Stratus Cloud Solution

Installation Guide

Stratus Technologies
For an Always-On World
www.stratus.com

Notice

The information contained in this document is subject to change without notice.

UNLESS EXPRESSLY SET FORTH IN A WRITTEN AGREEMENT SIGNED BY AN AUTHORIZED REPRESENTATIVE OF STRATUS TECHNOLOGIES, STRATUS MAKES NO WARRANTY OR REPRESENTATION OF ANY KIND WITH RESPECT TO THE INFORMATION CONTAINED HEREIN, INCLUDING WARRANTY OF MERCHANTABILITY AND FITNESS FOR A PURPOSE.

Stratus Technologies assumes no responsibility or obligation of any kind for any errors contained herein or in connection with the furnishing, performance, or use of this document. Software described in Stratus documents (a) is the property of Stratus Technologies Bermuda, Ltd. or the third party, (b) is furnished only under license, and (c) may be copied or used only as expressly permitted under the terms of the license.

Stratus documentation describes all supported features of the user interfaces and the application programming interfaces (API) developed by Stratus. Any undocumented features of these interfaces are intended solely for use by Stratus personnel and are subject to change without warning.

Copyrights

Manual Name: Stratus Cloud Solution Installation Guide

Product Release Number: Stratus Cloud Solution Release 1.5.0.0

Publication Date: Wednesday, February 11, 2015

Stratus Technologies, Inc.

111 Powdermill Road

Maynard, Massachusetts 01754-3409

Table of Contents

1

Chapter 1: Stratus Cloud Solution Installation Guide

This installation guide does not intend to provide a one-stop solution to all the issues in a production-grade cloud, but serves as guide to be used as a baseline for building the production OpenStack Stratus Cloud Solution.

This guide also provides technically knowledgeable field engineers with an option to set up a production-grade OpenStack cloud with all the features that are required for and supported by the Stratus Cloud Solution. The architecture of this implementation can be extended or simplified to meet your requirements.

Related Topics

"Stratus Cloud Solution Installation Overview" on page 2

"OpenStack Overview" on page 2

"Stratus Cloud Solution Hardware Overview" on page 4

"Stratus Cloud Solution Software Overview" on page 8

"OpenStack Installation and Configuration" on page 14

"OpenStack Verification and Testing" on page 26

"Installing the Stratus Cloud Solution" on page 29

"Installing Stratus Cloud Availability Services" on page 63

Stratus Cloud Solution Installation Overview

The Stratus Cloud Solution Solution (SCS) enables IT administrators to efficiently implement and manage a multiple availability level cloud, including support for highly available legacy applications. This allows IT administrators to provide an intuitive service catalog and application administration for end users.

OpenStack installation and configuration is not always an easy task. Each OpenStack installation is unique by virtue of the workload it intends to support, the differences in hardware and networking, and the security and compliance requirements. Note that SCS is deployed as a virtual appliance, which can be deployed as an instance (a virtual machine managed in the OpenStack cloud), or as a virtual machine, managed by a specific hypervisor.

Related Topics

"OpenStack Overview" on page 2

OpenStack Overview

OpenStack is a group of interrelated open-source projects designed to provide massively scalable public and private clouds. The following services and projects are used throughout this document.

Service	Project Name	Description
Dashboard	Horizon	Allows you to interact with OpenStack services to launch an instance, assign IP addresses, set access controls, and other parameters.
Compute	Nova	Provisions and manages large networks of virtual machines on demand.
Networking	Neutron	Enables network connectivity as a service among interface devices managed by other OpenStack services; usually Compute. Allows you to create and attach interfaces to networks. Neutron features a plugable architecture that supports many popular networking vendors and technologies.
Object Storage	Swift	Stores and gets files. Does not mount directories like a file server.

Service	Project Name	Description
Block Storage	Cinder	Provides persistent block storage to guest virtual machines.
Identity service	Keystone	Provides authentication and authorization for the OpenStack services. Also provides a service catalog within a particular OpenStack cloud.
Image service	Glance	Provides a registry of virtual machine images; used by Compute to provision instances.
Telemetry service	Ceilometer	Monitors and meters the OpenStack cloud for billing, benchmarking, scalability, and statistics purposes.
Orchestration service	Heat	Orchestrates multiple composite cloud applications by using either the native HOT template format or the AWS CloudFormation template format, through both an OpenStack-native REST API and a CloudFormation-compatible query API.

Stratus Cloud Solution Hardware Overview

This section provides a general overview of hardware requirements and recommendations. Your exact hardware requirements should be calculated by the number of instances and resource needs of the workloads.

Related Topics

"Stratus Cloud Solution Hardware Requirements" on page 5

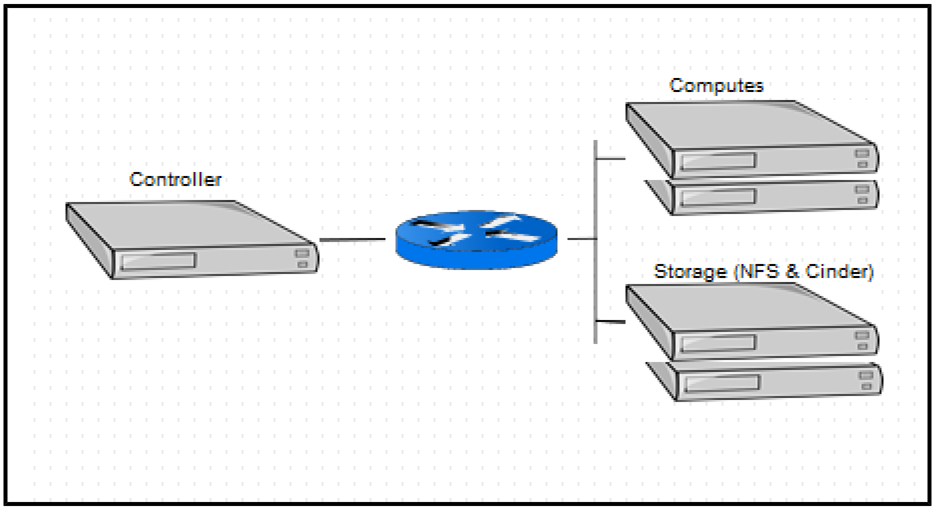
"Stratus Cloud Solution Hardware Recommendations" on page 4

Stratus Cloud Solution Hardware Recommendations

The Stratus Cloud Solution does not impose any hardware requirements. The Stratus Cloud Solution works with any OpenStack cloud implementation. However, Stratus recommends configuring redundancy into the hardware to mitigate downtime.

The minimum suggested OpenStack hardware configuration consists of a controller node that runs the OpenStack core services, and at least two compute nodes which host the workloads. Two compute nodes are required for failover purposes in order to make the instances highly available.

Shared storage is provided by NFS storage, and cinder node provides the block storage. A minimum deployment is shown in the following illustration.



Hardware requirements for the Stratus Cloud Solution are shown in the following table.

Node or Switch	Quantity	CPU	Memory	Storage	Example
Controller node	1	Intel Xeon E5 2.6 GHz 6-core	8 x16 GB	6 x 1 TB SATA	Supermicro CSE-119XTQ-BR 700 WB
Compute node	2	Intel Xeon E5 2.6 GHz 6-core	8 x16 GB	6 x 1 TB SATA	Supermicro CSE-119XTQ-BR 700 WB
Storage node	2	Intel Xeon E5 2.6 GHz 6-core	4 x16 GB	24 x 1 TB SATA	216BE26-R1K28LPB
Network switch	2	n/a	n/a	n/a	DCS-7050T-36-F

Note: The hardware models and configurations shown in the table are suggestions. You can select any vendor and configuration, though 10Gb switches are recommended. Stratus does not provide a warranty on the hardware.

Stratus Cloud Solution Hardware Requirements

OpenStack Services on the Controller

OpenStack projects can be configured to run on separate nodes. However, for simplicity and maintainability, the core projects (namely Horizon, Keystone, and Glance) are deployed on a single node. Neutron typically is configured to run on a separate node and requires high bandwidth. This installation bundles Neutron services on the same controller node.

Block Storage or Cinder node

Block storage (Cinder) is configured on separate node clusters with expandable storage.

Cinder resiliency must be supplied by your Cinder storage solution, especially if you deploy mission-critical applications.

A 10Gb storage network is recommended for best performance and reliability.

Compute nodes

Compute nodes:

- Provide CPU and memory for the instances
- Require many CPU cores and memory
- Can be horizontally scaled as your application needs grow

The following example shows typical calculations for determining your exact hardware compute node requirements.

Application Requirements:

- Instances to run: 100
- vCPUs/Instance: 2
- Memory/Instance: 4 GB
- Oversubscription: No

These application requirements translate to:

- CPU Requirements
  - 200 GHz of CPU capacity (100 virtual machines x 2 GHz/vCPU)
  - Approximate maximum: five cores (16 GHz / 2.4 GHz per core)

  Based on:

  - E5 2640 sockets (200 GHz / 2.4 GHz per CPU / six cores per socket)
  - 5 - 6 dual-core servers (11 sockets / two sockets per server)
  - 17 virtual machines per server (100 virtual machines / six servers)
- Memory Requirements
  - Approximately four 128 GB machines (400 GB / 128 GB; balanced with six machines for CPU)
  - To support 400 GB of total memory (100 virtual machines * 4 GB per virtual machine)
- Cent OS 6.5 Image Requirements
  - The image used for the Stratus appliance installation must provide at least 160 GB of root space.

    - To accomplish this, the QCOW2 file must have a virtual size of greater than or equal to 160 GB, and the flavor used to create the virtual machine must specify greater than or equal to 160 GB of root space.

- Cent OS Hardware Requirements

    - A minimum of 8192MB of RAM is required.

    - A minimum of four vCPUs is required.

Stratus Cloud Solution Software Overview

This section provides a general overview of software requirements, versioning, and recommendations.

> **Note**: Without the recommended software minimums, node evacuation will not work.

Related Topics

"Required Software" on page 8

"Required OpenStack Components" on page 10

"Supported Internet Browsers" on page 9

"Supported Operating Systems" on page 9

Required Software

The following software with the specified version number is required for the proper installation and operation of Stratus Cloud Solution.

Software	Version
IceHouse	1.3
MySQL Server	5.1.73
Python	2.6.6
Apache	2.2.15
Openvswitch	1.11.0
Puppet	3.7.0
Rabbitmq-server	3.1.5
Memcached	1.4.4
Libvirt	0.10.2
Python mod_wsgi	3.2.6

Supported Internet Browsers

The following table lists the supported operating systems and browsers.

Browsers

Browser	Version
Firefox (on Linux only)	27
Internet Explorer (Windows)	11
Firefox (Windows; Technology Preview only)	27
Google Chrome (Windows and Linux; Technology Preview only)	32.0

Supported Operating Systems

The following operating systems have been tested for deployment into a Stratus-managed OpenStack environment.

Windows Operating Systems

Operating System	Version
Windows Server 2008	R2
Windows Server 2012	R2

Linux Operating Systems

Operating System	Version
CentOS 64-bit	6.5
RedHat Enterprise	6.5
Linux Ubuntu	14.04

Operating System	Version
Fedora	20
SUSE	12.3

Required OpenStack Components

The OpenStack components and the version number required for proper installation and operation of Stratus Cloud Solution are listed as follows.

To find the versions currently running on your system, use the following command: `rpm -qa|grep <component name; for example: nova>`

Nova

Component	Version
OpenStack-nova-cert	1.1-3.el6
OpenStack-nova-conductor	1.1-3.el6
OpenStack-nova-common	1.1-3.el6
OpenStack-nova-novncproxy	1.1-3.el6
OpenStack-nova-scheduler	1.1-3.el6
Python-nova	1.1-3.el6
OpenStack-nova-console	1.1-3.el6
Python-novaclient	2.17.0-2.el6
OpenStack-nova-api	1.1-3.el6

Glance

Component	Version
Python-glance-client	0.12.0-1.el6
Python-glance	1.1-1.el6
OpenStack-glance	1.1-1.el6

Heat

Component	Version
OpenStack-heat-api-cfn	1.2-1.0.el6
OpenStack-heat-common	1.2-1.0.el6
OpenStack-heat-engine	1.2-1.0.el6
OpenStack-heat-api	1.2-1.0.el6
Python-heatclient	0.2.9-1.el6

Neutron

Component	Version
OpenStack-neutron	1.2-1.el6
Python-neutronclient	2.3.4-1.el6
Python-neutron	1.2-1.el6
OpenStack-neutron-openvswitch	1.2-1.el6
OpenStack-neutron-ml2	1.2-1.el6

Horizon

Component	Version
Python-django-horizon	1.1-4.el6

Cinder

Component	Version
OpenStack-cinder	1.1-3.el6
Python-cinder	1.1-3.el6
Python-cinderclient	1.0.9-1.el6

Keystone

Component	Version
Python-keystone	1.1-1.el6
OpenStack-keystone	1.1-1.el6
Python-keystoneclient	0.9.0-1.el6

RabbitMQ

Component	Version
rabbitmq-server	3.3.1-1

Sample Network Design

The following table shows the networks configured in this implementation. This installation further assumes that the networks are configured using VLANs on the bonded *eth1* interface, and that *eth0* is the administrative network.

Purpose	Is routed?	Network Name	Examples
Provides IPMI and SSH connectivity. This network is only available within the data-center.	Yes	Admin net	192.168.81.0/24
Routed network to access OpenStack APIs.	Yes	API net	192.168.82.0/24
Routed network that provides connectivity to the floating IPs assigned to the virtual machines.	Yes	External net	192.168.83.0/24
OpenStack internal messageQ communication non-routed network.	No	MGMT net	10.200.10.0/24
OpenStack virtual machine to virtual machine communication non-routed network.	No	Data net	10.10.1.0/24
OpenStack cinder and NFS storage non-routed network.	No	Cinder storage	10.200.11.0/24

Provider Networks

Provider networks allow cloud administrators to create OpenStack Networking networks that map directly to physical networks in the data center. The Provider networks are the backbone of a virtual network(s) which maps virtual network to physical network. In the Stratus, the provider network is the externally-routed network.

OpenStack Installation and Configuration

This section provides information for installations and configurations required for your OpenStack and Stratus Cloud Solution systems.

Note: Stratus labs are currently using CentOS 6.5. Unless otherwise stated, assume CentOS 6.5 as the operating system running on the systems.

Related Topics

"Heat Installation Prerequisites and Processes" on page 14

"Installation Overview Flowcharts" on page 15

"Physical Connectivity" on page 16

"Storage Considerations" on page 17

"Managing OpenStack Quotas" on page 17

"Configuring OpenStack for Evacuation and Migration" on page 19

"Supporting Instance Evacuations" on page 22

"Addressing Installation Errors" on page 23

"GRE Network Configuration" on page 24

"MySQL Connections" on page 24

Heat Installation Prerequisites and Processes

The following customer requirements and Heat procedures are required for the installation of the Stratus Cloud Solution.

Customer Site Requirements

For the installation of Stratus Cloud Solution, the customer must have:

- An installed and functioning Ice House version of OpenStack
- Heat enabled for cloud installation and operation
- A CentOS 6.5 image in Glance
- Internet access enabled from within the cloud

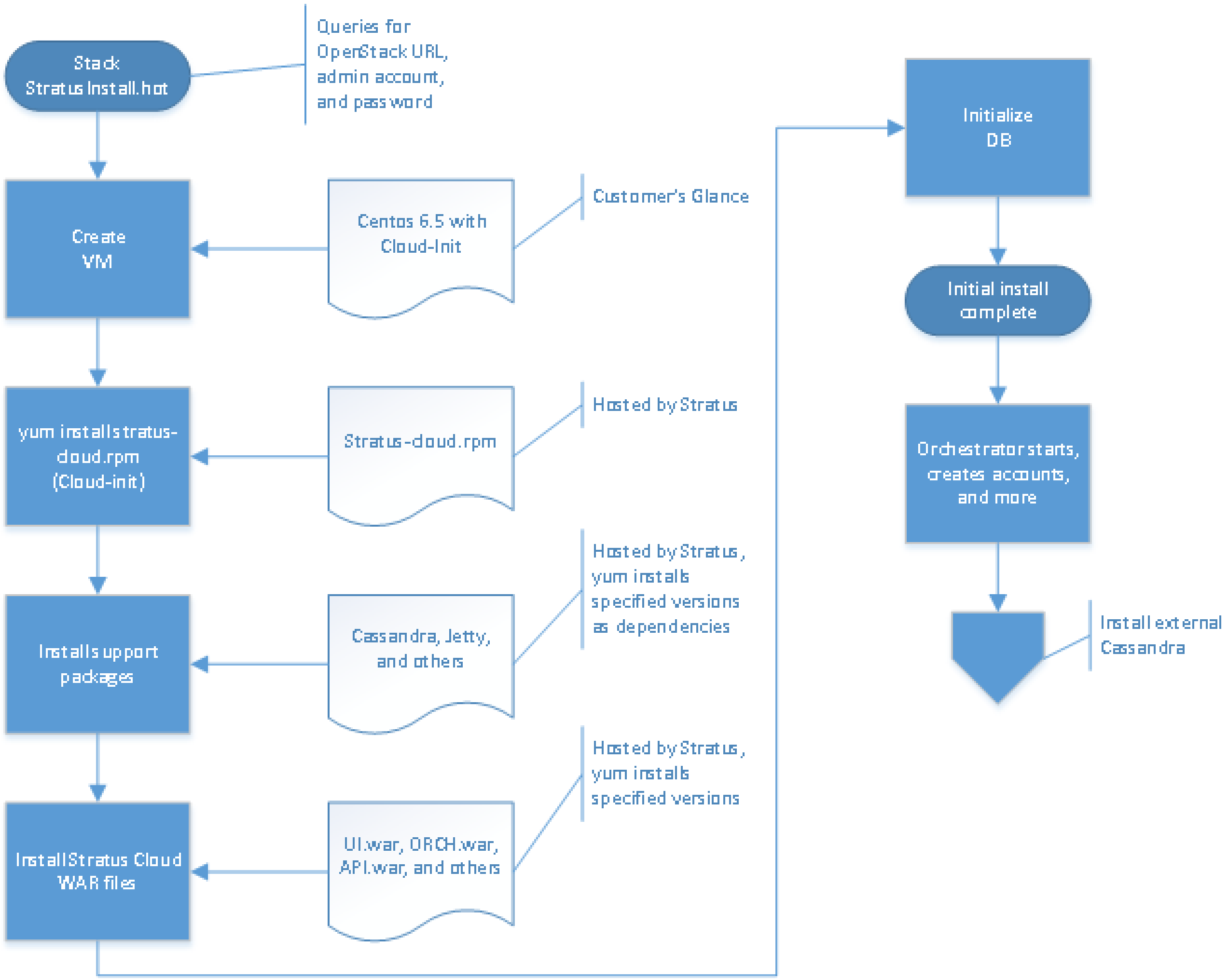
See also:

"Installation Overview Flowcharts" on page 15

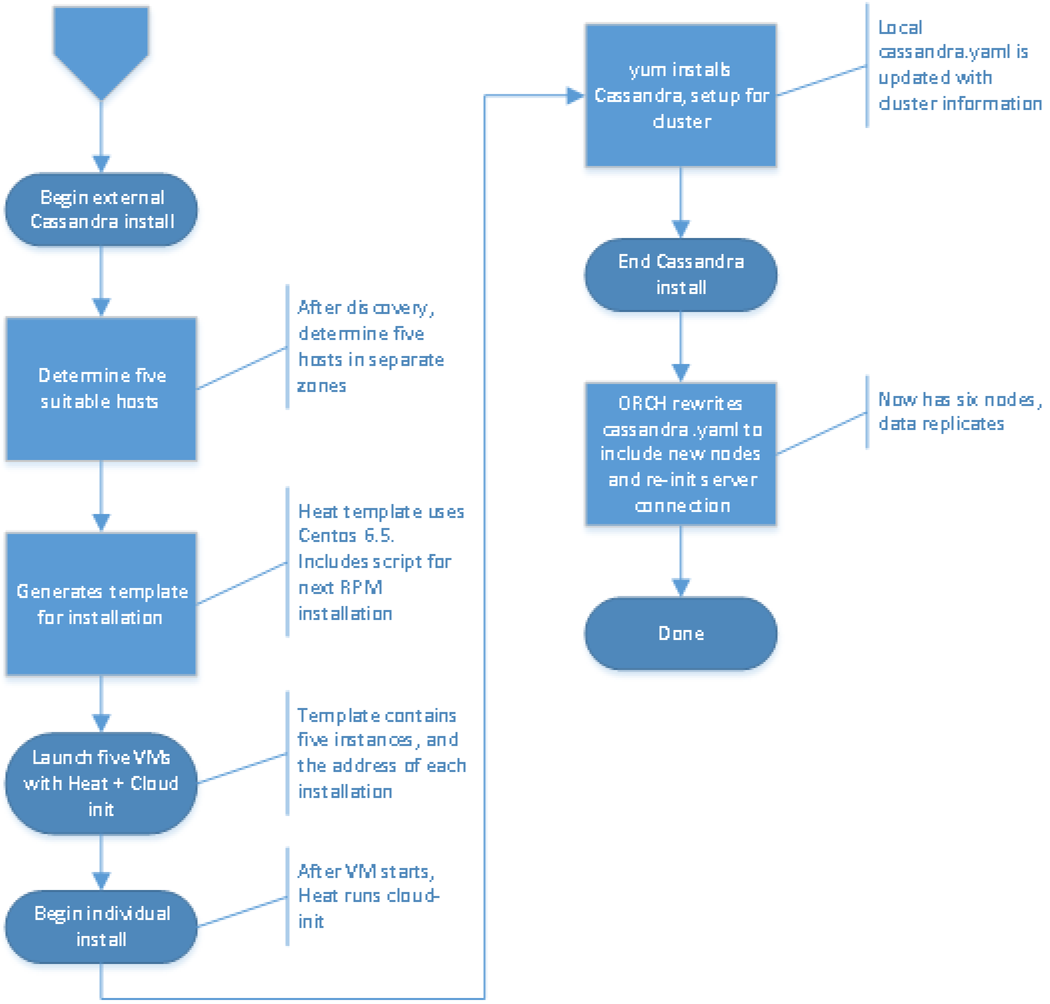
Installation Overview Flowcharts

Installing the Stratus Cloud Workload Servicesis a two-step process. The following flowcharts illustrate both steps of the Stratus Cloud Workload Services installation procedure.

Step 1:


Stack
Stratus Install.hot
Queries for OpenStack URL, admin account, and password
Create VM
Centos 6.5 with Cloud-Init
Customer's Glance
yum install stratus-cloud.rpm (Cloud-init)
Stratus-cloud.rpm
Hosted by Stratus
Install support packages
Cassandra, Jetty, and others
Hosted by Stratus, yum installs specified versions as dependencies
Install Stratus Cloud WAR files
UI.war, ORCH.war, API.war, and others
Hosted by Stratus, yum installs specified versions
Initialize DB
Initial install complete
Orchestrator starts, creates accounts, and more
Install external Cassandra

Step 2:


Begin external Cassandra install
Determine five suitable hosts
After discovery, determine five hosts in separate zones
Generates template for installation
Heat template uses Centos 6.5. Includes script for next RPM installation
Launch five VMs with Heat + Cloud init
Template contains five instances, and the address of each installation
Begin individual install
After VM starts, Heat runs cloud-init
yum installs Cassandra, setup for cluster
Local cassandra.yaml is updated with cluster information
End Cassandra install
ORCH rewrites cassandra.yaml to include new nodes and re-init server connection
Now has six nodes, data replicates
Done

See also:

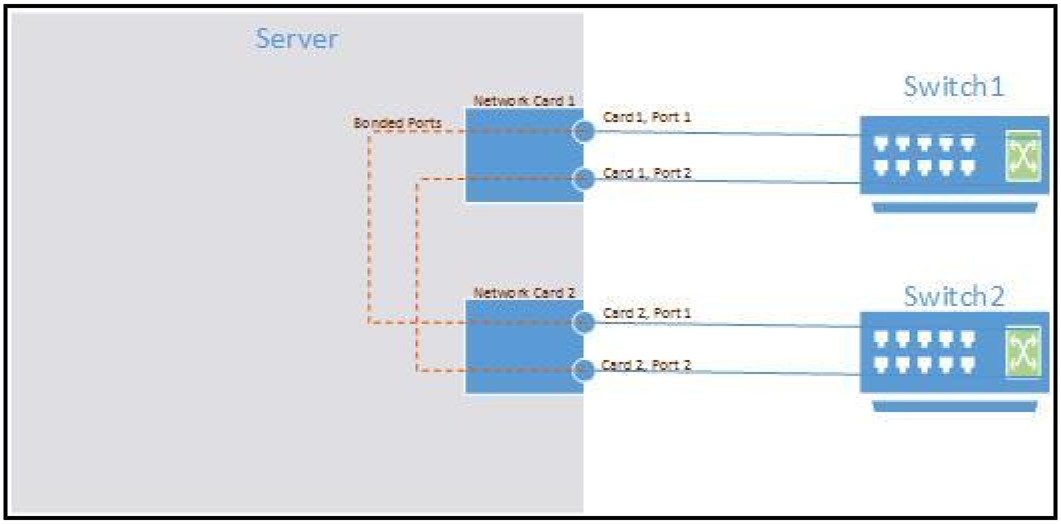
"Heat Installation Prerequisites and Processes" on page 14

Physical Connectivity

In order to achieve highest level of availability, the physical network connectivity must be redundant. The following is a non-exhaustive list of suggestions recommended by Stratus:

- Hardware configuration should include at least two NICs, with enough ports in the card to support your networking requirements.
- Bond two ports from two different physical cards to protect against NIC port and NIC failure.
- Connect each port of the server bonded network to separate switches to protect against switch failures.

In the following diagram, the server contains two network cards; each card has two ports. The ports are marked as Card1Port1 through Card2Port2. Bond Card1Port1 and Card2Port1, and connect the ports to two separate switches.



For the switch configuration, configure VLANs on the switch matching a similar configuration to the one in "Sample Network Design" on page 12. Assign a temporary IP address, and verify network connectivity.

Storage Considerations

Stratus recommends the following considerations when setting up your storage environment.

- Protect the boot volume with either RAID 5 or RAID 6. A single disk boot volume can result in system failure (and failure of all instances) if the disk fails.
- Shared storage should be highly available, as all instances live on the shared storage.
- Cinder block shared storage should be highly available. Unless a high-end storage solution is used in the backend, the disks must at least be RAID 5 or 6 for physical disk failures protection.
- Use a 10Gb storage network for best performance and reliability.

Managing OpenStack Quotas

This topic is under construction.

To prevent OpenStack system resources from being exhausted, you must modify the quotas that you set for each tenant to allow for the additional demands of applications that you will deploy with Stratus Cloud Workload Services.

OpenStack enforces quotas that control resources for the Nova (compute), Neutron (networking) services, and Cinder (block storage) services. For example, Nova quotas control the number of instances and the number of cores and amount of RAM available to each tenant's applications. Neutron quotas control the number of networks, ports, and subnets. (There is some overlap in quotas between Nova and Neutron, but Neutron quotas always take precedence.) Cinder quotas control the amount of storage space and number of volumes and snapshots per tenant.

To view the Nova quotas, open the console of your OpenStack controller and execute `nova quota-defaults`. For example:

```
$ nova quota-defaults

+-----------------------------+-------+

| Quota                       | Limit |

+-----------------------------+-------+

| instances                   | 10    |

| cores                       | 20    |

| ram                         | 51200 |

| floating_ips                | 10    |

| fixed_ips                   | -1    |

| metadata_items              | 128   |

| injected_files              | 5     |

| injected_file_content_bytes | 10240 |

| injected_file_path_bytes    | 255   |

| key_pairs                   | 100   |

| security_groups             | 10    |

| security_group_rules        | 20    |

+-----------------------------+-------+
```

To view the Neutron quotas, open the console of your OpenStack controller and execute `neutron quota-list`. For example:

```
$ neutron quota-list

+------------+---------+------+--------+--------+-------------------

----------------+
| floatingip | network | port | router | subnet | tenant_id
               |
+------------+---------+------+--------+--------+------------------
----------------+
|         20 |       5 |   20 |     10 |      5 |
6f88036c45344d9999a1f971e4882723 |
|         25 |      10 |   30 |     10 |     10 |
bff5c9455ee24231b5bc713c1b96d422 |
+------------+---------+------+--------+--------+------------------
----------------+
```

To view the Cinder quotas, open the console of your OpenStack controller and execute `cinder quota-defaults`. For example:

```
$ cinder quota-defaults TENANT_ID
```

```
+-----------+-------+
|  Property | Value |
+-----------+-------+
| gigabytes |  1000 |
| snapshots |   10  |
|  volumes  |   10  |
+-----------+-------+
```

Configuring OpenStack for Evacuation and Migration

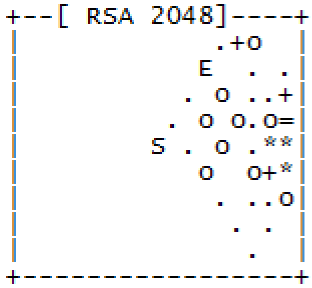
Stratus strongly recommends the following OpenStack compute node configuration to ensure the correct operation for evacuations and migrations. If this configuration is not implemented, evacuations and migrations may fail.

To configure OpenStack for proper evacuation and migration:

1. On each compute node where NFS shared storage is used, add the following options to the NFS mount entry in `/etc/fstab`:
   - `auto,lookupcache=none`
   - Example: `/etc/fstab:`

- # NFS shared storage for instances:
  - `10.200.11.70:/KVMDataStore /var/lib/nova/instances nfs auto,lookupcache=none 0 0`

2. Complete the following steps to ensure that your SSH keys are properly configured. For additional information, refer to the following websites:
   - https://lists.launchpad.net/openstack/msg24036.html
   - https://ask.openstack.org/en/question/10335/ssh-resize/
   - https://macnugget.org/projects/publickeys/
3. Use an existing SSH key for `/root`, or create a new keypair using the following command:
   - `ssh-keygen -t rsa`
4. Enter the file in which to save the key:
   - `/root/.ssh/id_rsa`
5. Enter the passphrase; leave the field blank for no passphrase.
6. Enter the same passphrase again.
   - Your identification (private key) is saved in `/root/.ssh/id_rsa`.
   - Your public key is saved in `/root/.ssh/id_rsa.pub.`
7. The key fingerprint is `55:45:fc:1f:2d:9b:f5:69:6d:03:5d:ef:2b:50:e8:11 root@<server_name>.<domain>.com`
8. The key's randomart image is:



```
+--[ RSA 2048]----+
|            .+o  |
|           E  . .|
|          . o ..+|
|         . o o.o=|
|        S . o .**|
|           o  o+*|
|            . ..o|
|             . . |
|              .  |
+-----------------+
```

9. A key pair is created, both public and private keys:
   - The private root key is located at `/root/.ssh/id_rsa`.
   - The public root key is located at `/root/.ssh/id_ras.pub`.
10. Enable the Nova user for login using the command: `usermod -s /bin/bash nova`
11. Create the folder required by SSH, and move the private key from step 1 into the folder using the following commands:
   - `mkdir -p /var/lib/nova/.ssh`
   - `cp /root/.ssh/id_rsa /var/lib/nova/.ssh`
   - `cat /root/.ssh/id_rsa.pub >> /var/lib/nova/.ssh/authorized_keys`
   - Add these to `/var/lib/nova/.ssh/config`
   - `Host *`
   - `StrictHostKeyChecking no`
   - `UserKnownHostsFile=/dev/null`
   - `cd /var/lib/nova/.ssh`
   - `chown nova *`
   - `chgrp nova *`
12. Repeat steps 2 and 3 on each compute node.
13. All nodes share the same key pair; do not generate a new one for the other compute nodes. Instead, copy the key for the compute node on which it was created in step 1. For example:
   - `(copy keys from compute-1 to compute-2) .. scp from compute-2`
   - `scp root@compute-1:/root/.ssh/id_rsa* /root/.ssh`
14. Verify that the key is working properly, using the following commands:

- `su nova`
- Example: `ssh nova@compute-1 // you will log in to the node-another without a password`

15. Make sure that all libvirt user IDs and group IDs match across all nodes:
    - For user ID:
      - `id -u qemu`
    - For group ID:
      - `id -g qemu`
      - `id -u nova`
      - `id -g nova`

16. Only on compute nodes that will run the KVM hypervisor, edit `/etc/libvirt/qemu.conf`; uncomment and change these values:

    > **Caution**: Do not uncomment or change these values on a compute node that will run the KVM-FT hypervisor.

    - `dynamic_ownership=0`
    - `user=root`
    - `group=root`

17. Reboot the compute node.

Supporting Instance Evacuations

Stratus will supply a patch for your version of OpenStack Nova-Compute; however, you must specify your version. For instance evacuation support, the following procedure must be implemented on each compute node.

> **Note**: After a YUM update on compute nodes that includes updates on the Nova compute service, manager.py is also updated. Therefore, manager.py must also be re-patched by executing the following process.

To support instance evacuations:

1. Navigate to `/usr/lib/python2.6/site-packages/nova/compute`.
2. In that directory, use the Vi editor to create a new file with the file name of: `evac-patch.txt`. For example, `vi evac-patch.txt`.
3. In the `evac-patch.txt` file, paste in the following commands:

```
— /usr/lib/python2.6/site-pack-
ages/nova/compute/manager.py 2014-09-15
20:47:17.272501082 -0400

+++ /usr/lib/python2.6/site-pack-
ages/nova/compute/manager.py.new 2014-09-15
16:23:14.735380543 -0400

@@ -2502,6 +2502,7 @@

files = self._decode_files(injected_files)

kwargs = dict(

+ recreate=recreate,

context=context,

instance=instance,

image_meta=image_meta
```

4. Save and close the `evac-patch.txt` file.
5. From the directory `/usr/lib/python2.6/site-packages/nova/compute`, execute the following commands in this order:
   - For backup, execute the command: `cp manager.py ~/ .`
   - Then, execute the patch command: `sudo patch < evac-patch.txt`.
6. Reboot the compute node.
7. Repeat this process on all compute nodes.

Addressing Installation Errors

If Errors are Encountered During Installation

When doing a clean installation of Stratus Cloud Workload Services, the installation script may fail if OpenStack cannot be verified. Should this occur and you attempt to run the install script again, it reports the installation is already complete. Address this issue using the following process.

To repair a failed Workload Services installation due to OpenStack verification issues:

1. Uninstall Workload Services using the command:

   ```
   sudo sh clouds-0.1.0.19.5.sh uninstall.
   ```

2. Address any OpenStack issues identified in the installation error messages.
3. Re-install Workload Services using the command:

   ```
   sudo sh clouds-0.1.0.19.5.sh install
   http://192.168.91.50:5000/v2.0 admin admin.
   ```

See also:

"OpenStack Installation and Configuration" on page 14

GRE Network Configuration

If you are using GRE networking, the maximum transmission unit (MTU) on the appliance must be set to 1400. If you are using VLAN networking, this configuration does not apply.

To configure GRE networking:

1. Edit the script located at `/etc/sysconfig/networking-scripts/ifcfg-eth0`.
2. In the script, change `MTU= "1500"` to `MTU="1400"`.
3. Save the changes in the script.

MySQL Connections

To prevent errors in Heat and Horizon, Stratus recommends setting the number of MySQL connections to 300.

To set MySQL connections:

1. Open the file `/etc/my.cnf`.
2. In the `/etc/my.cnf` file in the `[mysqld]` section, add the parameter: `max_connections = 300`. The following is an example of the the `/etc/my.cnf` file containing the correct MySQL connection settings:

   ```
   [mysqld]
   ```

```
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
user=mysql
# Disabling symbolic-links is recommended to prevent assorted security risks
symbolic-links=0
default-storage-engine = innodb
innodb_file_per_table
collation-server = utf8_general_ci
init-connect = 'SET NAMES utf8'
character-set-server = utf8
bind-address = 0.0.0.0
max_connections = 300
```

3. Save and close the `/etc/my.cnf` file.
4. Restart `mysqld` using the command `service mysqld restart`.

OpenStack Verification and Testing

OpenStack verification and testing allows you to troubleshoot and resolve issues with your OpenStack and Stratus Cloud Solution configurations. You can identify and resolve issues in:

- Image upload
- Instance creation
- Floating IP configurations
- Security groups
- High Availability testing
- Resiliency testing
- Nodes
- Storage
- Debugging

Related Topics

"Debugging OpenStack" on page 27

"OpenStack Verification" on page 26

"High Availability and Resiliency Testing" on page 26

OpenStack Verification

Use the following procedure for basic OpenStack testing:.

1. Log in to horizon: `controller-1.<yourdomain>.stratus.com`.
2. Upload an image.
3. Create an instance.
4. Create a floating IP.
5. Assign a floating IP to the instance.
6. Create a security group to allow ssh and ping.
7. Verify that you can ping and ssh into the instance.

High Availability and Resiliency Testing

Use the following procedure for High Availability and resiliency testing.

1. Power down one of the switches; then run the OpenStack verification tests described in "OpenStack Verification" on page 26.
2. Power on the switch and power down the other switch, then run the OpenStack verification tests described in "OpenStack Verification" on page 26.
3. Reboot all the nodes in the cluster, then run the OpenStack verification tests described in "OpenStack Verification" on page 26.
4. Storage tests: remove a disk from the RAID5 or RAID6 set. If you have RAID 5, then rebuilding the RAID array may be time-intensive.

See also:

"Debugging OpenStack" on page 27

Debugging OpenStack

Use the following procedures to debug your OpenStack installation and configuration.

1. Start with the controller node to verify that all services are up:

   ```
   $ nova-manage service list

   $ neutron service list

   $ cinder host list
   ```

2. Log files on the controller node are under `/var/log directory`:

   Nova logs: `/var/log/nova`

   Neutron logs: `/var/log/neutron`

   http logs: `/var/log/http`

3. For compute nodes, the logs are under `/var/log/nova`.

Installing the Stratus Cloud Solution

To install the Stratus Cloud Solution:

1. Ensure that your OpenStack environment meets the requirements for installation. See the overview information in the "Stratus Cloud Solution Installation Guide" on page 1.
2. Install a CentOS image to use for the Stratus virtual appliance and Cassandra database nodes. See "Installing CentOS" on page 29.
3. Create an installation configuration file to specify properties for the installation process. See "Creating an Installation Configuration File for Stratus Cloud Workload Services" on page 31.
4. Install the Stratus Cloud Workload Services software in the Stratus virtual appliance. See "Installing Stratus Cloud Workload Services" on page 35.
5. Configure settings as needed in the cloud properties file. See "Configuring the Properties File for the Stratus Cloud Workload Services" on page 40.

   Settings to modify include:

   - "Setting Up Your Mail Server" on page 50
   - "Setting the Logging Detail Level for Stratus Cloud Workload Services" on page 52
6. Learn about the purpose and management of the Cassandra database nodes that were created during the installation. See "Managing Cassandra Nodes" on page 53.
7. If applicable, install Stratus Cloud Availability Services on two or more KVM compute nodes. See "Installing Stratus Cloud Availability Services" on page 63.

Related Topics

"Upgrading Stratus Cloud Workload Services" on page 55

"Uninstalling Stratus Cloud Workload Services" on page 60

"Stratus Cloud Workload Services Installation Script Options" on page 61

Installing CentOS

The following procedure summarizes how to create and install a custom CentOS image that will serve as the basis for the Stratus appliance as well as the Cassandra database nodes that support Stratus Cloud

Workload Services. For a more detailed example of installing a CentOS image, see the OpenStack CentOS image guide.

To install CentOS for Stratus Cloud Workload Services:

1. Upload a CentOS version 6.5 ISO image with the following properties to the `/data/isos` directory of your OpenStack controller:
   - At least 20GB of disk space in the /root partition
   - 4 vCPUs
   - 8 GB RAM
2. Create a virtual hard disk for the image by entering:

   ```
   qemu-img create -f qcow2 /tmp/CentOS-6.5.qcow2 20GB
   ```
3. Use `virt-manager` or a similar tool to start the CentOS installation and do the following:
   - Use a custom disk
   - Install cloud-init
   - Create an SSH key using `cloud-user` (or the default). If a password is specified, it must be done from the console, as you cannot SSH to the virtual machine until *cloud-init* is installed. You can use `virt-manager` to access the console.
   - Delete the existing partitions
   - Create a `/root`20GB partition
   - And `/boot` using the remaining disk space, which is normally about 3 GB
4. After you have finished installing and configuring your CentOS image, upload the image to the OpenStack cloud in Horizon.
5. In OpenStack, create a new flavor for the Stratus appliance instance:
   - 4 vCPUs
   - 8192 MB RAM (no swap,no ephemeral)
   - 160 GB Root Disk

6. Create another new flavor for the Cassandra node instances:
   - 4 vCPUs
   - 8192 MB RAM (no swap,no ephemeral)
   - 20 GB Root Disk
7. Launch an instance for the Stratus appliance and do the following:
   - Enter the instance name, for example **StratusApp**
   - Select the custom flavor that you created for the appliance
   - Select your custom CentOS image
   - Import and select the SSH key associated with the image
   - Select an external network
8. After launching the Stratus appliance, create a configuration file for the installation process as described in "Creating an Installation Configuration File for Stratus Cloud Workload Services" on page 31, and then install the cloud software as described in "Installing Stratus Cloud Workload Services" on page 35.

Note: Installing Stratus Cloud Workload Services will automatically create the Cassandra node instances with the flavor that you specify to the installation script.

Creating an Installation Configuration File for Stratus Cloud Workload Services

Before installing Stratus Cloud Workload Services, you must create a configuration file to specify the settings needed by the installation program. Use the following table to the gather the installation settings.

To create the configuration file, open a text editor in the Stratus virtual appliance and insert a sample configuration file. You can copy the example configuration file that appears below the table or display the help for the installation program (`sudo ./install.sh -h`) and copy the sample file from the output. Paste the content into your text editor, replace the sample settings with the settings for your environment, and save the file (for example, save as `install.conf`).

After creating the configuration file, install the cloud software as described in "Installing Stratus Cloud Workload Services" on page 35. Specify the name of your configuration file to the installation program.

Installation Configuration File Settings

Setting	Description	Label
OpenstackURL	Specify the URL for your OpenStack controller. Find the end point for API access in Horizon, as follows: 1. Click **Compute**, click **Access & Security**, and then click the **API Access** tab. 2. Use the **Identity** service endpoint. For example: `http://192.168.100.50:5000/v2.0`	Required
OpenstackAdminName	Specify the OpenStack admin account.	Required
OpenstackAdminPassword	Specify the OpenStack admin password.	Required
OpenstackFloatingNetUUID	Specify the OpenStack Floating IP network to use. This should be the same floating network that the appliance uses, and it must be specified as a UUID.	Required
NTPServer	Specify an NTP server. For multiple NTP servers, specify one per line.	Optional
DbImage	Specify the image name that the Workload Services installation script will use to automatically launch the Cassandra node instances. By default, if you do not specify an image, the instances use the same image as the Stratus appliance.	Optional
DbFlavor	Specify the OpenStack flavor to use for the Cassandra nodes. You can specify a unique flavor that requires less disk space than the Stratus appliance, as described in "Installing CentOS" on page 29.	Optional
DbUser	Specify the login account to use for the Cassandra node image. The `cloud-user` is appropriate for most preinstalled CentOS cloud images; however, if you manually	Required

Setting	Description	Label
	created the image it may use the default `ec2-user` account or another account. If you are unsure of the correct setting, locate the value for the `instance_user` entry in the `/etc/heat/heat.conf` file on your OpenStack controller.	
DbNode	Specify the hypervisors on which to place the 4 dedicated Cassandra instances. To ensure the fault-tolerant operation of the Cassandra database, specify 4 unique hypervisors, one entry per line. If you specify fewer than 4 hypervisors, multiple Cassandra instances are placed on the same hypervisor, which limits redundancy. If no hypervisors are specified, the Cassandra nodes are automatically placed by Nova.	Optional

Example Installation Configuration File

```
# Specify the URL for openstack (REQUIRED)

OpenstackURL=http://192.168.84.50:35357/v2.0

# Specify the admin account (REQUIRED)

OpenstackAdminName=admin

# Specify the admin password (REQUIRED)

OpenstackAdminPassword=admin

#

# Specify the Openstack Floating IP network to use.
# This must be a UUID. (REQUIRED)
OpenstackFloatingNetUUID=d45a43c1-edd5-45b6-8024-8c7c1483fbe9
#
# If a specify NTP server or group of NTP servers must be used
# specify one entry per line (OPTIONAL)
NTPServer=192.168.87.150
#
# If the Cassandra instances should use a different image
# than the base appliance, specify the image name here (OPTIONAL)
DbImage=StratusCloud CentOS 6.5 Appliance
#
# Specify the Openstack flavor to use for the Cassandra nodes
# (OPTIONAL)
DbFlavor=StratusCloudAppliance
#
# Specify the login account to use for the Cassandra node image
# i.e. "cloud-user" is appropriate for most Centos Cloud images
# (REQUIRED)
DbUser=ec2-user
# Select hypervisors to place the 4 database instances
# It is recommended to specify (Unique) hypervisors using 4
# separate lines of the form
# availabilityZone:host
#
```

```
# If fewer than 4 nodes are specified, multiple db instances are
placed
# on the same hypervisor (Not recommended)
#
# If no hypervisors are specified, the Cassandra nodes
# will be automatically placed by Nova
#
DbNode=nova:compute-1.intcloud1.stratus.com
DbNode=nova:compute-2.intcloud1.stratus.com
DbNode=nova:compute-2.intcloud1.stratus.com
```

Installing Stratus Cloud Workload Services

Install Workload Services after you have installed CentOS ("Installing CentOS" on page 29) and created an installation configuration file ("Creating an Installation Configuration File for Stratus Cloud Workload Services" on page 31.

To install Workload Services:

1. In Horizon, open the console of the Stratus appliance that you created in the "Installing CentOS" on page 29 procedure. Log on as the *cloud-init* user and enter the password you assigned to *SSH creation* during installation. You may need to update the `/etc/udev/rules.d/70-persistent-net.rules` file and remove the `eth0` entry, and rename `eth1` to `eth0`. This sometimes occurs when you deploy.
2. Update these files as follows:
   - `/etc/sysconfig/network` file: specify the `HOSTNAME` of the appliance. Note that `**NOZEROCONF=yes` should already be there.
   - `/etc/hosts` : add an entry for `127.0.0.1` at the end for the hostname you just updated in the network file.
   - If you have not done so already, install the `cloud-init` using the OpenStack instructions in order to later use the SSH key. Cloud-init software allows an SSH key to be injected

to the instance when you launch or deploy an instance. Without cloud-init, you cannot log on using an SSH key.

3. Reboot after these updates.

4. Assign this instance a floating IP address so that you can SSH to it using your key.

5. Log on as the cloud-user and execute the su command to become the root user (or be prepared to use sudo to run commands as root).

6. Install the yum-utils package for access to additional yum commands:

   ```
   # yum install yum-utils
   ```

7. Verify that there are no unfinished yum transactions by entering the following yum command:

   ```
   # yum-complete-transaction --cleanup-only
   Loaded plugins: fastestmirror
   Loading mirror speeds from cached hostfile
   * base: mirror.sanctuaryhost.com
   * epel: mirror.cogentco.com
   * extras: centos.mirror.nac.net
   * updates: mirror.wiredtree.com
   No unfinished transactions left.
   ```

   If there are unfinished transactions, resolve them before continuing with the installation.

8. In the /opt directory, create a directory called Release:

   ```
   mkdir /opt/Release
   ```

9. Transfer the cloud installation script to the /opt/Release directory. For example, use a secure copy (SCP) utility to copy the file from another system. (If you copy the script to your /home/cloud-user account, move the script to the /opt/Release directory.)

10. In the Stratus appliance, switch to the /opt/Release directory:

    ```
    cd /opt/Release
    ```

11. Run the following command to make the installation script an executable file, where *script* is the name of the script:

```
chmod a+x script.sh
```

12. Locate the installation configuration file (for example, `install.conf`) that you created in "Creating an Installation Configuration File for Stratus Cloud Workload Services" on page 31 and move this file to the same `/opt/Release` directory.

13. Run the installation script specifying the `install` option and the name of the installation configuration file; for example, `./clouds-0.1.5.0.0.sh install` *`install.conf`*

Notes:

- For more information about the installation script options, see "Stratus Cloud Workload Services Installation Script Options" on page 61.
- If the installation fails or you stop the installation script before it can finish, you must uninstall the cloud software ("Uninstalling Stratus Cloud Workload Services" on page 60) and install it again. If you retry the installation without uninstalling the software, the script exits with the following error: `There are unfinished transactions remaining. You might consider running yum-complete-transaction first to finish them.`

The installation script begins the installation process for Stratus Cloud Workload Services. The script displays output similar to the following:

```
./clouds-0.1.5.24.3.sh install install.conf
Verifying archive integrity... All good.
Uncompressing Stratus Clouds 0.1.5.24.3.....................
/ \ / \ / \ / \ / \ / \ / \
( S | t | r | a | t | u | s )
\_/ \_/ \_/ \_/ \_/ \_/ \_/

_ _ _ _ _ _
/ \ / \ / \ / \ / \ / \
( C | l | o | u | d | s )
```

```
\_/ \_/ \_/ \_/ \_/ \_/

[12-16-2014 21:06:14] --> Checking current user...Ok

[12-16-2014 21:06:14] --> Running from </opt/Release>

[12-16-2014 21:06:14] --> Use config file <install.conf>

[12-16-2014 21:06:14] --> OpenStackUrl = http://192.168.99.50:35357/v2.0

[12-16-2014 21:06:14] --> OpenStackAdminName = admin

[12-16-2014 21:06:14] --> OpenStackAdminPassword = admin

[12-16-2014 21:06:14] --> DbUser = ec2-user

.

.

.

[12-16-2014 21:06:21] --> Welcome to the Stratus-Clouds Installation

[12-16-2014 21:06:21] --> Installing version 0.1.5.24.3

[12-16-2014 21:06:21] --> @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

[12-16-2014 21:06:21] --> A copy of this output will be located in:

[12-16-2014 21:06:21] --> /opt/stratus/logs/install_12-16-2014_21_06_14.log

[12-16-2014 21:06:21] --> Openstack Installation Location: http://192.168.99.50:35357/v2.0

[12-16-2014 21:06:21] --> Openstack Admin Tenant: admin

[12-16-2014 21:06:21] --> Updating existing packages, may take a few minutes...
```

```
[12-16-2014 21:06:22] --> Existing package updates complete.
[12-16-2014 21:06:23] --> Local ip == 10.10.10.21
[12-16-2014 21:06:23] --> Contact metadata server...
[12-16-2014 21:06:23] --> Metadata hostname: stratusap-
p.novalocal
[12-16-2014 21:06:23] --> Local hostname: stratuscloudqa3
[12-16-2014 21:06:23] --> There is an existing entry in
/etc/hosts
[12-16-2014 21:06:23] --> <10.10.10.21 stratuscloudqa3
stratusapp.novalocal>
[12-16-2014 21:06:23] --> Stopping necessary services...
[12-16-2014 21:06:24] --> Installing packages
.
.
.
[12-16-2014 21:28:13] --> Verifying that all Cassandra nodes
have joined the cluster....OK
[12-16-2014 21:28:26] --> Starting jetty...
[12-16-2014 21:28:56] --> Wait for applications to start....
[12-16-2014 21:28:57] --> Applications started.
[12-16-2014 21:28:57] --> Initializing database...
358..358..358..420..451..477..553..676..802..954..1076..1202..-
1322..1448..1577..1701..1831..1951..2082..2237..2354..2484..26-
16..2772..2891..3019..3176..3301..3427..3523..3678..3805..3932..4021..4139.
 DB
Total Time : 0 hours, 32 minutes, 31 seconds
```

```
[12-16-2014 22:01:28] --> Completed database initialization

[12-16-2014 22:01:28] --> Wait for application start....

[12-16-2014 22:01:28] --> Installation almost complete

[12-16-2014 22:01:28] --> Get metadata...

[12-16-2014 22:01:28] --> Contact metadata server...

[12-16-2014 22:01:29] --> Install Security Groups...

[12-16-2014 22:01:30] --> SecurityGroup: kvm-ax-quorum already
exists...OK

[12-16-2014 22:01:35] --> Add security group kvm-ax-quorum to
7f0f1753-07e4-4b9a-a71f-190cb54c1206...

[12-16-2014 22:01:36] --> Complete...
```

14. Optionally, verify the version number of Workload Services that you installed by entering a command similar to the following:

    ```
    # rpm -qa | grep stratus
    stratus-clouds-0.1.5.24.3-0.fc14.noarch
    ```

15. After a successful installation, update the `/opt/jetty/resources/CloudMgmtExt.properties` file to configure settings for Workload Services, as described in "Configuring the Properties File for the Stratus Cloud Workload Services" on page 40.

16. You can now go to `https://ThisCentOSFloatingIP`, and begin using Workload Services.

Related Topics

"Uninstalling Stratus Cloud Workload Services" on page 60

Configuring the Properties File for the Stratus Cloud Workload Services

After installing the Stratus Cloud Workload Services, edit the cloud properties file (`/opt/jetty/resources/CloudMgmtExt.properties`) to configure settings needed for your environment. In most cases, the properties are set automatically during the Workload Services installation, but, for example, you must set up a mail server and optionally set the logging detail level in this file, as described in the following topics:

- "Setting Up Your Mail Server" on page 50
- "Setting the Logging Detail Level for Stratus Cloud Workload Services" on page 52

The table summarizes the settings available in the `CloudMgmtExt.properties` file (and indicates if you should modify them in the **Modify** column). An example properties file appears below the table.

> **Note**: If you modify the `CloudMgmtExt.properties` file, you must restart the Jetty service to apply the changes. Restart Jetty by entering the command `service jetty restart`.

Cloud Properties File Settings

Setting	Description	Modify
KvmFtQuorum1Ip KvmFtQuorum2Ip	Specifies the IP addresses of the two nodes that run the fault-tolerant Quorum server service (QSS) for KVM-FT applications. You manually enter these IP addresses after installing the quorum servers, as described in "Installing Quorum Servers for Stratus Cloud Availability Services" on page 76. You cannot change the quorum server IP addresses later without redeploying your KVM-FT applications.	Yes
KvmFtDiskEnableTimeout	Specifies how long the KVM-FT orchestrator will wait (in minutes) before trying to automatically repair an `OFFLINE` or `FAILED` disk. Default is 10 minutes.	Yes
OrchestratorAPIEndpoint	Specifies the URL of the Heat orchestrator.	No

Setting	Description	Modify
UseHeatOrchestration	Enables Heat orchestration. Must always be set to the default of `true`.	No
BootstrapUsername	Specifies the OpenStack admin account.	No
BootstrapPassword	Specifies the OpenStack admin password.	No
KeystoneEndpoint	Specifies the URL for your OpenStack controller.	No
CassandraReplicationFactor	Specifies the number of Cassandra database nodes required to maintain the integrity of the back-end database for Workload Services operations. The default is a minimum of 5 Cassandra nodes, one of which is the Stratus appliance.	No
CassandraLocation	Specifies the IP address of each Cassandra node that was configured during the Workload Services installation.	No
HypervisorWorkloadUnlimited	Specifies if the cloud allows infinite oversubscription of resources. The default setting of `false` prevents oversubscription of resources. A setting of `true` allows you to continue deploying applications even if cloud resources are exhausted.	
RunCassandraEmbedded	Used only for internal testing or demonstration. Must always be set to the default of `false`.	No
Orchestrator	Used only for internal testing or demon-	No

Setting	Description	Modify
	stration. Must remain commented out. Setting to `local` enables a mock orchestrator that simulates the orchestration function without connecting to OpenStack.	
BootstrapTenantName	Specifies the OpenStack admin tenant name.	No
NodeToolPath	Specifies the path to Cassandra executables. The default path is `/opt/cassandra/bin`.	No
NodeTool	Name of the node tool script for Cassandra. The default name is `nodetool`.	No
DailyMaintenance24HourTime	Specifies the time of day (in 24 hour format) when daily Cassandra database maintenance occurs. Default is `23:00` (11 PM).	No
WeeklyMaintenanceDay	Specifies the day of the week when the Cassandra repair operation runs. Default is `WEDNESDAY`.	No
WeeklyMaintenance24HourTime	Specifies the time of day (in 24 hour format) when the Cassandra repair operations runs. Default is `03:00` (3 AM).	No
NodeHealthCheckMinutes	Specifies the interval (in minutes) when the Cassandra nodetool service runs to check Cassandra database status. Default is `15` minutes.	No
SearchHost	Specifies the elastic search path. Default is 127.0.0.1.	No

Setting	Description	Modify
SearchPort	Specifies the elastic search port. Default is 9300.	No
SearchHttpPort	Specifies the elastic search HTTP port. Default is 9200.	No
OSTokenMinutesToRenewBeforeExpires	Specifies renewal interval for OS token in minutes. Default is 15 minutes.	No

DataCollectionCommodityIntervalCode
DataCollectionMissionCriticalIntervalCode
DataCollectionBusinessCritiCalIntervalCode
DataCollectionDefaultIntervalCode
	Specifies the data collection interval in seconds for each availability type. Valid values are 10, 30, 60, 300, 600, 900, 1800, 2700, and 3600. If an invalid value is set, the software uses the default value. Defaults are as follows:
	DataCollectionCommodityIntervalCode=900
	DataCollectionMissionCriticalIntervalCode=60
	DataCollectionBusinessCritiCalIntervalCode=300
	DataCollectionDefaultIntervalCode=900
		No

cloud.mgmt.mail.server.host	Specifies the system mail server host to use for email notifications.	Yes
cloud.mgmt.mail.server.port	Specifies the system mail server port, which is 25 by default, and generally 465 for SSL and 587 for TLS.	Yes
cloud.mgmt.mail.sender.address	Specifies the email address that appears in the FROM header when mail is sent.	Yes

Setting	Description	Modify
cloud.mgmt.mail.secure.password.authentication.require	Specifies if secure password authentication (SPA) is required by email server. **NOTE:** If set to `true`, you must specify the next three properties (encryption type, username, and password).	Yes
cloud.mgmt.mail.encryption.type	Specifies the encryption type of the email server connection (DEFAULT, SSL or TLS). **NOTE:** Must also set cloud.mgmt.mail.secure.password.authentication.required to `true`.	Yes
cloud.mgmt.mail.account.username	Specifies the mail account username. **NOTE:** Must also set cloud.mgmt.mail.secure.password.authentication.required to `true`.	Yes
cloud.mgmt.mail.account.password	Specifies the mail account password. **NOTE:** Must also set cloud.mgmt.mail.secure.password.authentication.required to `true`.	Yes
cloud.mgmt.mail.password.reset.url	Specifies the callback URL pattern that is sent by the forgot password email. If necessary, enter the hostname or IP address.	Yes
cloud.mgmt.mail.password.initialize.url	Specifies the callback URL pattern that is sent by the initialize password email. If necessary, enter the hostname or IP address.	Yes

Setting	Description	Modify
cloud.mgmt.help.system.host	Specifies the URL of the online help system that appears when you click **Help** in Workload Services.	Yes
buggrabber	Specifies the location of the Stratus `bug-grabber` utility that collects log files and other information if needed for your service representative to troubleshoot your cloud configuration.	No
cloud.mgmt.api.logging.level cloud.mgmt.orchestrator.logging.level	Specify the logging level to use for Stratus logs in the `/opt/jetty/logs` directory. Both properties are set to `debug` by default. Possible values: • `fatal`: Shows messages at a FATAL level only • `error`: Shows messages classified as ERROR and FATAL • `warning`: Shows messages classified as WARNING, ERROR, and FATAL • `info`: Shows messages classified as INFO, WARNING, ERROR, and FATAL • `debug`: Shows messages classified as DEBUG, INFO, WARNING, ERROR, and FATAL • `trace` : Shows messages classified as TRACE,DEBUG, INFO,	Yes

Setting	Description	Modify
	WARNING, ERROR, and FATAL	

Example Cloud Properties File

```
KvmFtQuorum2Ip=192.168.101.183

KvmFtQuorum1Ip=192.168.101.135

KvmFtDiskEnableTimeout=10

OrchestratorAPIEndpoint=http://192.168.101.135/orchestrator

UseHeatOrchestration=true

BootstrapPassword=admin

BootstrapUsername=admin

KeystoneEndpoint=http://192.168.99.50:35357/v2.0

CassandraReplicationFactor=5

CassandraLocation=10.10.10.21,10.10.10.156,10.10.10.157

HypervisorWorkloadUnlimited=false

#CassandraLocation=127.0.0.1

#CassandraLocation=127.0.0.1:9042

#CassandraLocation=192.168.86.150,192.168.86.151,192.168.86.152,192.168.86.154,192.168.86.155

#CassandraReplicationFactor=5

RunCassandraEmbedded=false

#Orchestrator=local

# Devstack

#KeystoneEndpoint = http://192.168.27.100:5000/v2.0

#BootstrapUsername = admin

#BootstrapPassword = stratus

BootstrapTenantName = admin

# Cloud Management Database Maintenance
# Windows
#NodeToolPath=c:/CloudMgmtDeploy/cassandra/apache-cassandra/bin
#NodeTool=nodetool.bat
# Linux
NodeToolPath=/opt/cassandra/bin
NodeTool=nodetool
DailyMaintenance24HourTime = 23:00
WeeklyMaintenanceDay = WEDNESDAY
WeeklyMaintenance24HourTime = 03:00
NodeHealthCheckMinutes=15
#UseHeatOrchestration=true
SearchHost=127.0.0.1
SearchPort=9300
SearchHttpPort=9200
#minutes to renew before token expires
OSTokenMinutesToRenewBeforeExpires=15
#DATACOLLECTION INTERVAL CODE IN SECONDS
#VALID VALUES ARE (IF INVALID VALUE SET, it WILL DEFAULT to 900)
#10,30,60,300,600,900,1800,2700,3600
DataCollectionCommodityIntervalCode=900
DataCollectionMissionCriticalIntervalCode=60
DataCollectionBusinessCritiCalIntervalCode=300
DataCollectionDefaultIntervalCode=900
## system mail properties ##
# The system mail server host
cloud.mgmt.mail.server.host=<change_on_setup>
# The system mail server port (25 by default, generally 465 for SSL and 587 for TLS)
```

```
cloud.mgmt.mail.server.port=25
# The email address that receiver can see in the header FROM
cloud.mgmt.mail.sender.address=<change_on_setup>
# Set to true if secure password authentication (SPA) is required by email server
cloud.mgmt.mail.secure.password.authentication.required=true
# The encryption type of the email server connection (DEFAULT, SSL or TLS)
cloud.mgmt.mail.encryption.type=DEFAULT
# The mail account username, required if the cloud.mgmt.mail.secure.password.authentication.required set to true
cloud.mgmt.mail.account.username=<change_on_setup>
# The mail account password, required if the cloud.mgmt.mail.secure.password.authentication.required set to true
cloud.mgmt.mail.account.password=<change_on_setup>
## password reset mail ##
# The callback URL pattern that sent via the forgot password email. Change the host/ip if necessary
cloud.mgmt.mail.password.reset.url=https://<change_on_setup>/cloud/#login:passwordreset?useridentifier={0}&passwordresetcode={1}
## password initialize mail ##
# The callback URL pattern that sent via the initialize password email. Change the host/ip if necessary
cloud.mgmt.mail.password.initialize.url=https://<change_on_setup>/cloud/#login:passwordreset?useridentifier={0}&passwordresetcode={1}
# help system host
cloud.mgmt.help.system.host=http://clouddoc.stratus.com/1.5.0.0
#buggrabber=c:/cloud/buggraber.bat
buggrabber=sudo /opt/stratus/scripts/buggrabber.sh
# Orchestration API (currently needed for LAMO trap POSTs)
#OrchestratorAPIEndpoint=http://<change_on_setup>/orchestrator
# KVM-FT Quorum IPs
```

```
#KvmFtQuorum1Ip=<change_on_setup>

#KvmFtQuorum2Ip=<change_on_setup>

#### LOGGING LEVEL (OPTIONAL) Default : debug if not found

#POSSIBLE VALUES : DEBUG/INFO/WARN/ERROR/FATAL

#fatal: shows messages at a FATAL level only

#error: Shows messages classified as ERROR and FATAL

#warning: Shows messages classified as WARNING, ERROR, and FATAL

#info: Shows messages classified as INFO, WARNING, ERROR, and FATAL

#debug: Shows messages classified as DEBUG, INFO, WARNING, ERROR, and FATAL

#trace : Shows messages classified as TRACE,DEBUG, INFO, WARNING, ERROR, and FATAL

# APPLIES FOR BOTH API AND ORCHESTRATOR

cloud.mgmt.api.logging.level=debug

cloud.mgmt.orchestrator.logging.level=debug
```

Setting Up Your Mail Server

After installing the Stratus Cloud Workload Services, you must configure the cloud software to connect to the mail server in your environment. In the directory `/opt/jetty/resources`, edit your `CloudMgmtExt.properties` file as follows.

> **Note**: Contact your IT department for your specific mail server parameters, which are shown in red in the following example.

To set up your email server:

1. Log on to the Stratus appliance as the `cloud-user` and execute the `su` command to become the `root` user (or be prepared to use `sudo` to run commands as `root`).

2. Open the `/opt/jetty/resources/CloudMgmtExt.properties` file with a text editor and modify the following settings:

   ```
   ## system mail properties ##

   # The system mail server host
   ```

```
cloud.mgmt.mail.server.host=smtpmail.your_domain.com

# The system mail server port (25 by default, generally 465 for SSL and 587 for TLS)

cloud.mgmt.mail.server.port=25

# The email address that receiver can see in the header FROM

cloud.mgmt.mail.sender.address=user_name@your_domain.com

# Set to true if secure password authentication (SPA) is required by email server

cloud.mgmt.mail.secure.password.authentication.required=false

# The encryption type of the email server connection (DEFAULT, SSL or TLS)

cloud.mgmt.mail.encryption.type=DEFAULT

# The mail account username, required if the cloud.mgmt.mail.secure.password.authentication.required set to true

cloud.mgmt.mail.account.username=<change_on_setup>

# The mail account password, required if the cloud.mgmt.mail.secure.password.authentication.required set to true

cloud.mgmt.mail.account.password=<change_on_setup>

## password reset mail ##

# The callback URL pattern that sent via the forgot password email. Change the host/ip if necessary

cloud.mgmt.mail.password.reset.url=https://your_cloud_server.your_domain.com/cloud/#login:passwordreset?useridentifier={0}&passwordresetcode={1}

## password initialize mail ##
```

```
# The callback URL pattern that sent via the initialize password email. Change the host/ip if necessary

cloud.mgmt.mail.password.initialize.url=https://your_cloud_server.your_domain.com/cloud/#login:password?username={0}
```

3. Save and close the `CloudMgmtExt.properties` file.

4. Restart Jetty using the command `service jetty restart`.

Setting the Logging Detail Level for Stratus Cloud Workload Services

After installing Stratus Cloud Workload Services, optionally configure the logging detail level and log file behavior in the Stratus appliance.

To set the logging detail level and behavior for Workload Services:

1. Log on to the Stratus appliance as the `cloud-user` and execute the `su` command to become the `root` user (or be prepared to use `sudo` to run commands as `root`).

2. Open the `/opt/jetty/resources/CloudMgmtExt.properties` file in a text editor and modify the API and Orchestrator logging levels as shown here in red. By default, the logging detail level is set to `debug`, but you can specify other levels as described in the file:

```
#### LOGGING LEVEL (OPTIONAL) Default : debug if not found

#POSSIBLE VALUES : DEBUG/INFO/WARN/ERROR/FATAL

#fatal: shows messages at a FATAL level only

#error: Shows messages classified as ERROR and FATAL

#warning: Shows messages classified as WARNING, ERROR, and FATAL

#info: Shows messages classified as INFO, WARNING, ERROR, and FATAL

#debug: Shows messages classified as DEBUG, INFO, WARNING, ERROR, and FATAL

#trace : Shows messages classified as TRACE,DEBUG, INFO, WARNING, ERROR, and FATAL
```

```
# APPLIES FOR BOTH API AND ORCHESTRATOR

cloud.mgmt.api.logging.level=debug

cloud.mgmt.orchestrator.logging.level=debug
```

3. Save and close the `CloudMgmtExt.properties` file.
4. Open the `/opt/jetty/resources/log4j4OrchExt.xml` file in a text editor and modify the values shown here in red to set the number of log files to back up and the maximum log file size before the system rolls over to a new log file:

   ```
   # APPLIES FOR BOTH API AND ORCHESTRATOR

   <param value="20" name="MaxBackupIndex" />

   <param value="10MB" name="MaxFileSize" />
   ```

5. Save and close the `log4j4OrchExt.xml` file.
6. Restart Jetty by entering the command `service jetty restart`.

Managing Cassandra Nodes

Apache Cassandra provides the back-end database for operations in Stratus Cloud Workload Services. When you install Workload Services, the installation program automatically starts the Cassandra service in the Stratus virtual appliance and creates the database. The installation program also uses the CentOS image and flavor that you specify to deploy an additional 4 dedicated Cassandra nodes (instances), for a total of 5 nodes that run the Cassandra service and maintain the database.

All 5 Cassandra nodes are active and processing database operations at all times. All of the nodes must be running to maintain a quorum that ensures the fault-tolerant operation of the database. If a Cassandra node fails, the other nodes keep the database running; however, a minimum of 3 Cassandra nodes must be running to maintain the integrity of the database.

In most cases, you do not need to manage the Cassandra nodes, and you must not interfere with their operation. The Orchestrator automatically manages these nodes. For example, if a compute node is evacuated, the Orchestrator automatically restarts any affected Cassandra nodes on other compute nodes. However, if a Cassandra node is not working properly, you may need to monitor, troubleshoot, or restore the node, as follows:

- To create and specify CentOS image and flavor that the Stratus Cloud Workload Services installation program uses to deploy the Cassandra nodes, see "Installing CentOS" on page 29 and "Creating an Installation Configuration File for Stratus Cloud Workload Services" on page 31.
- To view the status of Cassandra nodes in Workload Services, open the **Deployed Applications** page, click **Instances**, and search for **SC_Cassnode_n** entries. The same nodes are also visible in OpenStack. The status of each Cassandra instance must be **Running**.
- To access the console of a Cassandra node for monitoring or troubleshooting, see "Connecting to the Stratus Appliance or a Cassandra Node with SSH" on page 54.
- To recover a failed Cassandra node by creating a new instance, see "Recovering a Cassandra Node" on page 55.

Connecting to the Stratus Appliance or a Cassandra Node with SSH

Open the console of the Stratus appliance or a Cassandra node if you need to access the command line of the guest operating system for monitoring or troubleshooting purposes.

You can directly open a console in Horizon or in Stratus Cloud Workload Services, but if you prefer to connect with a secure shell (SSH) utility, you need to obtain the SSH keys for the instance and specify them to the SSH utility as described in the following procedure.

To access the Stratus appliance, which also serves as the first Cassandra node, open an SSH connection to the hostname or IP address of the **StratusApp** instance. Log on with the default `cloud-user` account, unless you modified this username in your CentOS image. (If necessary, locate the value for the `default_user` entry in the `/etc/cloud/cloud.conf` file of the image.)

To access one of the four additional Cassandra nodes, open an SSH connection to the hostname or IP address of an **SC_Cassnode_*n*** instance. Log on with the default `ec2-user` account, unless you modified this username in the heat template on your OpenStack controller. (If necessary, locate the value for the `instance_user` entry in the `/etc/heat/heat.conf` file on your OpenStack controller.)

> **Caution**: The Stratus appliance and the Cassandra nodes must be running at all times. When accessing the console of a Cassandra node, be careful not to stop the Cassandra service or modify its default settings. If the Stratus appliance or a Cassandra node is not working properly, contact your service representative for assistance.

To connect to the console of the Stratus appliance or a Cassandra node with an SSH utility:

1. Locate the SSH keys associated with the instance:

   - To connect to the Stratus appliance itself, locate the SSH keys that you created when you installed the CentOS operating system.

   - To connect to the four additional Cassandra nodes, you need the keys that were automatically generated when you installed Workload Services. Log on to the Stratus appliance and locate the keys in the `/opt/stratus/keys/` directory.

2. If necessary, transfer the SSH keys to the system where your SSH utility is located. To open the SSH connection, you need only the private key file for each instance. For example, for the Cassandra nodes, you need the the `id_rsa` file (not the `id_rsa.pub` file).

3. Open an SSH connection and log on to the Stratus appliance (as the `cloud-user`) or a Cassandra node (as the the `ec2-user`), as follows:

   - From a Linux-based system, execute the `ssh` command. For example, to connect to one of the dedicated Cassandra nodes from the CentOS console of the Stratus appliance, enter:

     ```
     sudo ssh -i /opt/stratus/keys/id_rsa ec2-user@10.10.10.nn
     ```

   - From a Windows-based system, connect with an SSH utility such as Putty. See the documentation for your SSH utility for information about specifying the SSH key for the connection. For Putty itself, you must use the pre-generated private key file to create a `.ppk` file that is compatible with Putty.

Recovering a Cassandra Node

This topic is under construction. If you need to recover a Cassandra node, contact your service representative for assistance.

Upgrading Stratus Cloud Workload Services

This topic describes how to upgrade Stratus Cloud Workload Services to a newer version. Use this procedure only to upgrade Workload Services from Version 1.5 to 1.5.x or higher. If you need to upgrade a Version 1.0.x system, contact your service representative for assistance.

Upgrading Workload Services upgrades the Stratus appliance and the Cassandra nodes. If there are associated upgrades for the KVM-FT hypervisors and quorum servers, you must install them separately. See "Upgrading Stratus Cloud Availability Services" on page 80.

To upgrade Workload Services:

1. Log on to Workload Services and verify that your cloud and applications are in a healthy state. Resolve any outstanding advisories before upgrading the software.
2. Log on to the Stratus appliance as the `cloud-user` and execute the `su` command to become the `root` user (or be prepared to use `sudo` to run commands as `root`).
3. Optionally, verify the current version number of Workload Services by entering a command similar to the following:

   ```
   # rpm -qa | grep stratus
   stratus-clouds-0.1.5.24.3-0.fc14.noarch
   ```

4. If you have not already done so, install the `yum-utils` package for access to additional `yum` commands:

   ```
   # yum install yum-utils
   ```

5. Verify that there are no unfinished `yum` transactions by entering the following `yum` command:

   ```
   # yum-complete-transaction --cleanup-only
   Loaded plugins: fastestmirror
   Loading mirror speeds from cached hostfile
   * base: mirror.sanctuaryhost.com
   * epel: mirror.cogentco.com
   * extras: centos.mirror.nac.net
   * updates: mirror.wiredtree.com
   No unfinished transactions left.
   ```

   If there are unfinished transactions, resolve them before continuing with the upgrade.

6. If you have not already done so, in the `/opt` directory, create a directory called `Release`:

   ```
   mkdir /opt/Release
   ```

7. Transfer the new cloud installation script to the `/opt/Release` directory. For example, use a secure copy (SCP) utility to copy the file from another system.
8. In the Stratus appliance, switch to the `/opt/Release` directory:

   ```
   cd /opt/Release
   ```

9. Run the following command to make the installation script an executable file, where *script* is the name of the script:

   ```
   chmod a+x script.sh
   ```

10. Ensure that the installation configuration file for the appliance (for example, `install.conf`) is in the same `/opt/Release` directory. Verify that the settings in the configuration file are up to date. For information, see "Creating an Installation Configuration File for Stratus Cloud Workload Services" on page 31.

11. Run the install script specifying the `install` option and the name of the installation configuration file; for example, `./clouds-0.1.5.x.x.sh install install.conf`

    > **Notes**:
    >
    > - The `install` option automatically detects and upgrades the existing cloud software, if present. For more information about the installation script options, see "Stratus Cloud Workload Services Installation Script Options" on page 61.
    > - Do not stop an upgrade while it is running; otherwise, it will leave your cloud in an inconsistent state. If an upgrade fails for any reason, contact your service representative for assistance.

    The installation script begins the upgrade process for the Stratus Cloud management software. The script displays output similar to the following:

    ```
    ./clouds-0.1.5.25.8.sh install install.conf
    Verifying archive integrity... All good.
    Uncompressing Stratus Clouds 0.1.5.25.8....................
    / \ / \ / \ / \ / \ / \ / \
    ( S | t | r | a | t | u | s )
    \_/ \_/ \_/ \_/ \_/ \_/ \_/
    _ _ _ _ _ _
    / \ / \ / \ / \ / \ / \
    ( C | l | o | u | d | s )
    ```

```
\_/ \_/ \_/ \_/ \_/ \_/

[01-16-2015 09:46:58] --> Checking current user...Ok

[01-16-2015 09:46:58] --> Running from </home/cloud-user>

[01-16-2015 09:46:58] --> Use config file <install.conf>

[01-16-2015 09:46:59] --> OpenStackUrl =
http://192.168.76.50:5000/v2.0

[01-16-2015 09:46:59] --> OpenStackAdminName = admin

[01-16-2015 09:46:59] --> OpenStackAdminPassword = admin

[01-16-2015 09:46:59] --> DbUser = ec2-user

[01-16-2015 09:46:59] --> FIPNet = 5934adad-cff5-4a59-8e73-
e55d03425379

[01-16-2015 09:46:59] --> Override DbImage with "CentOS-6.5-
16G-Image"

[01-16-2015 09:46:59] --> Override DbFlavor with QA.medium

[01-16-2015 09:47:42] --> Checking for novaclient program...

[01-16-2015 09:47:48] --> python-novaclient..OK

Ok

[01-16-2015 09:47:48] --> 4 DbNodes specified...

[01-16-2015 09:47:50] --> 1 NTPServers specified...

[01-16-2015 09:47:59] -->
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

[01-16-2015 09:47:59] --> Welcome to the Stratus-Clouds
Upgrade

[01-16-2015 09:47:59] --> Your current Stratus-Clouds deploy-
ment

[01-16-2015 09:47:59] --> will be preserved
```

```
[01-16-2015 09:47:59] --> 0.1.5.25.6 -> 0.1.5.25.8

[01-16-2015 09:47:59] -->
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

[01-16-2015 09:47:59] --> A copy of this output will be loc-
ated in:

[01-16-2015 09:47:59] --> /opt/stratus/logs/install_01-16-
2015_09_46_58.log

.

.

.

[01-16-2015 09:49:32] --> Starting cassandra...

[01-16-2015 09:49:39] --> Waiting for local Cassandra node to
join the cluster.........OK

[01-16-2015 09:50:22] --> Starting elasticsearch...

[01-16-2015 09:50:22] --> Starting logstash...

[01-16-2015 09:50:22] --> Starting nginx...

[01-16-2015 09:50:23] --> This is an update, skipping database
initilaization[01-16-2015 09:50:23] --> Starting jetty...

[01-16-2015 09:50:59] --> Wait for applications to start....

[01-16-2015 09:51:00] --> Applications started.

[01-16-2015 09:51:00] --> Upgrade almost complete...

[01-16-2015 09:51:00] --> Get metadata...

[01-16-2015 09:51:00] --> Contact metadata server...

[01-16-2015 09:51:00] --> Install Security Groups...

[01-16-2015 09:51:02] --> SecurityGroup: kvm-ax-quorum already
exists...OK
```

```
[01-16-2015 09:51:07] --> Add security group kvm-ax-quorum to
087b13ad-33a1-4525-a872-1b7fe4afa68d...

[01-16-2015 09:51:08] --> Complete...
```

12. Optionally, verify the new version number of Workload Services by entering a command similar to the following:

```
# rpm -qa | grep stratus
stratus-clouds-0.1.5.25.8-0.fc14.noarch
```

13. Go to `https://ThisCentOSFloatingIP` and verify that Workload Services is functioning properly.

14. If needed, upgrade your KVM-FT hypervisors. See "Upgrading Stratus Cloud Availability Services" on page 80.

Related Topics

"Uninstalling Stratus Cloud Workload Services" on page 60

Uninstalling Stratus Cloud Workload Services

Uninstall Stratus Cloud Workload Services if the initial installation fails and you need to start over.

> **Note**: To uninstall Workload Services, you must use the installation script for the currently installed version of the software and not the installation script from another build or version. If you followed the installation procedure, the current script is in the `/opt/Release` directory of the Stratus appliance.

To uninstall Workload Services:

1. Log on to the Stratus appliance as the `cloud-user` and execute the `su` command to become the `root` user (or be prepared to use `sudo` to run commands as `root`).

2. In the Stratus appliance, switch to the directory where the existing `clouds` installation script is located, typically the `/opt/Release` directory:

```
# cd /opt/Release
```

3. Run the installation script and specify the `uninstall` option:

```
# ./clouds-0.1.5.x.x.sh uninstall
```

Stratus Cloud Workload Services Installation Script Options

This topic describes the usage and options of the Stratus Cloud Workload Services installation script.

For an overview of the Stratus Cloud Solution installation procedure, see "Installing the Stratus Cloud Solution" on page 29.

Usage

```
./clouds-n.n.n.n.sh subcommand [options]
```

Description

The `clouds` script installs, upgrades, and uninstalls Stratus Cloud Workload Services.

Subcommands

`install` *config-file*	Installs or upgrades Workload Services according to the options in the specified configuration file. To create an installation configuration file, see "Creating an Installation Configuration File for Stratus Cloud Workload Services" on page 31 To reinstall the software with this subcommand, you must uninstall the software first.
`uninstall`	Uninstalls Workload Services. To uninstall the software, you must use the `clouds` script for the currently installed release and not the installation script from another version. If you followed the installation procedure, the current script is in the `/opt/Release` directory of the Stratus appliance.
`-h`	Displays generic shell script help.
`-- help`	Displays cloud-specific script help. (You must insert a space between `--` and `help` in this subcommand.)
`--info`	Prints embedded information about the script.

`--list`	Prints a list of files in the installation archive.
`--check`	Verifies the integrity of the installation archive.

Examples

Install or upgrade the software:

```
./clouds-0.1.5.0.0.sh install install.conf
```

Uninstall the software:

```
./clouds-0.1.5.0.0.sh uninstall
```

Installing Stratus Cloud Availability Services

Installing Stratus Cloud Availability Services supplements the standard KVM hypervisor with Stratus availability extensions that allow you to deploy your mission-critical instances in fault-tolerant KVM (KVM-FT) pair groups. You can install Availability Services before or after installing Stratus Cloud Workload Services.

You may prefer to install Availability Services on your compute nodes when you configure your OpenStack environment to meet the requirements of the Stratus Cloud Solution, as described in other topics of the "Stratus Cloud Solution Installation Guide" on page 1.

To install Stratus Cloud Availability Services:

1. Prepare your OpenStack environment for the additional requirements of the KVM-FT hypervisor. See "KVM-FT Hardware and Software Requirements" on page 63.
2. Connect the Ethernet cables between the compute nodes that will run the KVM-FT hypervisor. See "Connecting Ethernet Cables Between KVM-FT Compute Nodes" on page 65.
3. Install the Availability Services software on the compute nodes. See "Installing Stratus Cloud Availability Services on KVM Compute Nodes" on page 68.
4. Install the Quorum server service (QSS) on two dedicated servers in your OpenStack environment. See "Installing Quorum Servers for Stratus Cloud Availability Services" on page 76.
5. Set the KVM-FT hypervisor pair group(s) and create a test application. See "Configuring the KVM-FT Hypervisor" on page 78.

Related Topics

"Upgrading Stratus Cloud Availability Services" on page 80

"Upgrading Quorum Servers for Stratus Cloud Availability Services" on page 83

"Uninstalling Stratus Cloud Availability Services" on page 84

KVM-FT Hardware and Software Requirements

In addition to the requirements discussed in "OpenStack Installation and Configuration" on page 14, ensure that your OpenStack environment includes:

- At least two dedicated Nova compute nodes that will run the KVM-FT hypervisor

  You install Stratus Cloud Availability Services on these compute nodes, and then select two nodes to be in each fault-tolerant KVM-FT pair group in Stratus Cloud Workload Services. Plan your KVM-FT pair groups carefully, because you cannot change them later without redeploying your KVM-FT applications.

- At least two dedicated nodes that will run the Quorum server service (QSS)

  You install and configure the quorum service on these nodes. The quorum service provides data integrity assurances and automatic restart capabilities for KVM-FT instances. Plan your quorum servers carefully, because you cannot change them later or change their IP addresses without redeploying your KVM-FT applications.

  The quorum service must be installed on servers that are reachable (over UDP) from the KVM-FT hypervisor. Most often, the quorum servers are installed in a similar manner to the OpenStack control plane servers such that the quorum servers are reachable through the OpenStack management network. The quorum protocol generates a small (<1K) packet every second and should not impact regular management traffic.

  The quorum service can be installed on any general-purpose computer with the following attributes:

  - Preferably a bare-metal system
  - Linux-based operating system
  - Small footprint
  - No other services running
  - Memory 512 MB or higher

- Fault-resilient and high-bandwidth Cinder block storage, if applicable

  Cinder resiliency must be supplied by your Cinder storage solution to protect your mission-critical applications.

  A 10Gb storage network is recommended for best performance and reliability, especially for high I/O applications running on Cinder boot and data volumes.

Be prepared to make the following physical connections for the compute nodes in each KVM-FT pair group:

- Two 10 gigibit (Gb) Ethernet links, known as A-links:
  - Either two 10Gb Ethernet adapters directly connected between the paired compute nodes (minimum configuration) or two 10Gb Ethernet adapters plugged into redundant 10Gb Ethernet switches that connect the paired compute nodes (recommended configuration)
  - Each Ethernet link located on a separate, single-port Ethernet adapter that can be easily replaced

Be prepared to install the following required software packages and repositories during the installation procedure:

- Kernel packages for CentOS 6.5:

  > **Note**: If you cannot locate these kernel packages, which are no longer available from the default `yum` repository, contact your service representative for assistance.

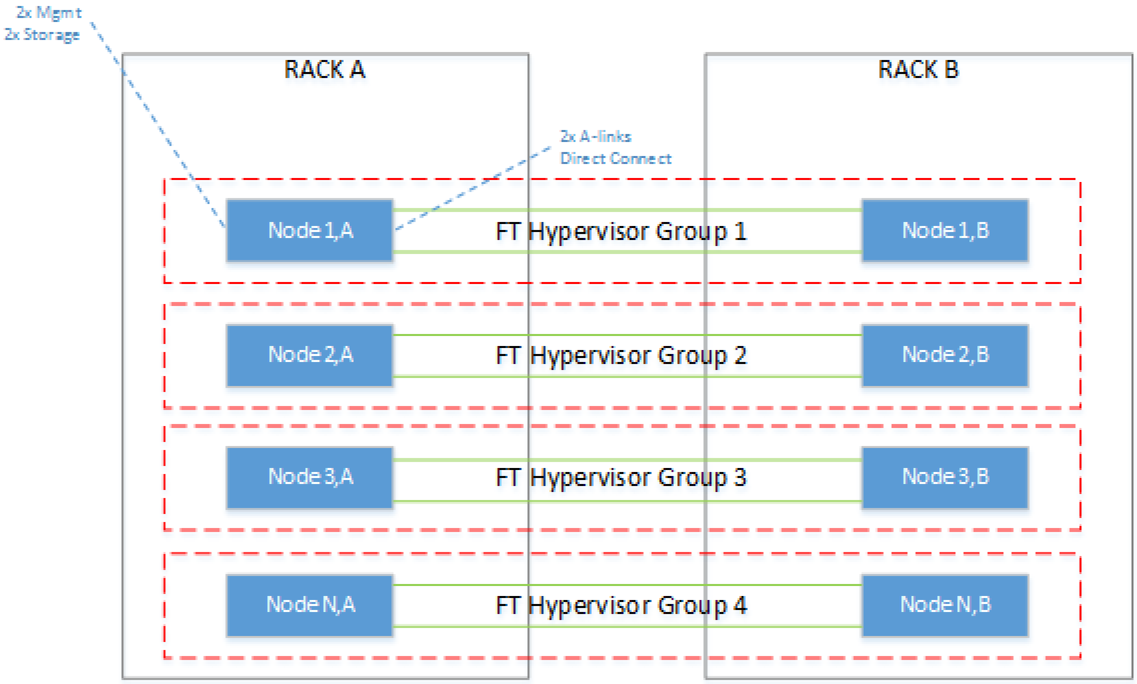
  - `kernel-2.6.32-431` (default kernel for CentOS 6.5, should already be installed)
  - `kernel-headers-2.6.32-431`
  - `kernel-devel-2.6.32-431`
  - `kernel-firmware-2.6.32-431`
- GNU Compiler Collection
  - `gcc` (not version specific)
- RPMforge Repository
  - `rpmforge-release-0.5.3-1.el6.rf.x86_64`

Connecting Ethernet Cables Between KVM-FT Compute Nodes

To establish the management network for KVM-FT operations, connect the A-Links between each pair of compute nodes that will run Stratus Cloud Availability Services. There are a few connection options, depending on the level of fault resiliency that you require.

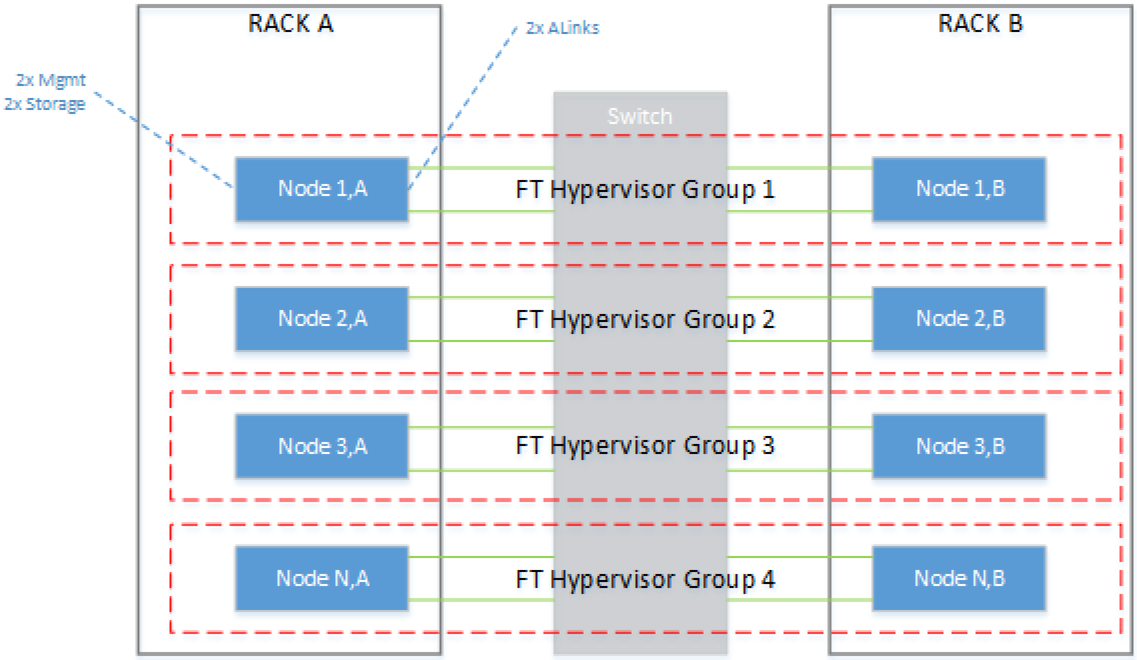
Direct Connection Configuration

For the most basic, minimum configuration, connect two Ethernet cables from 10Gb Ethernet ports on the first KVM-FT compute node to matching Ethernet ports on the second KVM-FT compute node.



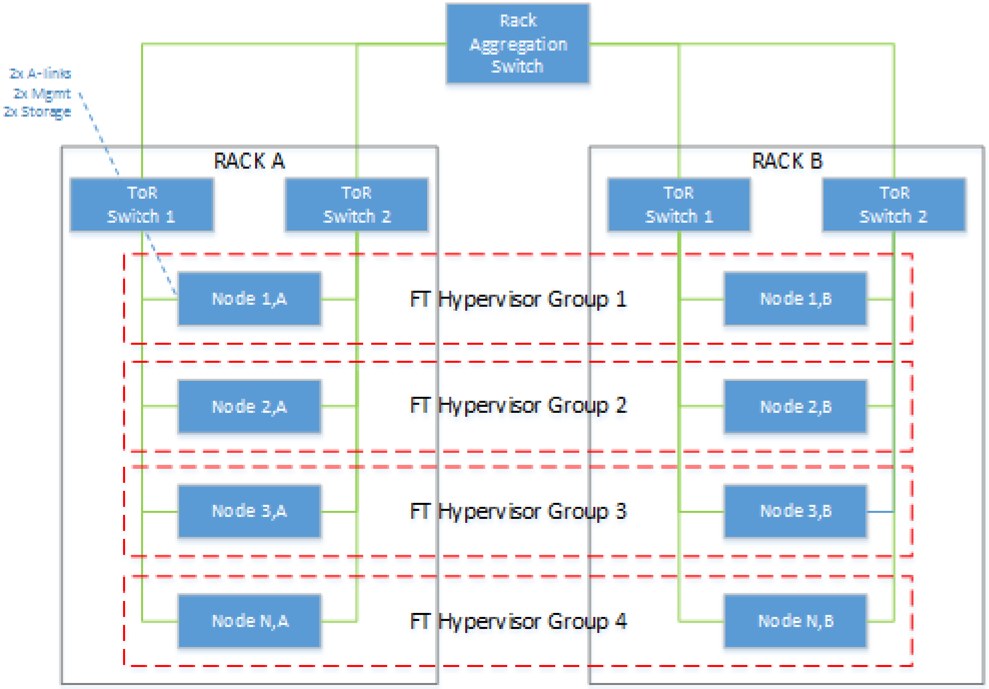
Single Switch Configuration

Alternatively, connect the two KVM-FT compute nodes through a single switch. Connect two Ethernet cables from 10Gb Ethernet ports on the first KVM-FT compute node to a 10Gb Ethernet switch, then connect two additional Ethernet cables from the switch to matching 10 Gb Ethernet ports on the second KVM-FT compute node.



Robust Configuration (Recommended)

For the highest level of fault resiliency, connect the A-Links through a series of redundant 10 Gb Ethernet switches. Even if a cable or switch fails in this configuration, the redundant connections keep your KVM-FT instances running until the problem is corrected.



Collecting Ethernet Device Names

Regardless of the configuration you use, make note of the Ethernet device names (for example, `eth1`) for the A-Links on each KVM-FT compute node. You need to specify these device names when you run the Availability Services installation script.

After connecting the cables, install the KVM-FT software as described in "Installing Stratus Cloud Availability Services on KVM Compute Nodes" on page 68.

Installing Stratus Cloud Availability Services on KVM Compute Nodes

Install Stratus Cloud Availability Services after you have prepared your OpenStack environment ("KVM-FT Hardware and Software Requirements" on page 63) and connected the Ethernet cables between the two compute nodes on which you will install the software ("Connecting Ethernet Cables Between KVM-FT Compute Nodes" on page 65).

To install Availability Services on KVM compute nodes:

1. Log on to the console of the compute node as `root` user, or be prepared to use `sudo` to run commands as `root`.
2. To prevent the `yum` utility from applying major version upgrades that are incompatible with Availability Services, edit the `/etc/yum.conf` file and ensure that the `exclude` line includes the

following entries:

```
exclude=kernel* redhat-release* centos-release* rdo-release*
```

These entries have the following effects:

- `kernel*` – prevents any kernel package or kernel extension package from being installed
- `Redhat-release*` – prevents Red Hat from upgrading your operating system version (for example, release 6.5 to 6.6)
- `Centos-release*` – prevents the CentOS release from being upgraded
- `Rdo-release*` – controls which version of OpenStack to install

3. Save the changes to the `yum.conf` file.

4. Install the `yum-utils` package for access to additional `yum` commands:

   ```
   # yum install yum-utils
   ```

5. Verify that there are no unfinished `yum` transactions by entering the following `yum` command:

   ```
   # yum-complete-transaction --cleanup-only
   Loaded plugins: fastestmirror
   Loading mirror speeds from cached hostfile
   * base: mirror.sanctuaryhost.com
   * epel: mirror.cogentco.com
   * extras: centos.mirror.nac.net
   * updates: mirror.wiredtree.com
   No unfinished transactions left.
   ```

   If there are unfinished transactions, resolve them before continuing with the installation.

6. Install the GNU Compiler Collection (`gcc`), as follows:

   ```
   # yum --exclude=*.i686 install gcc
   ```

7. Install the kernel packages that are required for the KVM-FT software. For example, execute the following command, where \ indicates line continuation:

> **Note**: If you cannot locate these kernel packages, which are no longer available from the default `yum` repository, contact your service representative for assistance. Each kernel package must match the currently installed kernel. If you have the required CentOS 6.5 kernel installed, `kernel-2.6.32-431`, the correct packages to install are `kernel-`*`package`*`-2.6.32-431`.

```
# rpm -i kernel-headers-2.6.32-431.el6.x86_64.rpm \
kernel-devel-2.6.32-431.el6.x86_64.rpm \
kernel-firmware-2.6.32-431.el6.x86_64.rpm
```

8. Add the RPMforge repository to your `yum` configuration, as follows:

```
# yum install http://pkgs.repoforge.org/rpmforge-release/rpmforge-release-0.5.3-1.el6.rf.x86_64.rpm
```

9. Examine the `/etc/libvirt/qemu.conf` file and verify that `dynamic_ownership` is set to the default of `1` (enabled).

   If you previously configured this compute node to run the standard KVM hypervisor with the Stratus Cloud Solution, you might have disabled `dynamic_ownership`, but it must be enabled for the KVM-FT hypervisor to function. If necessary, modify the setting as follows and save the file:

```
dynamic_ownership=1
```

10. If you modified the `qemu.conf` file, restart the compute node to apply the changes.

11. To prevent the `ip6tables` firewall service from interfering with KVM-FT hypervisor operations, disable the `ip6tables` service by entering the following commands:

```
# chkconfig ip6tables off
# service ip6tables stop
```

12. In the `/opt` directory, create a directory called `Release`:

```
# mkdir /opt/Release
```

13. Use a secure copy (SCP) utility to copy the KVM-FT installation shell script to the `/opt/Release` directory.

14. On the compute node, switch to the `/opt/Release` directory:

    ```
    # cd /opt/Release
    ```

15. Run the following command to make the installation script an executable file, where *script* is the name of the script:

    ```
    # chmod a+x script.sh
    ```

16. Run the installation script in the following format, where the *axlinkethdev1* and *axlinkethdev2* arguments represent the Ethernet devices to which the KVM-FT A-link cables are connected and *detectedLink* represents the network (adapter, virtual LAN, or channel bond) that handles data traffic for the instances:

    ```
    # ./kvm-ax-1.n.n install axlinkethdev1 axlinketdev2 detec-
    tedLink
    ```

    The *detectedLink* network is monitored for link up/down state transitions. A link down state indicates that KVM-FT instances may have lost network connectivity for this hypervisor. The KVM-FT software uses the state transitions to determine possible actions.

    Example output follows:

    ```
    # ./kvm-ax-1.0.6.sh install p5p1 p5p2 eth1.5

    Verifying archive integrity... All good.

    Uncompressing Availability eXtensions 1.0.6.............

    [12-16-2014 13:40:28] --> Checking current user...Ok

    [12-16-2014 13:40:28]
    @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

    [12-16-2014 13:40:28] _ ___ ____ ___ ___ __ __

    [12-16-2014 13:40:28] | | / / | | | \/ | / _ \ \ \ / /

    [12-16-2014 13:40:28] | |/ /| | | | . . |______/ /_\ \ \ V /

    [12-16-2014 13:40:28] | \| | | | |\/| |______| _ | / \

    [12-16-2014 13:40:28] | |\ \ \_/ / | | | | | | |/ /^\ \
    ```

```
[12-16-2014 13:40:28] \_| \_/\___/\_| |_/ \_| |_/\/ \/
[12-16-2014 13:40:28]
[12-16-2014 13:40:28] @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[12-16-2014 13:40:28] --> Install Stratus KVM
[12-16-2014 13:40:28] --> Availability eXtenstions
[12-16-2014 13:40:28] -->
[12-16-2014 13:40:28] --> Install output will be located in:
[12-16-2014 13:40:28] --> /opt/stratus/logs/install-201412161340.log
[12-16-2014 13:40:28]
[12-16-2014 13:40:28] ATTENTION
[12-16-2014 13:40:28] * Make sure p5p1, p5p2 are
[12-16-2014 13:40:28] not restricted by ip6tables, see documentation
[12-16-2014 13:40:28] for further details
[12-16-2014 13:40:28] * Make sure you have a valid kernel-devel
[12-16-2014 13:40:28] package installed
[12-16-2014 13:40:28] * Make sure you have a valid gcc install
[12-16-2014 13:40:28]
[12-16-2014 13:40:28] --> Checking for the kernel-devel package...
[12-16-2014 13:40:29] --> Install rpmforge-release repository...
[12-16-2014 13:40:29] --> Installing packages...
```

```
[12-16-2014 13:40:29] ----> ./fastcgi++-2.1-1.0.0.0_88.x86_
64.rpm
[12-16-2014 13:40:29] ----> ./fastcgi++-libs-2.1-1.0.0.0_
88.x86_64.rpm
[12-16-2014 13:40:29] ----> ./libjson-7.6.1-1.0.0.0_88.x86_
64.rpm
[12-16-2014 13:40:29] ----> ./lsb-ft-core-cloud-kvm-kmods-
1.0.0.0-88.x86_64.rpm
[12-16-2014 13:40:29] ----> ./lsb-ft-core-cloud-qemu-1.0.0.0-
88.x86_64.rpm
[12-16-2014 13:40:29] ----> ./lsb-ft-core-cloud-utils-1.0.0.0-
88.x86_64.rpm
[12-16-2014 13:40:29] ----> ./stratus-nova-driver-1.0.6-
1.el6.noarch.rpm
[12-16-2014 13:44:14] --> Checking for lighttpd...
[12-16-2014 13:44:14] --> Installing lighttpd...
[12-16-2014 13:44:44] --> Installing lighttpd-fastcgi...
[12-16-2014 13:44:47] --> lighttpd version 1.4.35 installed..
[12-16-2014 13:44:47] --> Update server location...
[12-16-2014 13:44:47] --> Update /etc/-
lighttpd/lighttpd.conf...
[12-16-2014 13:44:47] --> Update /etc/lighttpd/modules.conf...
[12-16-2014 13:44:47] --> Update /etc/-
lighttpd/conf.d/fastcgi.conf
Starting lighttpd: [ OK ]
```

```
[12-16-2014 13:44:47] --> Updating firewall rules for 80, 443,
8080...

-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT

[12-16-2014 13:44:47] ...rule exists... INPUT -p tcp -m tcp --
dport 80 -j ACCEPT

-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT

[12-16-2014 13:44:47] ...rule exists... INPUT -p tcp -m tcp --
dport 443 -j ACCEPT

[12-16-2014 13:44:48] Ok

[12-16-2014 13:44:48] --> Create directory /var/opt/ft/ax

[12-16-2014 13:44:48] --> Update /etc/nova/kvmax.conf with
p5p1, p5p2

[12-16-2014 13:44:48] --> The KVM-AX installation will modi-
fy/add

[12-16-2014 13:44:48] --> the following variables

[12-16-2014 13:44:48] --> defined in the file.

[12-16-2014 13:44:48] -->

[12-16-2014 13:44:48] --> net.core.rmem_default = 16777216

[12-16-2014 13:44:48] --> net.core.rmem_max = 20971520

[12-16-2014 13:44:48] --> net.core.wmem_default = 16777216

[12-16-2014 13:44:48] --> net.core.wmem_max = 20971520

[12-16-2014 13:44:48] --> net.core.optmem_max = 2048000

[12-16-2014 13:44:48] --> net.ipv4.tcp_rmem = 1024000 8738000
16777216

[12-16-2014 13:44:48] --> net.ipv4.tcp_wmem = 1024000 8738000
16777216
```

```
[12-16-2014 13:44:48] --> net.ipv4.tcp_mem = 1024000 8738000
16777216

[12-16-2014 13:44:48] --> net.ipv4.udp_mem =1024000 8738000
16777216

[12-16-2014 13:44:48] --> Install complete
```

17. When the installation is complete, verify that the correct KVM driver was loaded. Execute the following command and ensure that the `extra` subdirectory is included in the filename, as indicated:

    ```
    # modinfo kvm_intel

    filename: /lib/modules/2.6.32-431.el6.x86_64/extra/kvm-
    intel.ko

    license: GPL

    author: Qumranet
    ```

    If the `extra` subdirectory is not present, the incorrect KVM driver or build is loaded. Ensure the compute node meets the prerequisites for installing the KVM-FT software and that you have installed the correct `gcc` and `kernel` packages. Correct any problems, uninstall the KVM-FT software as described in "Uninstalling Stratus Cloud Availability Services" on page 84, and then run the installation script again.

18. If you are upgrading from a previous version of the KVM-FT software, optionally verify that the date of the kernel module is consistent with the version that you installed. Execute the following command, where the filename that you specify must match the `filename` from the output of the `modinfo kvm_intel` command from the previous step:

    ```
    # ls -l /lib/modules/2.6.32-431.el6.x86_64/extra/kvm-intel.ko
    -rw-r--r-- 1 root root 109960 Jan 26 10:35 /lib/-
    modules/2.6.32-431.el6.x86_64/extra/kvm-intel.ko
    ```

    The date of the kernel module must match the date when you ran the installation script.

19. If the KVM-FT installation was successful, restart the compute node.

20. Repeat the previous steps to install the KVM-FT software on the second compute node. If you plan to install the software on more than two compute nodes, you can install the software on all of the

compute nodes now, or continue with installing the quorum servers and configuring your first FT pair group so you can test an application.

21. Install the quorum servers, as described in "Installing Quorum Servers for Stratus Cloud Availability Services" on page 76.

Installing Quorum Servers for Stratus Cloud Availability Services

To maintain the integrity of KVM-FT instances against multiple network failure scenarios, you must install the fault-tolerant Quorum server service (QSS) on two dedicated, Linux-based computers in your OpenStack environment. For information about the system requirements for the quorum servers, see "KVM-FT Hardware and Software Requirements" on page 63.

Cautions:

1. You must install the quorum servers before deploying your first KVM-FT application. Select your quorum servers carefully, because you cannot change them later or change their IP addresses without redeploying your KVM-FT applications.
2. QSS must remain running on both quorum servers to ensure the fault-tolerant operation of your KVM-FT instances. If one node fails, the other node keeps the quorum service running; however, the KVM-FT instances are reported as DEGRADED until the problem is corrected.

To install the quorum servers:

1. Log on to the console of the first quorum server as the `root` user, or be prepared to use `sudo` to run commands as `root`.
2. In the `/opt` directory, create a directory called `Release`:

   ```
   # mkdir /opt/Release
   ```

3. Use a secure copy (SCP) utility to copy the quorum service RPM file to the `/opt/Release` directory.

   You can copy the quorum service RPM file (`lsb-ft-core-cloud-qss-`*n.n.n.n-nnn*`.x86_64.rpm`) from the `/opt/stratus/rpms` directory of one your KVM-FT compute nodes after you install Availability Services.

4. On the quorum server, switch to the `/opt/Release` directory:

```
# cd /opt/Release
```

5. Install the RPM file by executing the following command:

```
# rpm -i lsb-ft-core-cloud-qss-1.n.n.n-nnn.x86_64.rpm
```

6. Open port 4557 (UDP) through the firewall by entering the following commands:

```
# iptables -A INPUT -p udp --dport 4557 -j ACCEPT
# iptables -A OUTPUT -p udp --dport 4557 -j ACCEPT
# service iptables save
```

7. Verify that the quorum service is running by entering the following command:

```
# ps -ef|grep qss
```

   If the quorum service is running, it appears in the output as follows:

```
root      25913     1   0 Jan23 ?        00:06:45 /op-
t/ft/sbin/qss -f
500       31627 23021  0 18:19 pts/1    00:00:00 grep qss
```

8. Record the IP address of the quorum server. For example, execute the `ifconfig -a` command and note the IP address of the `eth0` interface:

```
# ifconfig -a
eth0       Link encap:Ethernet  HWaddr FA:16:3E:09:32:F8
inet addr:192.168.101.183  Bcast:192.168.101.255
Mask:255.255.255.0
inet6 addr: fe80::f816:3eff:fe09:32f8/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1400  Metric:1
RX packets:2719992304 errors:0 dropped:0 overruns:0 frame:0
TX packets:1960011351 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:3721803293741 (3.3 TiB)  TX bytes:1260482520546 (1.1
TiB)
```

```
.
.
.
```

9. Repeat the preceding steps on the second quorum server.
10. After installing the quorum service on both servers, log on to the Stratus appliance as the `cloud-user` and execute the `su` command to become the `root` user (or be prepared to use `sudo` to run commands as `root`).
11. Open the `/opt/jetty/resources/CloudMgmtExt.properties` file in a text editor and locate the `KvmFTQuorumnIP` entries. Uncomment these entries (remove `#`) and specify the IP addresses of the quorum servers where shown in red:

    ```
    # KVM-FT Quorum IPs
    #KvmFtQuorum1Ip=<change_on_setup>
    #KvmFtQuorum2Ip=<change_on_setup>
    ```

    Enter the IP addresses you collected from the quorum servers. For example:

    ```
    KvmFtQuorum2Ip=192.168.101.183
    ```

    ```
    KvmFtQuorum1Ip=192.168.101.135
    ```

12. Save and close the `CloudMgmtExt.properties` file.
13. Restart Jetty in the Stratus appliance by entering the command `service jetty restart`.
14. Configure the KVM-FT hypervisor, as described in "Configuring the KVM-FT Hypervisor" on page 78.

Configuring the KVM-FT Hypervisor

After installing the KVM-FT hypervisor ("Installing Stratus Cloud Availability Services on KVM Compute Nodes" on page 68), configure the hypervisors by adding each compute node to a KVM-FT pair group.

> **Caution**: Select your KVM-FT pair groups carefully, because you cannot change them later without redeploying your KVM-FT applications.

To set a KVM-FT hypervisor pair group:

1. In the main menu of Stratus Cloud Workload Services, click **Hypervisors** to display the **Hypervisors** page.

2. On the **Hypervisors** page, locate the first pair of KVM-FT hypervisors, or compute nodes, that you want to configure as a KVM-FT pair group.

3. Click the first KVM-FT hypervisor that you want to add to the pair group. In the option buttons, click ✎ to display the **Edit Hypervisor** panel.

4. In the **Edit Hypervisor** panel, scroll down to **Service Level Definitions**, and specify the following tags:

   - **Availability Level**: Select **Mission Critical.**

   - **Hypervisor Type**: Select **KVM-FT**.

   - **FT Pair Group**: If this is your first KVM-FT pair group, select **Default Pair Group**. If you are adding another pair group, select a different pair group name. (You can add pair group names as described below under **To add more KVM-FT pair groups**.)

     Note: The **FT Pair Group** field displays only when the selected hypervisor type is KVM-FT.

   - **Hypervisor Instance Storage Type**: Select the storage type for the hypervisor.

   - **Location**: Select one or more deployment locations for the hypervisor.

5. Complete any other fields as needed, and then click **Save**.

6. Repeat steps 3-5 to add the second KVM-FT hypervisor to the same KVM-FT pair group.

7.

8. Ensure that you have installed the two quorum servers required by the KVM-FT hypervisor, as described in "Installing Quorum Servers for Stratus Cloud Availability Services" on page 76.

   Caution: The quorum servers must be installed and running before you deploy your first KVM-FT application.

9. Create a test application to verify that your KVM-FT configuration is functioning properly. For an example that summarizes the process of creating an application, from configuring network con-

nections to creating and deploying a service catalog application, see How to Deploy an Application.

To add more KVM-FT pair groups (if applicable):

1. Ensure that you have connected the KVM-FT A-links and installed the KVM-FT software on the compute nodes.
2. In the main menu of Stratus Cloud Workload Services, select **Service Level Definitions** to display the **Service Level Definitions** page.
3. On the **Service Level Definitions** page, click **Add Tag** in the upper right corner of the page to display the **Create New Tag** panel.
4. In the **Create New Tag** panel, complete the following:
   - **Name**: Type a name for the new pair group. This name displays on the **Service Level Definitions** page.
   - **Standard Name**: Type a standard name for the new tag. This tag name gets propagated through the back end.
   - **Nest Tag Under**: Select **FT Pair Group**.
   - **Description**: Type descriptive information about the new tag. Information added here displays at the right of the tag name in the listing on the **Service Level Definitions** page.
5. Click **Create**.
6. Repeat steps 1-5 to create additional pair groups, if applicable.
7. To add compute nodes to each new pair group, repeat the procedure above **To set a KVM-FT hypervisor pair group**.

Upgrading Stratus Cloud Availability Services

This topic describes how to upgrade Stratus Cloud Availability Services on your KVM compute nodes. You may need to upgrade Availability Services to install updates specific to the KVM-FT hypervisor or to install new features in conjunction with a new Stratus Cloud Workload Services release.

Upgrade Availability Services on one compute node at a time and in one FT pair group at a time. For example, shut down each KVM-FT instance running on the first compute node, uninstall the older Availability Services release, and then install the new software release. Start each of the KVM-FT instances on the first node, one instance at a time, and verify that they return to the Running/Paired state. When the first compute node and all of its instances are up and running on the upgraded software, repeat the process on the second node of the FT pair group. In each case, the paired KVM-FT instances on the running compute node keep your applications running during the upgrade.

After upgrading Availability Services, you may also need to upgrade the quorum server service (QSS) on your quorum servers. For more information, see "Upgrading Quorum Servers for Stratus Cloud Availability Services" on page 83.

To upgrade Availability Services on KVM compute nodes:

1. In the main menu of Stratus Cloud Workload Services, click **Hypervisors**.
2. On the **Hypervisors** page, locate the KVM-FT hypervisors (compute nodes). Decide which hypervisor to upgrade first and record its name. Upgrade only one hypervisor at a time, in the same FT pair group.
3. Click the hypervisor that you want to upgrade and click 🔍 to view its summary page.
4. On the summary page, under **Deployed Instances**, record the names of the KVM-FT instances that are running on the hypervisor that you selected for upgrade. Close the summary page.
5. In the main menu, click **Deployed Applications**.
6. On the **Deployed Applications** page, next to **Group by**, click **Availability** and then click **Mission Critical** to expand the category. The **Mission Critical** category typically contains most or all of your KVM-FT instances, but you may need to check other categories as well.
7. Click each application to expand it, and locate the KVM-FT instances that are running on the hypervisor that you want to upgrade. For each application associated with these instances, ensure that one of the instances is in the **Running** state and that the second instance is in the **Paired** state, which indicates that the pair is running normally in fault-tolerant mode.

   > **Caution**: If any of the instances have advisories or are in a state other than Paired/Running, correct any problems before upgrading the hypervisor.

8. If all KVM-FT instances are paired, carefully locate and shut down only the instances on the hypervisor that you want to upgrade. Click the instance, click 🔍, and click ⏻ to stop the instance.

   As long as the application is currently fault-tolerant, and you stop only the instance on the hypervisor you want to upgrade, it does not matter whether that particular instance is in the **Running** or **Paired** state. The other instance keeps the application running.

9. Monitor the instances as they go from the **Stopped** to **Shutoff** state. Ensure that all of the instances are in the **Shutoff** state before you continue. You can monitor the transitions on the **Deployed Applications** page and also on the **Advisories** tab of the **Dashboard** page.
10. When all of the instances on the hypervisor that you want to upgrade are in the **Shutoff** state, uninstall the older version of Availability Services on the hypervisor as described in "Uninstalling Stratus Cloud Availability Services" on page 84.
11. After uninstalling the older version of Availability Services, install the new version as described in "Installing Stratus Cloud Availability Services on KVM Compute Nodes" on page 68.
12. Optionally, reboot the compute node. Typically, this is unnecessary, but you must reboot if you forgot to shut down a KVM-FT instance on the compute node before the upgrade. The compute node cannot switch to the new KVM-FT kernel module while instances are still accessing the old kernel module.
13. In the main menu of Workload Services, click **Deployed Applications**.
14. On the **Deployed Applications** page, next to **Group by**, click **Availability** and then click **Mission Critical** to expand the category.
15. Locate the KVM-FT instances that are on the hypervisor that you just upgraded.
16. Start only one KVM-FT instance and monitor its progress on the **Deployed Applications** page and on the **Dashboard** page as it transitions through various states. It is normal to see critical (red) and warning (orange) states on the **Dashboard** page as startup and sync proceeds.
17. When the **Dashboard** status reaches the normal (green) state and advisories are resolved, go back to the **Deployed Applications** page. For the KVM-FT instance that you started, ensure that the paired instances in the application have returned to the **Running** and **Paired** states.
18. Start the additional KVM-FT instances on the hypervisor that you upgraded one at a time in the same manner.
19. After starting the KVM-FT instances, verify that the new Availability Services version is recognized by Workload Services. On the **Hypervisors** page, click the upgraded hypervisor, click 🔍 to view the summary page, and verify the value in the **KVM-AX Version** field. (The version is displayed only if KVM-FT instances are deployed and running.)
20. Repeat steps 1-20 for the second hypervisor in the FT pair group.
21. Repeat steps 1-21 for additional FT pair groups.

22. If needed, upgrade the quorum service on your quorum servers.See "Upgrading Quorum Servers for Stratus Cloud Availability Services" on page 83.

Upgrading Quorum Servers for Stratus Cloud Availability Services

This topic describes how to upgrade the Quorum server service (QSS) on the quorum servers associated with Stratus Cloud Availability Services. You may need to upgrade the quorum service as a result of upgrading Availability Services to a new release.

To upgrade the quorum service, first uninstall the QSS package on the quorum server, and then install the new package.

Cautions:

1. Before upgrading the quorum servers, ensure that all of your KVM-FT instances are in the fault-tolerant Running/Paired state.
2. Upgrade one quorum server at a time. Do not upgrade the second quorum server until the first server is running the new software and your KVM-FT instances return to the Running/Paired state.
3. At least one quorum server must be running at all times to maintain the integrity of the KVM-FT instances. It is normal for the KVM-FT instances to become DEGRADED temporarily while a single quorum server is offline for the upgrade.

To upgrade the quorum servers:

1. Log on to Stratus Cloud Workload Services and ensure that all of your KVM-FT instances are in the fault-tolerant Running/Paired state, as follows:
   a. On the **Deployed Applications** page, next to **Group by**, click **Availability** and then click **Mission Critical** to expand the category. The **Mission Critical** category typically contains most or all of your KVM-FT instances, but you may need to check other categories as well.
   b. Click each application to expand it. Ensure that one of the KVM-FT instances is in the **Running** state and that the other instance is in the **Paired** state. If any of the instances have advisories or are in a state other than Running/Paired, correct any problems before upgrading the quorum servers.
2. Log on to the console of the first quorum server as the `root` user, or be prepared to use `sudo` to run commands as `root`.

3. Transfer the new quorum service RPM file to the `/opt/Release` directory. For example, use a secure copy (SCP) utility to copy the file from another system.

   The quorum service RPM file (`lsb-ft-core-cloud-qss-n.n.n.n-nnn.x86_64.rpm`) is available in the `/opt/stratus/rpms` directory of your KVM-FT compute nodes after you upgrade the KVM-FT software.

4. Determine the name of the currently installed quorum service RPM package. For example:

   ```
   # rpm -qa | grep qss
   lsb-ft-core-cloud-qss-1.0.0.0-112.x86_64
   ```

5. Uninstall the package by executing the following command:

   ```
   # rpm -e lsb-ft-core-cloud-qss-1.n.n.n-nnn.x86_64
   ```

6. On the quorum server, switch to the `/opt/Release` directory:

   ```
   # cd /opt/Release
   ```

7. Install the new RPM file by executing the following command:

   ```
   # rpm -i lsb-ft-core-cloud-qss-1.n.n.n-nnn.x86_64.rpm
   ```

8. Verify that the quorum service is running by entering the following command:

   ```
   # ps -ef|grep qss
   ```

   If the quorum service is running, it appears in the output as follows:

   ```
   root     25913     1  0 Jan23 ?       00:06:45 /opt/ft/sbin/qss -f
   500      31627 23021  0 18:19 pts/1    00:00:00 grep qss
   ```

9. In Workload Services, ensure that all of your KVM-FT instances are in the fault-tolerant Running/Paired state before upgrading the second quorum server.

10. Repeat the preceding steps to upgrade the second quorum server.

Uninstalling Stratus Cloud Availability Services

Uninstall Stratus Cloud Availability Services if you need to upgrade the software as described in "Upgrading Stratus Cloud Availability Services" on page 80, or if the initial installation failed and you need to start over.

> **Note**: To uninstall Availability Services, you must use the installation script for the currently installed version of Availability Services and not the installation script from another build or version. If you followed the installation procedure, the current script is in the `/opt/Release` directory of the KVM-FT compute node.

To uninstall Availability Services:

1. Log on to the console of the compute node as `root`, or be prepared to use `sudo` to run commands as `root`.
2. Delete any KVM-FT applications/instances that you have created.
3. Execute a command similar to the following to uninstall the software:

   ```
   # /opt/Release/kvm-ax-n.n.n.sh uninstall
   ```

4. If necessary, stop the lamo service. For example, execute:

   ```
   # killall lamo
   ```

5. Repeat these steps on the second KVM-FT compute node.