Citi Architecture and Technology Engineering (CATE)

CATE CitiSystems Server and OperatingEnvironment Engineering

Requirements, Testing & Release Notes

Project Name:	**Solaris Firmware Updates – 2018-Q1-1**
Project ID:	**CAT180086455**
Document Version:	1.1
Date Published:	02/20/2018

Disclaimer

If printed, content is valid only for the day it was printed. Always refer to the online document for the current version. If the user elects to maintain copies of this procedure, it is their responsibility to verify the currency of the document by checking it against the online version. This document must be promptly removed from use when obsolete.

TABLE OF CONTENTS

1 OVERVIEW

1.1 Script Lite Certification Types

Product Certification - A minor upgrade for existing infrastructure or platform technology standard that does not impact the security model. This may include product hardware and/or product software.

DO NOT DELETE ANY SECTIONS FROM THIS DOCUMENT. PLEASE USE SHORT DESCRIPTION FOR SECTIONS AND DETAILS THAT DO NOT APPLY.

Vulnerability Threat Management (VTM) - A minor upgrade due to a vulnerability (via VTMAS) for an existing infrastructure or platform technology standard that does not impact the security model. VTM related work can be a vendor software fix and/or configuration changes. Please note if the vulnerability has a major impact to the architecture and/or security model then the TDLC Create/Maintain project type must be used.

For either certification type any sections marked Not Applicable (N/A) must be accompanied with reason why the particular item does not apply.

- Example: N/A - This effort is for VTM vulnerability remediation and solution consisted of configuration change.

Please hover over **Choose an item**, left click and use the drop down menu below to identify certification type.

Product Certification **← Hovering will allow choosing SL cert type**

1.2 Document Purpose

The purpose of the template is to provide a standard document structure for completing all requirements for **Solaris Firmware Updates – 2018-Q1-1**

1.3 Revision History

Update the document history each time a draft is issued for review.

Date	Version	Author	Author Contact	Change (Topic, Section Page)
Feb 12, 2018	1.0	S Senthil/	senthil.shanmugavelu@citi.com	Initial RFT
Feb 20, 2018	1.1	S Senthil/	senthil.shanmugavelu@citi.com	Updated RFT with new release for T5-4(9.6.21.a)

1.4 Relevant Links

Provide titles and links to documentation supporting the product. These documents can be a combination of vendor documents and vendor sites (for example, Cisco, VMware). Wherever possible, vendor documents should be posted to internal sites to make sure they are accessible.

External References (E.g., Vendors etc.)

Document	URL
Oracle System Firmware Release Hub	http://www.oracle.com/technetwork/systems/patches/firmware/release-history-jsp-138416.html

Internal References

Provide a list of internal documents that have been used as an input to this document. Include design and configuration guidelines in this section.

Provide the document name, version number and publication date. Provide hyperlinks to each document as well.

Document	Version	Date
RFP | Release for Production : Solaris Firmware Updates-2017-Q3-1		10/31/2017
RFP | Release for Production : Solaris Firmware Updates-2016-Q4-1		12/9/2016
RFP | Release for Production: Sparc Firmware 2.7_A1		04/27/2016
RFP | Release for Production: Sparc Firmware 2.6_A5		07/22/2015

2 REQUIREMENTS, TESTING & RESULTS

2.1 Overview and Product Requirements

Oracle periodically releases firmware updates in the form of patches. This documentation includes details of the firmware patches included in the patchset and summarizes the steps required to install firmware onto a machine.

This patchset provides firmware patches for SPARC servers T5120, T5220, T5240, T5440, T3-1, T3-2, T3-4, T4-1, T4-2, T4-4, T5-4.

In this release the new patchces for T4-1, T4-2, T4-4, T5-4 which are released by ORACLE is added and the patches for T5120, T5220, T5240, T5440, T3-1, T3-2, T3-4 are same version as previous release Solaris Firmware Updates-2017-Q3-1. The patches available in this update are in detail as in below Table (New update marked in blue)

System	Current Patch	Current FW Version	update FW Patch	Updated FW Version
T5120/T5220	147307-15	7.4.11	147307-15	7.4.11
T5240	147310-15	7.4.11	147310-15	7.4.11
T5440	147311-13	7.4.11	147311-13	7.4.11
T3-1	152738-01	8.3.40	152738-01	8.3.40
T3-2	152739-01	8.3.40	152739-01	8.3.40
T3-4	152740-01	8.3.40	152740-01	8.3.40
T4-1	**152475-04**	**8.9.8**	**152475-06**	**8.9.9**
T4-2	**152476-04**	**8.9.8**	**152476-06**	**8.9.9**
T4-4	**152477-04**	**8.9.8**	**152477-06**	**8.9.9**
T5-4	**26407365**	**9.6.9.a**	**27353278**	**9.6.21.a**

2.2 Cloud Architecture Review Team Assessment (CART)

NOTE: If you created your Project on or after June 5, 2017, the following assessment will be captured in the Planview Tool within the required Combined Compliance Assessment Lifecycle screen. If you created your project before June 5, 2017, you must complete this section.

Assessment Question: Does your project involve or have any elements associated with External Hosting, whether traditional or Cloud?

- Externally Hosted (any system or service with Citi Data stored or processed outside Citi perimeter.) or Dedicated (Dedicated refers to physical server hardware dedicated to Citi use, ideally in a dedicated Citi cage) or Single Tenant Cloud or Lab/POC with no Citi data.
- Shared Cloud, no confidential or higher data stored or processed.
- Shared Cloud, confidential or higher data stored or processed.

If you answered No in the below table, then you do not need to contact the CART Team.

If you answered Yes in the below table, you must go to the CART SharePoint site and initiate a request for review. Ensure that a CART Approval Email or Waiver is obtained and uploaded to the Product Registration Activity in Planview before releasing to Production and marking the Project as Completed.

CART Assessment	Yes or No
Does your project involve or have any elements associated with External Hosting, whether traditional or Cloud?	No
If you answered Yes, have you contacted the CART Team and requested a Formal Approval or Waiver?	NA

2.3 Mobile Architecture Review Team Assessment (MART)

NOTE: If you created your Project on or after June 5, 2017, the following assessment will be captured in the Planview Tool within the required Combined Compliance Assessment Lifecycle screen. If you created your project before June 5, 2017, you must complete this section.

Assessment Question: Does your project or development activity includes any downloadable or installed component that runs/resides on a customer/end user device (mobile, tablet, laptop, etc.) then review and approval by the Mobile Architecture Review Team (MART) is required before releasing into production.

If you answered No, then you do not need to contact the MART Team.

If you answered Yes in the below table, you must go to the MART SharePoint site and initiate a request for review. Ensure that a MART Approval Email or Waiver is obtained and uploaded to the Product Registration Activity in Planview before releasing to Production and marking the Project as Completed.

MART Assessment	Yes or No
Does your project or development activity includes any downloadable or installed component that runs/resides on a customer/end user device (mobile, tablet, laptop, etc.)?	No

MART Assessment	Yes or No
If you answered Yes, have you contacted the MART Team and requested a formal approval or Waiver?	NA

2.4 Legal and Regulatory Assessment

NOTE: If you created your Project on or after June 5, 2017, the following assessment will be captured in the Planview Tool within the required Combined Compliance Assessment Lifecycle screen. If you created your project before June 5, 2017, you must complete this section.

Assessment Question: Does your project involve any of the following Legal and/or Regulatory Compliance elements?

- Electronic communications with clients by Citi employees (including e-mail, IM or other electronic messaging)
- Social networking related projects
- Employee telephone recordings
- Internal websites, wikis or other means by which Citi employees may be able to post/share information
- Any systems related to trading
- Data archiving or records management

If you answered No in the table below, then you do not need to contact your Control Officer or obtain a Legal and Regulatory review.

If you answered Yes in the below table, you must contact your Control Officer and request a Legal and Regulatory review. Ensure that the Legal and Regulatory finding or Approval Email to proceed is obtained in writing and uploaded to the Product Registration Activity in Planview before releasing to Production and marking the Project as Completed.

Legal and Regulatory Assessment	Yes or No
Does your project involve any of the following Legal and and/or Regulatory Compliance elements? • Electronic communications with clients by Citi employees (including e-mail, IM or other electronic messaging) • Social networking related projects • Employee telephone recordings • Internal websites, wikis or other means by which Citi employees may be able to post/share information • Any systems related to trading • Data archiving or records management	No
If you answered Yes, have you contacted your Control Officer and requested a Legal and Regulatory review.	NA

2.5 Vulnerability Threat Management (VTM) Requirements (Only if VTM related work)

VTM ID	CVE ID	CVE description	Vendor defect ID	Remarks
N/A	N/A	N/A	NA	Not applicable due to it is not VTM related work

2.6 Testing Scope

This test plan will make sure that firmware has been installed, tested and executed properly

This table is to identify what categories will be tested. Test Categories are derived from CSTLC. Section 2.9 will capture specific tests that align to this table. Please indicate Yes/No and provide details in Table 1, Section 2.9.1.

Test Category	Definition	Test Category Required (Yes or No)
System Integration Testing (Including: Interface Testing, Batch Testing)	System integration testing (SIT) is a testing process that exercises a software system's coexistence with others. With multiple integrated systems, assuming that each have already passed system testing, SIT proceeds to test their required interactions. Following this, the deliverables are passed on to acceptance testing. System Integration Testing verifies combined functionality.	Yes
Functional Testing	Testing software based on its functional requirements. It ensures that the program physically works the way it was intended and all required menu options are present. It also ensures that the program conforms to the industry standards relevant to that environment; for example, in a Windows program, pressing F1 brings up help. In this type of testing, the system is validated for its functional behavior. Functional testing does not deal with internal coding of the project.	Yes
VTM Testing	VTM related testing ensures that you have reviewed the CVEs and based on the impact and availability, feasible testing can be included in this section. (can include VTM scans and or tools available)	No
Non-Functional Testing	Testing the attributes of a component or system that do not relate to functionality, e.g. reliability, efficiency, usability, maintainability, and portability.	No
Technology Testing	Refers to all testing performed by the technology staff.	Yes
Other Testing	User Acceptance Testing, exploratory testing. This could include possible Operational, Regional and user feedback.	No

2.7 Testing Constraints

Test environment must meet the requirements detailed given in section 3.4.

Updating the firmware other than T4-4 system has not been tested by CATE due to resource limitations. If any of the SA teams to test on other Systems, we would be interested in feedback.

CATE have access to a below server type and the firmware has been installed successfully (it does not imply that the firmware has been fully tested by CATE)

Patch	System	Firmware Version	LDom version	Oracle Release Date	CATE installed
152477-06	T4-4	8.9.9	3.1.1	Sep 16, 2017	Yes

2.8 Testing Dependencies

Test environment must meet the requirements detailed given in section 3.4

2.9 Test Specifications, Defect Tracking

2.9.1 Test Category Tests

If you have external links to the test cases, you need to explicitly list the test categories from the above table under 2.3 Testing Scope. Please provide details only on those that have "Yes". There can be one or more specific tests for each test category.

Table 1

Test Category (Based on section 2.3 table)	Test specification	Expected Results	Actual Results	Pass / Fail
System Integration Testing, Functional Testing, Technology Testing	Install Firmware package on T4-4 Sparc server. Verify file sum and permissions	Firmware patch installed successfully. Verified the version installed .	Firmware patch installed successfully. Version reflected as expected result	Pass
System Integration Testing, Functional Testing, Technology Testing	Install Firmware package, confirm firmware installation, verify Firmware functionality.	Login functions, Firmware version reflected in the server	Login functions, firmware patch reflected as expected. Server rebooted normally.	Pass

2.9.2 Defect Tracking Log

There are no defects identified as part of the testing for this work effort

Defect ID	Description	Severity	Will the Defect Be Fixed (Y/N)	Comments (Additional detail about the defect)
NA	NA	NA	NA	NA

3 RELEASE DETAILS

3.1 Release Details

Product Vendor	Oracle
Product Name	Sparc
CTC Product ID	22862
CTC Version ID(s)	75963, 51445
Product Homepage	https://catecollaboration.citigroup.net/domains/platstor/osunix/wpages/ProductDetail.aspx?Name=Solaris&Publish=1

3.2 Source Code Management Repository

This section should include location of the Source Code (Custom files/Scripts) used for this release.

If Source Code was not used in the Software or Package, indicate “Not Applicable” (N/A) and provide explanation:

Not Applicable: No custom files/scripts have been used in this release

Repository Name	Repository URL	Source Code Identifier
1. NA	NA	NA
2. NA	NA	NA

3.3 Software and Packages –

Platform	Package Name	Repository	Size(bytes)	MD5 / SHA1 / SHA256 (if applicable)
SPARC-Solaris	Solaris-FW-2018-Q1.tgz	stealth	202708160	dad681eec93f24e9ac86d0d81d21d92d/311e3ce31413dd3e3075297497d85cce530fe918

Stealth: NFS://net/stealth.nam.nsroot.net/export1/home1.localhost/sw/outbound/vtt-testing/PSE

3.4 Pre-requisites

1) Recommendation for use of Sysfwdownload Utility on SPARC systems.

Under certain conditions, if the Service Processor is running low on memory, the sysfwdownload utility may fail to upgrade the firmware on SPARC T4 and T3 systems. Therefore, it is highly recommended that the Service Processor (SP) be reset prior to performing the firmware update. The steps to perform the reset are:

From the ILOM command shell execute the following command

```
-> reset /SP
```

If the first attempt fails retry with

```
-> reset -f /SP
```

After performing the reset, the usual steps can be followed for using the sysfwdownload utility

2) It is vital that all domains are shutdown, stopped and unbound cleanly with the secondary domain being the last prior to saving the hypervisor and shutting down the primary domain when updating the firmware on a T4-4 running a dual IO domain configuration (NOTE the T4-4 and T5-4 are the only CATE supported system capable of running dual IO domains).\

3) Make sure the system has installed latest version of LDOM, firmware and follow the steps which has been mentioned in previous release notes. Refer the internal release notes link in Section 1.4

4) When updating the firmware, it is recommended that a number of eeprom and SP variables are recorded. Some of the variables may be overwritten during the firmware update (or downgrade) of the machine. Refer the previous release notes for ILOM command details in Section 1.4 and ILOM Variables

5) SPARC T5 platforms, and any platforms supporting dual-bank FLASH storage for Sun System Firmware should use the "-u" option to automatically update the Sun System Firmware after the download. Problems have been reported when not using this automatic mode.

6) On SPARC T5, due to the change with bugid 22886949, prior to updating to **Sun System Firmware 9.6.5,** please check the content of /etc/system file for the existence of "xc_tick_limit_scale". If the tunable parameter exists, please remove it.

4 INSTALL AND/OR CONFIGURATION INSTRUCTIONS

4.1 Installation Procedure:

Prior to firmware updates on T-Series systems which have the Oracle VM for SPARC software (formerly called LDom) software installed the SA should ensure that the OVM for SPARC configuration stored in the System Controller (SC) and the Solaris environment is current, using the following command ldm add-config <config-name>

Further on the T-Series systems which are installing ILOM software version 8.2.0.a, or later, various Open Boot (OB) and SC parameters values should be recorded to ensure that they are not lost during the firmware update process, see ILOM variables for details.

Firmware patches generally require that the new System Controller (SC) software image is installed after the Solaris environment has been shut down. Individuals installing firmware are advised to review the installation instructions supplied with the patch to ensure that the relevant instructions are used for the platform.

In general, there are two types of installation method for T-Series systems, networked or Solaris based. Where the ILOM for a system is network connected it is recommended that the network installation method be used, the IP address of the jumpstart server for tftpboot downloads or the sysprofiler for http downloads will be required for this installation method.
At a high level the steps required will be;

1. The SA ensures that the LDom configuration (for systems running LDOms) is stored to the SC.
2. For the Solaris method – the SA downloads the new firmware to the SC
3. SA shuts down the Solaris system
4. The host system is powered down
5. The new firmware is loaded into the SC,the SC is rebooted as part of this process
6. For systems running LDoms check to ensure that the correct LDom configuration is defined
7. The host system is powered up

It is important to ensure that any hardware faults flagged by the system have been, investigated, resolved and cleared before the firmware is updated. It is also highly recommended that all guest ldoms are not only shutdown, but also stopped and unbound before saving the hypervisor state and beginning the firmware update.

4.2 Firmware installation steps for T3-x / T4-x

NOTE: These instructions were taken from the Oracle Firmware instructions included with the patches. Refer readme file from Oracle for any special instructions before upgrade the firmware

The steps required to install the firmware on T3-x/T4-x systems are as follows:

1. Logon to Solaris on the machine to be patched

2. Copy the sysfwdownload binary and firmware image to a temporary directory

```
#cd /net/stealth.nam.nsroot.net/export1/home1.localhost/sw/outbound/vtt-
testing/PSE
# scp Solaris-FW-2018-Q1.tgz <Target Host>:/var/tmp
```

3. Extract the zip file into local directory

```
#cd /var/tmp
#gzip -dc /var/tmp/Solaris-FW-2018-Q1.tgz | tar xf  -
```

4. Download the firmware image to the system controller, this will take several minutes

```

# /<Patchname>/sysfwdownload /<firmware_image>

For T4-4 servers
#/T4-4_8.9.9/sysfwdownload Sun_System_Firmware-8_9_9-SPARC_T4-4.pkg
```

5. Shut down, stop and unbind any non-I/O guest domains

6. Shut down, stop and unbind any active I/O domains (usually the ‘secondary’ domain)

7. Ensure that the current LDom configuration is saved in the SC [ldm add-config <config-name>]

8. Halt the primary domain:

```
# shutdown -i0 -g0 -y
```

9. From the ILOM: Power off the system (if the host was halted the power may already have been removed):

```
-> stop /SYS
```

10. Check that power is off (this can take a few minutes)

```
-> show /SYS
```

11. Check the keyswitch state of the machine (if the first command shows keyswitch_state not Normal, reset using the second command)

```
-> show /SYS keyswitch_state
-> set /SYS keyswitch_state=Normal
```

12. Verify the image is for the correct platform (the sysfwdownload utility does not verify the file and platform match during the download)

```
 -> show /SP/firmware/localimage
 /SP/firmware/localimage
    Targets:

    Properties:
        upload_date = Wed Jan 31 06:41:13 2018

        version = 3.2.6.6
    Commands:
        cd
        show
```

13. Record the values of the variables listed in Appendix C ILOM variables

14. Provided you have the correct firmware image loaded you can then install it

```
-> load -source /SP/firmware/localimage

NOTE: An upgrade takes several minutes to complete. ILOM
      will enter a special mode to load new firmware. No
      other tasks can be performed in ILOM until the
      firmware upgrade is complete and ILOM is reset.

Are you sure you want to load the specified file (y/n)? y
Preserve existing configuration (y/n)? y
.............................................................................
..
Firmware update is complete.
ILOM will now be restarted with the new firmware.
```

15. The load command will output two prompts

Are you sure you want to load the specified file (y/n)?
Do you want to preserve the configuration (y/n)?

16. Once the firmware has been uploaded the SC will be reset

17. Check the values of the variables listed in Appendix C ILOM variables and reset as necessary, it is expected that the HOST/bootmode config will need to be reset to the appropriate value.

18. When the system has rebooted the Solaris environment can be restarted using:

```
-> start /SYS
```

4.3 Firmware installation steps for T5-4

Note: Updating the firmware on T5-4 system has not been tested by CATE due to resource limitations. If any of the SA teams to test on this Systems, we would be interested in feedback. Refer readme file from Oracle for any special instructions before upgrade the firmware

The steps required to install the firmware on T5-4 systems are as follows:
1. Logon to Solaris on the machine to be patched
2. Copy the sysfwdownload binary and firmware image to a temporary directory

```
#cd /net/stealth.nam.nsroot.net/export1/home1.localhost/sw/outbound/vtt-
testing/PSE
# scp Solaris-FW-2018-Q1.tgz  <TargetHost>:/var/tmp
```

3. Extract the zip file into local directory

```
#cd /var/tmp
#gzip -dc /var/tmp/Solaris-FW-2018-Q1.tgz  | tar xf  -
```

4. Shut down, stop and unbind any non-I/O guest domains

5. Shut down, stop and unbind any active I/O domains (usually the ‘secondary’ domain)

6. Ensure that the current LDom configuration is saved in the SC [ldm add-config <config-name>]

7. Download the firmware image to the system controller, this will take several minutes

```
# /<Patchname>/Firmware/Sun_System_Firmware/sysfwdownload <firmware_image>
For T5-4 servers
#/ T5-4_9.6.21.A/Firmware/Sun_System_Firmware/sysfwdownload -u
Sun_System_Firmware-9_6_21_a-SPARC_T5-4+T5-8.pkg
```

The Oracle documentation indicates that the sysfwdownload procedure will perform the following actions;

- Download Sun System Firmware image
- Power down host
- Update Sun System Firmware
- Reset SP
- Power on host

Refer the known issue section if the system takes longer time for shutting down.

4.4 Firmware installation steps for T5XXX

Note: Updating the firmware on T5XXX system has not been tested by CATE due to resource limitations.If any of the SA teams to test on this systems, we would be interested in feedback. Refer readme file from Oracle for any special instructions before upgrade the firmware

The T5xx0 system natively uses an ILOM interface that uses a significantly different command set. In order to install the firmware on the T5xx0 system a user will need to be created, within the ILOM, which uses the ALOM interface by default. The following steps are required:

1. Logon to the ILOM interface via the root account
2. Create an account, a typical session is shown below (note <username> denotes a username to be created)

```
-> create /SP/users/<username> role=Administrator cli_mode=alom
Creating user….
Enter new password: ********
Enter new password again: *******
Created /SP/users/<username>
```

The steps required to install the firmware on T5XXX systems are as follows:

1. Logon to Solaris on the machine to be patched

2. Copy the sysfwdownload binary and firmware image to a temporary directory

```
#cd /net/stealth.nam.nsroot.net/export1/home1.localhost/sw/outbound/vtt-
testing/PSE
# scp Solaris-FW-2018-Q1.tgz  <TargetHost>:/var/tmp
```

3. Extract the zip file into local direcotary

```
#cd /var/tmp
#gzip -dc /var/tmp/Solaris-FW-2018-Q1.tgz  | tar xf  -
```

4. Download the firmware image to the system controller, this will take several minutes

```
# /<Patchname>/sysfwdownload /<firmware_image>
For example T5120 servers
#/ T5120_7.4.11/sysfwdownload Sun_System_Firmware-7_4_11-
SPARC_Enterprise_T5120+T5220.pkg
```

5. Shut down, stop and unbind any non-I/O guest domains

6. Shut down, stop and unbind any active I/O domains (usually the ‘secondary’ domain)

7. Ensure that the current LDom configuration is saved in the SC [ldm add-config <config-name>]

8. Halt the primary domain:

```
# shutdown -i0 -g0 -y
```

9. Connect to the system controller, via the <username> account created above (or another account with ALOM shell) for T5xx0 systems

10. Power off the system (if the host was halted the power may already have been removed):

```
sc> poweroff
```

11. Ensure the keyswitch is in the normal position:

```
sc> showkeyswitch
if not set to normal,
sc> setkeyswitch -y normal
```

12. Perform the firmware update, note this will take several minutes. When complete the message “Update complete. Reset device to use new software” will be displayed

```
sc> flashupdate -s 127.0.0.1
```

13. For T2000 systems reset the system controller (T5xx0 systems will automatically reset the system controller at the end of the firmware update):

```
sc> resetsc
```

4.5 ILOM commands

ILOM	**Description**
set /SP/users/username password	Changes the login password of the current user.
show /HOST	Displays information about the host system's hardware configuration, and whether the hardware is providing service. The -v option displays verbose information about the displayed components.
show /SP/sessions	Displays a list of users currently logged in to ILOM. The display for this command has a similar format to that of the UNIX command who. The -g option pauses the display after the number of lines you specify for lines.
show /HOST	Displays version information for host-side components
show target property	Displays the current non-volatile read-only memory (NVRAM) configuration parameters.
show /SP/clock datetime	Displays the ILOM date. ILOM CMT time is expressed in Coordinated Universal Time (UTC) rather than local time. The Solaris OS and ILOM time are not synchronized.
show /SP/users	Displays a list of all user accounts, permission levels, and whether passwords are assigned.
show -o table -level all /SYS	Displays the environmental status of the host server. This information includes system temperatures, power supply

	status, front panel LED status, hard disk drive status, fan status, voltage, and current sensor status.
show /SP/network	Displays the current network configuration information. The -v option shows additional information about your network, including information about your DHCP server.
start /SP/console	Connects to the host system console. The -f option forces the console write lock from one user to another.
set /HOST send_break_action=break set /HOST send_break_action=dumpcore	Drops the host server from running the Solaris OS software into OpenBoot PROM or kmdb depending upon the mode in which the Solaris software was booted.
reset /SYS reset -script /SYS	Generates a hardware reset on the host server. The -y option enables you to skip the confirmation question.
stop /SYS stop -script /SYS stop -force /SYS	Removes the main power from the host server. The -y option enables you to skip the confirmation question. ILOM attempts to shut the server down gracefully. The - f option forces an immediate shutdown.
start /SYS	Applies the main power to the host server or FRU.
Other Commands	
help	Displays a list of all ILOM commands with their syntax and a brief description of how each command works. Specifying a command name as an option enables you to view the help for that command.
reset /SP reset -script /SP	Reboots ILOM. The -y option enables you to skip the confirmation question.
exit	Logs out from shell session.

4.6 ILOM Variables

When updating the firmware it is recommended that a number of eeprom and SP variables are recorded. Those marked with Y in the FW reset column may be overwritten during the firmware update (or downgrade) of the machine. This appendix provides a table which can be used to save the configuration details.
For systems configured to run LDoms the SA should ensure that the running LDom configuration is current, and if not save using the command ldm add-config <config-name>

FW Reset	Command to display	Variable List	Current Value	Command to set
These commands would be used at the OBP (usually ok>) and require that the host be shut down but powered on				
N	printenv	auto-boot?		setenv auto-boot?=<value>
		boot-device		setenv boot-device=<value>
		use-nvramrc?		setenv use_nvramrc?=<value>

		nvramc		setenv nvramrc=<value>
These commands should be executed at the ILOM prompt (usually >)				
N	show SP/network	ipaddress		set SP/network pendingipaddress=<value> *
		ipdiscovery		set SP/network pendingipdiscovery=<value> *
		ipgateway		set SP/network pendingipgateway=<value> *
		ipnetmask		set SP/network pendingipnetmask=<value> *
Y	show HOST	autorunonerror		set HOST autorunonerror=<value>
		ioreconfigure		set HOST ioreconfigure=<value>
Y	show HOST/bootmode	config		set HOST/bootmode config=<value>
		error_reset_level		set HOST/diag error_reset_level=<value>
		error_reset_verbosity		set HOST/diag error_reset_verbosity=<value>
		hw_change_level		set HOST/diag hw_change_level=<value>
		hw_change_verbosity		set HOST/diag hw_change_verbosity=<value>
		level		set HOST/diag level=<value>
		mode		set HOST/diag mode=<value>
		power_on_level		set HOST/diag power_on_level=<value>
		power_on_verbosity		set HOST/diag power_on_verbosity=<value>
		trigger		set HOST/diag trigger=<value>
		verbosity		set HOST/diag verbosity=<value>
Y	show HOST/domain/control	auto-boot		set HOST/domain/control auto-boot=<value>
		boot_guests		set HOST/domain/control boot-guests=<value>
Y	show HOST/tpm	enable		set HOST/tpm enable=<value>
		activate		set HOST/tpm activate=<value>
		forceclear		set HOST/tpm forceclear=<value>
Y	show SYS	keyswitch_state		set SYS keyswitch_state=<value>
Y	show SP/powermgmt	policy		set SP/powermgmt policy=<value>

* In order to enable the IP settings for the ILOM the following setting is required, it should be set once from the ILOM prompt after all the IP settings above have been defined,
set SP/network commitpending=true

4.7 Patch Validation

There is no Validation Method provided by ORACLE

4.8 Patch Install Order

***Note that Below Patches are included in Firmware Update patch set.**

System	Patch	FW Version	Oracle Release	Firmware filename
T5120/T5220	T5120/T5220	7.4.11	8-Jul-17	Sun_System_Firmware-7_4_11-SPARC_Enterprise_T5120+T5220.pkg
T5240	T5240	7.4.11	8-Jul-17	Sun_System_Firmware-7_4_11-SPARC_Enterprise_T5140+T5240.pkg
T5440	T5440	7.4.11	8-Jul-17	Sun_System_Firmware-7_4_11-SPARC_Enterprise_T5440.pkg
T3-1	T3-1	8.3.40	8-May-17	Sun_System_Firmware-8_3_40-SPARC_T3-1.pkg
T3-2	T3-2	8.3.40	8-May-17	Sun_System_Firmware-8_3_40-SPARC_T3-2.pkg
T3-4	T3-4	8.3.40	8-May-17	Sun_System_Firmware-8_3_40-SPARC_T3-4.pkg
T4-1	T4-1	8.9.9	16-Sep-2017	Sun_System_Firmware-8_9_9-SPARC_T4-1.pkg
T4-2	T4-2	8.9.9	16-Sep-2017	Sun_System_Firmware-8_9_9-SPARC_T4-2.pkg
T4-4	T4-4	8.9.9	16-Sep-2017	Sun_System_Firmware-8_9_9-SPARC_T4-4.pkg
T5-4	T5-4	9.6.21.a	06-Dec-2017	Sun_System_Firmware-9_6_21_a-SPARC_T5-4+T5-8.pkg

5 KNOWN ISSUES

- SPARC T5 platforms, and any platforms supporting dual-bank FLASH storage for Sun System Firmware should use the "-u" option to automatically update the Sun System Firmware after the download. Problems have been reported when not using this automatic mode.

- Due to the change with bugid 22886949, prior to updating to Sun System Firmware 9.6.5, please check the content of /etc/system file for the existence of "xc_tick_limit_scale". If the tunable parameter exists, please remove it.

- **For using sysfwdownload –u option**

  CAUTION: Under conditions that the upgrade does not succeed in the ALOM/ILOM, users must get to ALOM/ILOM over the net or serial connection and check the error condition.

  NOTE 1: This option is supported on all ILOM-based SPARC platforms with Sun System Firmware 7.2.0 and later.
  NOTE 2: For the -u flag to operate properly, the system must be configured to automatically boot. Use the eeprom command to verify that the auto-boot? setting is set to true. If it is set to false, use the eeprom command to change the setting to true.
  NOTE 3: If the host (step (b) Power down host above) takes longer than 15 minutes to shutdown, then the sysfwdownload upgrade process will not be able to continue even if the host eventually powers off. If the host has been powered off, then the firmware update can be resumed by using the 'load' command from the ILOM command shell. If the host is still running, then check the host console output for messages indicating what prevented the host from shutting down.

  Determine what causes the messages and take the appropriate/necessary actions so the host can be shutdown in a timely manner.

  Example: see 'svcs -xv' for details

  then, disable the problematic service first and try again:

  ```
  # svcadm disable <service name>
  ```

6 BACK OUT PLANS

Firmware patches cannot be removed in the traditional sense and downgrades are not guaranteed.