STANDARD PROCEDURE FOR REPLACING A DEFECTIVE NODE OF CLUSTER (RMA)

THIS PROCEDURE IS APPLICABLE TO BOTH ACTIVE-PASSIVE (A/P) AND ACTIVE-ACTIVE (A/A) CLUSTERS

SUMMARY:

This document describes proper procedure for replacing a defective node of an SA cluster. The steps described here is applicable to any kind of cluster and whether the defective unit is the node which holds the main licenses or the CL license holder node (old licensing scheme in pre-7.0).

Essentially, the process of replacing a FIPS or non-FIPS node involves few simple steps and are similar in most ways except for the security world (or keystore) settings, such as the keystore restore password (for x500FIPS systems). Being ready with these preliminary information will ensure successful re-introduction of this RMA node to an existing cluster.

A combination of admin UI and also serial console to complete the replacement can be used but it is preferred that we use serial console mostly for this process especially for FIPS devices.

PRE-REQUISITES TO UPGRADE:

The following requirements and guidelines are necessary items to be done to replace a node in the cluster.

- Ensure that serial console is available as most of the activities are done via serial console
- Document or get the cluster configuration from your documentation, or get it from the existing working node
- Be ready with the cluster information and this node's local settings
    * Cluster name and password
    * IP address details of this node (has to be the same as the setting on defective unit it is replacing)
    * IP address of the existing main license node
    * Keystore restore password of the cluster (for x500FIPS)
- Create a backup of system, user accounts, and IVS (if used) configurations of the existing device (main license holder if using CL licensing scheme)
- Backup your licenses, as well
- Ensure that cluster connectivity between the existing node and this RMA node is functional or healthy
- Ensure that you have at hand the new license for the RMA unit either obtained via generating your own replacement licenses from the support LMS site or via Juniper customer care (**instructions at the bottom of this document**)
- Schedule the replacement during a maintenance window

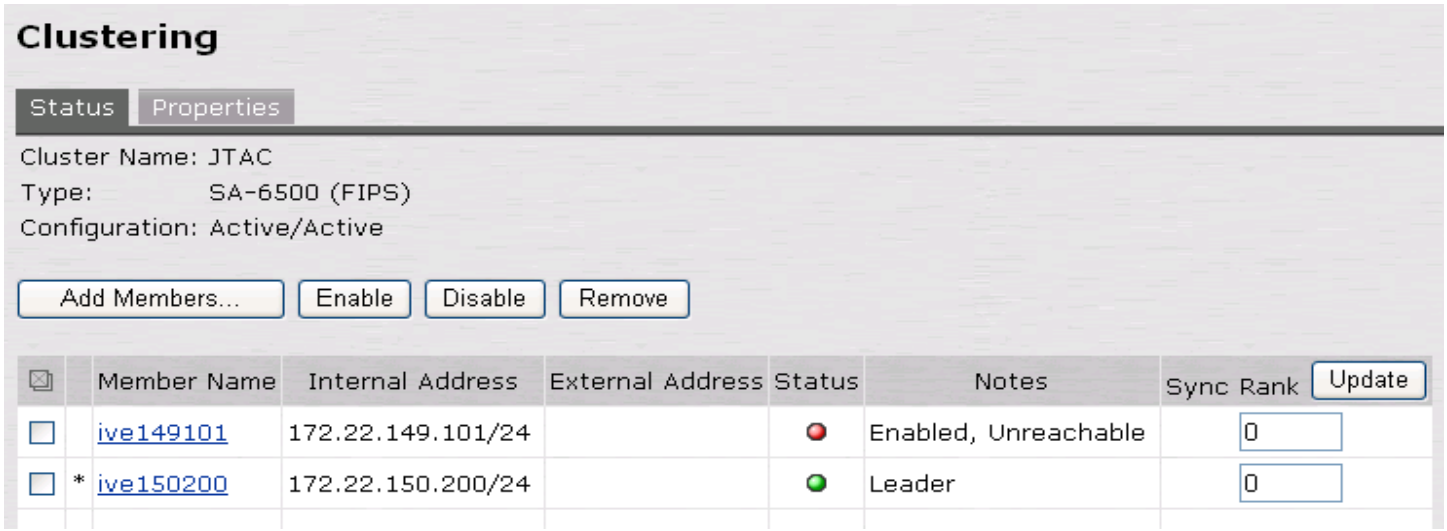
STEP-BY-STEP NODE REPLACEMENT PROCEDURE:

NOTES:

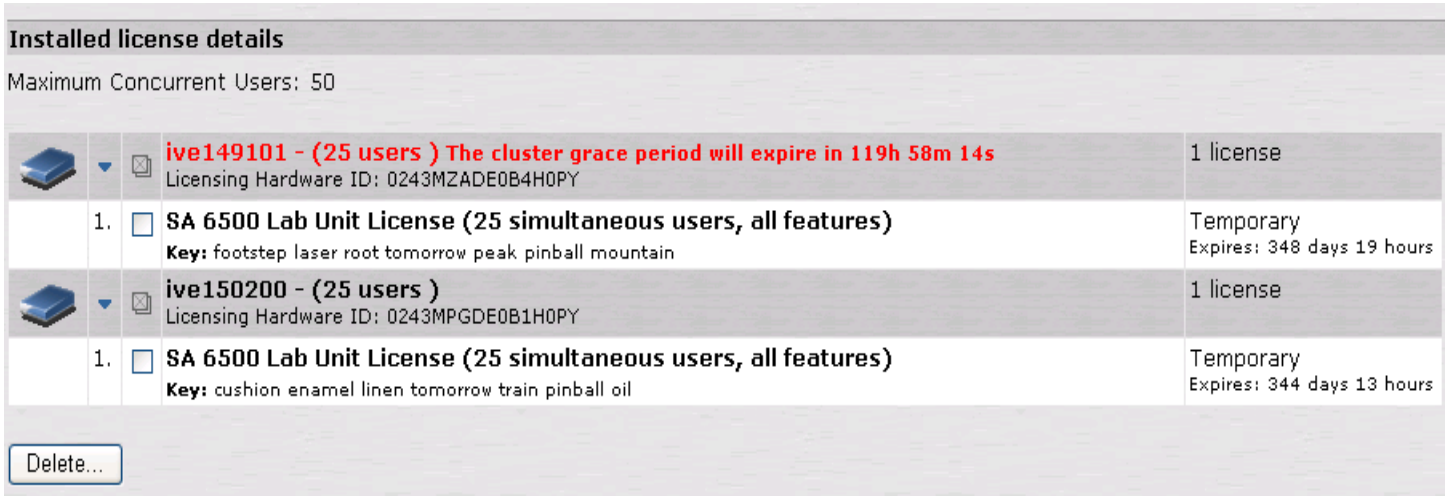
- When a node joins a cluster, its configuration essentially is wiped out and the other node sends the system, user and cluster configurations that were configured on the defective node to this joining node, including the keystore and certificates (if x500FIPS)
- Joining a node to an existing cluster as a new node is the same similar replacement steps except for adding the permanent license for this RMA unit (see procedure for generating your replacement license)
- After restore of cluster, the license that was in the old node will install as temporary license to this new node for 90 days and will be fine to use, however, it is better to install new license as soon as cluster is reformed and healthy
- X500FIPS and regular SA follows same RMA procedure of replacement except the security settings specific to FIPS

Status of cluster as exampled here is the primary node (main license holder) as the defective unit (**screenshots are from an SA-6500FIPS cluster running 7.1**).

Clustering status page:

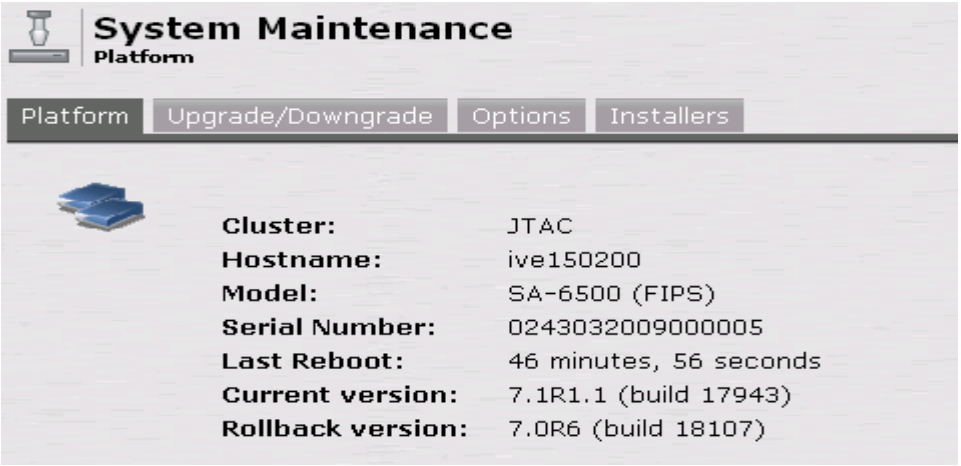


Licensing page (different if using pre-7.0):



The following chronological steps will introduce a new x500FIPS device to an existing cluster (either as a replacement or new node being added to the cluster). For non-x500FIPS, it is similar except for the FIPS module security settings setup:

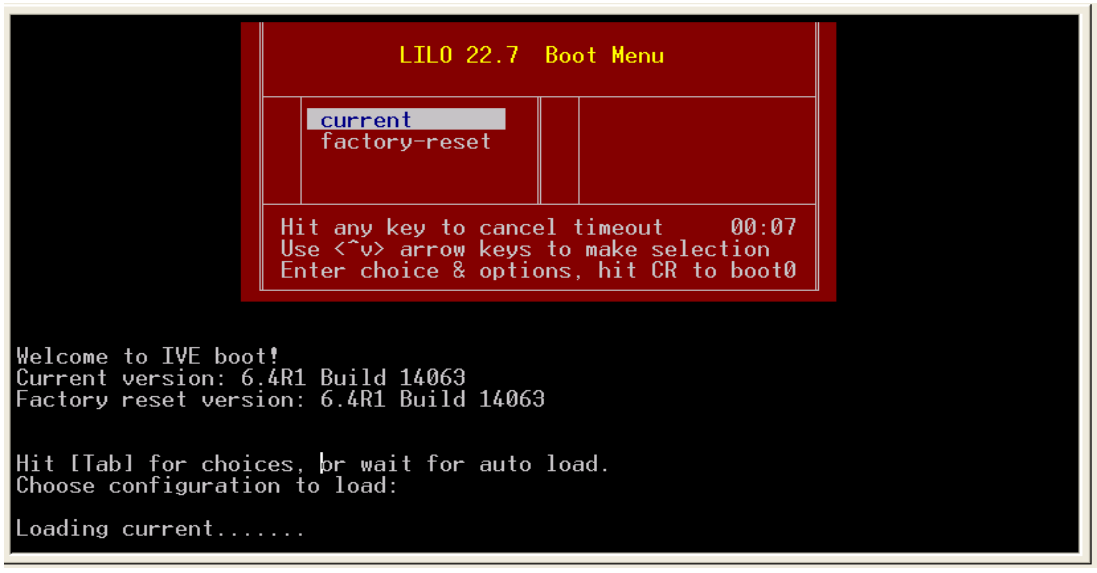
1. When a RMA unit is received from Juniper, check that it is the same model by looking at the serial number. You can also get the serial number and model number from the adminUI after it is initially configured:



2. If the defective or unit to be replaced is still powered up, power this down and remove
3. Install the new unit and proceed to do initial configurations until it is up as a standalone device.

Procedure: Steps in initializing a new x500-FIPS unit as an example

Upon power up, factory reset partition is booted up as the current partition (6.4R1 in earlier versions but have changed to 6.5R7 in new devices for x500FIPS only):



Answer "**y**" to the prompt:

```
Starting system software version 6.4R1 (build 14063)


Using drivers: igb e1000
........

Licensing Hardware ID: 0243MZADE0B4H0PY

No data to import
Creating initial default data
.
About to boot as a stand-alone IVE.
Hit TAB for clustering options, wait or hit Enter to continue.....
Starting Core Services

Welcome to the initial configuration of your server!
NOTE: Press 'y' if this is a stand-alone server or the first
machine in a clustered configuration.
If this is going to be a member of an already running cluster
press n to reboot. When you see the 'Hit TAB for clustering options'
message press TAB and follow the directions.
Would you like to proceed (y/n)?: _
```

Accept the license agreement and provide initial network information:

```
Do you agree to the terms of the license agreement (y/n/r)?: y


Please provide ethernet configuration information
  IP address:      172.22.149.101
  Network mask:    255.255.255.0
  Default gateway: 172.22.149.1
Please provide DNS nameserver information:
  Primary DNS server:   172.1.1.1
  Secondary (optional):
  DNS domain(s):    jtac.net
Please provide Microsoft WINS server information:
  WINS server (optional):

Please confirm the following setup:
  IP address:         172.22.149.101
  Network mask:       255.255.255.0
  Gateway IP:         172.22.149.1
  Link speed:         Auto
  Primary DNS server: 172.1.1.1
  Secondary DNS:
  DNS domain(s):      jtac.net
  WINS server:
Correct? (y/n):
```

Create admin login name and password:

```
  DNS domain(s):      jtac.net
  WINS server:
Correct? (y/n): y

Initial network configuration complete.

---------------------------------


Please create an administrator username and password.
Admin username: admin
Password:
Confirm password:

The administrator was successfully created.

---------------------------------

Sun SCA6000 firmware requires update. This will be followed
by an import of the currently installed key store.

Zeroizing device mca0, this may take a few minutes.
Please be patient.
```

(**For x550FIPS**) It resets the HSM card and updates the firmware of HSM to current supported and certified version 1.0, then provide the “security world” or keystore security settings such as:

Security Officer Name and password:

```
Please create an administrator username and password.
Admin username: admin
Password:
Confirm password:

The administrator was successfully created.

-----------------------------------

Sun SCA6000 firmware requires update. This will be followed
by an import of the currently installed key store.

Zeroizing device mca0, this may take a few minutes.
Please be patient.
Device mca0 zeroized.
Updating firmware on mca0, this may take a few minutes.
Please be patient.
Firmware update on mca0 complete.
Reset required to activate new firmware.

Please initialize SCA FIPS card.

Security Officer Name: _
```

(**For x500FIPS**) Restore Password and then Web server User Name and Password that webserver will use to authenticate to HSM:

```
Zeroizing device mca0, this may take a few minutes.
Please be patient.
Device mca0 zeroized.
Updating firmware on mca0, this may take a few minutes.
Please be patient.
Firmware update on mca0 complete.
Reset required to activate new firmware.

Please initialize SCA FIPS card.

Security Officer Name: jtac
Security Officer Password:
Confirm Password:

Please provide a restore password for the key store.

Restore Password:
Confirm Password:

Please provide key store user credentials for use by the web server.

User Name:
```

(**For x500FIPS**) Provide parameters for creation of self-signed digital cert for Web Server:

IVE Common Name and Organization Name:

```
Restore Password:
Confirm Password:

Please provide key store user credentials for use by the web server.

User Name: admin
User Password:
Confirm Password:



Please provide information to create a self-signed Web server
digital certificate.
  Common name (example: secure.company.com): ive109.jtac.net
  Organization name (example: Company Inc.): JTAC


Creating self-signed digital certificate - this may take several minutes..._
```

It then creates the cert and brings up IVE for use and this completes the initial configurations.

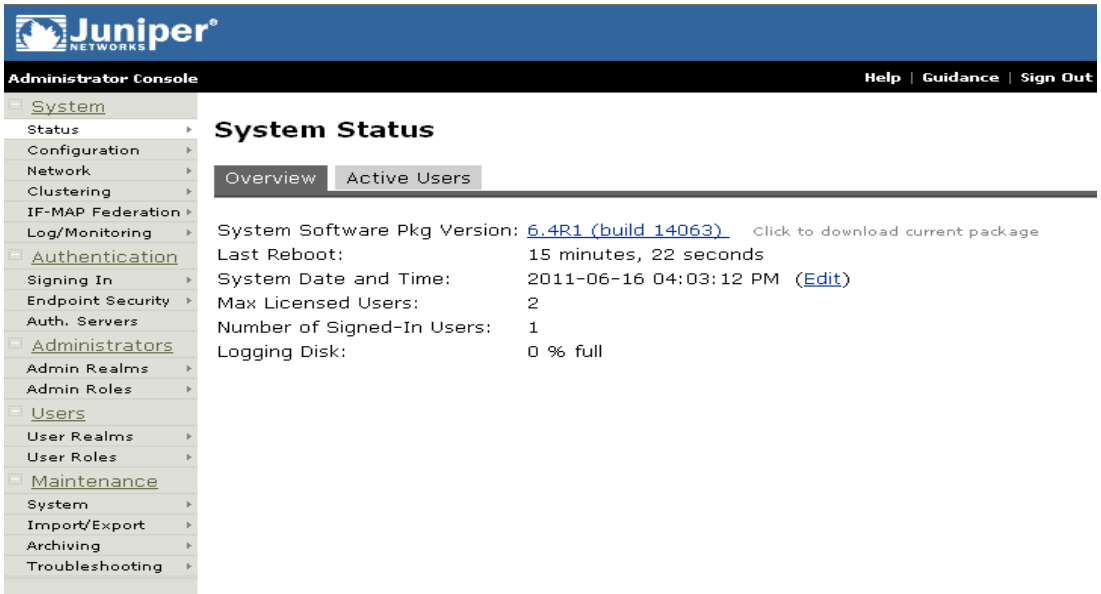
```
Creating self-signed digital certificate - this may take several minutes...
The self-signed digital certificate was successfully created.

---------------------------------
Congratulations!  You have successfully completed the
initial set up of your server.


    To administer the system, please browse to an appropriate URL:

    https://<IVE-IP-Address>/admin (note the 's' in https://)
    Example: https://10.10.22.34/admin

    If a DNS name already exists for this IVE, you can also use:

    https://<IVE-Host-Name>/admin
    Example: https://IVE.mycompany.com/admin

---------------------------------

System is now ready.

Press Enter to modify system settings._
```

4. After configuring as standalone device, login as Admin to this new box and upgrade the software code to the same release as the existing cluster. Although this step can be bypassed and just let the system automatically get upgraded by a package push from the existing node during cluster formation or re-formation, it will cut the time to do the RMA process

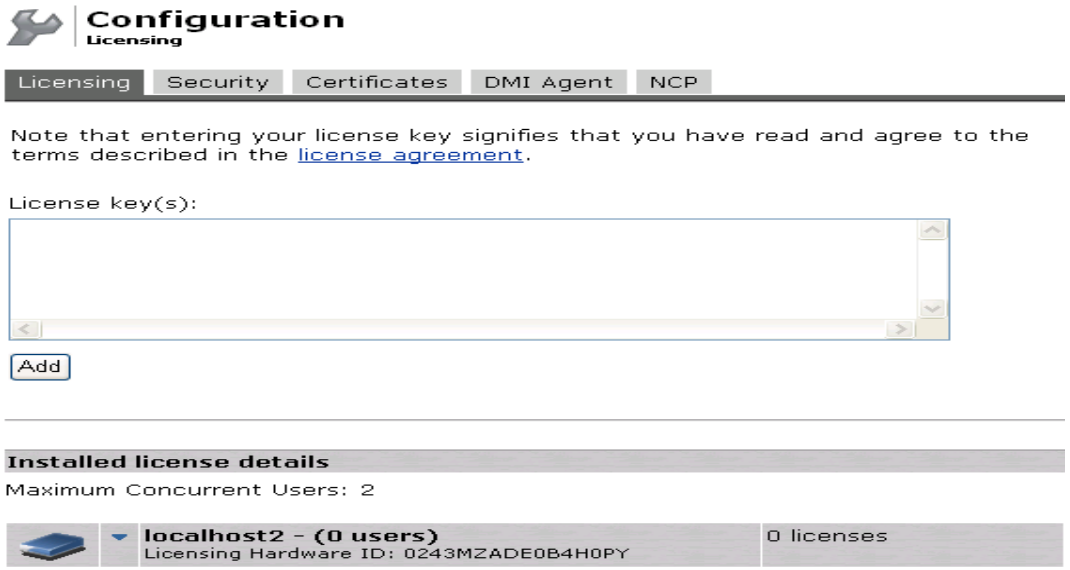
   NOTE: It is preferred not to downgrade from factory reset. Support for x500FIPS devices started in 6.4R1 so this is the bare minimum release x500-FIPS is supported.

   Procedure: **Steps in upgrading a system to a later release**

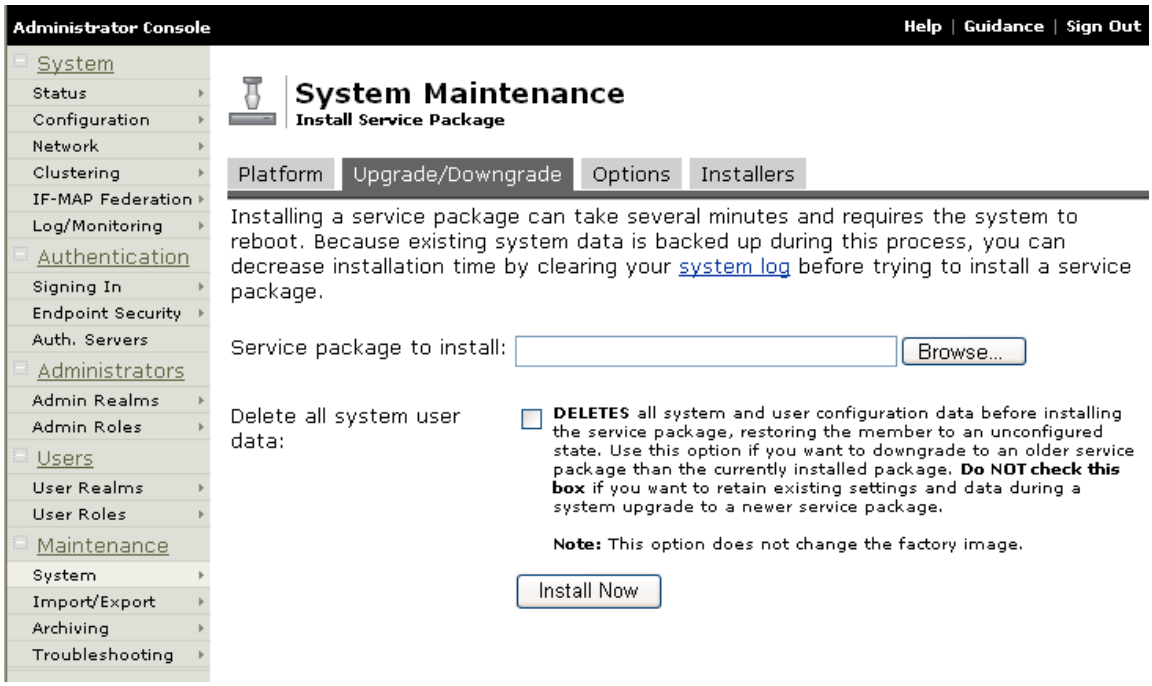
   Note existing version:



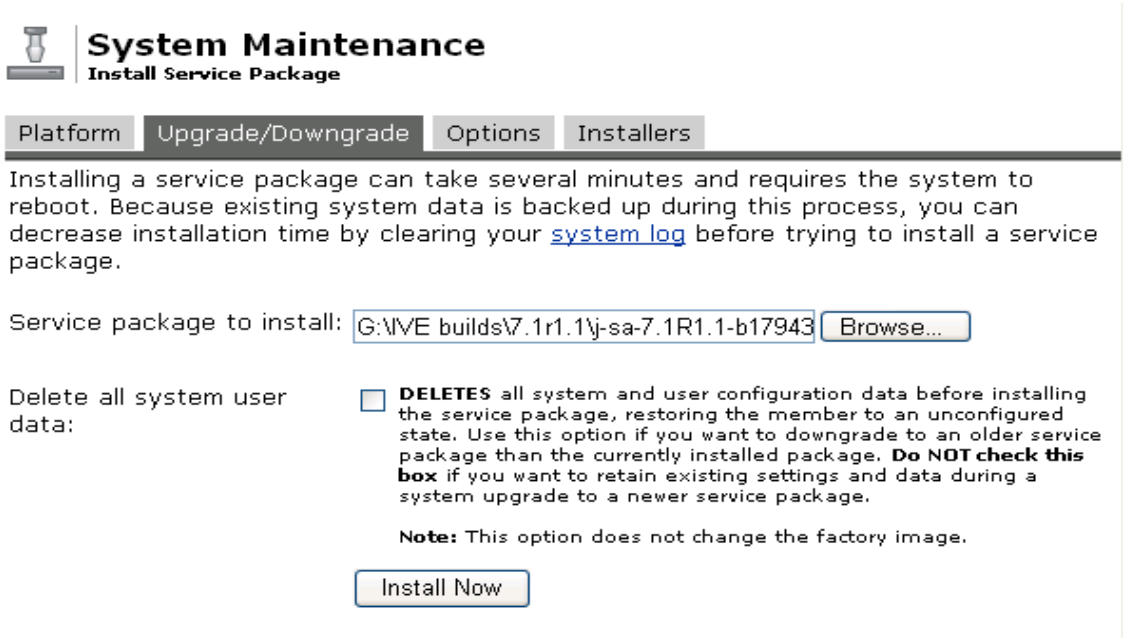
Do **not** install any license at this time:



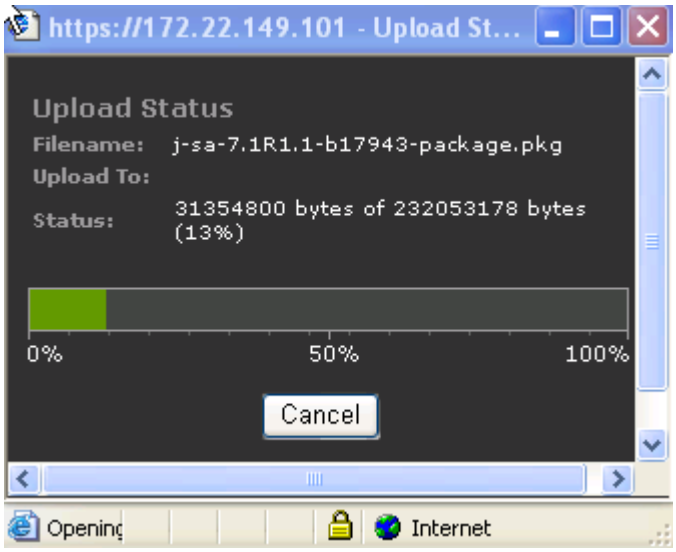
Go to **Maintenance>System>Upgrade/Downgrade**:



Browse the service package from a local drive and click "**Install Now**" (Do not check the "**Delete all system user data):**



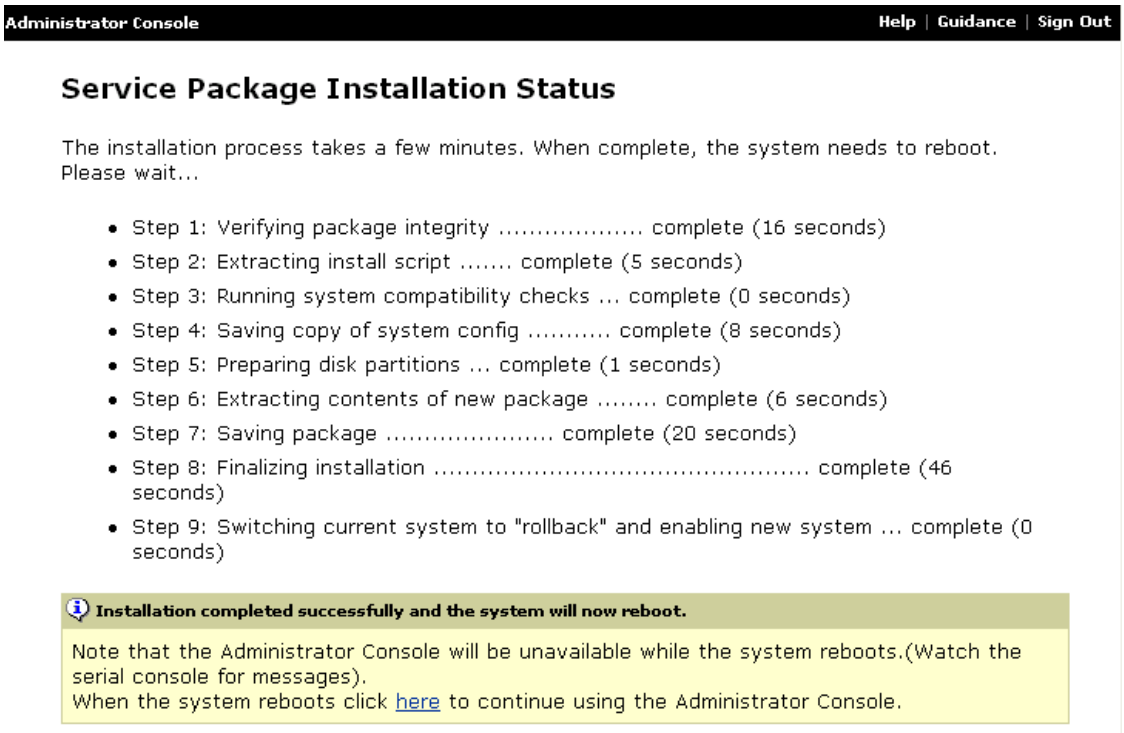
Status of upload shows up and you can close after it finished 100%:



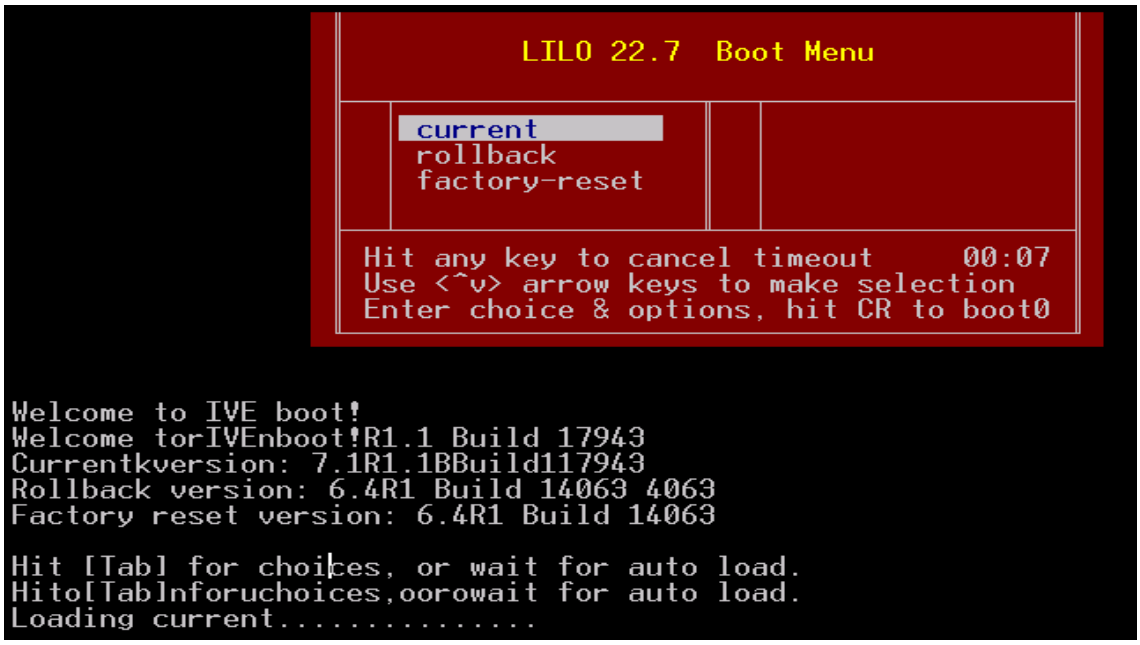
Monitoring serial console, you will see the following messages:

```
Press Enter to modify system settings.
Upgrading system...
Verifying package integrity ..................... complete
Extracting install script ....... complete (5 seconds)
Running system compatibility checks ... complete (0 seconds)
Saving copy of system config ........... complete (8 seconds)
Preparing disk partitions ... complete (1 seconds)
Extracting contents of new package ..|..... complete (6 seconds)
Saving package ..............
```

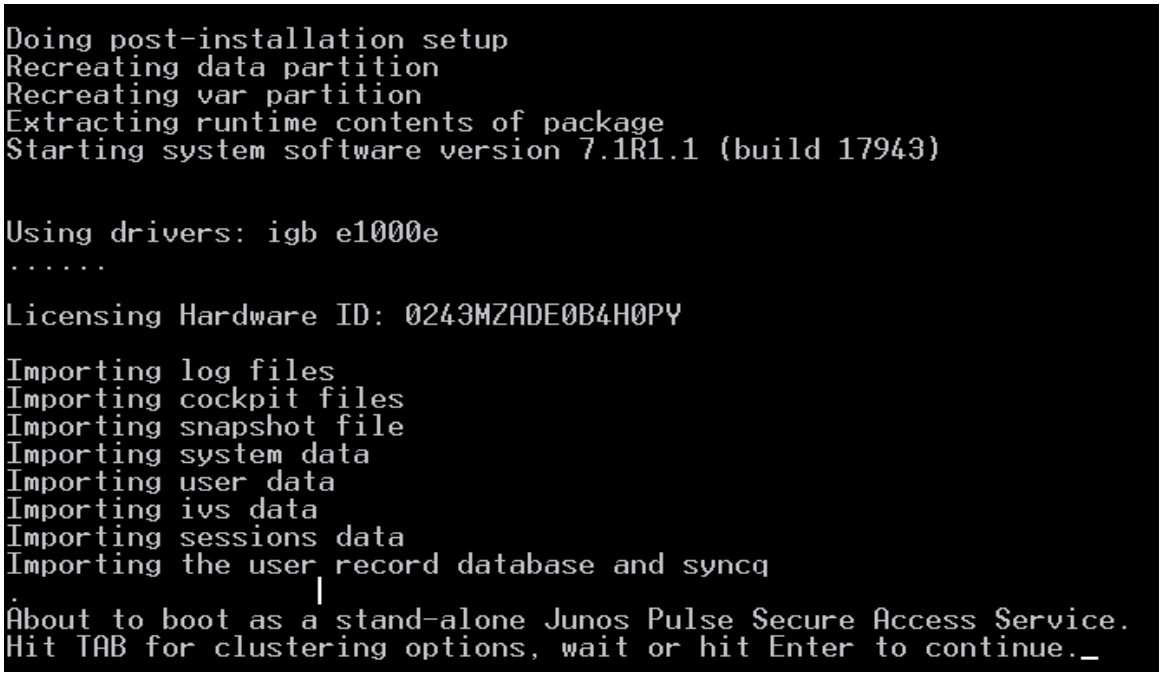
The admin UI also shows the same messages but after the system reboots, admin UI will be unresponsive until the system has completed the upgrade:



After initial reboot, it goes through post installation setup creating the new partition:



It proceeds to the post installation of importing data and logs files from the previous partition:



(For x500FIPS) It updates the Keystore Cache with the HSM cache:

```
Licensing Hardware ID: 0243MZADE0B4H0PY

Importing log files
Importing cockpit files
Importing snapshot file
Importing system data
Importing user data
Importing ivs data
Importing sessions data
Importing the user record database and syncq
.
About to boot as a stand-alone Junos Pulse Secure Access Service.
Hit TAB for clustering options, wait or hit Enter to continue.....
Starting Core Services


The key store state in cache is different from the one
installed on the local FIPS HSM.
We will now update the local key store state.
```

(For x500FIPS) It resets the HSM card and system comes back up. This completes the upgrade to the new code:

```
.
About to boot as a stand-alone Junos Pulse Secure Access Service.
Hit TAB for clustering options, wait or hit Enter to continue.....
Starting Core Services


The key store state in cache is different from the one
installed on the local FIPS HSM.
We will now update the local key store state.

Resetting device mca0, this may take a minute.
Please be patient.
Device mca0 reset ok.

Device Administration: https://<DEVICE-IP-ADDRSystem is now ready.

Press Enter to modify system settings._
```

Reboot the system just upgraded by choosing **Option 4>1**, and perform the join activity using the serial console

```
Welcome to the Juniper Networks Junos Pulse Secure Access Service Serial Console
!


Current version: 7.1R1.1 (build 17943)
Rollback version: 6.4R1 (build 14063)
Reset version: 6.4R1 (build 14063)

Licensing Hardware ID: 0243MZADE0B4H0PY
Serial Number: 0243032009000008

Please choose from among the following options:
   1. Network Settings and Tools
   2. Create admin username and password
   3. Display log/status
   4. System Operations
   5. Toggle password protection for the console (Off)
   6. Create a Super Admin session.
   7. System Snapshot
   8. Reset allowed encryption strength for SSL
   9. FIPS options
Choice:
```

5. Join the new node to the cluster

   NOTE: The cluster configuration from the surviving node is intact and has the information for the unit that is being replaced. This process will restore that configuration including the licenses (will be restored as Temporary 90-day license until replaced)

   Procedure: Steps in joining a node to an existing cluster via serial console

   During reboot, watch the serial console carefully and as soon as it comes to the clustering options, hit **TAB** key:

```
Starting system software version 7.1R1.1 (build 17943)


Using drivers: igb e1000e
......

Licensing Hardware ID: 0243MZADE0B4H0PY


About to boot as a stand-alone Junos Pulse Secure Access Service.
Hit TAB for clustering options, wait or hit Enter to continue.
------------------------------------------------------------
1. Continue as a stand-alone Junos Pulse Secure Access Service
2. Join an existing cluster
NOTE: To create a new cluster select 1 to continue as a stand-alone Junos Pulse
Secure Access Service
      and create the cluster from the WEB based Junos Pulse Secure Access Servic
e administrator console

Please select an option:
```

Select Option "**2. Join an existing cluster**", then provide the cluster join information as follows:

Cluster Name and password, Internal port IP of the existing cluster node Internal port, netmask and gateway IPs for this joining node

```
Please provide the following information:
Cluster name []:                                    JTAC
Cluster password:
Internal IP address of an active cluster member []:172.22.150.200
Internal IP address for this host []:               172.22.149.101
Netmask for this host []:                           255.255.255.0
Gateway for this host []:                           172.22.149.1

--------------------------------------------------------------------------------
This node will next set up its network as :
      (172.22.149.101/255.255.255.0/172.22.149.1),
contact the cluster member '172.22.150.200'
and ask to join the cluster.
If this succeeds the node will restart as member of the cluster.

WARNING: This host's entire state will be overwritten with the current
cluster configuration, including bookmarks, IP address, netmask etc.
Please select one of the options:

1. Continue join cluster operation
2. Abort and boot with the previous settings
3. Reenter network and cluster info

Enter 1,2 or 3:
```

Select option "**1. Continue join cluster operation**"

```
      (172.22.149.101/255.255.255.0/172.22.149.1),
contact the cluster member '172.22.150.200'
and ask to join the cluster.
If this succeeds the node will restart as member of the cluster.

WARNING: This host's entire state will be overwritten with the current
cluster configuration, including bookmarks, IP address, netmask etc.
Please select one of the options:

1. Continue join cluster operation
2. Abort and boot with the previous settings
3. Reenter network and cluster info

Enter 1,2 or 3: 1


About to join or form a cluster with the following members:

      name|              ip|       netmask|      gateway|enabled|
----------|----------------|--------------|-------------|-------|
*ive149101| 172.22.149.101| 255.255.255.0| 172.22.149.1|     on|
 ive150200| 172.22.150.200| 255.255.255.0| 172.22.150.1|     on|

Hit TAB for standalone options, wait or hit Enter to continue..._
```

Do not hit any key and let system automatically go to next process of synchronizing cache/data:

```
About to join or form a cluster with the following members:

      name|            ip|       netmask|     gateway|enabled|
----------|---------------|--------------|------------|-------|
*ive149101| 172.22.149.101| 255.255.255.0| 172.22.149.1|     on|
 ive150200| 172.22.150.200| 255.255.255.0| 172.22.150.1|     on|

Hit TAB for standalone options, wait or hit Enter to continue.....
Starting Cluster Services


Starting Core Services


State Server:........._
```

State synchronization between the 2 nodes of cluster can take a long time or short time depending on the size of the cache, but if it hangs for a long time, you may get this error:

```
Hit TAB for standalone options, wait or hit Enter to continue.....
Starting Cluster Services


Starting Core Services


State Server:.....................................................................
.....................................................................
.....................................................................
.....................
.....................................
...
.............

.
.....^[.....WARNING: Waited too long for TRANSITIONING_MASK to change
WARNING: If you are in a WAN, using a large configuration
WARNING: and delays between nodes are large, this could be expected.
WARNING: You may want to continue to wait in such scenarios.
WARNING: Otherwise, reboot and report the issue if the problem persist
Would you like to reboot (y/n)?:
.....
```

During synchronization, the other node is not going to show anything while state sync is happening

```
Current version: 7.1R1.1 (build 17943)
Rollback version: 7.0R6 (build 18107)
Reset version: 6.4R1 (build 14063)

Licensing Hardware ID: 0243MPGDE0B1H0PY
Serial Number: 0243032009000005

Please choose from among the following options:
   1. Network Settings and Tools
   2. Create admin username and password
   3. Display log/status
   4. System Operations
   5. Toggle password protection for the console (Off)
   6. Create a Super Admin session.
   7. System Snapshot
   8. Reset allowed encryption strength for SSL
   9. FIPS options
Choice:
Timeout


Press Enter to modify system settings.
```

If State Synchronization stalls or taking too long, try to do Ctl break and answer "**y"** to "**Would you like to reboot (y/n)?.** Do not break or do any manual intervention after reboot.

```
Using drivers: igb e1000e
......

Licensing Hardware ID: 0243MZADE0B4H0PY


About to join or form a cluster with the following members:

      name|             ip|       netmask|      gateway|enabled|
----------|---------------|---------------|-------------|-------|
*ive149101| 172.22.149.101| 255.255.255.0| 172.22.149.1|     on|
 ive150200| 172.22.150.200| 255.255.255.0| 172.22.150.1|     on|

Hit TAB for standalone options, wait or hit Enter to continue.....
Starting Cluster Services


Last time enabled in cluster was 1024 seconds ago
Host offline for more than 90 secs;
Waiting to give a chance to a host with more recent state to start cluster.
20 seconds left to start cluster. Press c to start now.....
Starting Core Services
```

Watch the state server synchronization again and it should say OK when completed.

(**For x500FIPS**) Provide the restore password after joining the cluster as it has to import the keystore and certificates to the new device.

```
Hit TAB for standalone options, wait or hit Enter to continue.....
Starting Cluster Services


Last time enabled in cluster was 1024 seconds ago
Host offline for more than 90 secs;
Waiting to give a chance to a host with more recent state to start cluster.
20 seconds left to start cluster. Press c to start now.....
Starting Core Services


State Server:.............................[OK]

You have joined a cluster. We will now install the
cluster's key store on this node.

Resetting device mca0, this may take a minute.
Please be patient.
Device mca0 reset ok.

Please provide the restore password
for the key store being installed: _
```

If a wrong password is entered, you will be prompted to try again. After entering proper restore password, it will reset and zeroize the HSM card.

```
Would you like to try this again (y/n)?

Please provide the restore password
for the key store being installed:

Resetting device mca0, this may take a minute.
Please be patient.
Device mca0 reset ok.
Zeroizing device mca0, this may take a few minutes.
Please be patient.
Device mca0 zeroized.
```

System is now ready and cluster should be up and running.

```
Device Administration: https://<DEVICE-IP-ADDR>|<DEVICE-DNS-NAME>/admin
System is now ready.

Press Enter to modify system settings.
```

```
Welcome to the Juniper Networks Junos Pulse Secure Access Service Serial Console
!


Current version: 7.1R1.1 (build 17943)
Rollback version: 6.4R1 (build 14063)
Reset version: 6.4R1 (build 14063)

Licensing Hardware ID: 0243MZADE0B4H0PY
Serial Number: 0243032009000008

Please choose from among the following options:
   1. Network Settings and Tools
   2. Create admin username and password
   3. Display log/status
   4. System Operations
   5. Toggle password protection for the console (Off)
   6. Create a Super Admin session.
   7. System Snapshot
   8. Reset allowed encryption strength for SSL
   9. FIPS options
Choice:
```

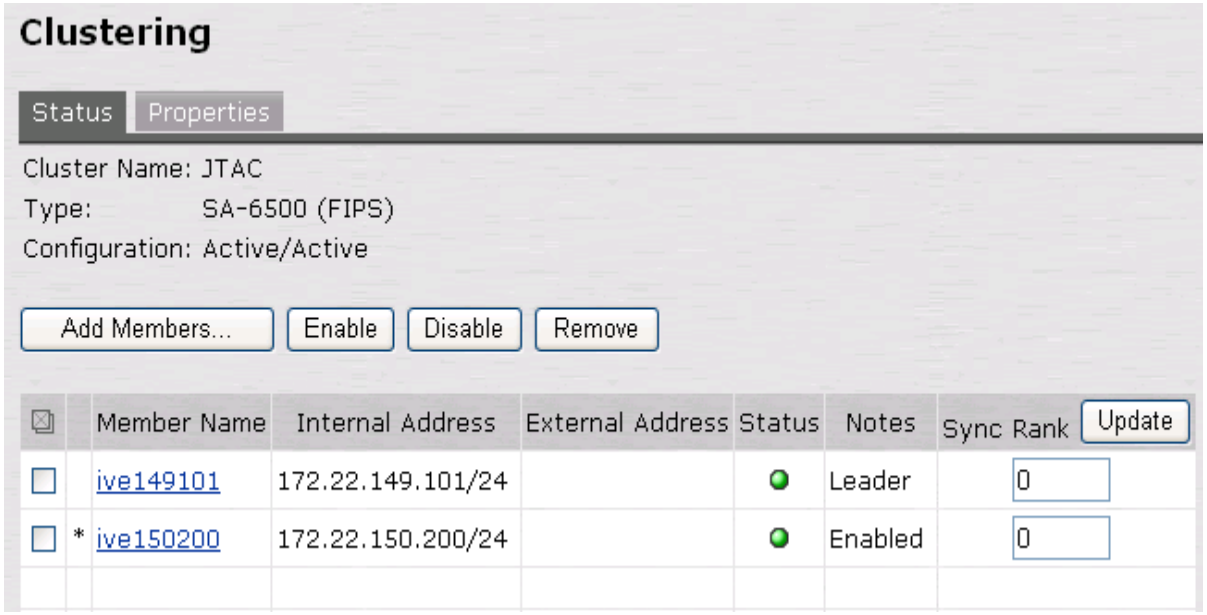
(**For x500FIPS**) During a normal keystore and certificate import to device, the next step is to ensure to complete the import by choosing "**9. FIPS Option**" then Option "**1. Complete import of key store and certificates**"

```
Please choose from among the following options:
   1. Network Settings and Tools
   2. Create admin username and password
   3. Display log/status
   4. System Operations
   5. Toggle password protection for the console (Off)
   6. Create a Super Admin session.
   7. System Snapshot
   8. Reset allowed encryption strength for SSL
   9. FIPS options
Choice: 9


Please choose the operation to perform:
 1. Complete import of key store and server certificates
 2. Change security officer password
 3. Change web user password
 4. Generate master key backup
 5. Reset the HSM
 6. Load firmware and re-import key store
 7. Load key store into cache
 <return to go back to main menu>
Choice:
```

If the keystore is up to date, it will say so "**The Keystore and Certificates are up to date!"**

```
The key store and server certificates are up to date!


Current version: 7.1R1.1 (build 17943)
Rollback version: 7.0R6 (build 18107)
Reset version: 6.4R1 (build 14063)

Licensing Hardware ID: 0243MPGDE0B1H0PY
Serial Number: 02430320090000005

Please choose from among the following options:
   1. Network Settings and Tools
   2. Create admin username and password
   3. Display log/status
   4. System Operations
   5. Toggle password protection for the console (Off)
   6. Create a Super Admin session.
   7. System Snapshot
   8. Reset allowed encryption strength for SSL
   9. FIPS options
Choice:
```

Cluster is now back as normal:



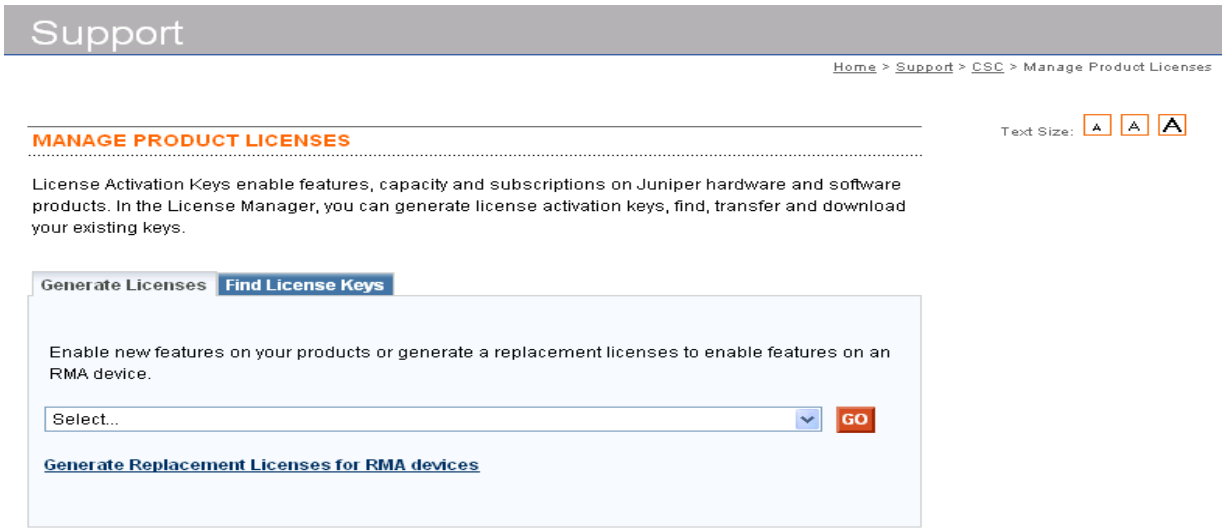
6. Final Step: Generating and applying proper permanent license/s for this new RMA device.

NOTE: Upon joining the node to the cluster, if the unit just joined is the same system with same hardware ID, it will restore licenses as permanent, but if it is a new RMA unit, then it has a different hardware licensing ID, so license will only be restored as temporary 90-day license highlighted in RED as temporary license status.

If license is not found or unable to generate from LMS support site, please contact customer care support to generate the licenses for you.

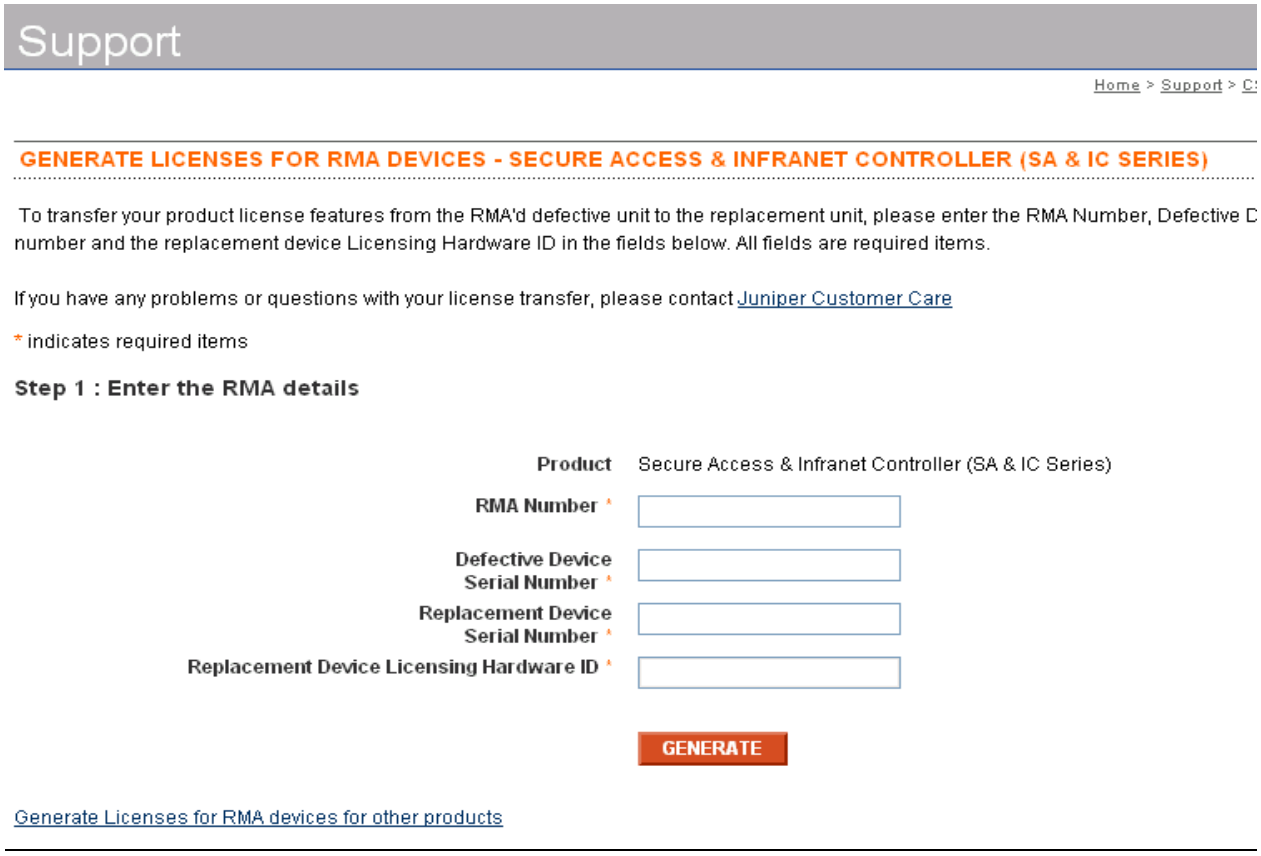
To generate replacement licenses for the RMA device, you must login to support site and follow the instructions.

Go online to: https://www.juniper.net/lcrs/license.do



Click on: **"Generate Replacement Licenses for RMA devices" and select product**

Select: “**Secure Access & Infranet Controller (SA & IC Series)”**



Enter all necessary information from the RMA paperworks and click on **“GENERATE”**

Apply this license/s to the RMA replacement unit without removing the RED marked temporary license. It will install and replace that temporary license with this permanent license.

IT IS RECOMMENDED TO COMPLETE THIS STEP AS SOON AS POSSIBLE BECAUSE LICENSE WILLL ONLY WORK FOR 90 DAYS AND IF FORGOTTEN, ACCESS WILL BE LOST AND WILL CAUSE DOWNTIME.

This completes the cluster join and RMA process. Check access to each box if A/A, and also check VIP failover if A/P cluster. Also check all the hosts, routes, virtual ports, NC pools and VLANs are in place, if applicable.