Sun Open Telecommunications Platform 2.0 Administration Guide

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 820–4154
March 2008

080411@19860

Contents

Preface 5

1 Solution Life-Cycle Management 11

Solution Administration 11

Managing Different Applications 11

Preparing Components For Backup and Restore 15

Preventing Management Stage Change 15

Converting a Stand-alone Sun OTP Host to a Clustered Sun OTP Host 16

▼ To Convert a Stand-alone Sun OTP Host to a Clustered Sun OTP Host 16

Enabling and Disabling the Sun OTP System Management Service and the Sun OTP Application Provisioning Service 19

▼ To Enable and Disable the Sun OTP System Management Service Using the CLI 19

▼ To Enable and Disable the Sun OTP Application Provisioning Service Using the CLI 19

▼ To Enable and Disable the Sun OTP System Management and Sun OTP Application Provisioning Service Using GUI 20

Administering Web SSO Users 21

Hardening and Unhardening the Sun OTP Host 26

▼ To Install the Sun OTP SST Driver 26

▼ To Uninstall the Sun OTP SST Driver 26

▼ To Harden the Sun OTP Host 27

▼ To Unharden the Sun OTP Host 28

Solution Updates and Patch Clusters 29

Sun OTP Patch Clusters 29

Updating Sun OTP Components 29

▼ To Update Sun OTP Components Using the GUI 30

▼ To Update Sun OTP Components Using CLI 31

Solution Upgrades 32

Upgrading Sun OTP 32
▼ To Upgrade Sun OTP 1.1 Provisioning Server to Version 2.0 33
Auditing the System 54
▼ To Audit Your System 54
Sun OTP Backup and Restore 56
Backing Up Sun OTP Services 56
▼ To Back Up the Sun OTP Services 56
▼ To Back Up Sun OTP Services at Scheduled Intervals 57
Restoring Sun OTP Services 58
▼ To Restore Sun OTP Services 58

A Sun OTP Upgrade Plan Worksheet 59
Sun OTP Plan Settings Descriptions 59
Sun OTP Plan Worksheet 63

Index 67

Preface

Sun Open Telecommunications Platform 2.0 Administration Guide describes how to administer the Sun™ Open Telecommunications Platform (Sun OTP) software in the development environment.

The following topics are discussed:

- "What is Sun OTP?" on page 5
- "Target Audience" on page 7
- "Component Product Mapping" on page 8
- "Sun OTP Documentation Set" on page 9
- "Sun Welcomes Your Comments" on page 10

What is Sun OTP?

Sun Open Telecommunications Platform (Sun OTP) provides integrated high availability services, system management services, application provisioning services, and security services that enable you to develop, deploy, host, and secure Network Equipment Provider (NEP) applications.

Sun OTP version 2.0 provides the following services:

- "Provisioning Service" on page 5
- "Management Service" on page 6
- "Availability Service" on page 6
- "Security Service" on page 7

Provisioning Service

Provisioning service consists of platform and application provisioning services.

Platform Provisioning

The platform provisioning service enables end-to-end provisioning of Sun OTP compute elements, including bare metal and firmware provisioning, operating system provisioning, and provisioning of Sun OTP software components.

Application Provisioning

The application provisioning service enables end-to-end provisioning of (NEP) applications, including initial application deployment, application upgrade, and application patching. Application provisioning services are capable of deploying applications on a single system, or on a group of systems that follow a set of defined grouping semantics. These services are also capable of deploying both single and multi-tier applications.

The following operations are supported by the application provisioning service:

- Creating application deployment descriptions
- Modifying application deployment descriptions
- Deleting application deployment descriptions
- Provisioning applications on hosts
- Provisioning a multi-tier application
- Inspecting deployed software on hosts at a specific point
- Removing applications from hosts
- Removing a multi-tier application
- Rolling back to previous version of applications
- Querying deployed applications on hosts

Management Service

Management service consists of platform management and application management services.

Platform Management

The platform management service enables monitoring and managing the Sun OTP compute elements. This includes monitoring and managing the bare metal hardware and deployed operating system instances. The platform management service can manage both stand-alone systems and two or more systems grouped together into an administrative group.

Application Management

The application management service enables management of NEP applications. Supported operations include application health monitoring, failure recovery and migration from one Sun OTP instance to another.

Availability Service

The availability service consists of platform availability and application availability services.

Platform Availability

The platform availability service enables availability of the Sun OTP compute elements.

Application Availability

The application availability service enables basic life cycle and availability management of NEP applications. Supported life cycle operations include registration, activation, and deactivation of applications.

The following operations are supported by the application life cycle and availability management services:

- Creating application manifests
- Modifying application manifests
- Deleting application manifests
- Creating application dependencies
- Modifying application dependencies
- Deleting application dependencies
- Registering applications
- Starting applications
- Stopping applications
- Querying application state
- Migrating applications from host A to host B
- Failing over applications from host A to host B
- Restarting applications on host X

Security Service

The security service is used to secure NEP applications by authenticating Web applications through a Web Single Sign-On (Web SSO) feature. Once you log into a web-based administration interface in Sun OTP, you can access the other web-based administration interfaces without any reauthentication. Additionally, you can use the Solaris Security Toolkit (SST) driver to harden the Sun OTP application hosting environment (AHE) to improve the overall network security.

Target Audience

OEM developers who wish to install Sun OTP in their development environment and integrate their applications with Sun OTP.

Component Product Mapping

The following figure shows the components that are part of Sun OTP 2.0.

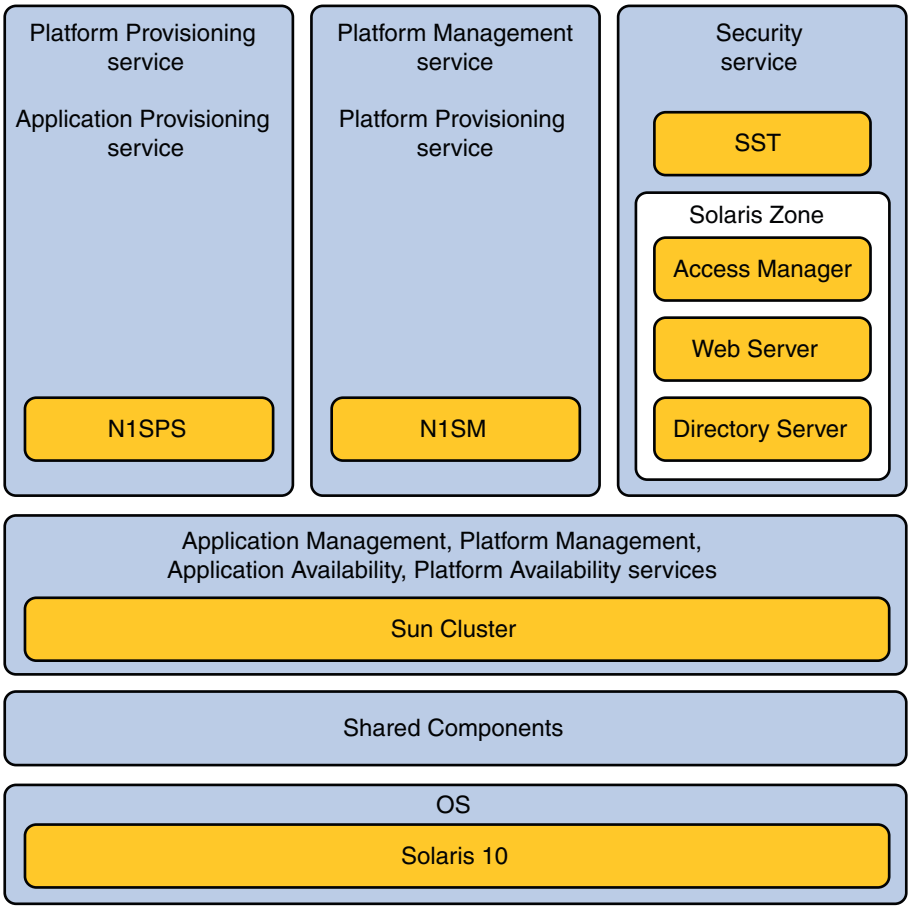

FIGURE P–1 Component Product Mapping

Supported Versions

The following table shows the OS and component versions that are supported by Sun OTP 2.0.

TABLE P–1 Sun OTP 2.0 Supported Versions

OS and Components	Version
Solaris™ OS	10 Update 3

TABLE P–1 Sun OTP 2.0 Supported Versions *(Continued)*

OS and Components	Version
Sun Cluster	3.2
Sun N1™ Service Provisioning System	5.2.4
Sun N1 System Manager	1.3.3
OS Provisioning Plug-in	3.2
Sun Java™ System Web Server	7.0 Update 1
Sun Java System Directory Server	6.1 Enterprise Edition
Sun Java System Access Manager	7.1
Solaris Security Toolkit	4.2

Sun OTP Documentation Set

Sun OTP guides are available as online files in PDF and HTML formats. The following table lists the tasks and concepts described in each guide.

TABLE P–2 Sun OTP Documentation Set

Documentation	Purpose
Sun Open Telecommunications Platform 2.0 Release Notes	Late-breaking information about the software and documentation
Sun Open Telecommunications Platform 2.0 Installation Guide	Provides the procedure for installing Sun OTP in the development environment
Sun Open Telecommunications Platform 2.0 Administration Guide	Provides the procedure for administrating Sun OTP in the development environment
Sun Open Telecommunications Platform 2.0 Developer's Guide	Describes how to develop and deploy applications using Sun OTP.

The complete Sun OTP documentation is available at `http://docs.sun.com/app/docs/coll/1629.4`.

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. To share your comments, go to `http://docs.sun.com` and click Send Comments. In the online form, provide the full document title and part number. The part number is located on the book's title page and in the document's URL. For example, the name of this book is Sun Open Telecommunications Platform 2.0 Administration Guide and the part number of this book is 820-4154.

◆ ◆ ◆ CHAPTER 1

Solution Life-Cycle Management

This chapter explains the procedure to administer, update, upgrade, back up, and restore Sun OTP.

- "Solution Administration" on page 11
- "Solution Updates and Patch Clusters" on page 29
- "Solution Upgrades" on page 32
- "Sun OTP Backup and Restore" on page 56

Solution Administration

NEPs can use Sun OTP to their deploy solutions. This section provides information on how to start, stop, and manage the network equipment provider (NEP) applications deployed on Sun OTP. The following topics are discussed:

- "Managing Different Applications" on page 11
- "Preparing Components For Backup and Restore" on page 15
- "Preventing Management Stage Change" on page 15
- "Converting a Stand-alone Sun OTP Host to a Clustered Sun OTP Host" on page 16
- "Enabling and Disabling the Sun OTP System Management Service and the Sun OTP Application Provisioning Service" on page 19
- "Administering Web SSO Users" on page 21
- "Hardening and Unhardening the Sun OTP Host" on page 26

Managing Different Applications

This section describes how to manage applications in the the following scenarios:

- **Scenario 1: Simple application on a single cluster** - This application runs only on a single cluster. The application can be modeled as a single cluster resource, which can then added to a single resource group. NEPs would then be able to manage their application by changing

the state of a resource group to `online` or `offline`. The command to bring the resource group to `online` state is `clresourcegroup online` and to bring the resource group to `offline` state is `clresourcegroup online`.

The other management states operations are

- `manage`: Resource groups are in an unmanaged state when they are created. Use the `manage` subcommand to bring the resource group to a managed state. If you use this subcommand in a non-global zone, it successfully operates only on resource groups whose node list contains that zone. If you use this subcommand in the global zone, it can operate on any resource group. See example:

  ```
  /usr/cluster/bin/clresourcegroup manage {+| resourcegroup?}
  ```

- `quiesce`: This command stops a resource group from continuously switching from one node or zone to another node. If you use this subcommand in a non-global zone, it operates only on resource groups whose node list contains that zone. If you use this subcommand in the global zone, it can operate on any resource group. Use the `-k` option to kill methods that are running on behalf of resources in the affected resource groups. If you do not specify the `-k` option, methods are allowed to continue running until they exit or exceed their configured timeout. See example:

  ```
  /usr/cluster/bin/clresourcegroup quiesce [*-k*] {+| resourcegroup?}
  ```

For more information on changing the state of a resource group, see `clrg`(1CL).

- **Scenario 2: Application using multiple components deployed on a single cluster** - This application can be managed by using multiple resource group. These resource groups can be managed using the provisioning service. However, the dependency issues between the resource groups should be considered. The state of resource group may have to be changed to `online` or `offline` in a sequential order. The administration provisioning service can be used to manage the resource groups lifecycle.
- **Scenario 3: Application using multiple components deployed on multiple clusters** - This application is a multi-tier application. Within a cluster, NEPs could assign the application or each application component to a resource group, as described in scenarios 1 and 2. These resource groups can be managed using the provisioning service. However, the dependency issues between resource groups and within each resource group should be considered.

  Consider an example of a 3 tier application where a simple start plan sequentially calls the start procedure for the components representing the 3 tiers of a sample application. Tier 1 is the access logic tier, tier 2 is the business logic tier, and tier 3 is the data tier. The sequence of the start order is 3, 2, and 1 and the stop order is 1, 2, and 3. Sample code of a composite plan for starting and stopping a 3 tier application is as follows. In this sample, `DbComponent`, `AsComponent`, and `WsComponent` representing tier 3, 2 and 1 respectively are installed and our example plans are run on three hosts, that is, one host per each tier.

  Sample code for starting a 3 tier application

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- generated by N1 SPS -->
```

```
<executionPlan xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
name='startThreeTierApp' version='5.2.4' xsi:schemaLocation='http://www.sun.com/schema/SPS plan.xsd'
xmlns='http://www.sun.com/schema/SPS'>
  <compositeSteps>
    <inlineSubplan planName='startTierThree'>
      <varList>
        <var name="hName" default=":[target(/):sys.hostName]"/>
      </varList>
      <simpleSteps implicitLocking='true'>
        <!-- plan runs on three hosts (one host for each tier). Start tier 3
if and only if this machine is hosting it.-->
        <if>
          <condition><equals value1=":[tierThreeHost]" value2=":[hName]"/></condition>
          <then>
            <call blockName='startDbComponent'>
              <installedComponent name='dbComponent' path='/some/path/db'></installedComponent>
            </call>
          </then>
        </if>
      </simpleSteps>
    </inlineSubplan>

    <inlineSubplan planName='startTierTwo'>
      <varList>
        <var name="hName" default=":[target(/):sys.hostName]"/>
      </varList>
      <simpleSteps implicitLocking='true'>
        <!-- plan runs on three hosts (one host for each tier). Start tier 2
if and only if this machine is hosting it.-->
        <if>
          <condition><equals value1=":[tierTwoHost]" value2=":[hName]"/></condition>
          <then>
            <call blockName='startAsComponent'>
              <installedComponent name='dbComponent' path='/some/path/as'></installedComponent>
            </call>
          </then>
        </if>
      </simpleSteps>
    </inlineSubplan>

    <inlineSubplan planName='startTierOne'>
      <varList>
        <var name="hName" default=":[target(/):sys.hostName]"/>
      </varList>
      <simpleSteps implicitLocking='true'>
        <!-- plan runs on three hosts (one host for each tier). Start tier 1
if and only if this machine is hosting it.-->
        <if>
```

```
          <condition><equals value1=":[tierOneHost]" value2=":[hName]"/></condition>
          <then>
            <call blockName='startWsComponent'>
              <installedComponent name='dbComponent' path='/some/path/ws'></installedComponent>
            </call>
          </then>
        </if>
      </simpleSteps>
    </inlineSubplan>

  </compositeSteps>
</executionPlan>
```

Sample code for stopping a 3 tier application

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- generated by N1 SPS -->
<executionPlan xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
name='stopThreeTierApp' version='5.2.4' xsi:schemaLocation='http://www.sun.com/schema/SPS plan.xsd'
xmlns='http://www.sun.com/schema/SPS'>
  <compositeSteps>

    <inlineSubplan planName='stopTierOne'>
      <varList>
        <var name="hName" default=":[target(/):sys.hostName]"/>
      </varList>
      <simpleSteps implicitLocking='true'>
        <!-- plan runs on three hosts (one host for each tier). Stop tier 1
if and only if this machine is hosting it.-->
        <if>
          <condition><equals value1=":[tierOneHost]" value2=":[hName]"/></condition>
          <then>
            <call blockName='stopWsComponent'>
              <installedComponent name='dbComponent' path='/some/path/ws'></installedComponent>
            </call>
          </then>
        </if>
      </simpleSteps>
    </inlineSubplan>

    <inlineSubplan planName='stopTierTwo'>
      <varList>
        <var name="hName" default=":[target(/):sys.hostName]"/>
      </varList>
      <simpleSteps implicitLocking='true'>
        <!-- plan runs on three hosts (one host for each tier). Stop tier 2
if and only if this machine is hosting it.-->
        <if>
```

```
          <condition><equals value1=":[tierTwoHost]" value2=":[hName]"/></condition>
          <then>
            <call blockName='stopAsComponent'>
              <installedComponent name='dbComponent' path='/some/path/as'></installedComponent>
            </call>
          </then>
        </if>
      </simpleSteps>
    </inlineSubplan>

    <inlineSubplan planName='stopTierThree'>
      <varList>
        <var name="hName" default=":[target(/):sys.hostName]"/>
      </varList>
      <simpleSteps implicitLocking='true'>
        <!-- plan runs on three hosts (one host for each tier). Stop tier 3
if and only if this machine is hosting it.-->
        <if>
          <condition><equals value1=":[tierThreeHost]" value2=":[hName]"/></condition>
          <then>
            <call blockName='stopDbComponent'>
              <installedComponent name='dbComponent' path='/some/path/db'></installedComponent>
            </call>
          </then>
        </if>
      </simpleSteps>
    </inlineSubplan>

  </compositeSteps>
</executionPlan>
```

Preparing Components For Backup and Restore

NEPs might need to save a state of an application, for example, save a state before running the backup plan. In this case, NEPs should stop the application and save the state. For details on how to manage applications, see "Managing Different Applications" on page 11.

Preventing Management Stage Change

You can configure the resource group property so that administrators will not be able to offline the resources. If the `RG_System` property is `TRUE` for a resource group, the resource group has restricted privileges and the operation of `clresource` and `clresourcegroup` commands are affected. This prevents accidental modification or deletion of critical resource groups and resources restricted privileges.

To enable the `RG_System` property on the resource group, type the following command:

```
/usr/cluster/bin/clrg set -p RG_System=true RG-Name
```

Example to set the OTP provisioning services group to system group

```
/usr/cluster/bin/clrg set -p RG_System=true otp-system-rg
```

To disable the`RG_System` property on the resource group, type the following command:

```
/usr/cluster/bin/clrg set -p RG_System=false RG-Name
```

Example to disable the `System` property on the OTP provisioning services group

```
/usr/cluster/bin/clrg set -p RG_System=false otp-system-rg
```

For more details on the `System` property, refer to the following Sun Cluster documents:

– Sun Cluster 3.2 Reference Collection for Solaris OS
`http://docs.sun.com/app/docs/coll/1029.6`

– `rg_properties`(5)

Converting a Stand-alone Sun OTP Host to a Clustered Sun OTP Host

This section provides the procedure to convert a stand-alone Sun OTP host to a clustered Sun OTP host. The conversion from stand-alone to clustered OTP host ensures that the following changes are performed on the host:

- The shared disk for the cluster is created.
- The provisioning services are moved to the shared disk and run from the shared disk.
- The RGM settings for the `otp-system-rg` resource group and its resources are updated accordingly.
- The host node type is changed from single to first node.

▼ To Convert a Stand-alone Sun OTP Host to a Clustered Sun OTP Host

1 Go to https://*Sun OTP host*:9090, where *Sun OTP host* is the IP address or the fully qualified name of the provisioning service logical hostname that is already configured during Sun OTP installation.

The Sun OTP common Single Sign-On login screen appears.

2 Type the user name and password.

The user name is `otpadmin`. The password is the password provided in the password file while setting up the Sun OTP provisioning server.

3 Click OTP Setup to display the Sun Open Telecommunications Platform utility tasks page.

4 Convert the Stand-alone Sun OTP host to the Clustered Sun OTP host.

Note – Before performing Step 4, make sure that the Sun OTP Plan settings have the correct value for the `privateInterface1` and `privateInterface2` variables.

---

a. Click Convert.

The Convert Single to Clustered plan details screen appears.

b. Click run.

The Convert Single to Clustered plan run screen appears.

c. Type the name of the stand-alone Sun OTP host that you want to convert to a clustered Sun OTP host in the target host field.

d. Click run plan (includes preflight).

5 Create the database and metaset on the stand-alone OTP host.

The shared storage should have a minimum of 1.5 gigabytes disk space.

For example,

```
metadb -a -f -c 6 c1t0d0s7
metaset -s sm-dg -a -h standalonehostname
metaset -s sm-dg -a /dev/did/rdsk/d6
metainit -s sm-dg d0 1 1 /dev/did/rdsk/d6s0
newfs /dev/md/sm-dg/rdsk/d0
```

6 Add the following entry to the `/etc/vfstab` file.

```
/dev/md/sm-dg/dsk/d0 /dev/md/sm-dg/rdsk/d0 /var/js ufs 2 no logging
```

7 Change the storage of the Sun OTP system management service and the Sun OTP application provisioning service from local disks to shared disks.

a. Create temporary mount points and mount the shared volumes onto the temporary mount points.

Type `mkdir /tmp/js`

Type `mount /dev/md/sm-dg/dsk/d0 /tmp/js`

b. Bring the `otp-system-rg` resource group offline.

```
clresourcegroup set -p RG_system=false otp-system-rg
clresourcegroup offline otp-system-rg
```

c. Move the Sun OTP system service contents from the local disk to the shared volume.

```
mv /var/js/* /tmp/js
umount /tmp/js
```

d. Disable all the resources in the `otp-system-rg` resource group.

```
clresource disable otp-lhn-rs
clresource disable otp-hasp-rs
clresource disable otp-nfs-rs
clresource disable otp-sm-rs
clresource disable otp-spsra-rs
clresource disable otp-spsms-rs
```

e. Modify the properties of the `HAStoragePlus` resource.

```
clresource set -p FilesystemMountPoints=/var/js otp-hasp-rs
clresource set -p GlobalDevicePaths=/dev/md/sm-dg/dsk/d0 otp-hasp-rs
```

f. Enable all the resources in the `otp-system-rg` resource group.

```
clresource enable otp-lhn-rs
clresource enable otp-hasp-rs
clresource enable otp-nfs-rs
clresource enable otp-sm-rs
clresource enable otp-spsra-rs
clresource enable otp-spsms-rs
```

g. Bring the `otp-system-rg` resource group online.

```
clresourcegroup online otp-system-rg
```

h. Set the system property of the `otp-system-rg` resource group to true.

```
clresourcegroup set -p RG_system=true otp-system-rg
```

Next Steps You can add new hosts to the cluster.

Enabling and Disabling the Sun OTP System Management Service and the Sun OTP Application Provisioning Service

This section provides procedures for enabling and disabling the system management service and the application provisioning service on a single Sun OTP host.

▼ To Enable and Disable the Sun OTP System Management Service Using the CLI

The following steps enable and disable the Sun OTP system management service on the entire cluster. Ensure to run this plan on the first (or single) node.

1 **Log in as root (`su - root`) to the Sun OTP host.**

2 **Use the `serviceManagement` script with the `n1sm` option to enable and disable the Sun OTP system management service.**

- **To enable the service, use the `start` option.**

  ```
  /opt/SUNWotp/cli/serviceManagement n1sm start
  ```

- **To disable the service, use the `stop` option.**

  ```
  /opt/SUNWotp/cli/serviceManagement n1sm stop
  ```

Tip – You can check the log information in the `/var/OTP/OTPSvcMgmt.log` file to verify whether the services are enabled or disabled.

▼ To Enable and Disable the Sun OTP Application Provisioning Service Using the CLI

Note –

- If the Sun OTP application provisioning service is running in the high availability mode, the provisioning service is enabled or disabled on all the hosts in the cluster.
- If the Sun OTP application provisioning service is not running in the high-availability mode, the Sun OTP application provisioning service is enabled or disabled only on the target host.

---

1 **Log in as root (`su - root`) to the Sun OTP host.**

2 **Use the `serviceManagement` script with the `n1sps` option to enable and disable the Sun OTP application provisioning service.**

- **To enable the service, use the `start` option.**

  ```
  /opt/SUNWotp/cli/serviceManagement n1sps start
  ```

- **To disable the service, use the `stop` option.**

  ```
  /opt/SUNWotp/cli/serviceManagement n1sps stop
  ```

▼ To Enable and Disable the Sun OTP System Management and Sun OTP Application Provisioning Service Using GUI

The graphical user interface cannot be used to disable the Sun OTP application provisioning service on the host on which it is running. In other words, if the service is running on `otpclient01`, you cannot use the graphical user interface on `otpclient01` to disable the application provisioning service. Instead, use the command- line interface to disable the application provisioning service.

1 **Go to https://*Sun OTP host*:9090 where *Sun OTP host* is the IP address or the fully qualified name of the Sun OTP host on which the resource group is active.**

2 **Type the user name and password.**

The user name is `otpadmin`. The password is the password provided in the password file while setting up the Sun OTP provisioning server.

3 **Click OTP Setup to display the Sun Open Telecommunications Platform utility tasks page.**

4 **Click Enable & Disable and click run.**

5 **Type the host name on which you want to enable or disable the services in the target host field.**

6 **Decide whether to enable or disable the services.**

- **Select the N1SPS should be running and N1SM should be running check boxes to enable the services.**
- **Do not select the N1SPS should be running and N1SM should be running check boxes to disable the services.**

7 **Select the Yes, I really want to modify state of services check box.**

8 **Click run plan (includes preflight)**

9 **Type the `clrg` command to check status of the `otp-system-rg` resource group.**

Tip – You can also check the log information in the `/var/OTP/SUNWotp-debug.log` file to verify whether the services are enabled or disabled.

Administering Web SSO Users

This section provides procedures to administer Web SSO users. Sun OTP 2.0 provides you the ability to administer Web Single Sign On (SSO) using the browser user interface (BUI) and the command-line interface (CLI). You can create new Web SSO users, change the password of existing users, and remove existing users.

The following topics are discussed:

- "Adding Web SSO User" on page 21
- "Changing the Password of Existing Web SSO User" on page 23
- "Removing Web SSO User" on page 24

Adding Web SSO User

You can add new Web SSO users.

This task creates user accounts for Sun OTP application provisioning service, Sun OTP system management service, and Sun OTP security service with the provided credentials. The timeout value for each user session on server is two hours.

▼ To Create a Role

You need to manually create a user role before assigning the role to the Web SSO user. You need to create a role on all the cluster hosts and on all the zones, if applicable.

1. **Log in as root (`su - root`) to the Sun OTP host.**

2. **Create a new role account.**

   For example, create a role by name `ssorole`.

   ```
   roleadd -s /bin/pfksh -d /export/home/ssorole -K defaultpriv=basic -P "Cluster
   Management,Web Console Management,Cluster Operation,Sun Cluster Commands,All"
   ssorole
   ```

   Note – It is mandatory to add a profile to the role that you create. Else, you will not be able to perform the administration task on a cluster. For more information on the `roleadd` command, see the `roleadd` man page.

3. **Change the password for the new role.**

   For example

```
passwd ssorole
```

Enter the new password for the role and confirm the password.

4 **Create a home directory for the role.**

```
mkdir /export/home/ssorole
```

```
chown ssorole:other /export/home/ssorole
```

5 **Restart the name service cache daemon for the new role to take effect.**

Perform this step after all the above steps are performed on all the cluster hosts and on all the zones, if applicable.

```
svcadm restart system/name-service-cache
```

▼ To Add Web SSO User Using GUI

Ensure that the resource group `otp-security-ds-rg group` is online on the first host of the cluster.

1 **Open a browser and log in to the Sun OTP application provisioning service on the Sun OTP provisioning server.**

Go to https://*install server*:9090 where *install server* is the IP address or the fully qualified name of the Sun OTP provisioning server.

2 **Type the user name and password.**

The user name is `otpadmin`. The password is the password provided in the password file while setting up the Sun OTP provisioning server.

3 **Click OTP Setup to display the Sun Open Telecommunications Platform utility tasks page.**

4 **Click Add User and click run.**

The `SynchronizeWebSSOUsers` plan run screen appears.

5 **Type the host name in the target host field.**

6 **Type the Web SSO user name in the WebSSO login name field.**

7 **Type the password in the WebSSO password field.**

8 **Confirm the password in the Retype WebSSO password field.**

9 **Type the user role in the User role field.**

You need to manually create a role before assigning it to the Web SSO user.

If there is no user role, do not specify any value for this field.

10 Click run plan (includes preflight).

▼ To Add Web SSO User Using the CLI

- The `ssocli` command needs to be executed on the same server which was used for the deployment.
- Ensure that the resource group `otp-security-ds-rg group` is online on the first host of the cluster.

1 Log in as root (`su - root`) to the provisioning server.

2 Type the following command to add Web SSO user.

`/opt/SUNWotp/cli/ssocli add -u` *ssousername* `-f` *oldpasswordfile* `-c` *clusterhostset* `-r` *role* `-i`

ssousername is the Web SSO user name.

oldpasswordfile is the file that contains the old or initial password on the first line.

clusterhostset is the cluster host set.

role is the role of the Web SSO user. You need to manuallycreate a role before assigning it to the Web SSO user.

If there is no user role, do not specify any value for *role*.

For example

```
/opt/SUNWotp/cli/ssocli add -u ssouser -f /tmp/pass -c cl-sso -r manager -i
```

Changing the Password of Existing Web SSO User

You can change the password of sn existing Web SSO user account.

▼ To Change the Password of Existing Web SSO User Using GUI

1 Open a browser and log in to the Sun OTP application provisioning service on the Sun OTP provisioning server.

Go to https://*install server*:9090 where *install server* is the IP address or the fully qualified name of the Sun OTP provisioning server.

2 Type the user name and password.

The user name is `otpadmin`. The password is the password provided in the password file while setting up the Sun OTP provisioning server.

3. **Click OTP Setup to display the Sun Open Telecommunications Platform utility tasks page.**
4. **Click Change User Password and click run.**
   The `ChangeWebSSOPassword` plan run screen appears.
5. **Type the host name in the target host field.**
6. **Type the Web SSO user name in the WebSSO login name field.**
7. **Type the old password in the Old WebSSO password field.**
8. **Type the new password in the New WebSSO password field.**
9. **Confirm the new password in the Retype New WebSSO password field.**
10. **Click run plan (includes preflight).**

▼ To Change the Password of Existing Web SSO User Using the CLI

- The `ssocli` command needs to be executed on the same server which was used for the deployment.
- Ensure that the resource group `otp-security-ds-rg group` is online on the first host of the cluster.

1. **Log in as root (`su - root`) to the provisioning server.**
2. **Type the following command to change the password.**
   `/opt/SUNWotp/cli/ssocli password -u` *ssousername* `-f` *oldpasswordfile* `-n` *newpasswordfile* `-c` *clusterhostset*

   ssousername is the Web SSO user name.

   oldpasswordfile is the file that contains the old or initial password on the first line.

   newpasswordfile is the file that contains the new password on the first line.

   clusterhostset is the cluster host set.

   For example

   ```
   /opt/SUNWotp/cli/ssocli password -u ssouser -f /tmp/oldpass -n /tmp/newpass -c
   cl-sso
   ```

Removing Web SSO User

You can remove Web SSO users.

To Remove Web SSO User Using GUI

1. **Open a browser and log in to the Sun OTP application provisioning service on the Sun OTP provisioning server.**

   Go to https://*install server*:9090 where *install server* is the IP address or the fully qualified name of the Sun OTP provisioning server.

2. **Type the user name and password.**

   The user name is `otpadmin`. The password is the password provided in the password file while setting up the Sun OTP provisioning server.

3. **Click OTP Setup to display the Sun Open Telecommunications Platform utility tasks page.**

4. **Click Remove User and click run.**

   The `RemoveWebSSOUsers` plan run screen appears.

5. **Type the host name in the target host field.**

6. **Type the Web SSO user to remove in the WebSSO login name field.**

7. **Click run plan (includes preflight).**

To Remove Web SSO User Using the CLI

- The `ssocli` command needs to be executed on the same server which was used for the deployment.
- Ensure that the resource group `otp-security-ds-rg group` is online on the first host of the cluster.

1. **Log in as root (`su - root`) to the provisioning server.**

2. **Type the following command to remove Web SSO user.**

   `/opt/SUNWotp/cli/ssocli remove -u` *ssousername* `-c` *clusterhostset*

   ssousername is the Web SSO user name.

   clusterhostset is the cluster host set.

   For example

   `/opt/SUNWotp/cli/ssocli remove -u ssouser -c cl-sso`

Hardening and Unhardening the Sun OTP Host

This section provides procedures for hardening and unhardening the system. Using Sun OTP 2.0, you can harden and unharden the Sun OTP host. Hardening is the process of modifying the Solaris™ operating system configuration to improve the network security of a system. By using the hardening process, you can close the ports and disable the services that might present a security risk to the system. You can unharden, that is, reopen the ports and enable the services that were closed by the hardening process. Hardening and unhardening must be done on both global and non-global zones.

▼ To Install the Sun OTP SST Driver

Solaris Security Toolkit (SST) driver must be installed on both global and non-global zones.

1. **Open a browser and log in to the Sun OTP application provisioning service on the Sun OTP provisioning server.**

   Go to the https://*install server*:9090 where *install server* is the IP address or the fully qualified name of the Sun OTP provisioning server.

2. **Type the user name and password.**

   The user name is `otpadmin`. The password is the password provided in the password file while setting up the Sun OTP provisioning server.

3. **Click OTP Setup to display the Sun Open Telecommunications Platform utility tasks page.**

4. **Click Install Driver and click run.**

5. **Click run.**

   The InstallSST plan run screen appears.

6. **Type the media directory in the Media Directory field.**

7. **Type the host name on which to install the driver in the target host field.**

8. **Click run plan (includes preflight).**

▼ To Uninstall the Sun OTP SST Driver

1. **Open a browser and log in to the Sun OTP application provisioning service on the Sun OTP provisioning server.**

   Go to the https://*install server*:9090 where *install server* is the IP address or the fully qualified name of the Sun OTP provisioning server.

2. **Type the user name and password.**

   The user name is `otpadmin`. The password is the password provided in the password file while setting up the Sun OTP provisioning server.

3. **Click OTP Setup to display the Sun Open Telecommunications Platform utility tasks page.**

4. **Click Uninstall Driver and click run.**

   The UninstallSST plan run screen appears.

5. **Type the host name on which to uninstall the driver in the target host field.**

6. **Click run plan (includes preflight).**

To Harden the Sun OTP Host

Hardening is the process of modifying the Solaris OS configuration to improve a system's security. By using the hardening process, you can close the ports and disable the services that might present a security risk to the system.

Before You Begin Install the Sun OTP SST Driver

1. **Open a browser and log in to the Sun OTP application provisioning service on the Sun OTP provisioning server.**

   Go to the https://*install server*:9090 where *install server* is the IP address or the fully qualified name of the Sun OTP provisioning server.

2. **Type the user name and password.**

   The user name is `otpadmin`. The password is the password provided in the password file while setting up the Sun OTP provisioning server.

3. **Click OTP Setup to display the Sun Open Telecommunications Platform utility tasks page.**

4. **Click Harden and click run.**

   The Harden plan run screen appears.

5. **Type the host name that you want to harden in the target host field.**

6. **Click run plan (includes preflight).**

Note – The plan does not close the ports and disable the services that are required by the Sun OTP components.

---

7. **Once the plan completes, reboot the Sun OTP host for hardening to take effect.**

▼ To Unharden the Sun OTP Host

Using unhardening, you can reopen the ports and enable the services that were closed by the hardening process.

Hardening is defined in certain configuration files. If you have changed certain configuration files, you can choose one of the following options during unhardening:

- Roll back only the unchanged configuration files to its default state. The changed files can be retained in its current state.
- Roll back all the configuration files, including the changed files, to its default state.

1. **Open a browser and log in to the Sun OTP application provisioning service on the Sun OTP provisioning server.**

   Go to the https://*install server*:9090 where *install server* is the IP address or the fully qualified name of the Sun OTP provisioning server.

2. **Type the user name and password.**

   The user name is `otpadmin`. The password is the password provided in the password file while setting up the Sun OTP provisioning server.

3. **Click OTP Setup to display the Sun Open Telecommunications Platform utility tasks page.**

4. **Choose the state of the configuration files.**

   - **To roll back only the unchanged configuration files to its default state, click UnHarden & Keep.**
   - **To roll back all the configuration files, including the changed files, to its default state, click UnHarden & Revert.**

5. **Click run.**

6. **Type the host name that you want to unharden in the target host field.**

7. **Click run plan (includes preflight).**

Solution Updates and Patch Clusters

This section gives an overview of patch clusters and the procedure to update Sun OTP.

The following topics are discussed:

- "Sun OTP Patch Clusters" on page 29
- "Updating Sun OTP Components" on page 29

Sun OTP Patch Clusters

Patch clusters are the consolidation of all Sun OTP and OTP-relevant component product packages and patches that are required for maintenance and maximized solution stack stability. All fixes for Sun OTP will be released as patch clusters. You can install patch clusters using both the CLI and N1SPS interfaces.

Sun OTP is a single unified solution stack consisting of integrated component products. Change management for the Sun OTP solution stack involves consolidating individual component product fixes into Sun OTP patch clusters and qualifying those patch clusters as a unified sets of change. Individual patches for constituent component products should not be used. Changes to a Sun OTP solution stack will be made through rigorously qualified patch clusters.

The patch clusters handle complexities such as dependencies, installation order, special instructions, reboots and reconfiguration, single user and multi-user modes.

Following are the two types of patch clusters:

- Critical patch cluster - A critical patch cluster includes fixes that are critical to the proper functioning and operation of Sun OTP. Critical patch clusters are time-sensitive and will be released periodically.
- Maintenance patch cluster - A maintenance patch cluster is the consolidation of component product fixes released on a periodic basis.

Updating Sun OTP Components

This section describes the method to apply Sun OTP patch cluster to update a system. You can update single or multiple components of Sun OTP by using the Command-Line Interface (CLI) or Graphical User Interface (GUI).

▼ To Update Sun OTP Components Using the GUI

1. **Open a browser and log in to the Sun OTP application provisioning service on the 1.1 Sun OTP provisioning server.**

   Go to URL https://*install server*:9090 where *install server* is either the IP address or the fully qualified name of the 1.1 Sun OTP provisioning server.

2. **Type the user name and password.**

   The user name is `otpadmin`. The password is the password provided in the password file while setting up the Sun OTP provisioning server.

3. **Import the Sun OTP Update plug-in.**

   a. **Click Administration in the left menu.**

   b. **Click the plug-ins link.**

   c. **Click the import link to import a new plug-in.**

   d. **Type the following path of the jar file in one line in the Import plug-in JAR field.**

      2.0_mediadir`/common/components/sunotp/SUNWotpupdate/reloc/SUNWotp/update/jar/com.sun.OTPUpdate_1.0.jar`

      2.0_mediadir is the fully qualified path name to the Sun Open Telecommunications Platform 2.0 installation source directory.

   e. **Click continue to import.**

      After successful import, the Sun OTP Update plug-in appears under Common Tasks.

4. **Prepare Sun OTP components for update.**

   a. **Click OTP Update in the left menu to display the OTP update steps page.**

   b. **Click Prepare and click run.**

   c. **Click select from list under variable settings.**

   d. **At the bottom of the select variable setting from list... screen, click create set to create a new variable set.**

   e. **Type a new variable set name in the Set Name field.**

f. Type the values for the following variables:

`mediaDirectory` - Fully-qualified path name to the Sun Open Telecommunications Platform 2.0 installation source directory.

`logFile` - Path of the log file that would contain the output of update operation

`Solaris` - `yes` or `no`, default value is `yes`

`SunCluster` - `yes` or `no`, default value is `yes`

`ManagementServices` - `yes` or `no`, default value is `yes`

`SecurityServices` - `yes` or `no`, default value is `yes`

g. Click save to save the variable set.

h. Close the select variable setting from list... screen.

i. In the Prepare screen, click the drop-down list under variable settings, and choose the new variable set.

j. Type the host name that you want to update in the target host field.

k. Click run plan (includes preflight).

5 Update Sun OTP components.

a. Click Update and click run.

b. Type the host name that you want to update in the target host field.

c. Click run plan (includes preflight).

The page is reloaded and a progress bar is displayed during the process. When the plan completes, wait for the Sun OTP host to boot into multi-user mode.

▼ To Update Sun OTP Components Using CLI

1 Log in as root (`su - root`) to the Sun OTP host that you want to update.

2 Navigate to the following directory.

`cd` *2.0_mediadir*`/common/components/sunotp`

2.0_mediadir is the fully-qualified path name to the Sun Open Telecommunications Platform 2.0 installation source directory.

3 **Add the `SUNWotpupdate` package on the Sun OTP host.**

```
pkgadd -d . SUNWotpupdate
```

4 **Run the `otp_update.sh` script.**

`/opt/SUNWotp/update/cli/otp_update.sh -L` *logfilepath* `-D` *2.0_mediadir components*

logfilepath is the path of the log file that contains the output of the update operation.

2.0_mediadir is the fully qualified path name to the Sun Open Telecommunications Platform 2.0 installation source directory.

components are Sun OTP components to update. *components* can be a combination of `solaris`, `n1sps`, `n1sm`, `suncluster`, and `jse`.

Solution Upgrades

This section provides procedures to upgrade Sun OTP. To upgrade Sun OTP, you first have to upgrade the provisioning server and then upgrade Sun OTP using one of the upgrade methods, that is, standard. dual-partition, or live upgrade. This section describes both the GUI and CLI upgrade procedures. Details on how to prepare a host before running the upgrade plan is also explained. At a certain point during the process of upgrading Sun OTP, NEPs can upgrade their application. The procedures described in this section gives pointer to such points.

Note – The procedures for command-line upgrade are examples and are provided only for demonstration purposes.

The following topics are discussed:

- "Upgrading Sun OTP" on page 32
- "Auditing the System" on page 54

Upgrading Sun OTP

You can upgrade Sun OTP 1.1 to version 2.0 by using one of the following upgrades methods:

- Standard upgrade. Shuts down the cluster before you upgrade the cluster nodes. You must return the cluster to production after all the nodes are fully upgraded.
- Dual-partition upgrade. Divides the cluster into two groups of nodes. You must bring down one group of nodes and upgrade those nodes. The other group of nodes continue to provide services. After you complete the upgrade of the first group of nodes, switch services to the upgraded nodes. You can then upgrade the remaining nodes and boot them back to the rest of the cluster. The cluster outage time is limited to the amount of time needed for the cluster to switch over services to the upgraded partition.

- Live upgrade. Maintains the previous cluster configuration until you have upgraded all nodes, and commit to the upgrade. If the upgraded configuration causes a problem, revert to your previous cluster configuration until you can rectify the problem.

TABLE 1–1 Task map: Description of various upgrade tasks

Task	Description
Upgrading Sun OTP 1.1 Provisioning Server to Version 2.0	This section describes the procedure to upgrade the provisioning server
"Upgrading Sun OTP Using Standard Upgrade" on page 34	This section describes the procedure to upgrade Sun OTP using the standard upgrade method. It includes both the GUI and CLI procedures, and details about how to upgrade the remaining service and install the security service.
"Upgrading Sun OTP Using Dual-Partition Upgrade" on page 40	This section describes the procedure to upgrade Sun OTP using the dual-partition method. It includes both the GUI and CLI procedures, and details about how to prepare the hosts for dual-partition upgrade.
"Upgrading Sun OTP Using Live Upgrade" on page 47	This section describes the procedure to upgrade Sun OTP using the live upgrade method. It includes both the GUI and CLI procedures, and details about how to prepare the hosts for dual-partition upgrade.

▼ To Upgrade Sun OTP 1.1 Provisioning Server to Version 2.0

Note – You can directly use the Sun OTP 2.0 provisioning server to upgrade Sun OTP. Sun OTP 2.0 provisioning server has the `SUNWotp`, `SUNWotpupdate`, and `SUNWotpupg` packages installed.

1 Log in as root (`su - root`) to the 1.1 Sun OTP provisioning server.

2 Remove the packages.

```
pkgrm SUNWotp SUNWotpcli SUNWotputil
```

If the OSP plug-in along with the `SUNWotpra` custom package was used to install the Solaris OS on this system, remove the `SUNWotpra` package.

```
pkgrm SUNWotpra
```

3 Change to the following directory.

```
cd 2.0_mediadir/common/components/sunotp
```

2.0_mediadir is the fully qualified path name to the Sun Open Telecommunications Platform 2.0 installation source directory.

4. **Add the following packages.**

   ```
   pkgadd -d . SUNWotp SUNWotpupdate SUNWotpupg
   ```

5. **Reconfigure the Sun OTP application provisioning service on the Sun OTP 1.1 Sun OTP provisioning server.**

   ```
   /opt/SUNWotp/upgrade/n1sps_reconfigure.pl --run reconfig --nodetype none
   --params mediadir=2.0_mediadir
   ```

   2.0_mediadir is the fully qualified path name to the Sun Open Telecommunications Platform 2.0 installation source directory.

Upgrading Sun OTP Using Standard Upgrade

This section describes the procedure to upgrade Sun OTP using the standard upgrade method. It includes both the GUI and CLI procedures, and details about how to upgrade the remaining service and install the security service.

▼ To Upgrade Sun OTP from 1.1 to Sun OTP 2.0 Using the GUI

Before You Begin Upgrade Sun OTP 1.1 Provisioning Server to Version 2.0

1. **Open a browser and log in to the Sun OTP application provisioning service on the Sun OTP provisioning server.**

   Go to URL https://*install server*:9090 where *install server* is either the IP address or the fully qualified name of the Sun OTP provisioning server.

2. **Type the user name and password.**

   The user name is `otpadmin`. The password is the password provided in the password file while setting up the Sun OTP provisioning server.

3. **Click OTP Upgrade in the left panel.**

4. **Set up the configuration for upgrade by creating two variable sets.**

   Run this plan on all the Sun OTP hosts.

   a. **Click Set up Configuration and click run.**

   b. **Click the select from list... option corresponding to the `/com/sun/OTP/Utilities/OTPConfig` directory.**

   c. **Click create set to create a new variable set.**

   d. **Type a new variable set name in the Set Name field.**

e. **Click the check boxes for the appropriate plan variables for which you want to type the values.**

f. **Type the values for the appropriate plan variables in the text fields. For description about the Sun OTP plan settings and the clustered Sun OTP host plan worksheet, see Appendix A Sun OTP Upgrade Plan Worksheet.**

Note – Do not specify the values for the zone-related variables and specify `RAW` for the `spsRAConnectionType` variable.

---

g. **Click save to save the variable set.**

h. **Close the select variable setting from list... screen.**

i. **Under variable settings, click the drop-down list corresponding to the `/com/sun/OTP/Utilities/OTPConfig` directory and choose the new variable set.**

j. **Click select from list... corresponding to the `/com/sun/OTPupgrade/Upgrade` directory.**

k. **Click create set to create a new variable set.**

l. **Type a new variable set name in the Set Name field.**

m. **Type the values for the following variables:**

`logFile` - Path of the log file that would contain the output of upgrade operation. For example, `/var/OTP/OTPUpgrade.log`.

`upgradeType` - standard

n. **Click save to save the variable set.**

o. **Close the select variable setting from list... screen.**

p. **Under variable settings, click the drop-down list corresponding to the `/com/sun/OTPupgrade/Upgrade` directory and choose the new variable set.**

q. **Type the host name in the target host field.**

r. **Enter and confirm the password.**

The password is the password provided in the password file while setting up the Sun OTP provisioning server. The password can be 8 to 12 alphanumeric characters. You need to use this password and the user name `otpadmin` as the access credentials for all Sun OTP components including Web SSO.

s. Click run plan (includes preflight).

5 Back up the Sun OTP system management data.

Run this plan only on the first Sun OTP host that is running the Sun OTP system management service.

a. Click Backup Data and click run.

b. Type the host name in the target host field.

c. Click run plan (includes preflight).

6 Upgrade the operating system.

Run this plan on all the Sun OTP hosts.

a. Click Upgrade OS and click run.

b. Type the host name in the target host field.

c. Click run plan (includes preflight).

The plan is complete after initiating the patch upgrade process. You need to monitor the consoles on all the hosts and wait until the completion of patch upgrade cluster.

7 Upgrade the Sun OTP high availability service.

Run this plan on all the Sun OTP hosts.

a. Click Upgrade HA Services and click run.

b. Type the host name in the target host field.

c. Click run plan (includes preflight).

8 Upgrade the NEP application and the NEP application agent

If a NFS agent is used as part of the hosted application, upgrade the NFS agent before activating Sun Cluster. You can upgrade the agents later too. For more details on upgrading Sun Cluster, see Chapter 8, "Upgrading Sun Cluster Software," in *Sun Cluster Software Installation Guide for Solaris OS*.

Note – The upgrade procedure is specific to the hosted application, and can be automated by NEP's end-to-end upgrade. See the application documentation for instructions.

---

9. **Activate the new cluster environment by rebooting all the Sun OTP hosts.**

   ```
   /usr/sbin/init 6
   ```

10. **Perform the common steps for all types of upgrade. See Upgrade Remaining Services and Install the Security Service.**

▼ To Upgrade Remaining Services and Install the Security Service Using GUI

1. **Upgrade the Sun OTP application provisioning service.**

   Run this plan simultaneously on all the Sun OTP hosts.

   a. **Click OTP Upgrade in the left panel.**

   b. **Click Upgrade Provisioning Services.**

   c. **Type the host name in the target host field.**

   d. **Click run plan (includes preflight).**

      Monitor the debug log in the `/var/OTP/SUNWotp-debug.log` file and wait until the reconfiguration of Sun OTP application provisioning service before running the next plan.

2. **Upgrade the Sun OTP system management service.**

   Run this plan on all the Sun OTP hosts.

   a. **Click Upgrade Management Service and click run.**

   b. **Type the host name in the target host field.**

   c. **Click run plan (includes preflight).**

3. **Install the Sun OTP security service.**

   Run this plan on all the Sun OTP hosts.

   a. **Click OTP Setup in the left panel.**

   b. **Click Install Security Service and click run.**

   c. **Type the host name in the target host field.**

   d. **Click run plan (includes preflight).**

4. **Configure the Sun OTP AHE components as highly available services.**
   Run this plan only on the first Sun OTP host.
   a. **Click Configure Components and click run.**
   b. **Type the host name in the target host field.**
   c. **Click run plan (includes preflight).**
5. **Restore the Sun OTP system management data that was backed up.**
   Run this plan only on the first Sun OTP host.
   a. **Click OTP Upgrade in the left panel.**
   b. **Click Restore Data and click run.**
   c. **Type the host name in the target host field.**
   d. **Click run plan (includes preflight).**
6. **Install Web SSO.**
   Run this plan on all the Sun OTP hosts.
   a. **Click OTP Setup in the left panel.**
   b. **Click Install WebSSO and click run.**
   c. **Type the host name in the target host field.**
   d. **Click run plan (includes preflight).**

▼ To Upgrade Sun OTP from 1.1 to 2.0 Using CLI

Before You Begin Upgrade Sun OTP 1.1 Provisioning Server to Version 2.0

1. **Log in as root (`su - root`) to the Sun OTP provisioning server.**
2. **Copy the `input_otp.dat` file to a NFS-mounted directory.**
   ```
   cp /opt/SUNWotp/cli/templates/input_otp.dat /export/
   ```
3. **Edit the `/export/input_otp.dat` file to add the values for each variable.**
   For description about the Sun OTP plan settings and the clustered Sun OTP host plan worksheet, see Appendix A Sun OTP Upgrade Plan Worksheet.

Note – Do not specify the values for the zone-related variables and specify `RAW` for the `spsRAConnectionType` variable.

For each host, specify the values for the following upgrade-related variables.

`h1_UpgradelogFile` - Path of the log file that would contain the output of upgrade operation. For example, `/var/OTP/OTPUpgrade.log`.

`upgradeType` - standard.

4 Set up the configuration for upgrade.

```
/opt/SUNWotp/cli/deploy_otp -u S -f /export/input_otp.dat -o "-P passwordfile"
```

passwordfile is the absolute path of the password file. You can create this file in your home directory. The password file must contain a line with a valid password for all Sun OTP components. The password can be 8 to 12 alphanumeric characters. You need to use this password and the user name `otpadmin` as the access credentials for all Sun OTP components including Web SSO.

5 Back up the Sun OTP system management data.

```
/opt/SUNWotp/cli/deploy_otp -u b -f /export/input_otp.dat -o "-B hostname"
```

hostname is the first host name that is running the Sun OTP system management service.

6 Upgrade the operating system.

```
/opt/SUNWotp/cli/deploy_otp -u P -f /export/input_otp.dat
```

The command is complete after initiating the patch upgrade process. You need to monitor the consoles on all the hosts and wait until the completion of patch upgrade cluster.

7 Upgrade the Sun OTP high availability service.

```
/opt/SUNWotp/cli/deploy_otp -u a -f /export/input_otp.dat
```

8 Upgrade the NEP application and the NEP application agent

If a NFS agent is used as part of the hosted application, upgrade the NFS agent before activating Sun Cluster. You can upgrade the agents later too. For more details on upgrading Sun Cluster, see Chapter 8, "Upgrading Sun Cluster Software," in *Sun Cluster Software Installation Guide for Solaris OS*.

Note – The upgrade procedure is specific to the hosted application, and can be automated by NEP's end-to-end upgrade. See the application documentation for instructions.

9 Activate the new cluster environment by rebooting all the Sun OTP hosts.

```
/usr/sbin/init 6
```

10 **Perform the common steps for all the types of upgrade. See Upgrade Remaining Services and Install the Security Service .**

▼ To Upgrade Remaining Services and Install the Security Service Using CLI

1 **Upgrade the Sun OTP application provisioning service.**

```
/opt/SUNWotp/cli/deploy_otp -u p -f /export/input_otp.dat
```

This command reconfigures the Sun OTP application provisioning service.

When the command is complete, monitor the debug log in the `/var/OTP/SUNWotp-debug.log` file and wait until the reconfiguration of the Sun OTP application provisioning service.

2 **Upgrade the Sun OTP system management service.**

```
/opt/SUNWotp/cli/deploy_otp -u m -f /export/input_otp.dat
```

3 **Install the Sun OTP security service.**

```
/opt/SUNWotp/cli/deploy_otp -i s -f /export/input_otp.dat
```

4 **Configure the Sun OTP AHE components as highly available services.**

```
/opt/SUNWotp/cli/deploy_otp -c h -f /export/input_otp.dat
```

5 **Restore the Sun OTP system management data that was backed up.**

```
/opt/SUNWotp/cli/deploy_otp -u r -f /export/input_otp.dat -o "-R hostname"
```

hostname is the first host name where Sun OTP system management data was backed up.

6 **Install Web SSO.**

```
/opt/SUNWotp/cli/deploy_otp --install websso --file /export/input_otp.dat
```

Upgrading Sun OTP Using Dual-Partition Upgrade

This section describes the procedure to upgrade Sun OTP using the dual-partition method. It includes both the GUI and CLI procedures, and details about how to prepare the hosts for dual-partition upgrade.

▼ To Prepare Hosts for Dual-Partition Upgrade

You must perform this procedure before you upgrade Sun Open Telecommunications Platform using dual-partition upgrade.

1 **Set the resource group property to `false`.**

```
clresourcegroup set -p RG_system=false otp-system-rg
```

Reset the value to `true` after completing the live upgrade.

2 Set up the `ssh` login between the hosts in the cluster.

Perform this step on all the hosts in the cluster.

a. Type the following command.

```
ssh-keygen -t rsa
```

b. Accept the default values on all nodes.

c. Append the contents of the `/.ssh/id_rsa.pub` file to the `/.ssh/authorized_keys2` file from each host to all the cluster hosts.

d. Edit the `/etc/ssh/sshd_config` file. Set the value of the `PermitRootLogin` variable to `yes`.

e. Restart the `ssh` instance.

```
svcadm restart svc:/network/ssh:default
```

f. Verify you are able to log in between all the cluster hosts without typing the password.

3 Set the `system` property for the `otp-system-rg` variable to false.

```
/usr/cluster/bin/scrgadm -c -g otp-system-rg -y rg_system=FALSE
```

4 Partition the cluster.

a. On the first host, unzip the cluster bundle.

```
unzip -d /tmp_dir 2.0_mediadir/solaris_sparc/components/cluster.zip
```

2.0_mediadir is the fully-qualified path name to the Sun OTP 2.0 installation source directory.

b. Type the following command.

```
/tmp_dir/cluster/Solaris_sparc/Product/sun_cluster/Solaris_10/Tools/scinstall
```

c. Select Option #3: Manage a dual-partition upgrade.

d. Assign the manager host to the second partition, and the managed host to the first partition. The managed host on the first partition will be halted.

Note – The first host or the manager host must remain in the second partition.

---

e. **Boot the hosts in the first partition in the non-cluster mode.**

```
ok boot -x
```

Note – For installing and administering Sun Cluster using the GUI, refer to Chapter 12, "Administering Sun Cluster With the Graphical User Interfaces," in *Sun Cluster System Administration Guide for Solaris OS*.

▼ To Upgrade Sun OTP from 1.1 to 2.0 Using the GUI

Before You Begin

- Upgrade Sun OTP 1.1 Provisioning Server to Version 2.0
- Prepare Hosts for Dual-Partition Upgrade

1 **Open a browser and log in to the Sun OTP application provisioning service on the Sun OTP provisioning server.**

Go to https://*install server*:9090 where *install server* is either the IP address or the fully qualified name of the Sun OTP provisioning server.

2 **Type the user name and password.**

The user name is `otpadmin`. The password is the password provided in the password file while setting up the Sun OTP provisioning server.

3 **Click OTP Upgrade in the left panel.**

4 **Set up the configuration for upgrade by creating two variable sets.**

Run this plan on all the Sun OTP hosts.

a. **Click Set up Configuration and click run.**

b. **Click select from list... corresponding to the `/com/sun/OTP/Utilities/OTPConfig` directory.**

c. **Click create set to create a new variable set.**

d. **Type a new variable set name in the Set Name field.**

e. **Click the check boxes for the appropriate plan variables for which you want to enter the values.**

f. **Type the values for the appropriate plan variables in the text fields. For description about the Sun OTP plan settings and the clustered Sun OTP host plan worksheet, see Appendix A Sun OTP Upgrade Plan Worksheet.**

Note – Do not specify the values for the zone-related variables and specify `RAW` for the `spsRAConnectionType` variable.

g. Click save to save the variable set.

h. Close the select variable setting from list... screen.

i. Under variable settings, click the drop-down list corresponding to the `/com/sun/OTP/Utilities/OTPConfig` directory and choose the new variable set.

j. Click select from list... corresponding to the `/com/sun/OTPupgrade/Upgrade` directory.

k. Click create set to create a new variable set.

l. Type a new variable set name in the Set Name field.

m. Type the values for the following variables:

`logFile` - Path of the log file that would contain the output of upgrade operation. For example, `/var/OTP/OTPUpgrade.log`.

`upgradeType` - standard.

n. Click save to save the variable set.

o. Close the select variable setting from list... screen.

p. Under variable settings, click the drop-down list corresponding to the `/com/sun/OTPupgrade/Upgrade` directory and choose the new variable set.

q. Type the host name in the target host field.

r. Enter and confirm the password.

The password is the password provided in the password file while setting up the Sun OTP provisioning server. The password can be 8 to 12 alphanumeric characters. You need to use this password and the user name `otpadmin` as the access credentials for all Sun OTP components including Web SSO.

s. Click run plan (includes preflight).

5 Back up the Sun OTP system management data.

Run this plan on the first Sun OTP host which is running the Sun OTP system management service.

a. Click Backup Data and click run.

b. Type the host name in the target host field.

c. Click run plan (includes preflight).

6 Upgrade the operating system.

Run this plan simultaneously on all the hosts of the partition that are currently booted in the non-cluster mode.

a. Click Upgrade OS and click run.

b. Type the host name in the target host field.

c. Click run plan (includes preflight).

The plan completes after initiating the patch upgrade process. You need to monitor the consoles on all the hosts and wait until the completion of the patch upgrade cluster.

7 Upgrade the Sun OTP high availability service.

Run this plan simultaneously on all the hosts of the partition that are currently booted in the non-cluster mode.

a. Click Upgrade HA Services.

b. Click run plan (includes preflight).

8 Upgrade the NEP application and the NEP application agent

If a NFS agent is used as part of the hosted application, upgrade the NFS agent before activating Sun Cluster. You can upgrade the agents later too. For more details on upgrading Sun Cluster, see Chapter 8, "Upgrading Sun Cluster Software," in *Sun Cluster Software Installation Guide for Solaris OS*.

Note – The upgrade procedure is specific to the hosted application, and can be automated by NEP's end-to-end upgrade. See the application documentation for instructions.

---

9 **Activate the new cluster environment.**

a. **On one of the hosts in the first partition, type the following command to activate the first partition.**

```
/usr/cluster/bin/scinstall
```

b. **Select Manage a dual-partition upgrade.**

c. **Select Apply dual-partition upgrade changes.**

The hosts in the first partition are rebooted into the cluster mode. Once they are successfully booted as active cluster members, the hosts in the second partition are halted.

d. **Boot the hosts in the second partition in the non-cluster mode.**

```
ok boot -x
```

e. **On the second partition, run all the steps from upgrading the OS (Upgrade Operating System plan).**

f. **Boot the second partition in cluster mode.**

i. **Run `/usr/cluster/bin/scinstall` on the second partition.**

ii. **Select option #3 Manage a dual-partition upgrade.**

iii. **Select sub option #4 Apply dual-partition upgrade changes.**

iv. **Press enter to reboot the node to cluster mode.**

10 **Perform the common steps for all the types of upgrade. See Upgrade Remaining Services and Install the Security Service.**

▼ To Upgrade Sun OTP from 1.1 to 2.0 Using CLI

Before You Begin

- Upgrade Sun OTP 1.1 Provisioning Server to Version 2.0
- Prepare Hosts for Dual-Partition Upgrade

1 **Log in as root (`su - root`) to the Sun OTP provisioning server.**

2 **Copy the `input_otp.dat` file to a NFS-mounted directory.**

```
cp /opt/SUNWotp/cli/templates/input_otp.dat /export/
```

3 Edit the `/export/input_otp.dat` file.

Type the values for each variable. For description about the Sun OTP plan settings and the clustered Sun OTP host plan worksheet, see Appendix A Sun OTP Upgrade Plan Worksheet.

Note – Do not specify the values for the zone-related variables and specify `RAW` for the `spsRAConnectionType` variable.

For each host, specify the values for the following upgrade-related variables.

`h1_UpgradelogFile` - Path of the log file that would contain the output of upgrade operation. For example, `/var/OTP/OTPUpgrade.log`.

`upgradeType` - standard.

4 Set up the configuration for upgrade.

```
/opt/SUNWotp/cli/deploy_otp -u S -f /export/input_otp.dat -o "-P passwordfile"
```

passwordfile is the absolute path of the password file. You can create this file in your home directory. The password file must contain a line with a valid password for all Sun OTP components. The password can be 8 to 12 alphanumeric characters. You need to use this password and the user name `otpadmin` as the access credentials for all Sun OTP components including Web SSO.

5 Back up the Sun OTP system management data.

```
/opt/SUNWotp/cli/deploy_otp -u b -f /export/input_otp.dat -o "-B hostname"
```

hostname is the first host name that is running the Sun OTP system management service.

6 Upgrade the operating system.

```
/opt/SUNWotp/cli/deploy_otp -u P -f /export/input_otp.dat -o "-T hostname"
```

hostname is the name of the host in the partition currently booted in the non-cluster mode. This command needs to be run for every host in this partition.

The command completes after initiating the patch upgrade process. You need to monitor the consoles on all the hosts and wait until the completion of the patch upgrade cluster.

7 Upgrade Sun OTP high availability service.

```
/opt/SUNWotp/cli/deploy_otp -u a -f /export/input_otp.dat -o "-T hostname"
```

hostname is the name of the host in the partition currently booted in non-cluster mode. This command needs to be run for every host in this partition.

8 **Upgrade the NEP application and the NEP application agent**

If a NFS agent is used as part of the hosted application, upgrade the NFS agent before activating Sun Cluster. You can upgrade the agents later too. For more details on upgrading Sun Cluster, see Chapter 8, "Upgrading Sun Cluster Software," in *Sun Cluster Software Installation Guide for Solaris OS*.

Note – The upgrade procedure is specific to the hosted application, and can be automated by NEP's end-to-end upgrade. See the application documentation for instructions.

---

9 **Activate the new cluster environment.**

a. **On one of the hosts in the first partition, type the following command to activate the first partition.**

```
/usr/cluster/bin/scinstall
```

b. **Select option #3 Manage a dual-partition upgrade.**

c. **Select sub option #4 Apply dual-partition upgrade changes.**

The hosts in the first partition are rebooted into the cluster mode. Once they are successfully booted as the active cluster members, the hosts in the second partition are halted.

d. **Boot the hosts in the second partition in the non-cluster mode.**

```
ok boot -x
```

e. **On the second partition, run all the steps from upgrading the OS (Upgrade Operating System plan).**

10 **Perform the common steps for all the types of upgrade. See Upgrade Remaining Services and Install the Security Service .**

Upgrading Sun OTP Using Live Upgrade

This section describes the procedure to upgrade Sun OTP using the live upgrade method. It includes both the GUI and CLI procedures, and details about how to prepare the hosts for dual-partition upgrade.

▼ To Prepare Hosts for Live Upgrade

You must perform this procedure before you upgrade Sun Open Telecommunications Platform by using live upgrade.

- **Create the live upgrade disk partition similar to the root disk.**

For example, `prtvtoc -h /dev/dsk/c0t0d0s2|fmthard -s "-" /dev/rdsk/c0t1d0s2`

To Transfer Global Devices to a New Root Disk

You must perform this procedure before you upgrade Sun Open Telecommunications Platform using live upgrade.

1. **Log in as root (`su - root`).**
2. **Backup the `/etc/vfstab` file.**

   ```
   cp /etc/vfstab /etc/vfstab.old
   ```

3. **Open the `/etc/vfstab` file for editing.**
4. **Locate the line that corresponds to `/global/.device/node@N`.**
5. **Edit the global device entry as follows:**

   a. **Change the DID names to the physical names.**

   b. **Change `/dev/did/{r}dsk/dYsZ` to `/dev/{r}dsk/cNtXdYsZ`.**

   c. **Remove global from the entry.**

   The following example shows the name of DID device `d3s3`, which corresponds to `/global/.devices/node@s`, changed to its physical device names and the global entry removed.

   Original:

   ```
   /dev/did/dsk/d3s3 /dev/did/rdsk/d3s3 /global/.devices/node@2 ufs 2 no global
   ```

   Changed:

   ```
   /dev/dsk/c0t0d0s3 /dev/rdsk/c0t0d0s3 /global/.devices/node@2 ufs 2 no -
   ```

6. **When the `/etc/vfstab` file is modified on all cluster nodes, run the OTP upgrade plan to upgrade the OS and cluster. See "Upgrading Sun OTP Using Standard Upgrade" on page 34.**
7. **After upgrading Sun OTP high availability service and before rebooting to the new boot environment (BE), restore the original `/etc/vfstab` file on each node of the un-upgraded BE.**

   ```
   cp /etc/vfstab.old /etc/vfstab
   ```

8. **Mount the new Boot Environment (BE).**

   ```
   lumount sunotp1.1-sunotp2.0 /altroot
   ```

9. **Locate the line that corresponds to `/global/.devices/node@N` and replace the dash (-) at the end of the entry with the word global.**

   ```
   /dev/dsk/cNtXdYsZ /dev/rdsk/cNtXdYsZ /global/.devices/node@N ufs 2 no global
   ```

10. **Unmount the new BE.**

    ```
    luumount sunotp1.1-sunotp2.0
    ```

11. **Check the BE status.**

    ```
    /usr/sbin/lustatus
    ```

12. **Activate the BE.**

    ```
    /usr/sbin/luactivate BEname
    ```

    `BEname` is the name of the boot environment variable.

13. **Reboot the system.**

    ```
    /usr/sbin/init 6
    ```

14. **Perform the common steps for all types of upgrade. See Upgrade Remaining Services and Install the Security Service .**

▼ To Upgrade Sun OTP Using the GUI

Before You Begin

- Upgrade Sun OTP 1.1 Provisioning Server to Version 2.0
- Prepare Hosts for Live Upgrade
- Transfer Global Devices to a New Root Disk

1. **Open a browser and log in to the Sun OTP application provisioning service on the Sun OTP provisioning server.**

   Go to https://*install server*:9090 where *install server* is either the IP address or the fully qualified name of the Sun OTP provisioning server.

2. **Type the user name and password.**

   The user name is `otpadmin`. The password is the password provided in the password file while setting up the Sun OTP provisioning server.

3. **Click OTP Upgrade in the left panel.**

4. **Set up the configuration for upgrade by creating two variable sets.**

   Run this plan on all the Sun OTP hosts.

   a. **Click Set up Configuration and click run.**

b. Click select from list... corresponding to the `/com/sun/OTP/Utilities/OTPConfig` directory.

c. Click create set to create a new variable set.

d. Type a new variable set name in the Set Name field.

e. Click the check boxes for the appropriate plan variables for which you want to enter the values.

f. Type the values for the appropriate plan variables in the text fields. For description about the Sun OTP plan settings and the clustered Sun OTP host plan worksheet, see Appendix A Sun OTP Upgrade Plan Worksheet.

Note – Do not specify the values for the zone-related variables and specify `RAW` for the `spsRAConnectionType` variable.

---

g. Click save to save the variable set.

h. Close the select variable setting from list... screen.

i. Under variable settings, click the drop-down list corresponding to the `/com/sun/OTP/Utilities/OTPConfig` directory and choose the new variable set.

j. Click select from list... corresponding to the `/com/sun/OTPupgrade/Upgrade` directory.

k. Click create set to create a new variable set.

l. Type a new variable set name in the Set Name field.

m. Type the values for the following variables:

`logFile` - Path of the log file that would contain the output of upgrade operation. For example, `/var/OTP/OTPUpgrade.log`.

`upgradeType` - live-upgrade.

`BEname` - Name of the boot environment.

`diskLayout` - Layout of the disk to be used for live upgrade.

Syntax of `diskLayout`:

`mount1:disk_slice1-mount2:disk_slice2-mount3:disk_slice3`

Information for / (root), swap and /globaldevices is mandatory.

Example:

```
/:c2t3d0s0-swap:c2t3d0s1-/globaldevices:c2t3d0s3
```

n. **Click save to save the variable set.**

o. **Close the select variable setting from list... screen.**

p. **Under variable settings, click the drop-down list corresponding to the** `/com/sun/OTPupgrade/Upgrade` **directory and choose the new variable set.**

q. **Type the host name in the target host field.**

r. **Click run plan (includes preflight).**

5 **Back up Sun OTP system management data.**

Run this plan only on the first Sun OTP host that is running the Sun OTP system management service.

a. **Click Backup Data and click run.**

b. **Type the host name in the target host field.**

c. **Click run plan (includes preflight).**

6 **Upgrade the operating system.**

Run this plan on all the Sun OTP hosts.

a. **Click Upgrade OS and click run.**

b. **Type the host name in the target host field.**

c. **Click run plan (includes preflight).**

Wait for the plan completion. The plan is upgraded on the alternate boot disk.

7 **Upgrade Sun OTP high availability service.**

Run this plan on all the Sun OTP hosts.

a. **Click Upgrade HA Services and click run.**

b. **Type the host name in the target host field.**

c. **Click run plan (includes preflight).**

8 **Upgrade the NEP application and the NEP application agent**

If a NFS agent is used as part of the hosted application, upgrade the NFS agent before activating Sun Cluster. You can upgrade the agents later too. For more details on upgrading Sun Cluster, see Chapter 8, "Upgrading Sun Cluster Software," in *Sun Cluster Software Installation Guide for Solaris OS*.

Note – The upgrade procedure is specific to the hosted application, and can be automated by NEP's end-to-end upgrade. See the application documentation for instructions.

---

9 **Activate the new cluster environment.**

Run this step on all the Sun OTP hosts.

a. **Check the boot environment.**

```
/usr/sbin/lustatus
```

b. **Activate the boot environment.**

```
/usr/sbin/luactivate BEname
```

BEname is the name of the boot environment.

c. **Reboot all the Sun OTP hosts.**

```
/usr/sbin/init 6
```

10 **Perform the common steps for all the types of upgrade. See Upgrade Remaining Services and Install the Security Service.**

▼ To Upgrade Sun OTP Using CLI

Before You Begin

- Upgrade Sun OTP 1.1 Provisioning Server to Version 2.0
- Prepare Hosts for Live Upgrade
- Transfer Global Devices to a New Root Disk

1 **Log in as root (`su - root`) to the Sun OTP provisioning server.**

2 **Copy the `input_otp.dat` file to a NFS-mounted directory.**

```
cp /opt/SUNWotp/cli/templates/input_otp.dat /export/
```

3 **Edit the `/export/input_otp.dat` file.**

Type the values for each variable. For description about the Sun OTP plan settings and the clustered Sun OTP host plan worksheet, see Appendix A Sun OTP Upgrade Plan Worksheet.

Note – Do not specify the values for the zone-related variables and specify `RAW` for the `spsRAConnectionType` variable.

For each host, specify the values for the following upgrade-related variables.

`h1_UpgradelogFile` - Path of the log file that would contain the output of upgrade operation. For example, `/var/OTP/OTPUpgrade.log`.

`upgradeType` - live-upgrade.

`h1_BEname` - Name of the boot environment.

`h1_diskLayout` - Layout of the disk to be used for live upgrade.

4 Set up the configuration for upgrade.

`/opt/SUNWotp/cli/deploy_otp -u S -f /export/input_otp.dat -o "-P` *passwordfile*"

passwordfile is the absolute path of the password file. You can create this file in your home directory. The password file must contain a line with a valid password for all Sun OTP components. Password can be 8 to 12 alphanumeric characters. You need to use this password and the user name `otpadmin` as the access credentials for all Sun OTP components including Web SSO.

5 Back up the Sun OTP system management data.

`/opt/SUNWotp/cli/deploy_otp -u b -f /export/input_otp.dat -o "-B` *hostname*"

hostname is the first host name that is running the Sun OTP system management service.

6 Upgrade the operating system.

```
/opt/SUNWotp/cli/deploy_otp -u P -f /export/input_otp.dat
```

Wait for the plan completion. The plan is upgraded on the alternate boot disk.

7 Upgrade the Sun OTP high availability service.

```
/opt/SUNWotp/cli/deploy_otp -u a -f /export/input_otp.dat
```

8 Upgrade the NEP application and the NEP application agent

If a NFS agent is used as part of the hosted application, upgrade the NFS agent before activating Sun Cluster. You can upgrade the agents later too. For more details on upgrading Sun Cluster, see Chapter 8, "Upgrading Sun Cluster Software," in *Sun Cluster Software Installation Guide for Solaris OS*.

Note – The upgrade procedure is specific to the hosted application, and can be automated by NEP's end-to-end upgrade. See the application documentation for instructions.

9 **Activate the new cluster environment.**

Run this step on all the Sun OTP hosts.

a. **Check the boot environment.**

```
/usr/sbin/lustatus
```

b. **Activate the boot environment.**

```
/usr/sbin/luactivate BEname
```

BEname is the name of the boot environment.

c. **Reboot all the Sun OTP hosts.**

```
/usr/sbin/init 6
```

10 **Perform the common steps for all the types of upgrade. See Upgrade Remaining Services and Install the Security Service.**

Troubleshooting In case of a live upgrade failure, follow these steps to rollback the OS and Sun OTP availability service.

- Activate the original boot environment.

  `/usr/sbin/luactivate` *old BE*
- Reboot to the selected boot environment.
- Delete the failed upgrade partition.

  `ludelete` *new BE*
- Restart the upgrade process from OS.

Auditing the System

The audit plan installs the audit package (`SUNWotpaudit`) on the target hosts and generates a report. The audit report contains the system overview, OTP components summary, runtime summary, firmware summary, package and patch information.

▼ To Audit Your System

Before You Begin Ensure that Sun Explorer 5.7 is installed and running in the system.

1 **Open a browser and log in to the Sun OTP application provisioning service on the Sun OTP provisioning server.**

Go to https://*install server*:9090 where *install server* is either the IP address or the fully qualified name of the Sun OTP provisioning server.

2. **Type the user name and password.**

   The user name is `otpadmin`. The password is the password provided in the password file while setting up the Sun OTP provisioning server.

3. **Click OTP Upgrade in the left panel.**

4. **Click Configuration Audit and click run.**

5. **Under variable settings, click select from list.**

6. **Click create set and provide a name for the variable set in the Set Name field.**

7. **Specify the values for the following parameters.**

   - `installPath` - The default is `/opt`
   - `mediaDirectory` - Path of the (`SUNWotpaudit`) package
   - `explorerPath` - Path of the explorer output file

8. **Click save to save the variable set and close the select variable setting from list... screen.**

9. **In the ConfigAudit screen, click the drop-down list under variable settings, and choose the new variable set.**

10. **Type the target host where the audit packages have to be installed and run.**

11. **Select the OTP version to audit (audit OTP v1.1 or audit OTP v2.0).**

12. **Click run plan (includes preflight).**

    On successful completion, the plan does the following.

    - Installs the `SUNWotpaudit` package in the `installPath`.
    - Generates an audit report `report.txt` at `/var/SUNWotpaudit/output`.

Note – For running the configuration audit tool on non OTP systems, refer to the latest README file present in the `SUNWotpaudit` package. This plan does not give the entire information about the OTP components present.

Sun OTP Backup and Restore

This section explains the procedure to back up and restore the Sun OTP services. Backup and restore of solution can include backup and restore of the various components they are dependent on. That is, if you want to backup or restore your solution, you can integrate the backup and restore of the various component products on which your solution is dependent upon into your solution backup and restore.

The following topics are discussed:

- "Backing Up Sun OTP Services" on page 56
- "Restoring Sun OTP Services" on page 58

Backing Up Sun OTP Services

The Sun OTP backup process is component specific. Sun OTP copies and creates the required configuration for backup. You can back up individual Sun OTP services or all running Sun OTP services. The backup and restore process uses the installation framework for its implementation. Therefore, you cannot back up the Sun OTP services that run on the remote host.

▼ To Back Up the Sun OTP Services

Perform this procedure only from the global zone even when Sun OTP security service is running in the non-global zone.

Before You Begin In a clustered system, ensure that the Sun OTP service that needs to be backed up is running on the current Sun OTP host.

1. **Log in as root (`su - root`) to the Sun OTP host.**

2. **Determine the Sun OTP services that you want to back up.**

   - **To back up all the running Sun OTP services, type:**

     `/opt/SUNWotp/cli/backup_otp -o` *backupdirectory* `-l` *logfile*

     backupdirectory is a directory name on the Sun OTP host. This directory can be any valid NFS path name that can be accessed by the Sun OTP host with write permission. The back up data is stored in a tar file under this backup directory.

     logfile is the name of the log file that contains the output of the backup operation.

   - **To back up the Sun OTP high availability service, type the following command:**

     `/opt/SUNWotp/cli/backup_otp -c h -o` *backupdirectory* `-l` *logfile*

- **To back up the Sun OTP system management service, type the following command:**
  `/opt/SUNWotp/cli/backup_otp -c m -o` *backupdirectory* `-l` *logfile*
- **To back up the Sun OTP application provisioning service, type the following command:**
  `/opt/SUNWotp/cli/backup_otp -c p -o` *backupdirectory* `-l` *logfile*
- **To back up the Sun OTP security service, type the following command:**
  `/opt/SUNWotp/cli/backup_otp -c s -o` *backupdirectory* `-l` *logfile*

Data Backed Up By the Backup Plan

The following table lists the data that is backed up by the backup plan.

TABLE 1–2 Data Backed Up By the Backup Plan

Sun OTP Service	Data Backed Up
Sun OTP registry files	`/var/OTP` directory
Sun OTP high availability service	`/etc/cluster` directory
Sun OTP application provisioning service	Database, plug-in, and SPS database data, and custom tasks data
Sun OTP system management service	Configuration files and SCS database
Sun OTP security service	`/opt/SUNWotp/accessmgr` directory
	`/var/opt/SUNWotp/webserver/local-server/web-app` directory
	`/var/opt/SUNWotp/config/alias` file
	`/var/opt/SUNWotp/webserver/admin-server/config-store/` directory
	`/etc/opt/SUNWotp/web-sso` file
	`/opt/SUNWjass/Drivers/sunotp` driver
	Instance of the Directory Server.

▼ To Back Up Sun OTP Services at Scheduled Intervals

You can perform scheduled backup of the Sun OTP services. For more details, `crontab`(1).

1. **Open the crontab file.**
2. **To back up Sun OTP services at 1 a.m. each Saturday, for example, add the following line to the crontab file.**

```
0 1 * * 6 /opt/SUNWotp/cli/backup_otp -o /var/otp/backup -l /var/otp/backup.log
```

In this example, the backup tar files are stored in the `/var/otp/backup` directory.

3 **To automatically delete old backup tar files at 1 a.m. each Sunday, for example, add the following line to the crontab file.**

```
0 1 * * 7 find /var/otp/backup -name '*.tar' -mtime +10 -exec /bin/rm -f {} \;
```

In this example, the backup tar files are stored in the `/var/otp/backup` directory.

Restoring Sun OTP Services

You can restore the Sun OTP services only on the same host where they are backed up. Before the restore process, stop the Web Server from the cluster control. Once you complete the restore process, restart the Web Server.

▼ To Restore Sun OTP Services

Perform this procedure only from the global zone even when Sun OTP security service is running in the non-global zone.

The backup tar file created by the backup plan determines the Sun OTP service to be restored. For example, if the backup tar file contains only the backup data for the Sun OTP application provisioning service, then only the Sun OTP application provisioning service is restored.

Before You Begin In a clustered system, make sure that the Sun OTP service to be restored is running on the current Sun OTP host.

1 **Log in as root (`su - root`) to the Sun OTP host.**

2 **To restore the Sun OTP services, type the following command:**

`/opt/SUNWotp/cli/restore_otp -t` *tarfile* `-l` *logfile*

tarfile is the backup tar file created by the backup CLI.

logfile is the name of the log file that contains the output of the restore operation.

Note – Sun OTP configuration data and Sun OTP high availability service is not restored.

◆ ◆ ◆ APPENDIX A

Sun OTP Upgrade Plan Worksheet

This appendix describes the Sun OTP upgrade variables, and contains a sample plan worksheet.

The following topics are discussed:

- "Sun OTP Plan Settings Descriptions" on page 59
- "Sun OTP Plan Worksheet" on page 63

Sun OTP Plan Settings Descriptions

The following list describes each of the Sun OTP system plan settings that are used by Sun OTP.

- **mediaDirectory**

  The fully-qualified path name to the Sun Open Telecommunications Platform installation source directory.

- **clusterName**

  Name of the cluster. The length of the cluster name has to be less than 19 characters.

- **mgmtHost**

  Logical host name used by the Sun OTP system management service. The logical host name must correspond to the management logical IP address.

- **mgmtIP**

  Logical IP address used by the Sun OTP system management service. The IP address must be an unused IP address.

- **jesHAHost**

  Host name for Sun OTP security service shared address.

- **jesHANodeList**

  List of host names and respective zones on which the Sun OTP security service is running.

  For deployment without zones, use the following syntax:

h1_hostName+h2_hostName...

For deployment with zones, use the following syntax:

h1_hostName:h1_zoneName+h2_hostName:h2_zoneName...

- **mmrHostList**

  List of host names or zone host names between which the master-to-master replication of data between directory server instances are provided.

  For deployment without zones, use the following syntax:

  h1_hostName+h2_hostName...

  For deployment with zones, use the following syntax:

  h1_zoneHostname+h2_zoneHostname...

- **applyAllPatches**

  Specifies whether all patches or only mandatory patches are to be installed. The default value is `yes`, which specifies that all patches must be installed. To install only mandatory patches, specify `no`.

- **spsRAConnectionType**

  Specifies the connection type between Sun OTP application provisioning service master server and the remote agent. The values can be `SSH` or `RAW`. The default and recommended value is `SSH`.

  This variable must match the connection type that is provided while setting up the Sun OTP provisioning server and installing the remote agent.

- **hostName**

  The host name of the Sun OTP host. The length of the host name has to be less than 19 characters.

- **hostType**

  Type of host in the cluster. The possible values are `single`, `first`, and `additional`. For stand-alone host, the host type is `single`. For clustered configuration, the host type is `first` for the first host in the cluster and `additional` for the remaining hosts in the cluster.

- **sponsorNode**

  The name of the first Sun OTP host in a clustered Sun OTP system. The first Sun OTP host is the sponsoring node for all the additional Sun OTP hosts. This setting is required when installing the Sun Open Telecommunications Platform on two or more hosts.

  This variable is required only for hosts of host type `additional`.

- **autoConfigureIPMP**

  Setting to determine whether IPMP is configured automatically. The Possible values are `yes` and `no`. The default value is `no`.

  You should configure all physical interfaces of a multipathing group with a test IP address. Test addresses are required to detect failures.

If you set `autoConfigureIPMP=yes`, then you must also specify the following values:

- **secondaryInterface**

  Interface used as the failover interface if a fault is detected on the primary interface.

- **secondaryIP**

  IP address of the secondary interface that is used for failover. This variable is the same as **testIPAddress** but used for the secondary interface.

- **testIPAddress**

  An unused IP address that is to be assigned as a routable, no-failover, and deprecated test IP address to the adapter. IP network multipathing uses test addresses to detect network path failures, switch port faults, and partial network equipment outages.

- **privateInterface1**

  The first private network interface on Sun OTP host. Required when **hostType** is `first` or `additional`.

- **privateInterface2**

  The second private network interface on Sun OTP host. Required when **_hostType** is `first` or `additional`.

- **transportTypeInterface1**

  The transport type of the first private interconnect adapter on Sun OTP host. The required value is `dlpi`. Do not change the value.

  For more information, refer to *dlpi(7P)* man page.

- **transportTypeInterface2**

  The transport type of the second private interconnect adapter on Sun OTP host. The required value is `dlpi`. Do not change the value.

  For more information, refer to *dlpi(7P)* man page.

- **nodeAuthentication**

  Setting to establish the authentication policies for hosts. The possible values are `sys` and `des`. The default value is `sys`.

- **quorumAutoConfiguration**

Note – Quorum automatic configuration applies only to two-host clusters.

Quorum automatic configuration provides an option to enable or disable automatic configuration of the quorum device in a two-host only clustered Sun OTP system.

The possible values are `yes` and `no`. The default value is `yes`.

Note – If this value is set to `no`, a manual administrative procedure is required to configure the quorum disk in a two-host clustered Sun OTP system. The cluster must be manually reset from the install mode to the normal mode. For details about how to configure quorum disks, refer to the `scconf` command documentation in `scconf`(1M) man page.

- **rootDisk**

  Name of the root disk that is used to store the Solaris Volume Manager (SVM) database.

- **diskSlice**

  The disk slice where the Solaris Volume Manager (SVM) state database replicas are stored. The default value is `s7`. Refer to *Solaris Volume Manager Administration Guide* for more information.

- **zoneName**

  Name of the non-global zone for the Sun OTP security service. This variable has to be filled or remain empty for deployment with or without zones respectively.

- **zoneInterface**

  Network interface to be used for the non-global zone, typically the primary interface of the host.

- **zoneIPAddress**

  IP address of the non-global zone.

- **zoneHostName**

  Host name of the non-global zone corresponding to **zoneIPAddress**.

- **zonePath**

  Path to store the non-global zone.

- **zoneMask**

  Network mask of the non-global zone.

- **zoneDefaultRoute**

  Network default route of the non-global zone. **zoneDefaultRoute** must be on the same logical subnet as **zoneIPAddress**.

- **managementInterface**

  Name of the network interface used for Sun OTP system management services. The name of the interface depends on the platform type.

- **provisioningInterface**

  Name of the network interface used for Sun OTP application provisioning services. The name of the interface depends on the platform type.

- **domainName**

Domain name used by the Sun OTP security service.

- **ssoCookieDomain**

  Domain name for the Web SSO cookies. The Domain name must start with a dot (.) symbol.

- **logFile**

  Name of the log file that contains the output of upgrade operation. The value can be `/var/OTP/OTPUpgrade.log`.

- **upgradeType**

  Type of upgrade that is used to upgrade Sun OTP from 1.1 to 2.0. For standard upgrade and dual-partition upgrade, the value of `upgradeType` is `standard`. For live upgrade, the value is `live-upgrade`.

- **BEname**

  (Applicable only for live upgrade) Name of the boot environment to be used for live upgrade.

- **diskLayout**

  (Applicable only for live upgrade) Layout of the disk to be used for live upgrade.

Sun OTP Plan Worksheet

The following table lists the settings that you need to provide for each host while upgrading Sun OTP on a clustered Sun OTP system. For a plan worksheet for a stand-alone host, see "Stand-alone Sun OTP Host Plan Worksheet" in *Sun Open Telecommunications Platform 2.0 Installation Guide*

Tip – Print a copy of the following table for each host and then fill out the required information to use when upgrading the Sun Open Telecommunications Platform on a clustered Sun OTP system.

TABLE A–1 Sun OTP Upgrade Worksheet

Setting Name	Example
mediaDirectory	`/cdrom/otp_20_dvd/otp2.0`
clusterName	`otp-cluster`
mgmtHost	`otp-node1b`
mgmtIP	`20.20.20.#`
jesHAHost	`otp-node1c`

TABLE A–1 Sun OTP Upgrade Worksheet *(Continued)*

Setting Name	Example
jesHANodeList	otp-node1:jeszone+otp-node2:jeszone
mmrHostList	otp-node1d+otp-node2d
applyAllPatches	yes
spsRAConnectionType	SSH
hostName	otp-node1
hostType	first
sponsorNode	h2_sponsorNode=OTPfirsthost
autoConfigureIPMP	yes
secondaryInterface	bge1
secondaryIP	20.20.20.#
testIPAddress	20.20.20.#
privateInterface1	bge2
privateInterface2	bge3
transportTypeInterface1	dlpi
transportTypeInterface2	dlpi
nodeAuthentication	sys
quorumAutoConfiguration	yes
rootDisk	c0t0d0
diskSlice	s7
zoneName	jeszone
zoneInterface	bge0
zoneIPAddress	20.20.20.#
zonePath	/zone/jeszone
zoneHostname	otp-host1
zoneMask	100.100.100.0
zoneDefaultRoute	20.20.20.#
managementInterface	bge0
provisioningInterface	bge0

TABLE A–1 Sun OTP Upgrade Worksheet *(Continued)*

Setting Name	Example
domainName	`lab.sun.com`
ssoCookieDomain	`.sun.com`
logFile	`/var/OTP/OTPUpgrade.log`
upgradeType	`live-upgrade`
BEname	`sunotp1.1-sunotp2.0`
diskLayout	`/:c2t3d0s0-swap:c2t3d0s1-/globaldevices:c2t3d0s3`

Index

A

add, web SSO user, 21-23
availability service
  application, 7
  platform, 6

C

change password, existing web SSO user, 23-24
CLI
  enabling and disabling management service, 19
  enabling and disabling service provisioning, 19-20
clustered Sun OTP hosts, converting stand-alone Sun OTP host to, 16-18
command line
  enabling and disabling management service, 19
  enabling and disabling service provisioning, 19-20
configuration, IPMP, 60
converting, stand-alone host to clustered Sun OTP host, 16-18
critical patch cluster, 29

E

enable and disable
  service provisioning
    command line, 19-20
    GUI, 20-21
  system management
    command line, 19
enable and disable, system management *(Continued)*
    GUI, 20-21
existing web SSO user, change password, 23-24

G

GUI
  enabling and disabling management service, 20-21
  enabling and disabling service provisioning, 20-21

H

harden
  Sun OTP
    GUI, 27
host, converting stand-alone host to clustered Sun OTP host, 16-18

I

install
  Sun OTP SST driver
    GUI, 26
IPMP, configuration, 60

M

maintenance patch cluster, 29

management service
application, 6
enabling and disabling
command line, 19
GUI, 20-21
platform, 6

N

node, converting stand-alone host to clustered Sun OTP host, 16-18

O

OTP
enable and disablesystem management
command line, 19

P

patch cluster types, 29
provisioning service
application, 6
enable and disable
command line, 19-20
GUI, 20-21
platform, 5

R

remove, web SSO user, 24-25

S

service provisioning
enable and disable
command line, 19-20
GUI, 20-21
services
application availability, 7
services *(Continued)*
application management, 6
application provisioning, 6
platform availability, 6
platform management, 6
platform provisioning, 5
security, 7
stand-alone Sun OTP host, converting to clustered Sun OTP host, 16-18
Sun OTP
enable and disableservice provisioning
command line, 19-20
GUI, 20-21
enable and disablesystem management
GUI, 20-21
harden
GUI, 27
product mapping, 8-9
services, 5-7
unharden
GUI, 28
update, 30-31
Sun OTP SST driver
install
GUI, 26
uninstall
GUI, 26-27
system management
enabling and disabling
command line, 19
GUI, 20-21

U

unharden
Sun OTP
GUI, 28
uninstall
OTP SST driver
GUI, 26-27
Updating Sun OTP components, 30-31
upgrade
dual-partition, 32
live, 33

upgrade *(Continued)*
standard, 32

W

web SSO user
add, 21-23
remove, 24-25