subsequent section of these Release Notes.

- **VM Scheduling and Support**
  - Compute Node platform utilization-aware VM scheduling
    - VM Scheduling now considers the CPU loading and memory utilization of the platform
    - Prevents scheduling a VM on a host whose platform cores or memory are over-utilized
- **Usability**
  - Customer documentation has been restructured to offer documents with improved focus
  - GUI panel and tab organization revised for improved usability

Deprecation Notices

Interface consolidation

- The following interface consolidation combinations on the same physical or LAG interface are deprecated in R3 (that is, they are still supported in R3, but support is planned to be removed in R4):
  - OAM + MGMT + INFRA + DATA
  - OAM + MGMT + DATA
  - OAM + INFRA + DATA
  - MGMT + INFRA + DATA
  - OAM + DATA
  - INFRA + DATA
- Support continues for the following interface consolidation combinations on the same physical or LAG interface:
  - OAM + MGMT
  - MGMT + INFRA
  - OAM + MGMT + INFRA

Keystone CLI

- The keystone CLI has been deprecated and is no longer supported for Identity v3. Use the Openstack unified CLI instead.

A Note on SDN Support in this Release

Helion OpenStack Carrier Grade 4.0 provides an OpenFlow v1.3 interface for integration in data centers that use software defined networking (SDN) as the networking backbone.

This feature is provided for evaluation purposes.

3

Usage Caveats

There are some usage issues you should be aware of when working with this release.

15.12 ini files are not forward compatible with 16.10

Files must be updated to include two new mandatory keys: MULTICAST_CIDR for MGMT_NETWORK & OAM_NETWORK. The VERSION field must be updated to 16.10.

For HP ProLiant GEN 9 Servers

For HP ProLiant GEN 9 servers, turn off RMRR requests in the BIOS before installing or upgrading to this software release. Contact the hardware vendor for more details on the upgrade procedure.

The minimum firmware version required for Fortville NICs is NVM version 5.04

Please upgrade the firmware before installing or upgrading to this software release. Contact the hardware vendor for more details on the upgrade procedure.

Swift Containers and Objects are not saved as part of Backup

Contact Wind River for a manual procedure to re-create swift stores post restore.

The auto recovery property in the image metadata is ignored

To turn auto recovery off for instances booting from volume, set the auto recovery property in the flavor instead.

VMs reported as ACTIVE before compute nodes are recovered

During a system recovery (for example, after a site power outage), when the controller is available but before the compute nodes are available, the Nova service shows an **Active** status for VMs . Until the compute nodes are available, this should be an **Error** status.

Mismatch of interface settings in LAG group

If the interfaces in a LAG group have mismatched speed or duplex settings, they are marked as incompatible by the system. To prevent this, ensure both interfaces in a LAG group use the same speed and duplex settings.

A node must be re-installed after MAC address change on management interface

Any change to the management interface configuration that results in a change of MAC address requires the node to be re-installed. The management interface MAC address can change if the physical Ethernet port is changed (for example, from enpos8 to enpos9), or if a LAG configuration is changed in a way that removes the Ethernet port associated with the LAG MAC address (for example, if the interface originally used for PXE boot is removed or replaced).

Neutron security groups are not stateful for ICMP protocol

If a security group does not explicitly allow ingress for ICMP, then incoming responses to outgoing packets using ICMP are blocked. This is in contrast to the OpenStack implementation, where response packets are allowed regardless of ingress rules.

Hypervisor CPU usage is reported using special notation

Partial vcpu notation (y.x) is adopted to show shared and dedicated vpcu model usage on the same compute node.

4

Known Problems and Limitations

You may encounter some known limitations when working with this release.

Upgrades Notes / Limitations

- System must be fully provisioned before starting the upgrade
- Verify that installation parameters are correct on controller-0
  - The installation parameters for controller-0 may have default values, which may be incorrect for your system. Before upgrading, ensure that the installation parameters for controller-0 are accurate for your configuration. The **system host-show controller-0** command will display the installation parameters. The boot_device, rootfs_device, console, and install_output parameters may need to be updated. These values can be updated with the **system host-update controller-0** command.
- After upgrades, VMs using VIRTIO are not automatically updated to use vhost-user as a backend. The VMs have to be re-launched to make use of vhost-user.

Interface or interface consolidation limitations

- Consolidation of a management or PXE boot interface over a bonded data interface is not supported.
- Consolidation of a data VLAN over a bonded management or PXE boot interface is not supported.
- Consolidation of a management VLAN over a bonded data interface is not supported.
- Stacked VLANs are not supported. On a consolidated management or infrastructure interface, a VLAN provider network can be associated directly with the untagged interface. Flat or VXLAN provider networks must be associated with a consolidated VLAN data interface.
- Unaccelerated data interfaces are only supported over ethernet interfaces without interface consolidation or LAG.

Mellanox limitations

- For a Mellanox CX3, all ports must be used either for data interfaces, or for non-data interfaces. It is not possible to use some ports for data interfaces and others for non-data interfaces on the same Mellanox CX3 NIC.

Other limitations

- Setting promisc mode on/off on a Fortville port causes the link to go down, then come back up. This may result in a host reboot if the port in question is used for the management interface. This is a known driver issue.
- **vhost-user** is not supported for VM's backed by 4K memory pages.
- The maximum swift file upload from horizon is limited by the free space in the /scratch filesystem.
- Only 10 VMs with ephermeral and swap disks can be launched in parallel.
- Initial swift container creation fails intermittently. Try the operation again.
- Host aggregrates for provider networks are not deleted automatically upon the deletion of the last provider network in the aggregate group.
- When using two NUMA nodes for the guest, the flavor must specify an even number of vCPUs, or specify the number of vCPUs for each NUMA node.
- A resize operation fails when attempting to resize an instance to a flavor if the number of vCPUs cannot be evenly divided across the number of virtual NUMA nodes