ORACLE
UNIVERSITY

Integrated Cloud Applications & Platform Services

Oracle Solaris 11 Advanced System Administration

Electronic Presentation

D72965GC60
Edition 6.0 | May 2017

Learn more from Oracle University at **education.oracle.com**

ORACLE

Author

Raghavendra JS

Technical Contributors and Reviewers

Harald van Breederode
Glynn Foster
Uma Sannasi

Graphic Designers

Seema Bopaiah
Prakash Dharmalingam

Kavya Bellur

Editors

Nikita Abraham
Raj Kumar

Aju Kumar

Publishers

Sujatha Nagendra

Pavithran Adka
Syed Ali
Asief Baig
Sumesh Koshy
Raghunath M

1

Introduction

Agenda

- Course goals
- Course agenda
- Introductions
- Your learning center
- Your lab environment

Course Goals

After completing this course, you should be able to :

- Perform advanced Oracle Solaris 11 system administration tasks successfully and efficiently
- Carry out advanced system administration responsibilities, including:
  - IPS package repository creation
  - OS installation by using AI
  - Virtual switch, network high availability, packet filter
  - Kernel zones, Oracle Solaris 10 system migration and RBAC configuration
  - Data backup and restore, services, and process management
  - System evaluation, monitoring, and troubleshooting
- Complete the exercises in the practices

ORACLE

Course Agenda: Day 1

- Lesson 1: Introduction
- Lesson 2: Managing Services and Service Properties by Using SMF
- Lesson 3: Managing Software Packages by Using IPS

Note: Class is from 9:00 AM to 5:00 PM each day. There will be several short breaks throughout the day, plus one hour for lunch.

Course Agenda: Day 2

- Lesson 4: Managing Data Backup and Restore by Using ZFS
- Lesson 5: Configuring the Network

Course Agenda: Day 3

- Lesson 6: Administering Network Services
- Lesson 7: Advanced Administration of Zones

Course Agenda: Day 4

- Lesson 8: Securing the Oracle Solaris 11 OS
- Lesson 9: Managing Processes and Priorities
- Lesson 10: Installing Oracle Solaris 11 on Multiple Hosts

ORACLE

Course Agenda: Day 5

- Lesson 10: Installing Oracle Solaris 11 on Multiple Hosts (continued)
- Lesson 11: Implementing System Messaging and Diagnostic Facilities
- Lesson 12: Introducing Oracle Solaris 11 on the Cloud

ORACLE

Introductions

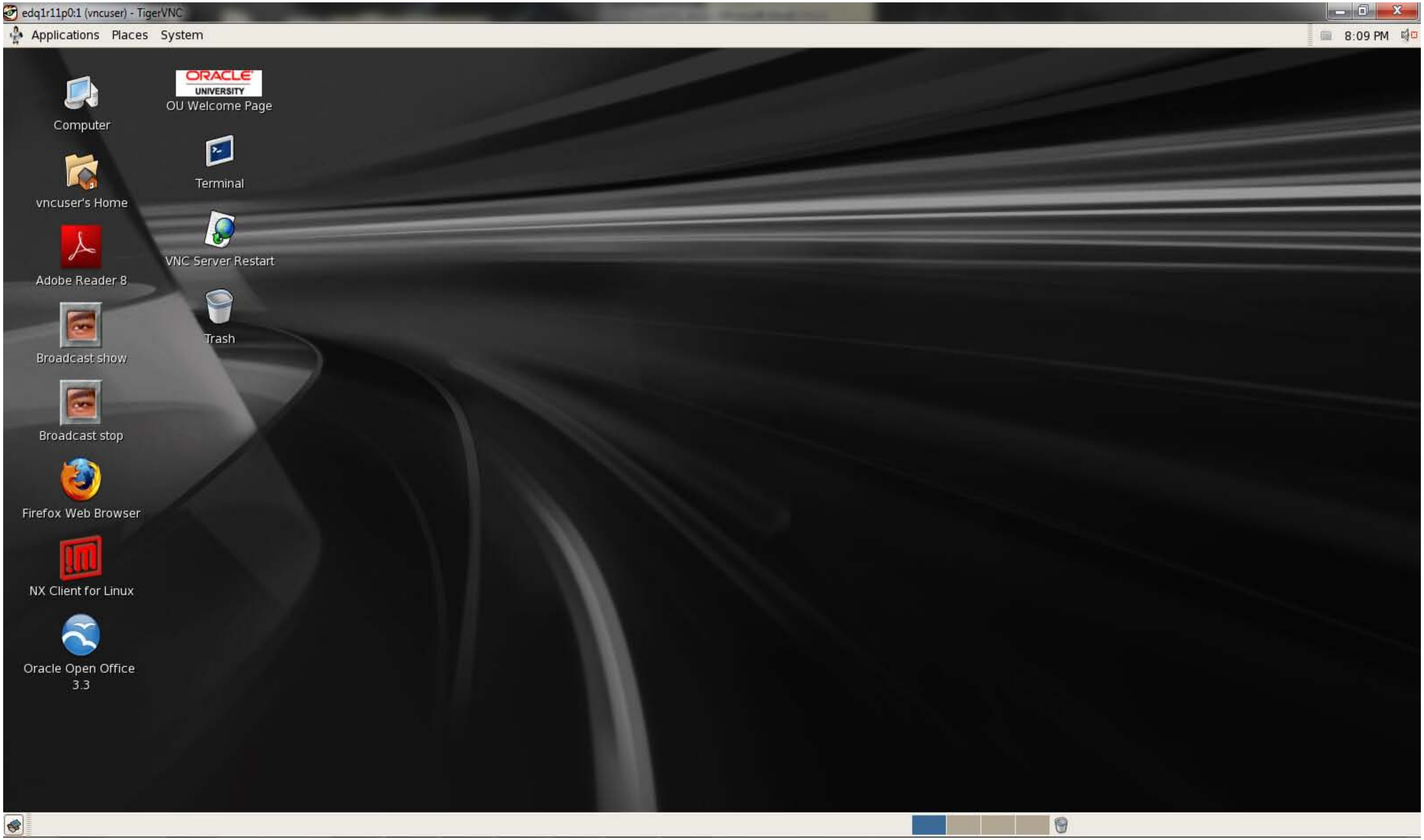
- Name
- Company affiliation
- Title, function, and job responsibility
- Experience related to the topics presented in this course
- Reasons for enrolling in the course
- Expectations for the course

ORACLE

Your Learning Center

- Logistics
  - Restrooms
  - Break rooms and designated smoking areas
- Cafeterias and restaurants in the area
- Emergency evacuation procedures
- Instructor contact information
- Cell phone usage
- Online course attendance confirmation form

Your Lab Environment



2

Managing Services and Service Properties by Using SMF

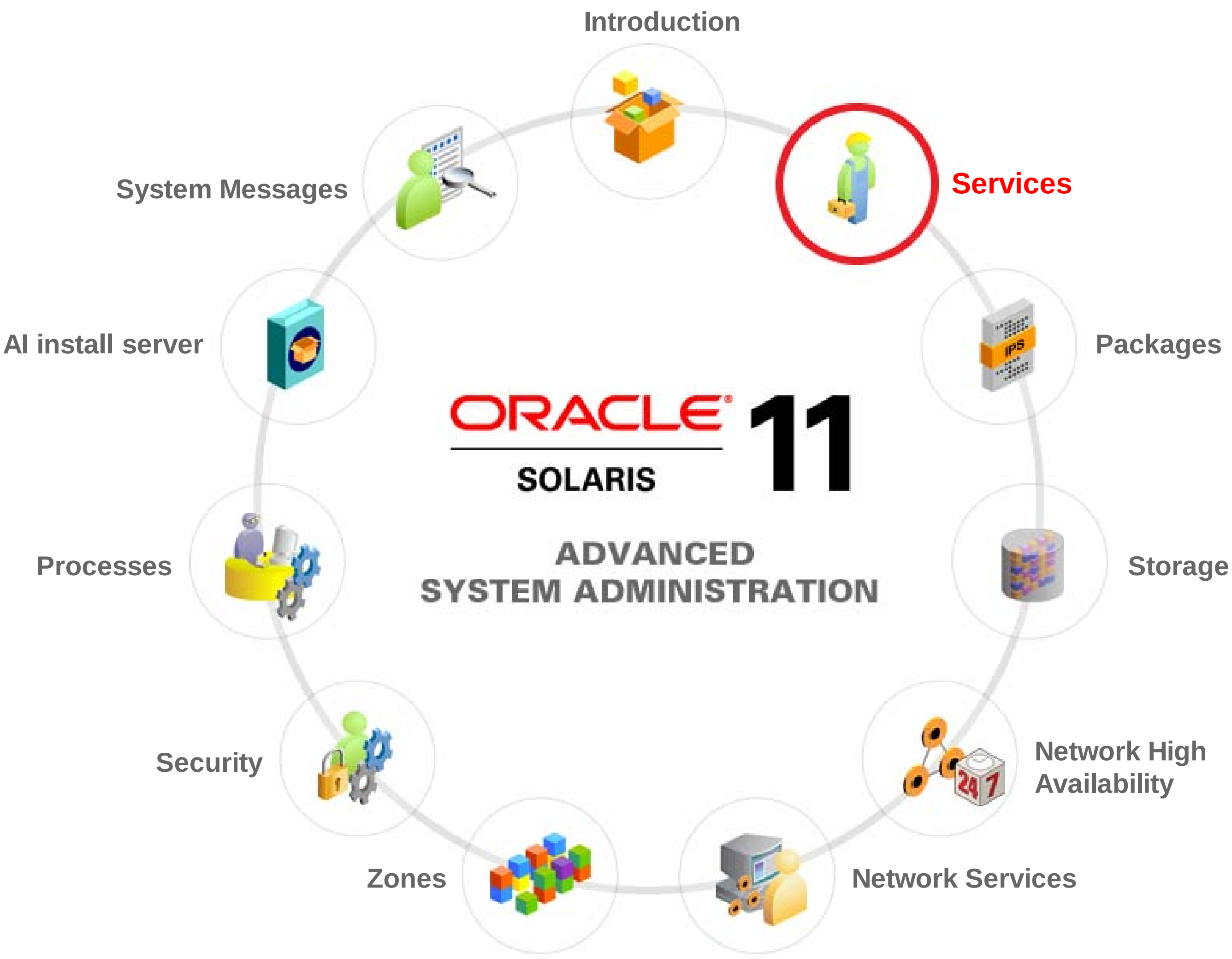
ORACLE

Objectives

After completing this lesson, you should be able to:

- Describe the advanced features of SMF
- Configure SMF services
- Troubleshoot SMF services

Job Workflow



Agenda

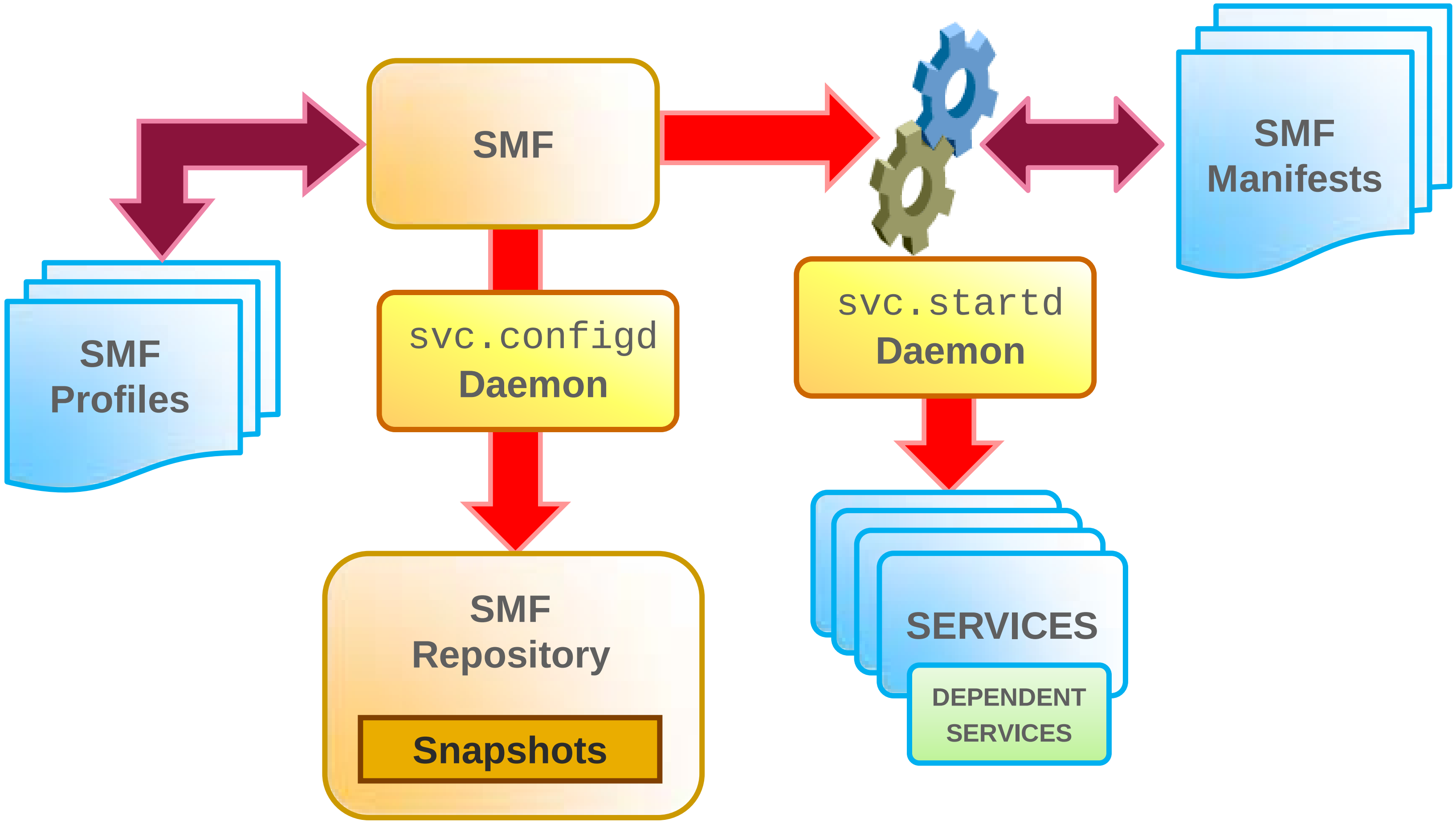
- Advanced features of SMF
- Configuring SMF services
- Troubleshooting SMF services

Importance of Service Configuration

Service configuration helps to ensure that:

- Appropriate services are enabled and running
- Existing services can be easily modified
- Downed services can be recovered and restored quickly
- New services can be created to meet emerging business needs

Advanced Features of SMF



SMF Profiles

- An SMF profile is an XML file that enables you to customize services and instances that are delivered by the system.
- Profiles delivered with the operating system include the following:

Profile	Description
`/etc/svc/profile/generic_open.xml`	Enables standard services
`/etc/svc/profile/generic_limited_net xml`	Disables many Internet services
`/etc/svc/profile/ns_*.xml`	Enables services associated with the name service that is configured to run on the system
`/etc/svc/profile/platform_*.xml`	Enables services associated with particular hardware platforms

SMF Profile: Example

```
<?xml version='1.0'?>
<!DOCTYPE service_bundle SYSTEM
    '/usr/share/lib/xml/dtd/service_bundle.dtd.1'>
<!--
<header content omitted>
<service_bundle type='profile' name='generic_open'
 xmlns:xi='http://www.w3.org/2003/XInclude' >
  <!--
      Include name service profile, as set by system id tools.
  -->
  <xi:include href='file:/etc/svc/profile/name_service.xml' />

  <!--
      svc.startd(1M) services
  -->
  <service name='system/coreadm' version='1' type='service'>
    <instance name='default' enabled='true'/>
  </service>
  <service name='system/cron' version='1' type='service'>
    <instance name='default' enabled='true'/>
  </service>
```

ORACLE

When SMF Profiles Are Applied

- `/etc/svc/profile/generic.xml` profile:
  - Applied during the first boot after a new installation or an upgrade
  - Symbolically linked to `generic_open.xml` or `generic_limited_net.xml`
- The contents of `site.xml` in `/etc/svc/profile`:
  - Applied when the system is booted
  - Applied when the `svcadm restart manifest-import` command is run
- Profiles in `/etc/svc/profile` are applied during early manifest import.

SMF Manifests

- An SMF manifest is an XML file that describes a service and a set of instances.
- Manifests are imported to load the properties of that service and its instances into the service configuration repository.
- The preferred location for manifests is `/lib/svc/manifest`.
- Manifests are imported and upgraded by the `svc:/system/early-manifest-import:default` service during the boot process before any services start.
- The `/lib/svc/manifest/site` and `/var/svc/manifest/site` directories are reserved for site-specific use. Manifests in the site directory can be modified directly.

SMF Manifest: Example

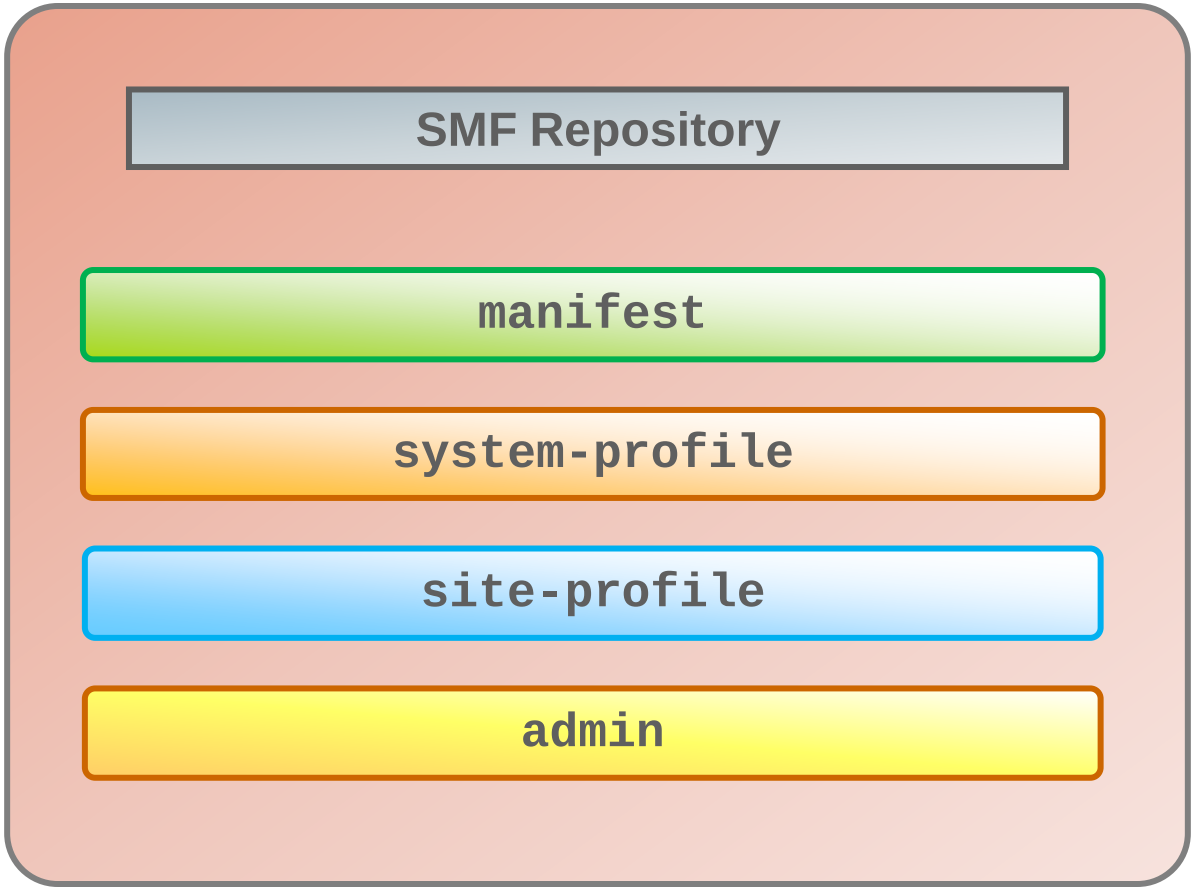
```
<?xml version="1.0"?>
<!DOCTYPE service_bundle SYSTEM
"/usr/share/lib/xml/dtd/service_bundle.dtd.1">
<!–
<header and copyright content omitted>
<service_bundle type='manifest' name='SUNWzoner:zones'>
<service
        name='system/zones'
        type='service'
        version='1'>
<create_default_instance enabled='false' />

<single_instance />

---
---
```

Service Configuration Repository

- Stores persistent configuration information as well as SMF runtime data for services
- Is located in `/etc/svc/repository.db`
- Is managed by the `svc.configd` daemon
- Is distributed among local memory and local files
- Can be manipulated or queried only by using SMF interfaces
- Provides a consistent and persistent way to enable or disable a service
- Provides a consistent view of service state

ORACLE

SMF Administrative Layers



SMF Repository Backups

- SMF automatically takes the following backups:
  - **Boot backup:** Taken immediately before the first change to the repository is made during each system startup
  - **`manifest_import` backups:** Occur after `svc:/system/early-manifest-import:default` or `svc:/system/manifest-import:default` completes, if the service imported new manifests or ran upgrade scripts
- The system maintains four copies of each type.
- Backups are stored as `/etc/svc/repository-`*`type-YYYYMMDD_HHMMSWS`* for the date and time when the backup was taken.
- The repository can be restored from these backups if an error occurs.

SMF Repository Snapshots

- Snapshots are taken per service at the time when a service is successfully started.
- Standard snapshots include:
  - **`initial`:** Taken on the first import of the manifest
  - **`running`:** Taken when `svcadm refresh` is run
  - **`start`:** Taken at the last successful start
- The SMF service always executes with the `running` snapshot.
- Current property values for a service are incorporated into the `running` snapshot with the `svcadm refresh` command.
- Instance configurations can be viewed or reverted to in a previous snapshot by using the `svccfg` command.

ORACLE

Implementing Service Administration

In the next section, you learn how to:

- Create a new service and incorporate it into SMF
- Modify a service configuration
- Restore and recover a service

Quiz

The preferred location for manifests is /lib/svc/manifest.

a. True

b. False

Quiz

Which of the following profiles is used to enable standard services?

a. `/etc/svc/profile/generic_open.xml`

b. `/etc/svc/profile/generic_limited_net.xml`

c. `/etc/svc/profile/ns_*.xml`

d. `etc/svc/profile/platform_*.xml`

Quiz

Which daemon manages the service configuration repository?

a. `svc.ipfd`

b. `svc.configd`

c. `svc.startd`

Quiz

The SMF service always executes with one of the following service configuration repository snapshots. Which one is it?

a. `initial`
b. `running`
c. `start`

Agenda

- Advanced features of SMF
- Configuring SMF services
- Troubleshooting SMF services

Configuring SMF Services

This section covers the following topics:

- Creating a new service script
- Creating a service
- Modifying a service's manifest
- Changing an environment variable for a service
- Changing a property for an `inetd`-controlled service
- Creating and applying an SMF profile
- Changing services and their configurations by using the `netservices` command

Creating New Service Scripts

1. Determine the process for starting and stopping your service.
2. Establish a name for the service and its category.
3. Determine whether your service runs multiple instances.
4. Identify dependency relationships between this service and other services.
5. If a script is required to start and stop the process, create the script and place it in a local directory, such as `/usr/local/svc/method`.
6. Create a service manifest file for your service.
7. Incorporate the script into the SMF by using the `svccfg` utility.

ORACLE

Creating a Service

1. Create the script by using the following command:
   `vi /usr/local/svc/method/`*`servicename`*
2. Grant the execute permission on the script so it can be executed by using the following command:
   `chmod 544 /usr/local/svc/method/`*`servicename`*
3. Change directories to `/lib/svc/manifest/site` and edit the manifest `.xml` file for your new service.
4. Import the new service into SMF by using the following command:
   `svcadm restart system/manifest-import`
5. Verify that the new service is available by using the `svcs` *`servicename`* command.

Creating a Service: Example

```
# mkdir -p /usr/local/svc/method/newservice
# vi /usr/local/svc/method/newservice
#!/sbin/sh
#
# ident "@(#)newservice 1.14 04/08/30 SMI"
case "$1" in
'start')
/usr/bin/newservice &
;;
'stop')
/usr/bin/pkill -x -u 0 newservice
;;
*)
echo "Usage: $0 { start | stop }"
;;
esac
exit 0
# chmod 544 /usr/local/svc/method/newservice
```

Creating a Service: Example

```
# cd /var/svc/manifest/site
# vi newservice.xml
<?xml version='1.0' encoding='UTF-8' ?>
<!DOCTYPE service_bundle SYSTEM
    '/usr/share/lib/xml/dtd/service_bundle.dtd.1'>
<service_bundle type='manifest' name=‘OPTnew:newservice'>
  <service name='site/newservice' type='service' version='1'>
    <create_default_instance enabled=‘true'/>
    <single_instance/>
    <exec_method name='start' type='method'
    exec=’/usr/local/svc/method/newservice start’
    timeout_seconds=‘30'>
    </exec_method>
    <exec_method name='stop' type='method' exec=':true'
    timeout_seconds=‘30'>
    </exec_method>
    <property_group name='startd' type='framework'>
    <propval name='duration' type='astring' value='transient'/>
    </property_group>
  </service>
</service_bundle>
```

Creating a Service: Example

```
# svccfg validate /var/svc/manifest/site/newservice.xml
# svcadm restart system/manifest-import
# svcs newservice
STATE  STIME   FMRI
online 8:43:45 svc:/site/newservice:default
```

Creating a Service: Example

```
# svcadm -v disable site/newservice
svc:/site/newservice:default disabled.
# svcs newservice
STATE    STIME   FMRI
disabled 9:11:38 svc:/site/newservice:default
# svcadm -v enable site/newservice
svc:/site/newservice:default enabled.
# svcs newservice
STATE  STIME   FMRI
online 9:11:54 svc:/site/newservice:default
#
```

Modifying a Service's Manifest

1. Modify the manifest.
2. Reimport the manifest by running `svcadm restart system/manifest-import` if in the standard location. If not in the standard location, run `svccfg import <manifest>`.
3. Importing the service will refresh it. However, a restart may be required.

Modifying a Service’s Manifest: Example

```
# pfedit crmsvc.xml
# grep monitor crmsvc.xml
     <exec_method name='start' type='method'
    exec='/export/home/sstudent/smf/monitor1.crm' timeout_seconds='60'/>
# svcadm restart manifest-import
# svcadm restart crmsvc
# svcadm enable crmsvc
# svcs crmsvc
STATE          STIME      FMRI
online         10:27:25  svc:/site/crmsvc:default
```

ORACLE

Changing an Environment Variable for a Service

1. Verify that the service is running by using `svcs` *`FMRI`*.
2. Set environment variables by using `svccfg -s` *`FMRI`* `setenv` *`envar value`*.
3. Refresh the service by using `svcadm refresh` *`FMRI`*.
4. Restart the service by using `svcadm restart` *`FMRI`*.
5. Verify that the change has been made by using ``pargs -e `pgrep -f /usr/sbin/FMRI` ``.

Changing an Environment Variable for a Service: Example

```
# svcs system/cron
STATE          STIME    FMRI
online         13:02:52 svc:/system/cron:default
# svccfg -s system/cron:default setenv UMEM_DEBUG default
# svccfg -s system/cron:default setenv LD_PRELOAD libumem.so
# svcadm refresh system/cron
# svcadm restart system/cron
# pargs -e `pgrep -f /usr/sbin/cron`
2479:      /usr/sbin/cron
envp[0]: LOGNAME=root
envp[1]: _=*2476*/usr/sbin/cron
envp[2]: LANG=
envp[3]: LC_ALL=en_US.UTF-8
envp[4]: LC_COLLATE=
envp[5]: LC_CTYPE=
envp[6]: LC_MESSAGES=
envp[7]: LC_MONETARY=
envp[8]: LC_NUMERIC=
envp[9]: LC_TIME=
envp[10]: LD_PRELOAD=libumem.so
envp[11]: PATH=/usr/sbin:/usr/bin
envp[12]: PWD=/root
envp[13]: SHLVL=2
envp[14]: SMF_FMRI=svc:/system/cron:default
envp[15]: SMF_METHOD=start
envp[16]: SMF_RESTARTER=svc:/system/svc/restarter:default
envp[17]: SMF_ZONENAME=global
envp[18]: TZ=localtime
envp[19]: UMEM_DEBUG=default
envp[20]: A__z="*SHLVL#
```

Changing a Property for an `inetd`-Controlled Service

1. List the properties for the specific service by using `inetadm -l` *`FMRI`*.
2. Change the property for the service by using `inetadm -m` *`FMRI property-name=value`*.
3. Verify that the property has changed by using `inetadm -l` *`FMRI`*.
4. Confirm that the change has taken effect.

Changing a Property for an `inetd`-Controlled Service: Example

```
# inetadm -l svc:/network/telnet
SCOPE     NAME=VALUE
          name="telnet"
          endpoint_type="stream"
          proto="tcp6"
          isrpc=FALSE
          wait=FALSE
          exec="/usr/sbin/in.telnetd"
          user="root"
default   bind_addr=""
default   bind_fail_max=-1
default   bind_fail_interval=-1
default  max_con_rate=-1
default  max_copies=-1
default  con_rate_offline=-1
default  failrate_cnt=40
default  failrate_interval=60
default  inherit_env=TRUE
default  tcp_trace=FALSE
default  tcp_wrappers=FALSE
default  connection_backlog=10
default  tcp_keepalive=FALSE
```

Changing a Property for an `inetd`-Controlled Service: Example

```
# inetadm -m telnet tcp_trace=TRUE
# inetadm -l svc:/network/telnet
SCOPE    NAME=VALUE
         name="telnet"
         endpoint_type="stream"
         proto="tcp6"
         isrpc=FALSE
         wait=FALSE
         exec="/usr/sbin/in.telnetd"
         user="root"
default  bind_addr=""
default  bind_fail_max=-1
default  bind_fail_interval=-1
default  max_con_rate=-1
default  max_copies=-1
default  con_rate_offline=-1
default  failrate_cnt=40
default  failrate_interval=60
default  inherit_env=TRUE
         tcp_trace=FALSE
default  tcp_wrappers=FALSE
default  connection_backlog=10
default  tcp_keepalive=FALSE
```

Changing a Property for an `inetd`-Controlled Service: Example

```
# tail -1 /var/adm/messages
Dec 15 08:04:39 client1 inetd[655]: [ID 317013 daemon.notice]
    telnet[2390] from 192.168.0.100 34098
# grep /var/adm/messages /etc/syslog.conf
*.err;kern.debug;daemon.notice;mail.crit  /var/adm/messages
```

Creating and Applying an SMF Profile

1. Create a profile by using `svccfg extract> profile.xml`.
2. Edit the `profile.xml` file to make changes:
   a. Change the name of the profile in the `service_bundle` declaration.
   b. Remove services that should not be managed by this profile.
   c. Add services that should be managed by this profile.
   d. If necessary, change the enabled flag for selected services.
3. When necessary, apply the new profile by using `svccfg apply profile.xml`.

ORACLE

Creating and Applying an SMF Profile: Example

```
# svccfg extract > profile.xml
# vi profile.xml
# cat profile.xml
  ...
<service_bundle type=`profile` name=`profile`
    xmIns::xi='http://www.w3.org/2003/XInclude'
  ...
 <service name='network/ldap/client' version='1' type='service'>
         <instance  name='default' enabled='true'/>
 </service>
  ...
<service  name='network/smtp' version='1' type='service'>
    <instance  name='sendmail' enabled='false'/>
  </service>
  ...
# svccfg apply profile.xml
```

ORACLE

Changing Services and Their Configurations by Using the `netservices` Command

Run the `netservices` command to select either open (traditional) or limited network exposure.

- For open (traditional) network exposure, run `/usr/sbin/netservices open`.
- For limited network exposure, run `/usr/sbin/netservices limited`.

ORACLE

Modifying a Property Value of an SMF Service

1. Identify the SMF service whose property value that you want to modify.
2. List the properties of the SMF service by using the `svcprop` *`FMRI`* command
3. Identify the property of the SMF service that you want to modify.
4. Modify the property value by using the `svccfg –s` *`FMRI`* `setprop` *`property`*`=`*`value`* command.
5. Refresh the SMF service instance so that the changes take effect.

Modifying a Property Value of an SMF Service: Example

In the following example, the host name of the system is modified:

```
root@s11-server1:~# svcprop svc:/system/identity:node
config/enable_mapping boolean true
config/ignore_dhcp_hostname boolean false
config/loopback astring “”
config/nodename astring s11-server1
...
...
root@s11-server1:~# svccfg -s identity:node describe config/nodename
config/nodename astring solaris
     Network name of the computer
root@s11-server1:~# svccfg -s svc:/system/identity:node \
 setprop config/nodename=solaris11
root@s11-server1:~# svcadm refresh svc:/system/identity:node
root@s11-server1:~# Hostname:solaris11
Aug 5 10:33:12 s11-server1 rpcbind: rpcbind terminating on signal.
root@s11-server1:~# svcadm restart identity:node
root@s11-server1:~# Hostname:solaris11
root@s11-server1:~# exit
logout
oracle@s11-server1:~$ exit
logout
solaris11 console login: oracle
Password: oracle1
oracle@solaris11:~$
```

ORACLE

Quiz

Which of the following commands should you use to validate the manifest file?

a. `svcs`

b. `svcadm`

c. `svccfg`

Quiz

If you want to display a list of services that are enabled or disabled on the current system, which of the following commands should you use?

a. `svccfg list`

b. `svccfg extract`

c. `svccfg export`

Practice 2-1 and Practice 2-2 Overview: Configuring SMF Services and Working with Service Profiles

These practices cover the following topics:

- Creating and exporting a service
- Modifying a service configuration
- Changing an environment variable for a service
- Changing a property for a service controlled by `inetd`
- Creating an SMF profile
- Applying an SMF profile
- Changing the services and their configuration by using the `netservices` command

ORACLE

Agenda

- Advanced features of SMF
- Configuring SMF services
- Troubleshooting SMF services

Troubleshooting SMF Services

This section covers the following topics:

- Debugging a service that is not starting
- Restoring a service that is in maintenance state
- Reverting to an SMF snapshot
- Repairing a corrupt repository
- Debugging services during a system boot
- Addressing `system/filesystem/local:default` service failures during a boot

Debugging a Service That Is Not Starting

1. Request information about the hung service by using `svcs -xv servicename`.
2. Enable the service by using `svcadm enable serviceinstance`.
3. Verify that the service is online by using `svcs -a servicename`.

ORACLE

Debugging a Service That Is Not Starting: Example

```
# svcs -xv
svc:/network/sendmail-client:default (sendmail SMTP client queue runner)
 State: disabled since September  4, 2015 06:41:18 AM IST
Reason: Disabled by an administrator.
   See: http://support.oracle.com/msg/SMF-8000-05
   See: man -M /usr/share/man -s 1M sendmail
Impact: 1 dependent service is not running:
        svc:/system/fm/smtp-notify:default

svc:/system/ocm:default (Oracle Configuration Manager (OCM))
 State: maintenance since September  4, 2015 06:42:16 AM IST
Reason: Method failed.
   See: http://support.oracle.com/msg/SMF-8000-8Q
   See: http://download.oracle.com/docs/d/E23562_01/doc.1035/e22050/toc.htm
   See: man -M /usr/share/man -s 1M configCCR
   See: /var/svc/log/system-ocm:default.log
Impact: This service is not running.
# svcadm enable svc:/network/sendmail-client:default
# svcadm disable svc:/system/ocm:default
# svcs ocm
STATE          STIME    FMRI
disabled       5:09:54  svc:/system/ocm:default
# svcs sendmail-client
STATE          STIME    FMRI
online         5:29:17  svc:/network/sendmail-client:default
# svcs -xv
```

Restoring a Service That Is in Maintenance State

1. Determine why the service is in maintenance by using `svcs -x` *`FRMI`*.
2. Determine whether processes that are dependent on the service have stopped by using `svcs -o CTID` *`FMRI`*.
3. (Optional) Kill any remaining processes as required by using `pkill -9` *`PID`* for all process that are displayed by the `svcs` command.
4. Restore the service by using `svcadm clear` *`FMRI`*.

Restoring a Service That Is in Maintenance State: Example

```
# svcs -x svc:/system/ocm:default
svc:/system/ocm:default (Oracle Configuration Manager (OCM))
 State: maintenance since September 12, 2015 06:39:11 AM IST
Reason: Method failed.
   See: http://support.oracle.com/msg/SMF-8000-8Q
   See:
http://download.oracle.com/docs/cd/E23562_01/doc.1035/e22050/toc.htm
   See: configCCR(1M)
   See: /var/svc/log/system-ocm:default.log
Impact: This service is not running.
# svcs -o CTID svc:/system/ocm:default
CTID
      218
You have new mail in /var/mail/root
# pkill -9 218
# svcadm clear svc:/system/ocm:default
# svcs svc:/system/ocm:default
STATE          STIME    FMRI
disabled        6:40:16 svc:/system/ocm:default
```

ORACLE

Reverting to an SMF Snapshot

1. Run the `svccfg` command.
   a. Select the service instance that you want to fix.
   b. Generate a list of available snapshots by using `listsnap`.
   c. Select to revert to the `start` snapshot by using `revert start`.
   d. Quit `svccfg` by using `quit`.
2. Update the information in the service configuration repository by using `svcadm refresh` *`FMRI`*.
3. Restart the service instance by using `svcadm restart` *`FMRI`*.

Reverting to an SMF Snapshot: Example

```
# svccfg
svc:> select system/console-login:default
svc:/system/console-login:default> listsnap
previous
running
start
svc:/system/console-login:default> revert start
svc:/system/console-login:default> quit
# svcadm refresh system/console-login:default
# svcadm restart system/console-login:default
# svcs console-login:default
STATE   STIME    FMRI
online  18:15:32 svc:/system/console-login:default
```

ORACLE

Configuration Repository Failed Integrity Check Process

A message is sent to the console if the integrity check fails:

```
<MESSAGE DISPLAYED BY SMF>
svc.configd: smf(5) database integrity check of:

    /etc/svc/repository.db

  failed.  The database might be damaged or a media error might have
  prevented it from being verified.  Additional information useful to
  your service provider is in:

    /etc/svc/volatile/db_errors

  The system will not be able to boot until you have restored a working
  database.  svc.startd(1M) will provide a sulogin(1M) prompt for
  recovery purposes. The command:

    /lib/svc/bin/restore_repository

  can be run to restore a backup version of your repository. See
  http://sun.com/msg/SMF-8000-MY for more information.
```

ORACLE

Repairing a Corrupt Repository

1. Enter the `root` password at the `sulogin` prompt.
2. Run the following command:
   `/lib/svc/bin/restore_repository`
3. Enter the appropriate response.
4. Enter `yes` to remedy the fault.

Repairing a Corrupt Repository: Example

```
# cd /lib/svc/bin
#:/lib/svc/bin# ./restore_repository

<output omitted>

The following backups of /etc/svc/repository.db exist, from oldest to newest:

manifest_import-20111215_035411
boot-20151214_124026
boot-20151215_150206

Please enter either a specific backup repository from the above list to restore it,
or one of the following choices:

CHOICE                ACTION
----------------      ------------------------------
boot                  restore the most recent post-boot ba
manifest_import       restore the most recent manifest_i     backup
-seed-                restore the initial starting rep     ory  (All
                      customizations will be lost, i    uding those
                      made by the install/upgrade   ocess.)
-quit-                cancel script and quit

Enter response [boot]: boot-20151215_150206
```

Here, you are reverting to the service repository version created on December 15, 2015

Repairing a Corrupt Repository: Example

```
<output continued from previous page>
…
…
After confirmation, the following steps will be taken:

svc.startd(1M) and svc.configd(1M) will be quiesced, if running.
/etc/svc/repository.db
    -- renamed --> /etc/svc/repository.db_old_20151215_060922
/etc/svc/repository-boot-20151215_150206
    -- copied --> /etc/svc/repository.db
and the system will be rebooted with reboot(1M).

Proceed [yes/no]? yes
```

Debugging the Services During a System Boot

1. Log in to the system as `root`.
2. Enable all services by using `svcadm milestone all`.
3. Determine where the boot process is hanging:
   a. Run `svcs -a` to determine which services are not running.
   b. Look for error messages in the log files in `/var/svc/log`.
4. After fixing the problems, verify that all services have started:
   a. Verify that all needed services are online by using `svcs -x`.
   b. Verify that the `console-login` service dependencies are satisfied by using `svcs -l system/console-login:default`.
5. Continue the normal booting process.

Addressing `system/filesystem/local:default` Service Failures During a Boot

1. Modify the `system/console-login` service by using `svccfg -s svc:/system/console-login`:

```
svc:/system/console-login> addpg site,filesystem-local dependency
svc:/system/console-login> setprop site,filesystem-local/entities = fmri:
 svc:/system/filesystem/local
svc:/system/console-login> setprop site,filesystem-local/grouping = astring:
 require_all
svc:/system/console-login> setprop site,filesystem-local/restart_on = astring: none
svc:/system/console-login> setprop site,filesystem-local/type = astring: service
svc:/system/console-login> end
```

2. Refresh the service by using `svcadm refresh console-login`.

Practice 2-3 Overview: Restoring and Recovering a Service

This practice covers the following topics:

- Restoring a service in the `maintenance` state
- Reverting to a previous SMF snapshot
- Repairing a corrupt repository
- Debugging a service that is not starting

ORACLE

Summary

In this lesson, you should have learned how to:

- Describe the advanced features of SMF
- Configure SMF services
- Troubleshoot SMF services

3

Managing Software Packages by Using IPS

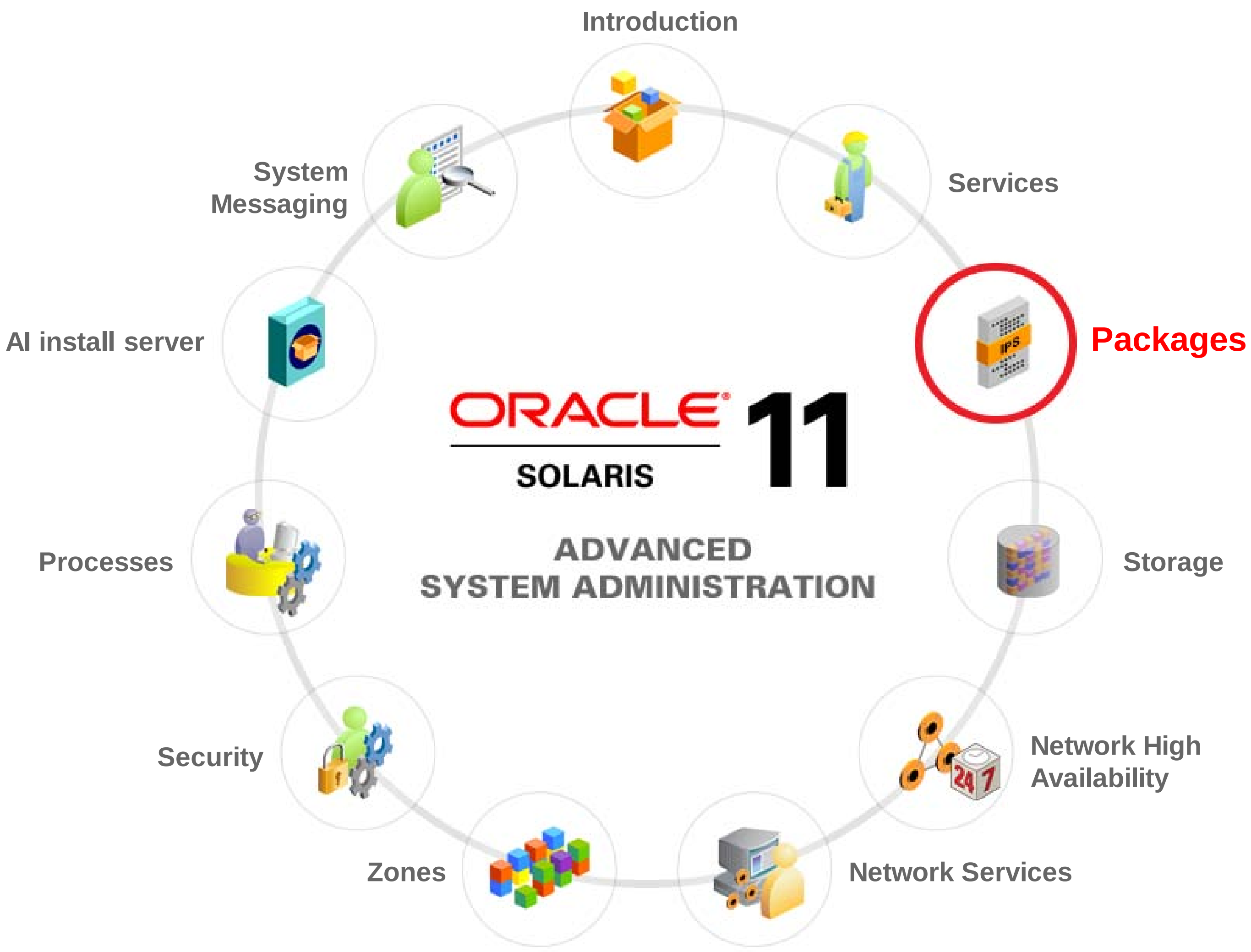
ORACLE

Objectives

After completing this lesson, you should be able to:

- Describe Image Packaging System (IPS)
- Configure a local IPS package repository

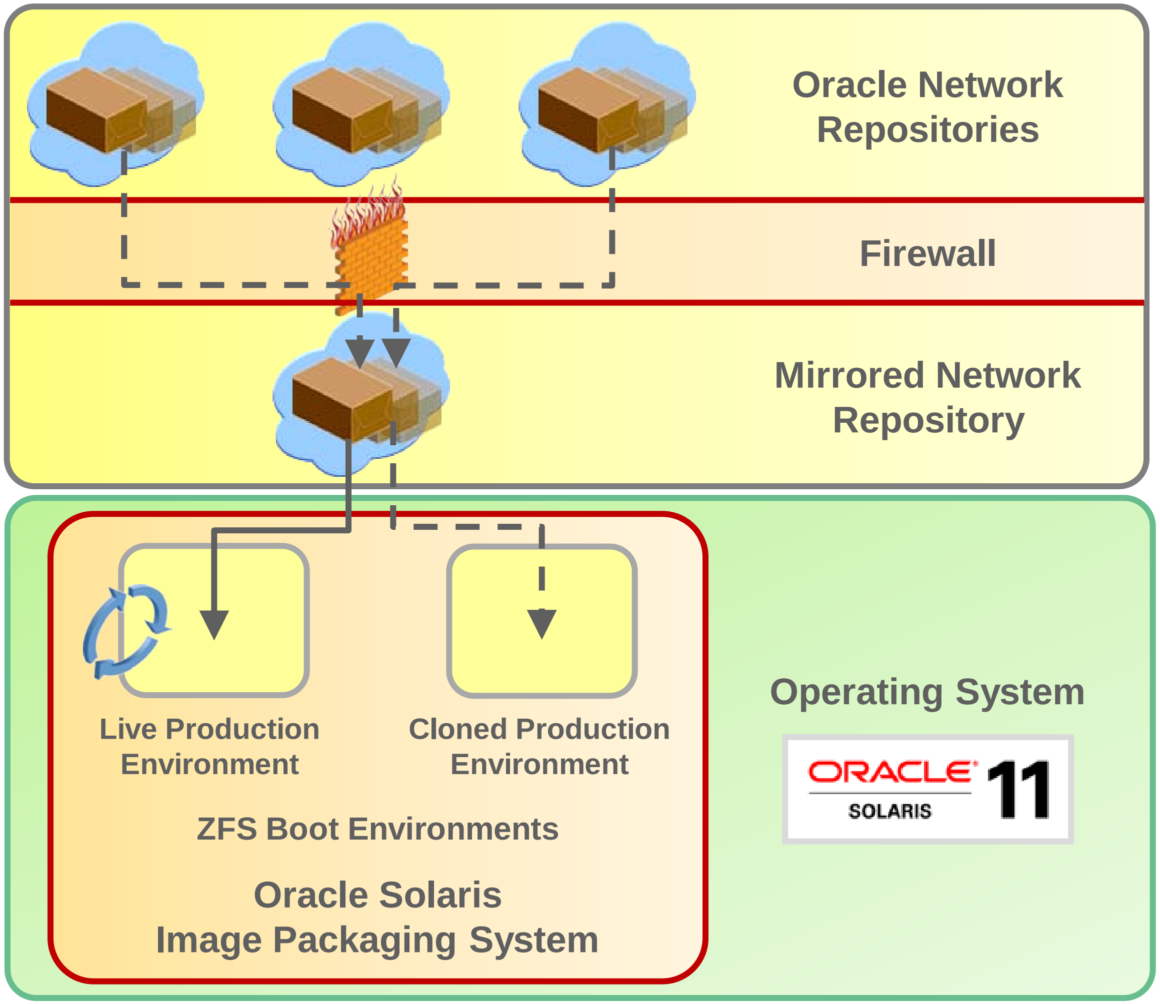
Job Workflow



Agenda

- Describing Image Packaging System (IPS)
- Configuring a local IPS package repository

IPS: Overview



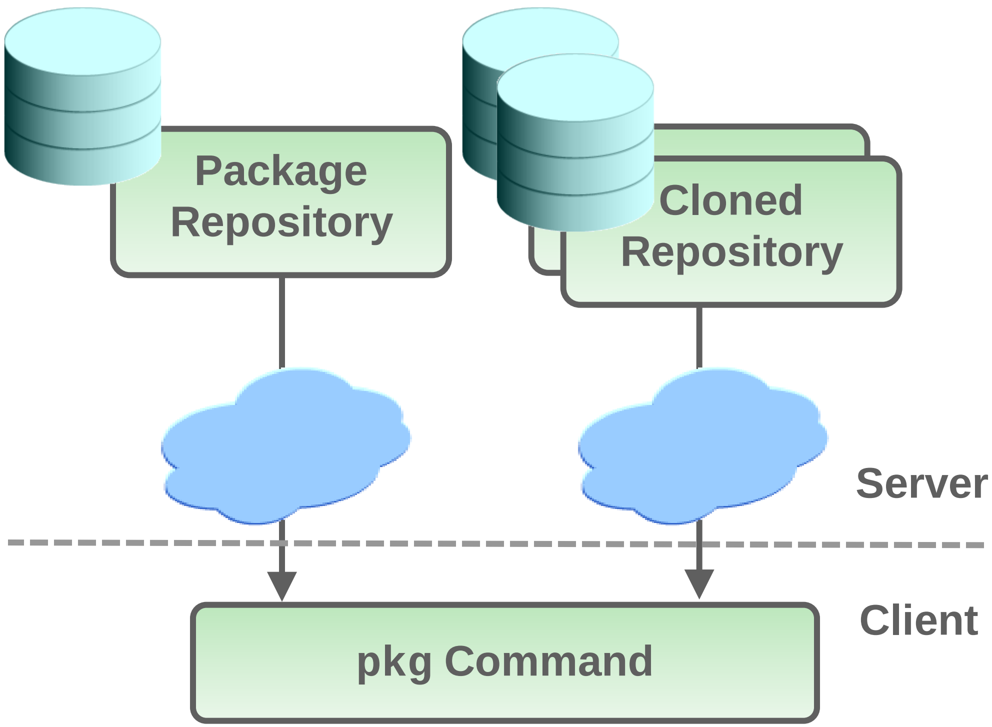
IPS: Overview

Using IPS, you can perform the following tasks:

- Create and manage images.
- Search the IPS packages on your system and in IPS repositories.
- Copy, mirror, create, and administer package repositories.
- Create and publish IPS packages to a package repository.
- Republish the content of an existing package in a package repository.
- Upgrade the system with the help of ZFS boot environments.

IPS Components

- Package
- FMRI
- Publisher
- Repository
- Package archive
- Repository origin
- Repository mirror
- Image
- Boot environment (BE)
- Facet
- Variant
- Package management utility, `pkg(1)`



Agenda

- Describing Image Packaging System (IPS)
- Configuring a local IPS package repository

Identifying IPS Server System Requirements

Hardware and Software	Requirement
System	x86 or SPARC
Operating system	Oracle Solaris 11
Disk space	16 GB of free space

Local IPS Repository

- The Oracle Solaris release repository is available at:

  http://pkg.oracle.com/solaris/release/
- Reasons for creating a local IPS repository:
  - Accessibility
  - Performance
  - Security
  - Change control
  - Custom packages

ORACLE

Creating a Local IPS Repository

You can create a local IPS repository by:

- Copying an IPS repository from a file
  - Copying an IPS repository from `zip` files
  - Copying an IPS repository from an `iso` file
- Copying an IPS repository from the Internet
  - Copying an IPS repository from the Internet
  - Automatically copying an IPS repository from the Internet

ORACLE

Copying an IPS Repository from `zip` Files

1. Create a ZFS file system for the new repository.
2. Get the Oracle Solaris IPS repository `.zip` files along with the `install-repo.ksh` script, the `README`, and checksum files.
3. Make the repository installation script executable.
4. Run the repository installation script.
5. Verify the new repository content.
6. Take a snapshot of the new repository.

Copying an IPS Repository from an `iso` File

1. Create a ZFS file system for the new repository.
2. Get the Oracle Solaris IPS repository image file.
3. Mount the image file.
4. Copy the repository content to the new location.
5. Unmount the image file.
6. Verify the new repository content.
7. Take a snapshot of the new repository.

Copying an IPS Repository from the Internet

1. Create a ZFS file system for the new repository.
2. Create the required repository infrastructure.
3. Copy the repository content to the new location.
4. Verify the new repository content.
5. Take a snapshot of the new repository.

Automatically Copying an IPS Repository from the Internet

The `svc:/application/pkg/mirror` SMF service:

- Updates the local master repository from a defined IPS repository, automatically
- Performs a periodic `pkgrecv` operation from the `solaris` publisher origins defined in the image to `/var/share/pkg/repositories/solaris`, which starts at 2:30 AM one day each month
- Refreshes the repository catalog at the end of each successful run of the service

ORACLE

Providing Access to Your Local IPS Repository

You can enable clients to retrieve packages in your local IPS repository by using:

- A file interface
- An HTTP interface

Enabling Users to Retrieve Packages by Using a File Interface

1. Configure an NFS share.
2. Confirm that the NFS share is published.
   - Search for the repository in the shared file system table.
   - Determine whether the repository is accessible from a remote system.
3. Set the origin of the publisher.
   - Determine the name of the publisher.
   - Check the suitability of this publisher origin.
   - Set the publisher origin.

Enabling Users to Retrieve Packages by Using an HTTP Interface

1. Create a depot server instance.
2. Set the path to the repository.
3. Set the port number (optional).
4. Start the package depot server service.
5. Test whether the repository server is working.
6. Set the origin of the publisher.
   – Determine the name of the publisher.
   – Check the suitability of this publisher origin.
   – Set the publisher origin.

ORACLE

Configuring a Local IPS Package Repository: Example

Required tasks:

1. Creating a ZFS file system to hold the repository
2. Obtaining software packages from the Oracle Solaris download site
3. Configuring the repository server service
4. Starting the repository service
5. Setting the local IPS publisher
6. Testing IPS on the local server

ORACLE

Creating a ZFS File System to Hold the Repository

Create a ZFS file system for the local package repository in the root pool.

```
# zfs create -o atime=off -o compression=on rpool/export/IPS/repo
# zfs list
NAME                              USED  AVAIL  REFER  MOUNTPOINT
rpool                            13.2G  2.20G  4.97M  /rpool
rpool/ROOT                       4.49G  2.20G    31K  legacy
rpool/ROOT/solaris               4.49G  2.20G  4.08G  /
rpool/ROOT/solaris/var            353M  2.20G   197M  /var
rpool/VARSHARE                    132K  2.20G  69.5K  /var/share
rpool/VARSHARE/pkg                 63K  2.20G    32K  /var/share/pkg
rpool/VARSHARE/pkg/repositories    31K  2.20G    31K
/var/share/pkg/repositories
rpool/dump                        792M  2.22G   768M  -
rpool/export                     6.88G  2.20G    34K  /export
rpool/export/IPS/repo            6.77G  2.20G  6.77G  /export/IPS/repo
rpool/export/home                 108M  2.20G    32K  /export/home
rpool/export/home/oracle          108M  2.20G   108M  /export/home/oracle
rpool/swap                       1.03G  2.23G  1.00G  -
```

Obtaining Software Packages from the Oracle Solaris Download Site

1. Go to the Oracle Solaris download site:
   http://www.oracle.com/technetwork/server-storage/solaris11/downloads/index.html
2. Download the following files:
   – README file (`README-zipped-repo.txt`)
   – Repository assembly script (`install-repo.ksh`)
   – MD5 checksum file
   – Five IPS repository parts (zip files)
3. Copy the files to the ZFS repository file system.
4. Make sure the script file is executable.
5. Run the repository installation script `install-repo.ksh`.
6. Verify the repository image.

ORACLE

Configuring the Repository Server Service

Use the SMF `svccfg` command to configure the repository server service.

```
# svccfg -s application/pkg/server setprop pkg/inst_root=/export/IPS/repo
# svccfg -s application/pkg/server setprop pkg/readonly=true
# svcprop -p pkg/inst_root application/pkg/server
/export/IPS/repo
```

ORACLE

Starting the Repository Service

Use the SMF `svcadm` command to start the repository service.

```
# svcadm refresh application/pkg/server
# svcadm enable application/pkg/server
# svcs application/pkg/server
STATE    STIME            FMRI
online   17:00:56 svc:/application/pkg/server:default
```

Setting the Local IPS Publisher

Use the `pkg set-publisher` command to set the publisher to the local IPS repository.

```
# pkg publisher
PUBLISHER           TYPE    STATUS P LOCATION
solaris             origin  online F http://pkg.oracle.com/solaris/release
# pkg set-publisher -G '*' -g http://s11-server1.mydomain.com/ solaris
# pkg publisher
PUBLISHER           TYPE    STATUS P LOCATION
solaris             origin  online F http://s11-server1.mydomain.com/
```

ORACLE

Testing IPS on the Local Server

Search for a package to verify that your IPS server is correctly set up.

```
# pkg search entire
INDEX          ACTION    VALUE              PACKAGE
pkg.fmri     set        solaris/entire   pkg:/entire@0.5.11-0.175.3.0.0.30.0
```

ORACLE

Maintaining Multiple Identical Local Repositories

You might want to maintain multiple copies of package repositories with the same content to meet the following goals:

- Increase the availability of the repository by maintaining copies on different nodes.
- Enhance the performance of repository accesses if you have many users or if your users are spread across a great distance.

Quiz

What benefits does a local IPS repository provide?

a. Greater capacity for more packages in the repository
b. Automatically created backup BEs
c. Increased performance for package retrieval

Summary

In this lesson, you should have learned how to:

- Describe Image Packaging System (IPS)
- Configure a local IPS package repository

Practice 3-1 Overview: Configuring a Local IPS Package Repository

This practice covers the following topics:

- Task 1: Configuring the local IPS repository
  - Verifying that the `/export/IPS` file system has been configured on the system
  - Determining whether the IPS service is available
  - Setting up the `application/pkg/server` service
  - Adding a new publisher
  - Testing IPS on the local server
- Task 2: Creating multiple local repositories on a single system (demonstration)

4

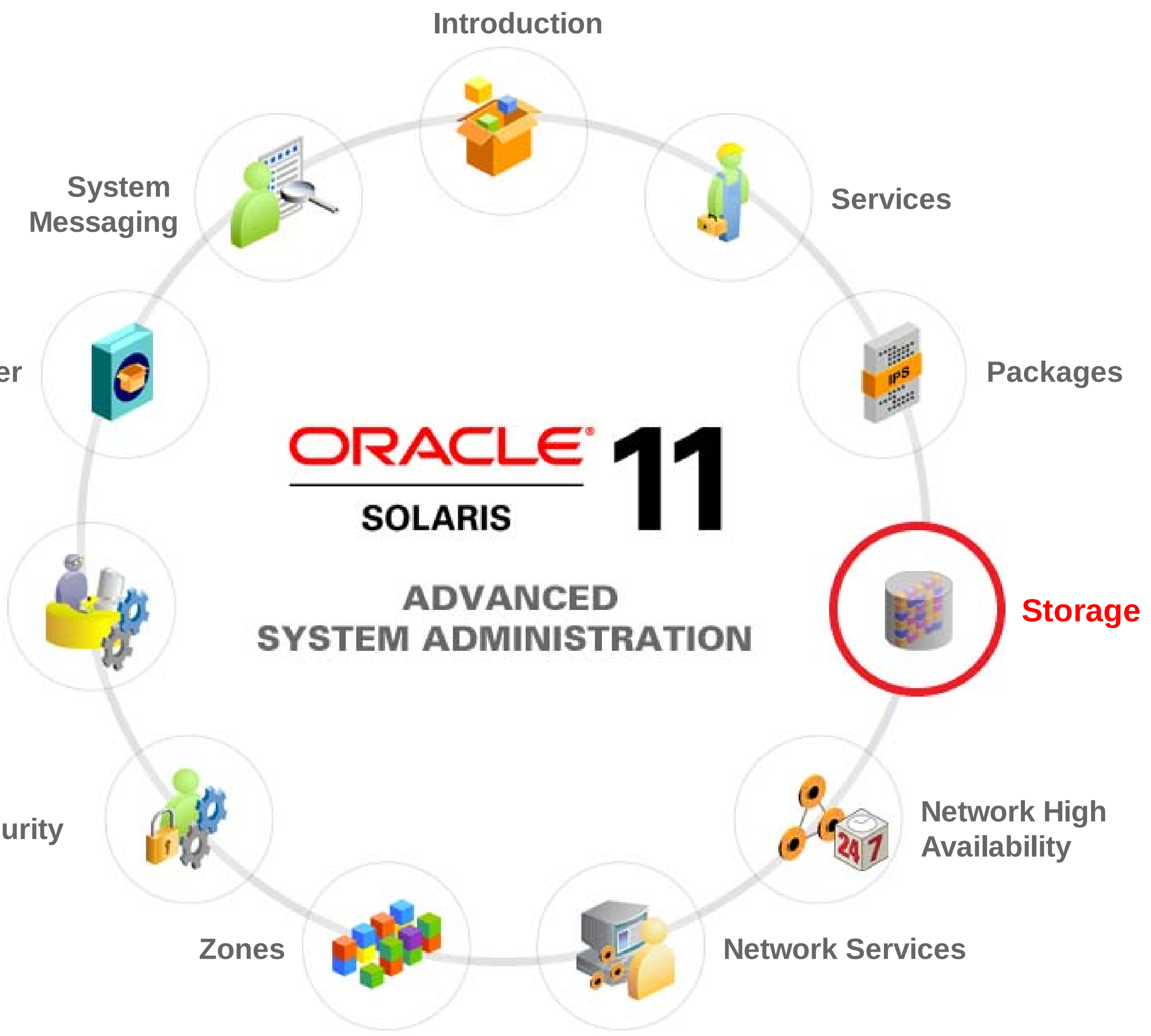
Managing Data Backup and Restore by Using ZFS

Objectives

After completing this lesson, you should be able to:

- Plan for data storage configuration and backup
- Manage data redundancy with mirrored storage pools
- Back up and restore data by using ZFS snapshots
- Manage data storage space with ZFS file system properties
- Troubleshoot ZFS failures

Job Workflow



Agenda

- Planning for data storage configuration and backup
- Managing data redundancy with mirrored storage pools
- Administering data backup and restore by using ZFS snapshots
- Managing data storage space with ZFS file system properties
- Troubleshooting ZFS failures

Planning for Data Storage Configuration and Backup

- Ensure that critical business application data is protected, backed up, recoverable, and accessible.
- You can support business applications by:
  - Providing data redundancy by using mirrored storage pools
  - Setting up file systems to store the data
  - Backing up the file systems by using snapshots and saving them on a remote system
  - Minimizing storage space by using the ZFS file system `compression` property

Identifying Data Backup and Restore Requirements

As part of planning for data backup and restore, it is important to consider the following questions:

- How will data be backed up?
- How often will data be backed up?
- How can these backups be used to recover data in case of data loss?

Determining Storage Pool Requirements

As part of planning, the following storage pool requirements should be identified:

- Devices
  - Disks that are at least 128 MB in size
  - Disks that are not in use by other parts of the operating system
  - Individual slices on a preformatted disk or entire disks formatted as a single, large slice
  - Use of log and cache devices for improved performance
- Level of data redundancy
  - Non-redundant (striped) configurations
  - Mirrored
  - RAID-Z

ORACLE

Identifying Replication Features of a ZFS Storage Pool

Data replication features:

- Mirrored storage pool configuration
  - Requires at least two disks
  - Makes it possible to create more than one mirror in each pool
  - Provides data redundancy through its configuration options and self-healing data features
- RAID-Z storage pool configuration
  - **Single-parity RAID-Z (`raidz` or `raidz1`):** Similar to RAID-5
  - **Double-parity RAID-Z (`raidz2`):** Similar to RAID-6
  - **Triple-parity RAID-Z (`raidz3`):** Similar to `raidz2` with an additional parity protection level
- Self-healing data
  - Supported in a mirrored or RAID-Z configuration
  - Automatically detects and repairs bad data blocks

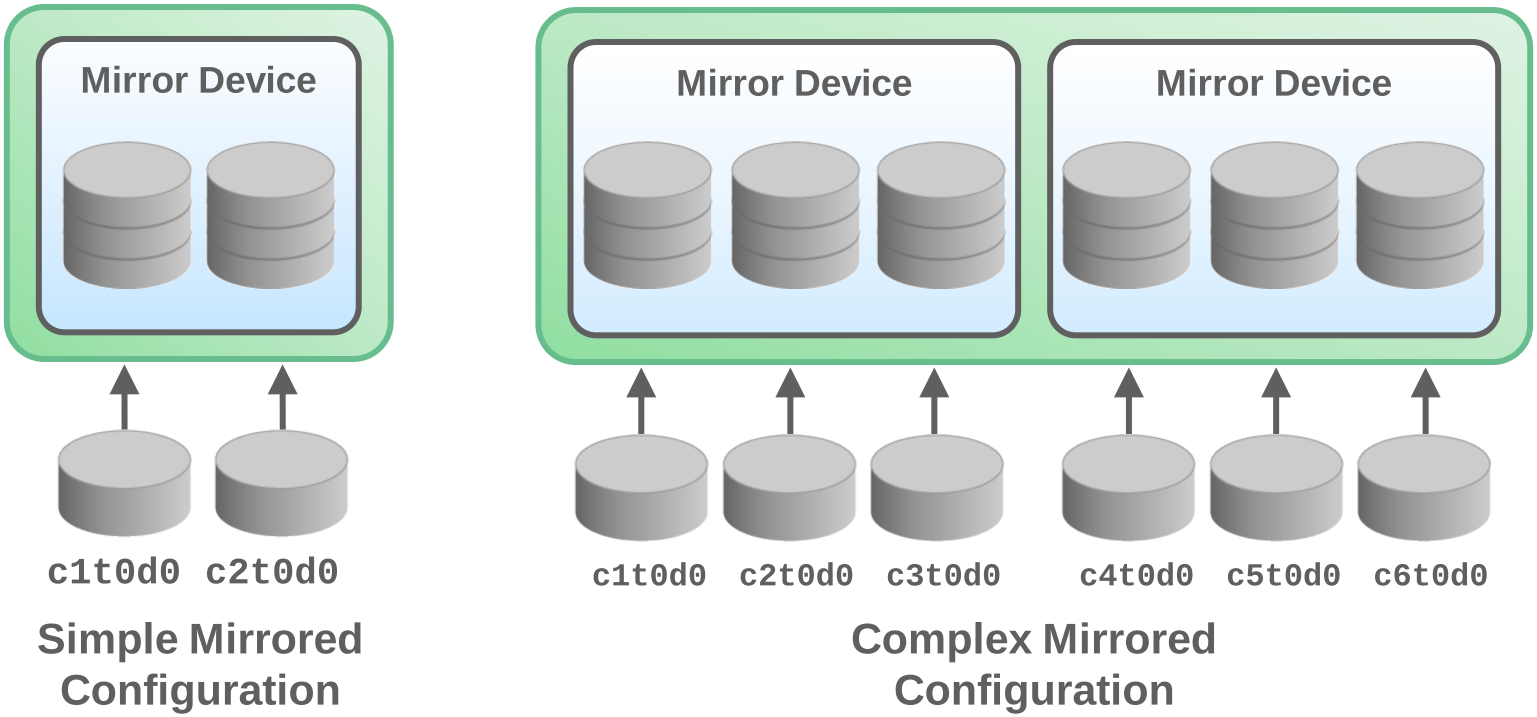
Identifying Replication Features of a ZFS Storage Pool

Data replication features:

- ZFS hybrid storage pool
  - Is available in the Oracle ZFS Storage Appliance
  - Is a special storage pool that combines DRAM, SSDs, and HDDs
  - Improves performance and increases capacity while reducing power consumption
  - Enables you (through this product’s management interface) to select the ZFS redundancy configuration of the storage pool and easily manage other configuration options
- Dynamic striping

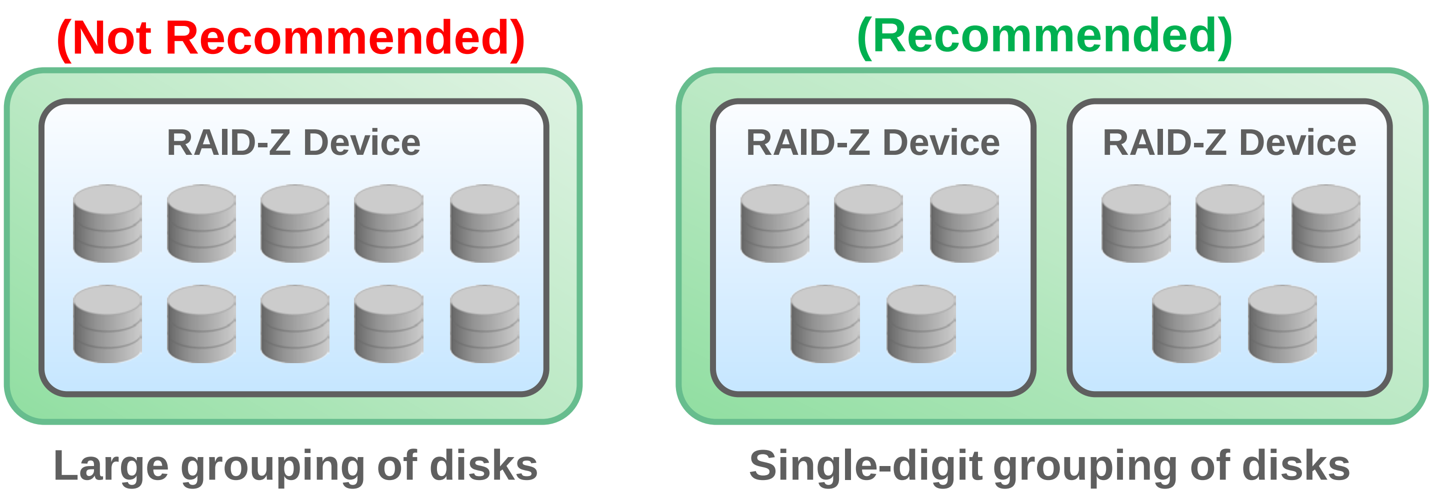
Mirrored Storage Pool Configuration

- At least two disks are required.
- Many disks can be used.
- Multiple mirrors can be created in each pool.



RAID-Z Storage Pool Configuration

- Minimum disk usage recommendations by RAID-Z level
  - **`raidz` or `raidz1`:** Use at least three disks (2 + 1).
  - **`raidz2`:** Use at least five disks (3 + 2).
  - **`raidz3`:** Use at least eight disks (5 + 3).
- For better performance, configure storage pools with single-digit groupings of disks.



Self-Healing Data

- A mirrored or RAID-Z configuration provides support for self-healing data.
- When a bad data block is detected:
  - Correct data is fetched from another replicated copy
  - Bad data is repaired by replacement with the good copy

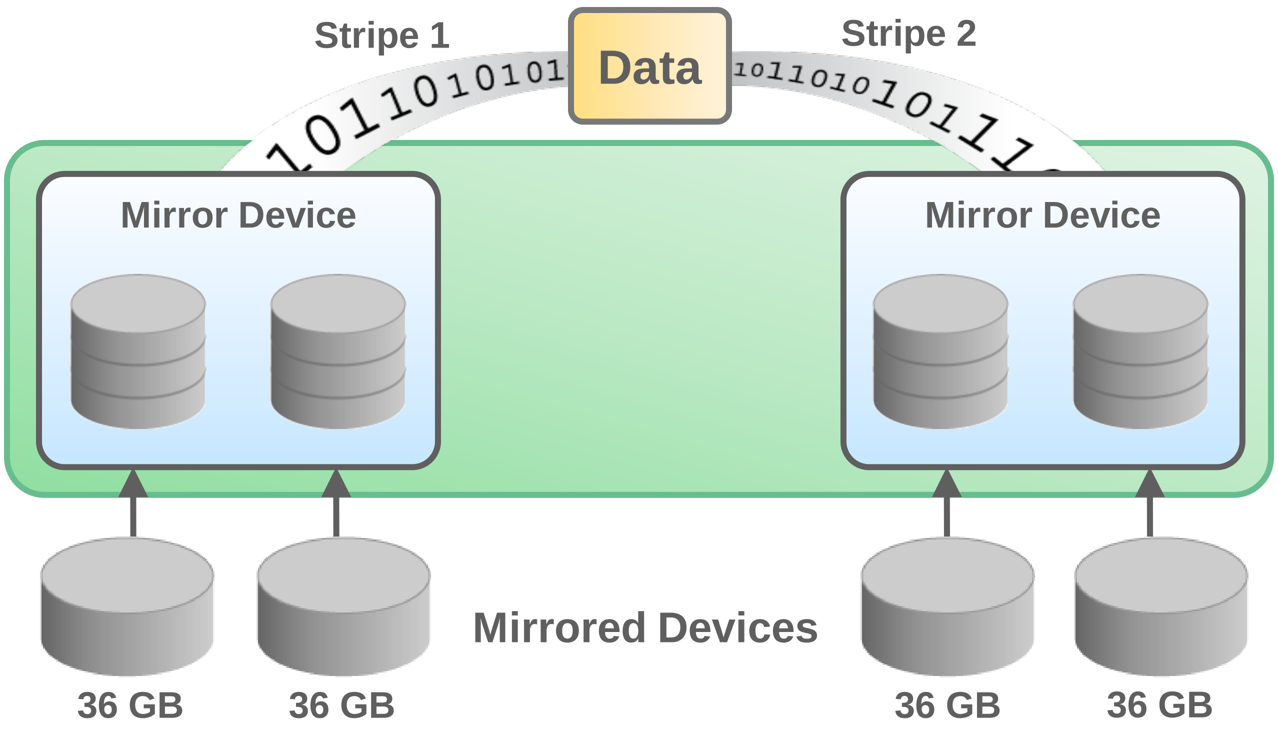
ORACLE

Dynamic Striping

- Data is dynamically striped across all top-level virtual devices.
- Data placement is done at write time.
- When a new virtual device is added, data is gradually allocated to the new device.

Note: Although ZFS supports combining different types of virtual devices within the same pool, the recommended practice is to use top-level virtual devices of the same type with the same redundancy level in each virtual device.

Dynamic Striping in a Mirrored Pool



ORACLE

Recommended Storage Pool Practices

- Keep pool capacity below 90% for best performance.
- For random read/write workloads, mirrored pools are recommended instead of RAID-Z pools.
- Separate your log devices.
- Monitor the following:
  - Pool health
  - Storage pool space
  - Pool and device failures

Determining File System Requirements

- Determine how to set up your file systems to:
  - Store business application data efficiently
  - Facilitate data backup and restore operations
- One recommended approach is to:
  - Create one file system for the main application
  - Create subfile systems for each subapplication
- This approach ensures that the following actions are easy:
  - Backing up the entire file system
  - Backing up the data on each subfile system
  - Restoring the entire file system
  - Setting file system properties at the highest level and having subfile systems inherit the property values

Identifying Your Data Backup and Restore Strategy

As part of planning, you should identify your data backup and restore strategy:

- Use ZFS snapshots to create file system backups and save them on a remote system.
- Use send and receive commands for saving incremental changes between snapshots or for remote replication.

Determining Ways to Save Data Storage Space

ZFS offers a file system `compression` property that:

- Is used to enable or disable compression for a file system
- Compresses only new data on an existing file system if it is enabled after file system creation
- The following compression algorithms are available:

Compression Algorithms	**Description**
`gzip`	Standard UNIX compression
`gzip-`*`N`*	Selects a specific `gzip` level. `gzip-1` provides the fastest gzip compression, `gzip-9` provides the best data compression and `gzip-6` is the default
`lz4`	Provides better compression with lower CPU overhead
`lzjb`	Optimized for performance while providing decent compression
`zle`	Zero length encoding is useful for datasets with large blocks of zeros

Implementing the Data Storage Configuration and Backup Plan

- Configure and test the functionality of a mirrored storage pool.
- Create snapshots of the file systems in the mirrored storage pool to use as backups.
- Set and test the ZFS `compression` property on the file systems.
- Troubleshoot ZFS device and data issues.

Quiz

In a mirrored storage pool configuration, ZFS supports data redundancy but does not support dynamic striping.

a. True

b. False

Quiz

If you want better performance when working with RAID-Z pools, you should configure the pools with single-digit groupings of disks.

a. True

b. False

Quiz

With a RAID-Z storage pool, the data is dynamically striped across all the virtual devices in the pool and redundant among the devices in a single vdev.

a. True
b. False

Quiz

Which RAID-Z parity option does ZFS support?

a. `raidz / raidz1` only

b. `raidz / raidz1` and `raidz2` only

c. `raidz / raidz1, raidz2,` and `raidz3`

d. `raidz / raidz1, raidz2, raidz3,` and `raidz4`

Quiz

Which ZFS file system property enables you to minimize the amount of data storage space that is used in a storage pool?

a. `minimize`

b. `restrictsize`

c. `compressratio`

d. `compression`

Agenda

- Planning for data storage configuration and backup
- Managing data redundancy with mirrored storage pools
- Administering data backup and restore by using ZFS snapshots
- Managing data storage space with ZFS file system properties
- Troubleshooting ZFS failures

ORACLE

Managing Data Redundancy with Mirrored Storage Pools

This section covers the following topics:

- Creating a mirrored storage pool
- Adding log and cache devices to a storage pool
- Managing devices in a ZFS storage pool

Creating a Mirrored Storage Pool

To create a new ZFS mirrored storage pool, use `zpool create` followed by the pool name, the `mirror` keyword, and the storage devices that will compose the mirror.

```
# zpool create hrpool mirror c1t0d0 c2t0d0 mirror c3t0d0 c4t0d0
```

Data is:

- Dynamically striped across both mirrors
- Redundant between each disk within a mirror

Adding Log Devices to a Storage Pool

A log device:

- Can be added as part of, or after, pool creation
- Can be removed
- Is designated by the `log` keyword

```
# zpool create datapool mirror c1t1d0 c1t2d0 log mirror c1t5d0 c1t8d0
```

Adding Cache Devices to a Storage Pool

Cache devices:

- Can be added as part of, or after, pool creation
- Can be removed
- Cannot be mirrored and cannot be part of a RAID-Z configuration
- Are designated with the `cache` keyword

```
# zpool create appool mirror c0t2d0 c0t4d0 cache c0t0d0
```

Note: You can monitor cache statistics with `zpool iostat`.

ORACLE

Managing Devices in ZFS Storage Pools

The tasks that you can perform with the devices in a pool include:

- Adding top-level virtual devices
- Attaching and detaching devices
- Taking a device offline
- Bringing a device online
- Designating hot spares

Adding Devices to a Storage Pool

To add a new virtual device to a pool, use the `zpool add` command.

```
# zpool add appool mirror c2t1d0 c2t2d0
```

By adding a new top-level virtual device, space is:

- Dynamically added to the pool
- Immediately available to all the datasets in the pool

Note: A dataset is a generic name for the following ZFS entities:

- File systems
- Snapshots
- Volumes

ORACLE

Attaching Devices to a Storage Pool

To attach a new device to an existing mirrored or nonmirrored pool, use the `zpool attach` command.

```
# zpool attach appool c1t1d0 c2t1d0
```

Attaching Devices to a Storage Pool

```
# zpool attach appool c1t1d0 c2t1d0
# zpool status
  pool: appool
 state: ONLINE
 scrub: resilver completed after 0h0m with 0 errors on Fri Dec
13 14:11:33 2013
config:
    NAME          STATE     READ   WRITE  CKSUM
    appool        ONLINE       0       0      0
      mirror-0    ONLINE       0       0      0
        c0t1d0    ONLINE       0       0      0
        c1t1d0    ONLINE       0       0      0
        c2t1d0    ONLINE       0       0      0 73.5K resilvered
```

Resilvering: The process of transferring data from one device to another device

Taking Devices Offline in a Storage Pool

To take a device offline, use `zpool offline` followed by the pool name and the device name.

```
# zpool offline hrpool c1t0d0
```

When a device is offline:

- ZFS does not send it any requests
- It remains offline after a system reboot

  Note: Use `zpool offline -t` to take a device offline temporarily.
- It is not detached from the storage pool

Detaching Devices from a Storage Pool

To detach a device from a mirrored storage pool, use the `zpool detach` command.

```
# zpool detach appool c2t1d0
```

Note: This operation is refused if there are no other valid replicas of the data.

Bringing Devices Online in a Storage Pool

To bring a device online, use `zpool online` followed by the pool name and the device name.

```
# zpool online hrpool c1t0d0
bringing device c1t0d0 online
```

When a device is brought back online, data that was added to the storage pool while the device was offline resilvers to the device.

Note: You cannot use `zpool online` to replace a disk.

Replacing Devices in a Storage Pool

To replace a failed device with another device in the same location, use `zpool replace` followed by the pool name and the device name.

```
# zpool replace hrpool c1t1d0
```

If the device is in a different location, specify both devices.

```
# zpool replace hrpool c1t1d0 c1t2d0
```

Note: The size of the replacement device must be greater than or equal to the minimum size of all the devices in a mirror or RAID-Z configuration.

Designating Hot Spares in a Storage Pool

With the ZFS hot spares feature, you can:

- Identify disks to replace a failed or faulted device in one or more storage pools
- Designate these devices as hot spares:
  - When you create the pool (`zpool create`)
  - After you creating a pool (`zpool add`)

  Note: The size of the designated device must be equal to or larger than the size of the largest disk in the pool.
- After a failed device is replaced and resilvered, the spare is automatically detached and made available.
- An in-progress spare replacement can be canceled.
- If the faulted device is detached, the spare assumes its place and is removed from the spare's list of all active pools.

ORACLE

Designating Hot Spares in a Storage Pool

To designate hot spares in a pool that you are creating, use `zpool create` followed by the pool name, the configuration, the keyword `spare`, and the names of the spares.

```
# zpool create appool mirror c1t1d0 c2t1d0 spare c1t2d0 c2t2d0
# zpool status appool
pool: appool
 state: ONLINE
 scrub: none requested
config:
        NAME        STATE     READ  WRITE  CKSUM
        appool      ONLINE       0      0      0
          mirror-0  ONLINE       0      0      0
            c1t1d0  ONLINE       0      0      0
            c2t1d0  ONLINE       0      0      0
        spares
          c1t2d0    AVAIL
          c2t2d0    AVAIL
```

Designating Hot Spares in a Storage Pool

To add hot spares to an existing pool, use `zpool` add followed by the pool name, the keyword `spare`, and the names of the hot spares.

```
# zpool add appool spare c1t3d0 c2t3d0
# zpool status appool
pool: appool
 state: ONLINE
 scrub: none requested
config:
    NAME          STATE      READ   WRITE    CKSUM
    appool        ONLINE        0       0        0
      mirror-0    ONLINE        0       0        0
       c1t1d0     ONLINE        0       0        0
       c2t1d0     ONLINE        0       0        0
    spares
      c1t3d0      AVAIL
      c2t3d0      AVAIL
```

Designating Hot Spares in a Storage Pool

Example of a hot spare replacing a faulted device:

```
# zpool status appool
pool: appool
 state: DEGRADED
status: One or more devices could not be opened.  Sufficient replicas
    exist for the pool to continue functioning in a degraded state.
action: Attach the missing device and online it using 'zpool online'.
   see: http://www.sun.com/msg/ZFS-8000-2Q
 scrub: resilvered completed 0h12m with 0 errors on Fri Dec 13 14:16:04
    2013
config:
    NAME           STATE      READ     WRITE   CKSUM
    appool         DEGRADED     0          0       0
      mirror-0     DEGRADED     0          0       0
        c1t1d0      ONLINE      0          0       0
         spare-1   UNAVAIL      0          0       0
          c2t1d0   UNAVAIL      0          0       0 cannot open
          c1t3d0   ONLINE       0          0       0 58.5K resilvered
    spares
      c1t3d0       INUSE       currently in use
      c2t3d0       AVAIL
```

ORACLE

Removing Hot Spares in a Storage Pool

To remove a hot spare, use `zpool remove` followed by the pool name and the name of the hot spare.

```
# zpool remove appool c1t2d0
# zpool status appool
pool: appool
(output omitted)
    spares
      c1t3d0      AVAIL
```

Note: You cannot remove a hot spare if it is currently being used by the storage pool as an active device.

Practice 4-1 Overview: Managing Data Redundancy with a ZFS Mirrored Pool

This practice covers the following topics:

- Creating ZFS mirrored pools
- Adding disks to a ZFS storage pool
- Adding a cache device to a ZFS storage pool
- Destroying a ZFS storage pool

Agenda

- Planning for data storage configuration and backup
- Managing data redundancy with mirrored storage pools
- Administering data backup and restore by using ZFS snapshots
- Managing data storage space with ZFS file system properties
- Troubleshooting ZFS failures

ORACLE

Backing Up and Recovering Data with ZFS Snapshots

This section covers the following topics:

- Creating and destroying a ZFS snapshot
- Displaying a ZFS snapshot
- Sending ZFS snapshot data
- Receiving ZFS snapshot data
- Remote replication of ZFS snapshot data

ORACLE

Creating and Destroying a ZFS Snapshot

To create a snapshot, use `zfs snapshot` followed by the snapshot name.

```
# zfs snapshot hrpool/home/qarpt@friday
```

To destroy a snapshot, use `zfs destroy` followed by the snapshot name.

```
# zfs destroy hrpool/home/qarpt@friday
```

ORACLE

Displaying a ZFS Snapshot

- To display only snapshots, use `zfs list -t snapshot`.

```
# zfs list -t snapshot
NAME                             USED  AVAIL  REFER  MOUNTPOINT
hrpool/home/qarpt@tuesday        18K       -    21K  -
hrpool/home/qarpt@wednesday      19K       -   280K  -
hrpool/home/qarpt@thursday        0        -   538K  -
```

- To list the snapshots created for a specific file system, enter `zfs list -r -t snapshot` followed by the file system name.

```
# zfs list -r -t snapshot -o name,creation hrpool/home
NAME                                 CREATION
hrpool/home/qarpt@tuesday        Wed Dec 11 10:03 2013
hrpool/home/qarpt@wednesday      Thu Dec 12 10:03 2013
hrpool/home/qarpt@thursday       Fri Dec 13 10:03 2013
hrpool/home/bonus@now            Sat Dec 14 11:04 2013
```

- The snapshots of a file system are accessible in the `.zfs/snapshot` directory in the root of the file system.

```
# ls /home/qarpt/.zfs/snapshot
tuesday wednesday thursday
```

ORACLE

Identifying ZFS Snapshot Differences

- You can determine ZFS snapshot differences by using the `zfs diff` command.
- The `zfs diff` command gives a high-level description of the differences between a snapshot and a descendant dataset.
- The type of change is described along with the name of the file:
  - "`+`" indicates that the file was added in the later dataset.
  - "`–`" indicates that the file was removed in the later dataset.
  - "`M`" indicates that the file was modified in the later dataset.
  - "`R`" indicates that the file was renamed in the later dataset.

Identifying ZFS Snapshot Differences: Example

```
# zfs snapshot newpool/mydata@before
# touch /newpool/mydata/newfile
# zfs snapshot newpool/mydata@after

# zfs list -r -t snapshot -o name,creation
NAME                                                 CREATION
newpool/mydata@before                                Fri Sep 11  4:02 2015
newpool/mydata@after                                 Fri Sep 11  4:02 2015
rpool/ROOT/solaris@install                           Tue Sep  1  5:14 2015
rpool/ROOT/solaris@2015-09-07-21:44:29               Mon Sep  7 13:44 2015
rpool/ROOT/solaris/var@install                       Tue Sep  1  5:14 2015
rpool/ROOT/solaris/var@2015-09-07-21:44:29           Mon Sep  7 13:44 2015
rpool/zones/zone1@send-to-nfs                        Thu Sep 10  9:47 2015
rpool/zones/zone1/rpool@send-to-nfs                  Thu Sep 10  9:47 2015
rpool/zones/zone1/rpool/ROOT@send-to-nfs             Thu Sep 10  9:47 2015
rpool/zones/zone1/rpool/ROOT/zbe-0@send-to-nfs       Thu Sep 10  9:47 2015
rpool/zones/zone1/rpool/ROOT/zbe-0/var@send-to-nfs   Thu Sep 10  9:47 2015
rpool/zones/zone1/rpool/export@send-to-nfs           Thu Sep 10  9:47 2015
rpool/zones/zone1/rpool/export/home@send-to-nfs      Thu Sep 10  9:47 2015
rpool/zones/zone2/rpool/ROOT/zbe-0@zflash.150910.09.34.33  Thu Sep 10  8:34 2015
rpool/zones/zone2/rpool/ROOT/zbe-0@zflash.150910.09.39.35  Thu Sep 10  8:39 2015

# zfs diff newpool/mydata@before newpool/mydata@after
M         /newpool/mydata/
+         /newpool/mydata/newfile
```

ORACLE

Sending ZFS Snapshot Data

The `zfs send` command:

- Is used to send ZFS snapshot data for backup purposes
- Sends a copy of a snapshot to another pool
  - On the same system
  - On a different system
- Creates a stream representation of a snapshot that is written to standard output
  - By default, a full stream is generated.
  - The output can be redirected to a file, to a different system, or to a device.
- Displays an estimate of the size of the send stream

ORACLE

Sending ZFS Snapshot Data

Remember the following key points when you send a file system snapshot:

- Use the `zfs send -I` option to send all incremental streams from one snapshot to a cumulative snapshot, or to send an incremental stream from the original snapshot to create a clone.
  The original snapshot must already exist on the receiving side to accept the incremental stream.
- When you use the `zfs send -r` option without the `-c` option and when you use the `zfs send -R` option, stream packages omit the origin of clones in some circumstances.
- Use the `zfs send -n` option with the `-v` option to see what snapshots would have been sent.
- Use the `zfs send -s` *`streamsize`* option to specify the size of the stream in bytes.
  - `-s` cannot be used with `–v`.
  - *`streamsize`* is the only valid option to `-s`.

ORACLE

Sending ZFS Snapshot Data

To send a ZFS snapshot, enter `zfs send` followed by the snapshot name and destination.

```
# zfs send hrpool/data@snap1 > /backup/hrdata
```

To send incremental ZFS snapshot data, use `zfs send -i`.

```
# zfs send -i hrpool/data@snap1 hrpool/data@snap2 > \
/backup/hrdata
```

ORACLE

Receiving ZFS Snapshot Data

The `zfs receive` command:

- Is used to receive ZFS snapshot data
- Receives the snapshot from:
  - Another pool
    - On the same system
    - On a different system
  - A file or device
- Creates a snapshot whose content is specified in the stream that is provided on standard input
- Has the alias `recv`

Note: If a full stream is received, a new file system is created as well.

ORACLE

Receiving ZFS Snapshot Data

Remember the following key points when you receive a file system snapshot:

- The snapshot and the file system are received.
- The file system and all the descendant file systems are unmounted.
- The file systems are inaccessible while they are being received.
- The original file system to be received must not exist while it is being transferred.
- If a conflicting file system name exists, `zfs rename` can be used to rename the file system.
- Use the `zfs send -R` option to send a replication stream of all descendant file systems. When the replication stream is received, all properties, snapshots, descendant file systems, and clones are preserved.

Receiving ZFS Snapshot Data

To receive a ZFS file system snapshot, use `zfs receive` followed by the snapshot name and the location from which you want to retrieve the file system.

```
# zfs send hrpool/jobdesc@1215 > /bkups/jobdesc.121511
# zfs receive hrpool/jobdesc2 < /bkups/jobdesc.121511
# zfs rename hrpool/jobdesc hrpool/jobdesc.old
# zfs rename hrpool/jobdesc2 hrpool/jobdesc
```

Remote Replication of ZFS Snapshot Data

To remotely copy snapshot data from one system to another system, use `zfs send` and `zfs receive`.

```
# zfs send hrpool/report@today | ssh newsys zfs recv sandbox/restfs
```

ORACLE

Practice 4-2 Overview: Using ZFS Snapshots for Backup and Recovery

This practice covers the following topics:

- Creating ZFS snapshots
- Sending ZFS snapshot data
- Receiving and saving snapshot data
- Rolling back to recover lost data

Agenda

- Planning for data storage configuration and backup
- Managing data redundancy with mirrored storage pools
- Administering data backup and restore by using ZFS snapshots
- Managing data storage space with ZFS file system properties
- Troubleshooting ZFS failures

Managing Data Storage Space with ZFS File System Properties

This section covers the following topics:

- Mounting and sharing ZFS file systems
  - Overriding a default ZFS mount point
  - Managing legacy mount points
  - Sharing and unsharing ZFS file systems
- Setting ZFS quotas and reservations

Overriding Default ZFS Mount Points

- By default, all ZFS file systems are mounted:
  - By ZFS at boot by using an SMF service
  - Under `/path`, where *`path`* is the name of the file system
- The default mount point can be overridden by setting the `mountpoint` property to a specific path by using `zfs set`.
- When a default mount point is overridden, ZFS automatically:
  - Creates the mount point if needed
  - Mounts the file system to the new mount point

Note: There is no need to edit the `/etc/vfstab` file.

`mountpoint` Property

- Is inherited
- Can be set to `none` to prevent the file system from being mounted automatically
- Can be set to `legacy` to manage through legacy mount interfaces
  - This setting prevents ZFS from automatically mounting and managing the file system.
  - The file system must be managed by using legacy tools (`mount`, `umount`) and `/etc/vfstab`.

Note: To determine whether a file system can be mounted, check the value of the `canmount` property and the `mountpoint` property.

ORACLE

Automatic Mount Point Behavior

- When changing from a `legacy` or `none` mount point, ZFS automatically mounts the file system.
- If ZFS is managing the file system but is currently unmounted, and if the `mountpoint` property is changed, the file system remains unmounted.
- When the `mountpoint` property is changed, ZFS automatically reassigns the mount point.
- Mount point directories are created as needed.
- A dataset whose `mountpoint` property is not legacy is managed by ZFS.

Note: A default mount point can be created by using `zpool create -m`.

ORACLE

Legacy Mount Point Behavior

- Legacy file systems must be managed by using the `mount` and `umount` commands and the `/etc/vfstab` file.
- ZFS does not automatically mount legacy file systems on boot.
- The ZFS `mount` and `unmount` commands do not operate on legacy file systems.
- To automatically mount a legacy file system on boot, you must add an entry to the `/etc/vfstab` file.

Managing Legacy Mount Points

To manage ZFS file systems with legacy tools, use `zfs set` followed by `mountpoint=legacy` and the file system name.

```
# zfs set mountpoint=legacy hrpool/home/reports
```

To mount the file system, use `mount -F` followed by the file system type, the file system name, and a mount point.

```
# mount -F zfs hrpool/home/reports /mnt
```

ORACLE

`share.nfs` Property: Introduction

- ZFS automatically shares file systems by using the `share.nfs` property.
- The `share.nfs` property is a comma-separated list of options to pass to the `share` command.
  - The value `on`:
    - Is an alias for the default share options
    - Provides read/write permissions to anyone
  - The value `off` indicates that the file system is no longer shared.
- All file systems whose `share.nfs` property is not `off` are shared during boot.

Setting the `share.nfs` Property

To share a new file system, use the `zfs set` syntax (similar to the following example):

```
# zfs set share.nfs=on hrpool/home/reports
```

- The `share.nfs` property is inherited.
- Setting `share.nfs` to `off`:
  - Prevents a file system from automatically being shared
  - Allows the file system to be shared by using legacy methods

ORACLE

Unsharing ZFS File Systems

To explicitly unshare a file system, use `zfs unshare` followed by the file system name or mount point.

```
# zfs unshare hrpool/home/reports
```

To unshare all ZFS file systems, use `zfs unshare` with the `-a` option.

```
# zfs unshare -a
```

Sharing ZFS File Systems

To share a file system, use `zfs share` followed by the file system name.

```
# zfs share hrpool/home/reports
```

To share all ZFS file systems, use `zfs share` with the `-a` option.

```
# zfs share -a
```

Setting ZFS Quotas and Reservations

This section covers the following topics:

- Setting quotas on ZFS file systems
  - User quotas
  - Group quotas
- Setting default user and group quotas
- Displaying user and group space usage
- Removing user and group quotas
- Setting reservations on ZFS file systems

`quota`, `reservation`, `refquota`, `refreservation`, and `used` Properties

Property	Description
`quota`	Sets a limit on the pool space used by a file system
`refquota`	Sets the amount of disk space that a dataset can consume
`reservation`	Guarantees a specified amount of space for a file system from a pool
`refreservaton`	Sets the minimum amount of disk space that is guaranteed to a dataset, not including descendants (such as snapshots and clones)
`used`	Read-only property that identifies the amount of disk space consumed by a dataset and all its descendants

Setting Quotas for ZFS File Systems

To set a quota on a file system, use `zfs set` followed by `quota=`, the space amount, and the file system name.

```
# zfs set quota=10g hrpool/home/reports
```

To display the quota setting for a file system, use `zfs get` followed by `quota` and the file system name.

```
# zfs get quota hrpool/home/reports
NAME                 PROPERTY       VALUE    SOURCE
hrpool/home/reports  quota          10g      local
```

Note: The quota cannot be less than the current dataset usage.

Setting Quotas for ZFS File Systems

To limit the amount of disk space that a dataset can consume, use `zfs set` followed by `refquota=`, the space amount, and the dataset name.

```
# zfs set refquota=10g hrstaff/tsmith
# zfs list -t all -r hrstaff
NAME                          USED  AVAIL  REFER  MOUNTPOINT
hrstaff                       150M  66.8G    32K  /hrstaff
hrstaff/tsmith                150M  9.85G   150M  /hrstaff/tsmith
hrstaff/tsmith@yesterday         0      -   150M  -
# zfs snapshot hrstaff/tsmith@today
# zfs list -t all -r hrstaff
hrstaff                       150M  66.8G    32K  /hrstaff
hrstaff/tsmith                150M  9.90G   100M  /hrstaff/tsmith
hrstaff/tsmith@yesterday     50.0M      -   150M  -
hrstaff/tsmith@today             0      -   100M  -
```

Setting a User Quota on a ZFS File System

To set a user quota on a file system, use `zfs set` followed by `userquota@<name>=`, the space amount, and the file system name.

```
# zfs create finance/tax
# zfs set userquota@rsmart=10g finance/tax
```

To display the user quota setting for a file system, use `zfs get` followed by `userquota@<name>` and the file system name.

```
# zfs get userquota@rsmart finance/tax
NAME                PROPERTY            VALUE      SOURCE
finance/tax         userquota@rsmart    10g        local
```

ORACLE

Setting a Group Quota on ZFS File System

To set a group quota on a file system, use `zfs set` followed by `groupquota@<name>=`, the space amount, and the file system name.

```
# zfs create finance/ar
# zfs set groupquota@ar=20GB finance/ar
```

To display the group quota setting for a file system, use `zfs get` followed by `groupquota@<group>` and the file system name.

```
# zfs get groupquota@ar finance/ar
NAME                PROPERTY            VALUE     SOURCE
finance/ar          groupquota@ar       20G       local
```

ORACLE

Setting Default User and Group Quotas

- Default user or group quota is applied automatically for anyone who does not have a specific quota defined.
- Default user and group quotas are not inheritable to descendant file systems.
- Example
  - You can set a default user or group quota on a file system by:

```
# zfs set defaultuserquota=30gb students/labstaff/admindata
# zfs set defaultgroupquota=120g students/math
```

Displaying User and Group Space Usage

To display general user space usage, use `zfs userspace` followed by the file system name.

```
# zfs userspace finance/tax
TYPE          NAME      USED      QUOTA
POSIX User    root      227M      none
POSIX User    rsmart    455M      10g
```

To display general group space usage, use `zfs groupspace` followed by the file system name.

```
# zfs groupspace finance/ar
TYPE          NAME      USED      QUOTA
POSIX Group   root      217M      none
POSIX Group   ar        217M      20G
```

Identifying User and Group Space Usage

To identify individual user space usage, use `zfs userused@<name>` followed by the file system name.

```
# zfs get userused@rsmart finance/tax
NAME                PROPERTY            VALUE     SOURCE
finance/tax         userused@rsmart     455M      local
```

To identify group space usage, use `zfs groupused@<name>` followed by the file system name.

```
# zfs get groupused@ar finance/ar
NAME                PROPERTY            VALUE     SOURCE
finance/ar          groupused@ar        217M      local
```

Removing User and Group Quotas

To remove a user quota, use `zfs set userquota@<name>=none` followed by the file system name.

```
# zfs set userquota@rsmart=none finance/tax
```

To remove a group quota, use `zfs set groupquota@<name>=none` followed by the file system name.

```
# zfs set groupquota@ar=none finance/ar
```

Identifying Reservation Restrictions

- A ZFS *reservation* is an allocation of space from the pool that is guaranteed to be available to a dataset.
- Space cannot be reserved for a dataset if that space is not currently available in the pool.
- The total amount of all outstanding unconsumed reservations cannot exceed the amount of unused space in the pool.
- A dataset can use more space than it has reserved in the following situation:
  - Unreserved space is available in the pool.
  - Its current usage is below its quota.
- A dataset cannot consume space that is reserved for another dataset.

Setting Space Reservations on Datasets and Snapshots

To set a space reservation on a dataset and snapshot, use `zfs set` followed by `reservation`, the space amount, and the file system name.

```
# zfs set reservation=20g finance/ap
# zfs list
NAME            USED     AVAIL     REFER    MOUNTPOINT
finance         20.0G    13.2G     19K      /finance
finance/ap      10g      33.2G     18K      /finance/ap
```

Setting a Space Reservation on a Dataset

To set a space reservation on a specific dataset, use `zfs set` followed by `refreservation=`, the space amount, and the file system name.

```
# zfs set refreservation=10g finance/ap
# zfs list
NAME            USED    AVAIL    REFER    MOUNTPOINT
finance         10.0G   23.2G    19K      /finance
finance/ap      10g     33.2G    18K      /finance/ap
```

- The space consumed by descendants, snapshots, and clones is not included.
- The setting counts against the parent dataset's quotas and reservation.

Displaying Reservation Values

To see the values of both reservations, use `zfs get` followed by `reservation`, `refreservation`, and the file system name.

```
# zfs get reservation,refreservation finance/ap
NAME              PROPERTY          VALUE     SOURCE
finance/ap        reservation       20G       local
finance/ap        refreservation    10g       local
```

Note: If `refreservation` is set, a snapshot is allowed only if enough free pool space exists outside this reservation to accommodate the current number of referenced bytes in the dataset.

Quiz

To set the amount of disk space that a dataset can consume, which of the following properties should you use?

a. `refreservation`

b. `reservation`

c. `quota`

d. `refquota`

Practice 4-3 Overview: Configuring ZFS Properties

This practice covers the configuration of:

- Quota and reservation properties
- The `share` property
- ZFS compression

Agenda

- Planning for data storage configuration and backup
- Managing data redundancy with mirrored storage pools
- Administering data backup and restore by using ZFS snapshots
- Managing data storage space with ZFS file system properties
- Troubleshooting ZFS failures

Troubleshooting ZFS Failures

- Identifying problems in ZFS
- Repairing:
  - A damaged ZFS configuration
  - A missing device
  - A damaged device
  - Damaged data

Identifying Problems in ZFS

This section covers the following topics:

- Overview of ZFS troubleshooting
- Basic recovery process
- Configuring `syslog` for FMD messages
- Determining problems in a ZFS storage pool
- Interpreting `zpool status` output

Troubleshooting in ZFS: Overview

The `zpool status` command is central to ZFS troubleshooting. This command does the following:

- Analyzes various failures in the system
- Identifies the most severe problem
- Presents:
  - A suggested action
  - A link to a knowledge article for more information
  - Only a single problem

ORACLE

Basic Recovery Process

1. Identify errors through the Fault Management Daemon (FMD) messages displayed in the system console or in `/var/adm/messages`.
2. Find further repair instructions in `zpool status -x`.
3. Repair the failures:
   – Replace the faulted or missing device and bring it online.
   – Restore the faulted configuration or corrupted data from a backup.
4. Verify the recovery by using `zpool status -x`.
5. Back up the restored configuration, if applicable.

ORACLE

Configuring syslog for FMD Messages

1. Create a new file named /var/adm/messages.fmd for Fault Management Daemon to log the device-related messages.
2. Back up the current /etc/syslog.conf file.
3. Edit the /etc/syslog.conf file by entering a new line below the existing line as follows:

```
*.err;kern.debug;daemon.notice;mail.crit          /var/adm/messages
daemon.err                                        /var/adm/messages.fmd
```

4. Restart the syslog service for the new configuration to take effect by using svcadm restart system-log.

Determining Problems in a ZFS Storage Pool

- Use `zpool status -x` to determine if a known problem exists.
- If no bad pools exist, the “all pools are healthy” status is returned.

```
# zpool status -x
all pools are healthy
```

- Without the `-x` flag, the status of all pools (regardless of health) is displayed.

Interpreting `zpool status` Output

Header section

```
# zpool status hrpool
  pool: hrpool
 state: DEGRADED
status: One or more devices has been taken offline by the
        administrator. Sufficient replicas exist for the pool to
        continue functioning in a degraded state.
action: Online the device using 'zpool online' or replace the
        device with 'zpool replace'.
 scrub: none requested
config:
       NAME              STATE       READ   WRITE   CKSUM
       hrpool            DEGRADED       0       0       0
         mirror-0        DEGRADED       0       0       0
           c1t0d0        ONLINE         0       0       0
           c1t1d0        OFFLINE        0       0       0
errors: No known data errors
```

Interpreting `zpool status` Output

Configuration (`config`) field: first section

```
# zpool status hrpool
  pool: hrpool
 state: DEGRADED
status: One or more devices has been taken offline by the
        administrator. Sufficient replicas exist for the pool to
        continue functioning in a degraded state.
action: Online the device using ’zpool online’ or replace the
        device with ’zpool replace’.
 scrub: none requested
config:
       NAME              STATE      READ   WRITE  CKSUM
       hrpool            DEGRADED      0       0      0
         mirror-0        DEGRADED      0       0      0
           c1t0d0        ONLINE        0       0      0
           c1t1d0        OFFLINE       0       0      0

errors: No known data errors
```

Interpreting `zpool status` Output

Configuration (`config`) field: second section

```
# zpool status hrpool
  pool: hrpool
 state: DEGRADED
status: One or more devices has been taken offline by the
        administrator. Sufficient replicas exist for the pool to
        continue functioning in a degraded state.
action: Online the device using ’zpool online’ or replace the
        device with ’zpool replace’.
 scrub: none requested
config:
       NAME              STATE         READ   WRITE   CKSUM
       hrpool            DEGRADED         0       0       0
         mirror-0        DEGRADED         0       0       0
           c1t0d0        ONLINE           0       0       0
           c1t1d0        OFFLINE          0       0       0

errors: No known data errors
```

Determining Problems in a ZFS Storage Pool

ZFS displays `syslog` messages for the following:

- Device state transition
- Data corruption
- Pool failures and device failures

Repairing a Damaged ZFS Configuration

- ZFS maintains a cache of active pools and their configuration on the root file system in `/etc/zfs/zpool.cache`.
- To recover the configuration, you can:
  - Export the pool (if it is visible at all)
  - Reimport it

ORACLE

Repairing a Missing Device

If a device cannot be opened, `UNAVAIL` is displayed in the `zpool status` output.

```
# zpool status hrpool
  pool: hrpool
state: DEGRADED
status: One or more devices could not be opened.  Sufficient replicas exist for
        the pool to continue functioning in a degraded state.
action: Attach the missing device and online it using 'zpool online'.
   see: http://www.sun.com/msg/ZFS-8000-2Q
scrub: none requested
config:

        NAME        STATE     READ WRITE CKSUM
        hrpool        DEGRADED     0     0     0
          mirror-0  DEGRADED     0     0     0
            c1t0d0  ONLINE       0     0     0
            c1t1d0  UNAVAIL      0     0     0  cannot open

errors: No known data errors
```

Repairing a Missing Device

- An `UNAVAIL` status means that:
  - The device could not be opened when the pool was first accessed
  - The device has since become unavailable
- If the device causes a top-level virtual device to be unavailable, nothing in the pool can be accessed.
- To restore normal operation, reattach the device to the system.

Reattaching a Device

Device Type	Action
Network-attached drive	Restore connectivity.
USB or other removable media	Reattach to the system.
Local disk	Determine if it is a disk problem or a controller problem.

Repairing a Missing Device

- ZFS might not automatically detect device availability if:
  - The pool was degraded
  - The device was replaced while the system was up
- Use `zpool online` to notify ZFS that the device is now available and ready to be reopened.

```
# zpool online hrpool c0t1d0
```

Repairing a Damaged Device

This section covers the following topics:

- Determining the cause of device failure
- Clearing transient errors
- Replacing a device in a ZFS storage pool
- Viewing resilvering status

Determining the Cause of Device Failure

Possible causes of device failure:

- Bit rot
- Misdirected reads or writes
- Administrator error
- Temporary outage
- Bad or flaky hardware
- Offlined device

Determining the Cause of Device Failure

Use `zpool status -v` to examine the error counts.

```
# zpool status -v
  pool: hrpool
 state: UNAVAIL
status: One or more devices are faulted in response to IO failures.
action: Make sure the affected devices are connected, then run 'zpool
        clear'.
   see: http://www.sun.com/msg/ZFS-8000-HC
 scrub: scrub completed after 0h0m with 0 errors on Tue Oct  4 13:08:42 2011
config:

        NAME        STATE     READ WRITE CKSUM
        hrpool      UNAVAIL      0     0     0  insufficient replicas
          c1t0d0    ONLINE       0     0     0
          c1t1d0    UNAVAIL      4     1     0  cannot open

errors: Permanent errors have been detected in the following files:

/hrpool/data/aaa
/hrpool/data/bbb
/hrpool/data/ccc
```

Determining the Cause of Device Failure

Check the system log:

- If there are a large number of SCSI or Fibre Channel driver messages, the system has serious hardware problems.
- If no `syslog` messages are generated, the damage is likely to be transient.

Clearing Transient Errors

- To clear the error counters for RAID-Z or mirrored devices and to clear errors associated with the device, use `zpool clear` *`poolname devicename`*.

```
# zpool clear hrpool c1t0d0
```

- To clear errors associated with the virtual devices in the pool and to clear data error counts associated with the pool, use `zpool clear` *`poolname`*.

```
# zpool clear hrpool
```

Replacing a Device in a ZFS Storage Pool

- For a device to be replaced, the device must be part of a replicated configuration.
- The disk is part of a replicated configuration. Therefore, sufficient replicas from which to retrieve good data must exist.
- A device cannot be safely replaced if:
  - The loss of a device causes the pool to become faulted
  - The device contains too many data errors in an unreplicated configuration

ORACLE

Replacing a Device in a ZFS Storage Pool

- To replace a device with a new device in the same location, use `zpool replace` *`poolname devicename`*.

```
# zpool replace hrpool c1t0d0
```

- To replace a damaged device with a different device, use `zpool replace` *`poolname devicename devicename`*.

```
# zpool replace hrpool c1t0d0 c2t0d0
```

ORACLE

Viewing Resilvering Status

Resilvering:

- Is the process of moving data from one device to another
- Is monitored by using `zpool status`
- Resilvers only the minimum amount of necessary data
- Is interruptible and safe

Scrubbing

- Examines all data to discover silent errors due to hardware faults or disk failure
- Supports automatic repair of damage discovered during the scrub
- Is monitored by using `zpool status`
- Cannot be run if:
  - Another scrub is already in progress
  - A resilver is in progress
- Is begun by using `zpool scrub` *`pool`*

Repairing Damaged Data

This section covers the following topics:

- Overview of data corruption
- Identifying the type of data corruption
- Repairing a corrupted file or directory
- Repairing damage to a ZFS storage pool

Data Corruption: Overview

- Data corruption can occur if:
  - The pool is not replicated
  - Corruption occurred while the pool was degraded
  - An unlikely series of events caused the corruption of multiple copies of a piece of data
- Two basic types of data can be corrupted:
  - Pool metadata
  - Object data

ORACLE

Identifying the Type of Data Corruption

Use `zpool status -v` *`poolname`* to identify the type of data corruption.

Example of object data corruption:

```
# zpool status -v hrpool
  pool: hrpool
 state: ONLINE
status: One or more devices has experienced an error resulting in data
        corruption. Applications may be affected.
action: Restore the file in question if possible. Otherwise restore
        the entire pool from backup.
   see: http://www.sun.com/msg/ZFS-8000-8A
<output omitted>
errors: Permanent errors have been detected in the following files:
/hrpool/data/abc
/hrpool/data/def.txt
/hrpool/data/ghi.txt
```

ORACLE

Identifying the Type of Data Corruption

Example of pool metadata corruption:

```
# zpool status -v sales
pool: sales
   id: 1422736890544688191
 state: FAULTED
status: The pool metadata is corrupted.
action: The pool cannot be imported due to damaged devices or data.
   see: http://www.sun.com/msg/ZFS-8000-72
config:
         sales FAULTED corrupted data
         c1t1d0 ONLINE
```

Repairing a Corrupted File or Directory

- The system may still be able to function.
- Any damage is effectively unrecoverable.
- No good copies of the data exist anywhere on the system.
- If the data is valuable, restore the affected data from backup.
- If the damage is in a file data block, remove the file.

Repairing Damage to a ZFS Storage Pool

If you cannot open or import a pool because of damage to the pool metadata, you must perform one of the following actions:

- Attempt to recover the pool by using `zpool clear -F` *`poolname`* or `zpool import -F` *`poolname`*.
  - An attempt is made to roll back to an operational state.
  - To review a damaged pool and see recommended recovery steps, use `zpool status`.
- Restore the pool and all its data from a backup copy.
  - Save the pool configuration as displayed in `zpool status`.
  - Destroy the pool by using `zpool destroy -f` *`poolname`*.
  - Keep a file of the dataset layout and local property settings.
  - Reconstruct the complete pool configuration.
  - Populate the data by using the backup / restore strategy.

ORACLE

Practice 4-4 Overview: Troubleshooting ZFS Failures

This practice covers the troubleshooting of:

- ZFS device issues
- ZFS data errors in a mirror pool

Summary

In this lesson, you should have learned how to:

- Plan for data storage configuration and backup
- Manage data redundancy with mirrored storage pools
- Back up and restore data by using ZFS snapshots
- Manage data storage space with ZFS file system properties
- Troubleshoot ZFS failures

5

Configuring the Network

ORACLE

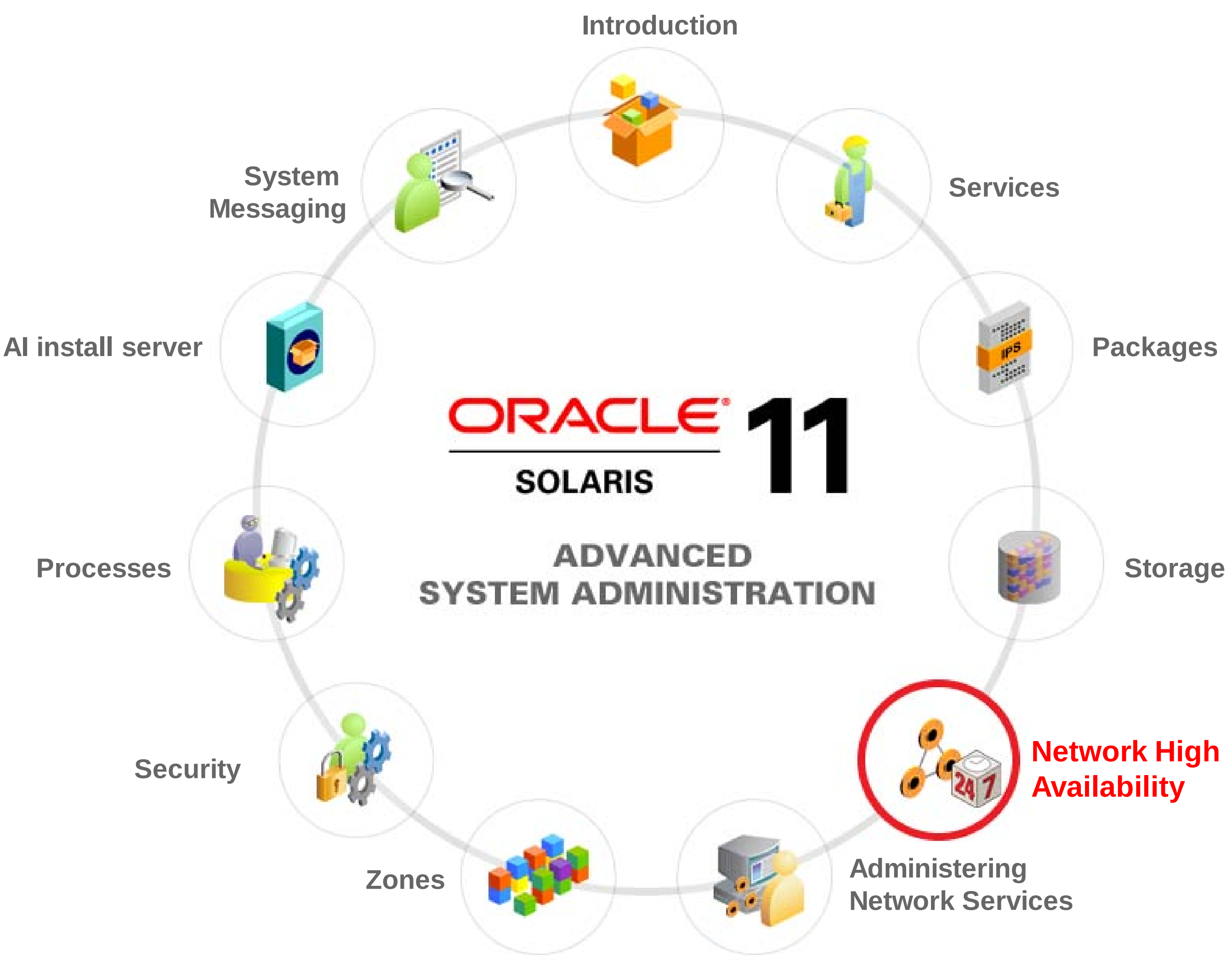
Objectives

After completing this lesson, you should be able to configure:

- A virtual switch
- Link aggregation for high performance
- IPMP for IP high availability
- Packet Filter to control network access

ORACLE

Job Workflow



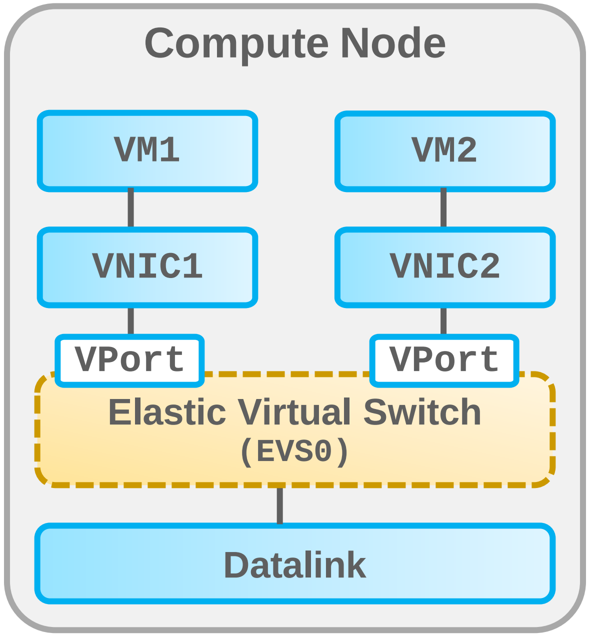
Agenda

- Configuring virtual switches
- Configuring link aggregation for high performance
- Configuring IPMP for IP high availability
- Configuring Packet Filter to control network access

Elastic Virtual Switch: Overview

An elastic virtual switch (EVS):

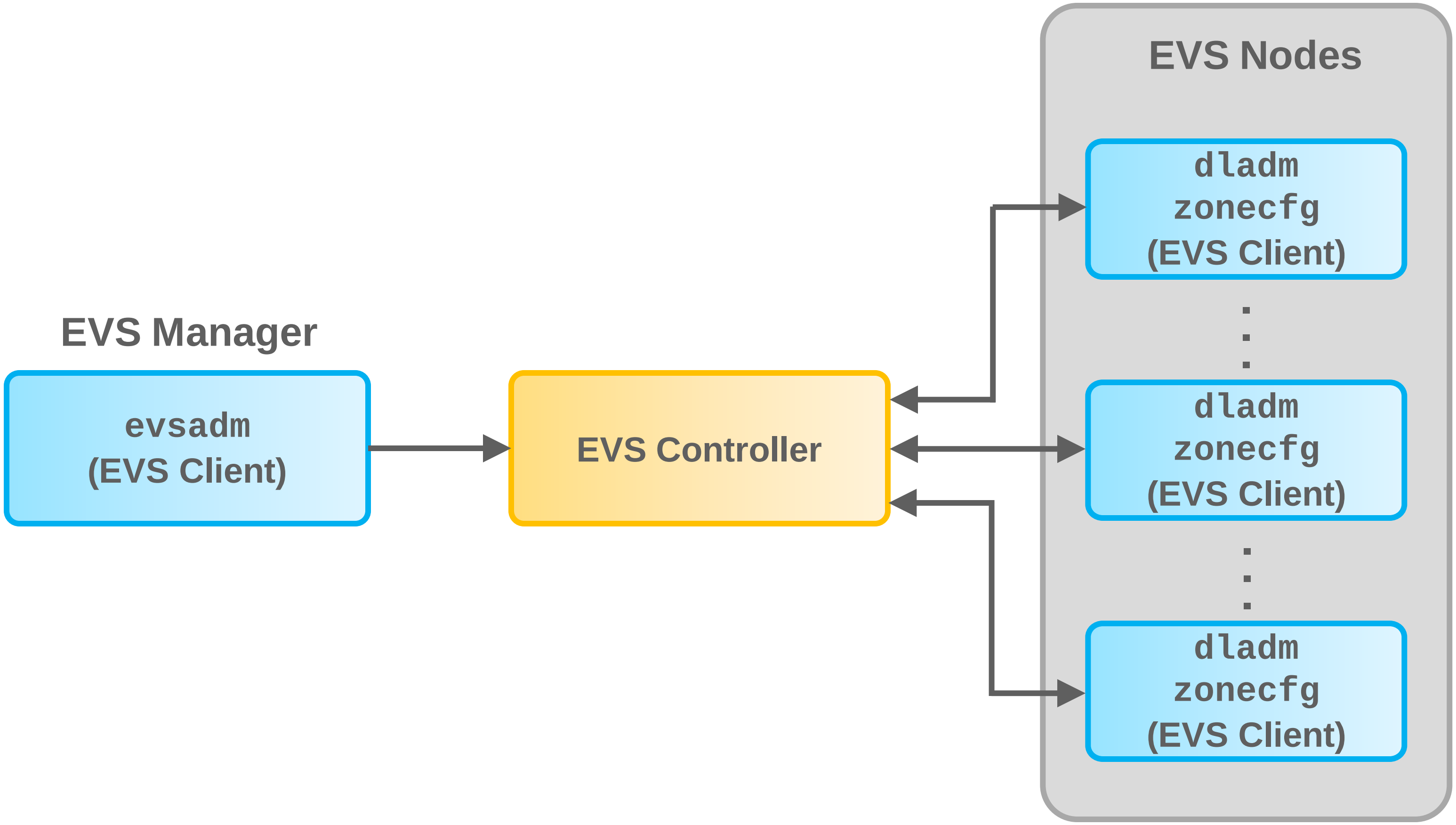
- Is an entity that represents explicitly created virtual switches that belong to the same Layer 2 (L2) segment
- Enables you to create and administer a virtual switch that spans one or more physical machines (nodes)
- Provides network connectivity between VMs connected to it from anywhere in the network



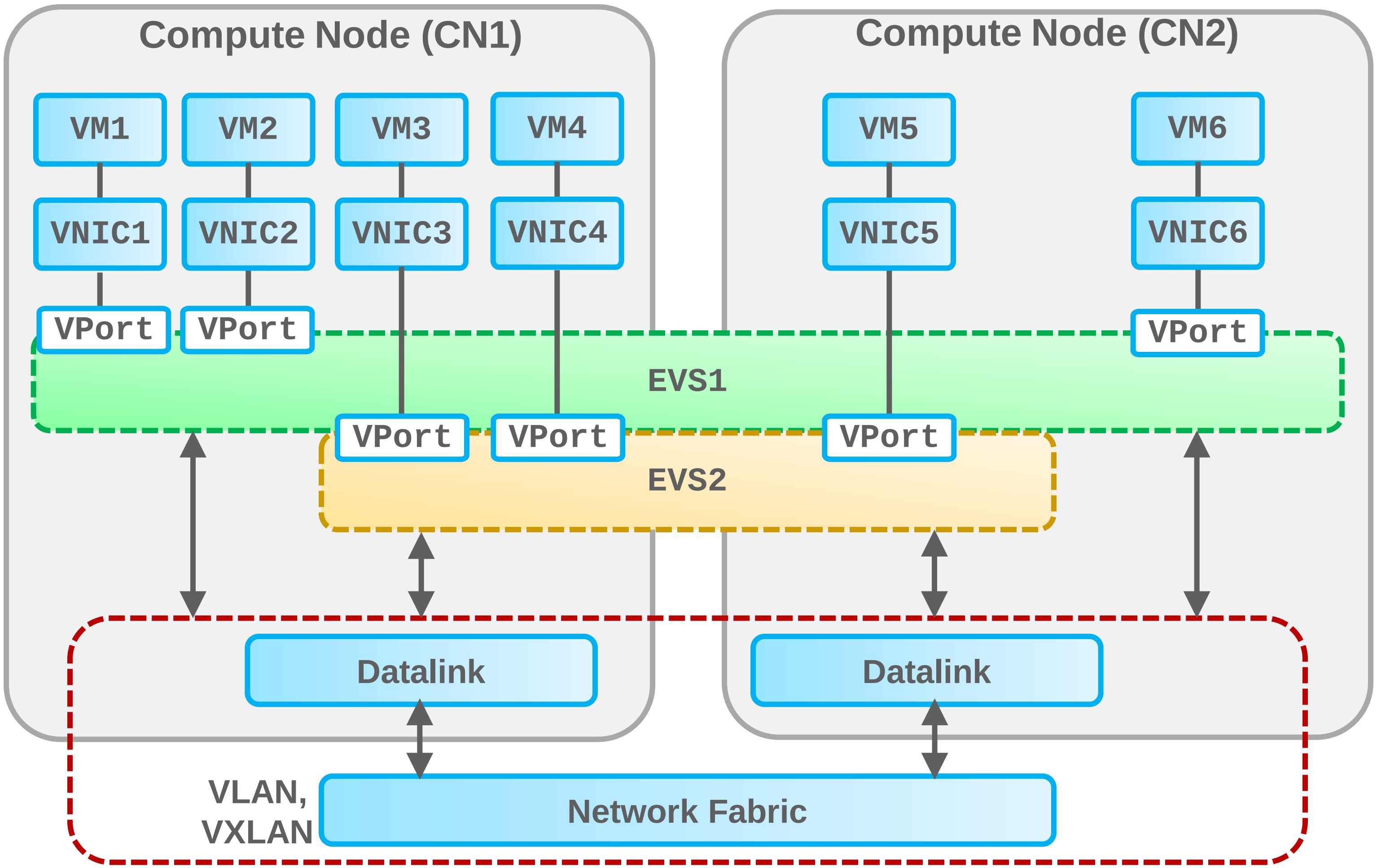
Benefits of Using the EVS Feature

- Creates a virtual network between VMs that are on multiple servers, thus providing network connectivity
- Supports addition of virtual ports with custom SLAs or profiles
- Provides network isolation by using VLANs or VXLANs
- Supports multitenant virtual networks that share the same underlying infrastructure
- Provides centralized management of:
  - MAC address and IP address for the virtual ports
  - SLAs on a per-virtual-switch or per-virtual-port basis
  - Monitoring the runtime network traffic statistics of the virtual ports
- Is integrated with Oracle Solaris Zones and Oracle Solaris Kernel Zones

EVS Components



EVS: Example


Compute Node (CN1)
Compute Node (CN2)
VM1
VM2
VM3
VM4
VM5
VM6
VNIC1
VNIC2
VNIC3
VNIC4
VNIC5
VNIC6
VPort
VPort
VPort
EVS1
VPort
VPort
VPort
EVS2
Datalink
Datalink
VLAN,
VXLAN
Network Fabric

EVS Administrative Commands

Commands	Description
`evsadm`	You use the `evsadm` command to communicate with the EVS controller and manage the elastic virtual switch, IPnet, and VPorts.
`evsstat`	You use the `evsstat` command to display the network traffic statistics for all the VPorts in a data center or for all the VPorts of the specified elastic virtual switch.
`dladm`	You can administer the VNICs connected to an elastic virtual switch by using the following `dladm` commands: • **`create-vnic`:** Enables you to create a VNIC and specify the elastic virtual switch name to which you must connect the VNIC. Optionally, you can specify the VPort of the elastic virtual switch. • **`show-vnic`:** Enables you to display the EVS information for a specific VNIC. The output of the `dladm show-vnic` command also displays the fields `TENANT`, `EVS`, and `VPORT`. However, these fields are not visible from within a zone.
`zonecfg`	You use the enhanced `zonecfg` command to configure a zone's VNIC `anet` resource for an elastic virtual switch.

Planning an EVS Configuration

1. Install the mandatory EVS packages on the EVS controller, EVS manager, and EVS nodes.
2. Set up EVS authentication with the preshared public key for `evsuser`:
   - From the EVS manager to the EVS controller
   - From the EVS controller to each EVS node
   - From each EVS node to the EVS controller
3. Specify the EVS controller by setting the `controller` property. You must specify the host name or IP address of the EVS controller on the EVS nodes, EVS manager, and EVS controller.

ORACLE

Planning an EVS Configuration

4. Configure the EVS controller, during which you must consider the following:
   - Determine whether you are implementing the elastic virtual switch by using a VLAN, VXLAN, or both.
     - If you use a VLAN, you must set the properties `uplink-port` and `vlan-range`.
     - If you use a VXLAN, you must set the properties `vxlan-range` and `uplink-port` or `vxlan-addr`.
   - If the compute nodes do not have the same datalink, then for every compute node, you must specify the datalink for the `uplink-port` property.
5. Configure the elastic virtual switch by using the EVS manager.
6. Create VNICs on the EVS nodes and connect the VNICs to the elastic virtual switch.

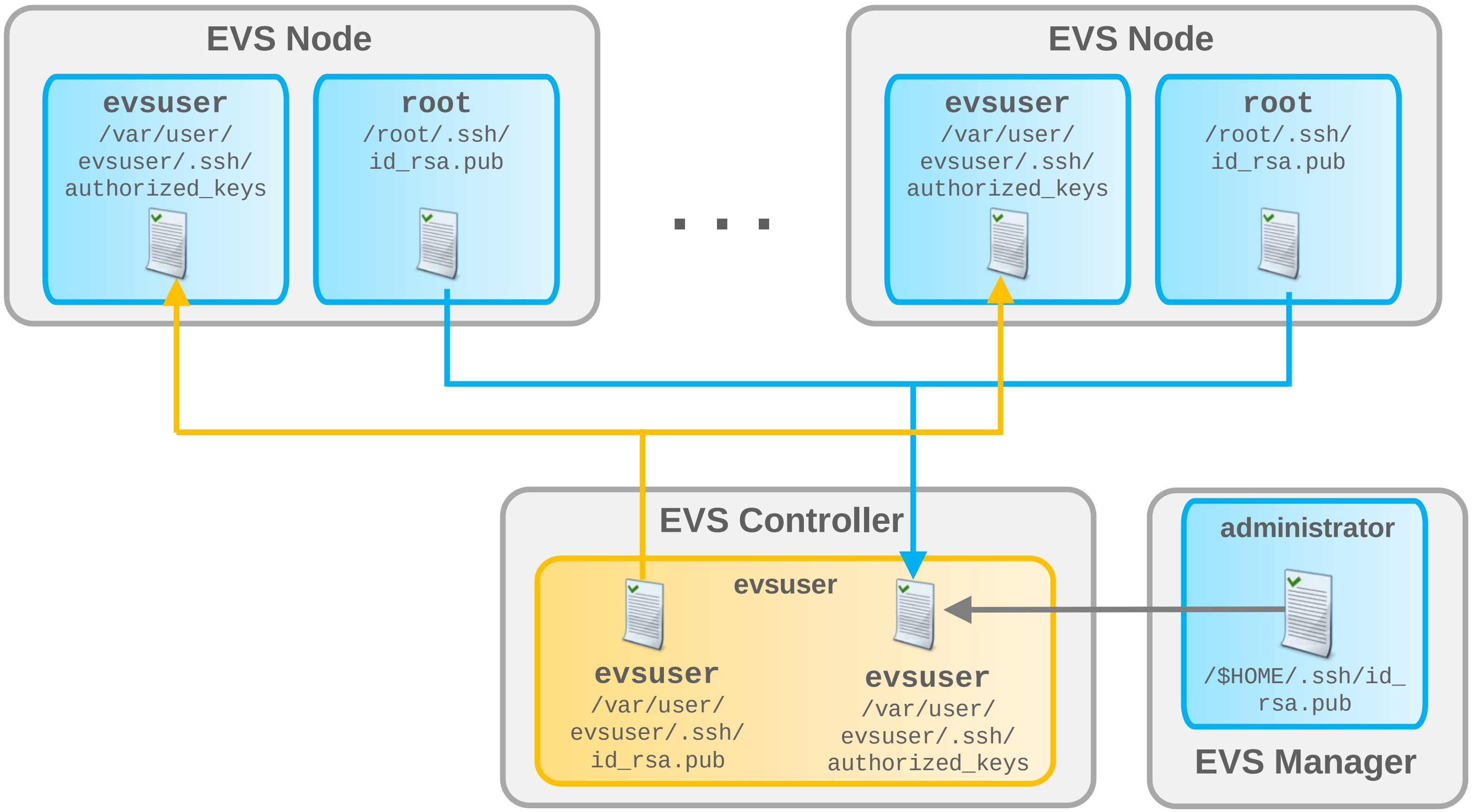
ORACLE

Installing the Mandatory EVS Packages

You must install the following packages before using EVS:

Packages	Description
`pkg:/service/network/evs`	You must install this core package on the EVS manager, EVS controller, and EVS nodes. This package contains the following components: • `evsadm` • `evsstat` • `svc:/network/evs:default`
`pkg:/system/management/rad/module/rad-evs-controller`	You must install this package only on the system that acts as an EVS controller. This package contains the SMF service named `svc:/network/evs-controller:default`.

Setting Up SSH Authentication



Note: The assumption here is that the `controller` property is set to `ssh://evsuser@evs-controller.example.com` on each host.

Configuring an EVS Controller

1. Set the EVS controller.

```
# evsadm set-prop -p controller=[value[...,]]
```

2. Display the configured EVS controller.

```
# evsadm show-prop [[-c] -o field[,...]] [-p prop[,...]]
```

3. Set the properties for the EVS controller.

```
# evsadm set-controlprop [-h host] -p prop=[value[...,]]
```

4. Display the properties of the EVS controller.

```
# evsadm show-controlprop [[-c] -o field[,...]] [-p prop[,...]]
```

ORACLE

Configuring an EVS

1. Create an elastic virtual switch.

```
# evsadm create-evs [-T tenant-name] [-p {prop=value[,...]}[,..]] EVS-switch-name
```

2. Add an IPnet to the elastic virtual switch.

```
# evsadm add-ipnet [-T tenant-name] -p subnet=value[{,prop=value[,...]}[,...]]  \
EVS-switch-name/IPnet-name
```

3. Add a VPort to the elastic virtual switch.

```
# evsadm add-vport [-T tenant-name] [-p {prop=value[,...]}[,...]] \
EVS-switch-name/VPort-name
```

4. Display the configured elastic virtual switch.

```
# evsadm
```

ORACLE

Creating VNICs for an Elastic Virtual Switch

1. Configure a VNIC for an elastic virtual switch.

```
# dladm create-vnic -t -c EVS-switch-name[/VPort-name] \
[-T tenant-name] VNIC-name
```

2. Display information about the VNICs that are connected to an elastic virtual switch.

```
# dladm show-vnic -c
```

EVS and Zones

- Oracle Solaris Zones and Oracle Solaris Kernel zones support the EVS feature.
- Kernel zones support VNICs that you create for EVS.
- The VNIC that is created in the Kernel zone works only if the VNIC uses the factory MAC addresses that are associated with the `zvnet` driver.
- In the Kernel zone, you can connect the VNIC to the VPort that is created by using the `evsadm add-vport` command.

EVS and Zones

- For an `anet` resource that connects to an EVS with the `evs` and `vport` properties set, the properties of that `anet` resource are encapsulated in the `evs` and `vport` pair.
- You can also set the `tenant` resource if you have configured a tenant for an EVS.
- You can set the following properties for an EVS `anet` resource:
  - `linkname`
  - `evs`
  - `vport`
  - `configure-allowed-address`

Creating a VNIC `anet` Resource or an EVS

This example shows you how to create a zone that has a VNIC `anet` resource `evszone/net1`, which is connected to `ORA` and `vport0` of the tenant `tenantA`.

```
# zonecfg -z evszone
Use 'create' to begin configuring a new zone
zonecfg:evszone> create
create: Using system default template 'SYSdefault'
zonecfg:evszone> set zonepath=/export/zones/evszone
zonecfg:evszone> set tenant=tenantA
zonecfg:evszone> add anet
zonecfg:evszone:net> set evs=ORA
zonecfg:evszone:net> set vport=vport0
zonecfg:evszone:net> end
zonecfg:evszone> exit
# zoneadm -z evszone install
# zoneadm -z evszone boot
# dladm show-vnic -c
LINK         TENANT    EVS VPORT    OVER   MACADDRESS        VIDS
evszone/net1 tenantA   ORA vport0   net2   2:8:20:89:a1:97   200
```

ORACLE

Quiz

You do not need to set up SSH authentication between the EVS manager and EVS nodes.

a. True

b. False

Quiz

Which of the following commands should you use to administer EVS clients? (Choose two.)

a. `zonecfg`

b. `evsadm`

c. `dladm`

d. `evsstat`

Practice 5-1 Overview: (Demonstration) Configuring EVS

In this practice, you watch an EVS configuration demonstration and observe the following processes:

- Setting up SSH authentication
- Configuring the EVS controller, EVS manager, and EVS nodes
- Configuring nonglobal zones to use elastic virtual switches

Note: This practice comprises only the demonstration.

Agenda

- Configuring virtual switches
- Configuring link aggregation for high performance
- Configuring IPMP for IP high availability
- Configuring Packet Filter to control network access

Importance of Network High Availability

Network high availability is required to ensure that:

- Network needs of the business and the user community are supported
- Network communications remain uninterrupted
- Network performance is good

What Does 99.99% Mean?

- Availability is usually expressed as a percentage of uptime in a given year, and is referred to as 5 nines, 6 nines, and so on.
- Uptime is a function of down time and recovery time.
- To achieve high availability, you must have low down time and low recovery time.
- So what does 99.99% mean?
  - 99.99% (referred to as 4 nines), means the following:
    - `4 nines -> (365×24) - .9999(365×24) = 8760 - 8759.124 = 0.876 hours = 52 min and 30 secs`
  - 99.99% implies a down time of 52.30 minutes per year.

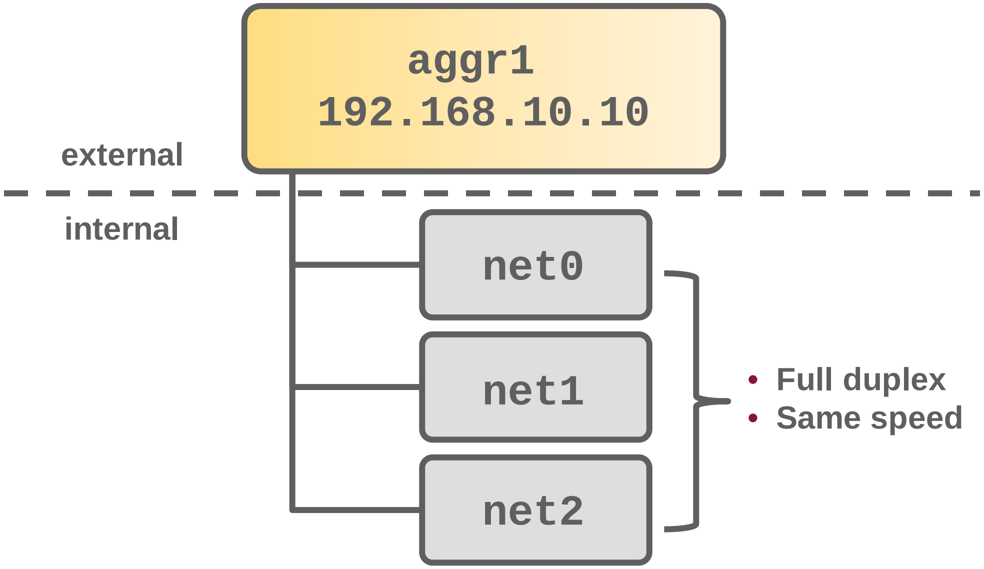
ORACLE

High Availability: Overview

- The term *high availability* (HA) refers to a state in which a point of failure is instantly taken over by a redundant system to ensure business continuity.
- HA is architected into domains such as server, storage, applications, and network.
  - In the network domain, HA can be implemented at various levels such as link, IP, and router.
- The following are some of the HA features of Oracle Solaris 11:
  - Link aggregation
  - IP Network Multipathing (IPMP)

Link Aggregation: Overview

- Link aggregation enables multiple network interface cards (NICs) to be grouped into a single logical interface.
- Link aggregations are useful for increasing bandwidth as well as providing HA.
  - Links must be of the same speed, full duplex, and point-to-point.
  - You use the `dladm` command.



Link Aggregation Types

Based on single or multiple switch capability, link aggregation can be of two types:

- **Trunk aggregation:** Works only with a single switch
- **Datalink Multipathing (DLMP) aggregation:** Spans multiple switches
  - For DLMP aggregation, no switch-side configurations are required.
  - Switches are therefore unaware of the link aggregation and treat each port individually.

ORACLE

Aggregation Modes and Switches

LACP switch modes:

- **Off:** Default mode; no LACPDUs
- **Active:** LACPDUs at specified regular intervals
- **Passive:** LACPDUs only when received from switch

Load Balancing and Aggregation Policies

In policy making, determination of the outgoing link is done by hashing the specific header of each packet:

- **L2 (Networking):** MAC header
- **L3 (Addressing):** IP header
- **L4 (Communication):** TCP/UDP or other ULP header

Commands to Administer Link Aggregation

Command	Description
`dladm create-aggr`	Create a link aggregation.
`dladm add-aggr`	Add a link to an aggregation.
`dladm show-aggr -x`	Display link aggregation details.
`dladm delete-aggr`	Delete a link aggregation.
`dladm remove-aggr`	Remove a link from an aggregation.
`dladm modify-aggr`	Switch between link aggregation types or modify a trunk aggregation.

ORACLE

Preparing for Link Aggregation

Before configuring the link aggregation:

1. Make sure that the links to be combined are full-duplex and point-to-point, and that they operate at identical speeds.
2. Use the `dladm show-link` command to verify state.

   Note: If an IP interface is created over the datalink, remove the IP interface first.

```
# dladm show-link
LINK               CLASS   MTU     STATE           OVER
net0               phys    1500    unknown         --
net1               phys    1500    unknown         --
net2               phys    1500    unknown         --
net3               phys    1500    unknown         --
```

Creating Link Aggregation

Use the following commands to create and display link aggregation:

- `dladm create-aggr`
- `dladm show-aggr`

```
# dladm create-aggr -l net0 -l net1 aggr1
# dladm show-link
LINK      CLASS     MTU  STATE   OVER
net0      phys      1500 up      --
net1      phys      1500 up      --
net2      phys      1500 unknown --
net3      phys      1500 unknown --
aggr1     aggr      1500 up      --     net0 net1
# dladm show-aggr
LINK     MODE  POLICY  ADDRPOLICY  LACPACTIVITY     LACPTIMER
aggr1    trunk L4      auto        off              short
```

Modifying Link Aggregation

Use the following commands to modify link aggregation:

- `dladm modify-aggr`
- `dladm add-aggr`
- `dladm remove-aggr`

```
# dladm modify-aggr --policy=L3 aggr1
# dladm add-aggr -l net2 -l net3 aggr1
# dladm remove-aggr -l net0 aggr1
```

ORACLE

Deleting Link Aggregation

Use the following command to delete aggregation:

`dladm delete-aggr`

```
# dladm delete-aggr aggr1
```

Creating a DLMP Aggregation

```
# dladm create-aggr -m dlmp -l net0 -l net1 -l net2 -l net3 speedway0
# dladm show-link
LINK      CLASS     MTU      STATE   OVER
net0      phys      1500     up      --
net1      phys      1500     up      --
net2      phys      1500     up      --
net3      phys      1500     up      --
speedway0 aggr      1500     up      net0 net1 net2 net3
# dladm show-aggr
LINK       MODE  POLICY   ADDRPOLICY  LACPACTIVITY  LACPTIMER
speedway0  dlmp  --       --          --            --
```

Quiz

Which of the following commands should you use to display the link aggregation details?

a. `dladm show-link –x`

b. `dladm show-aggr –x`

c. `dladm list-aggr -x`

Practice 5-2 Overview: Configuring a Link Aggregation

This practice covers the following topics:

- Creating a link aggregation
- Removing a link aggregation

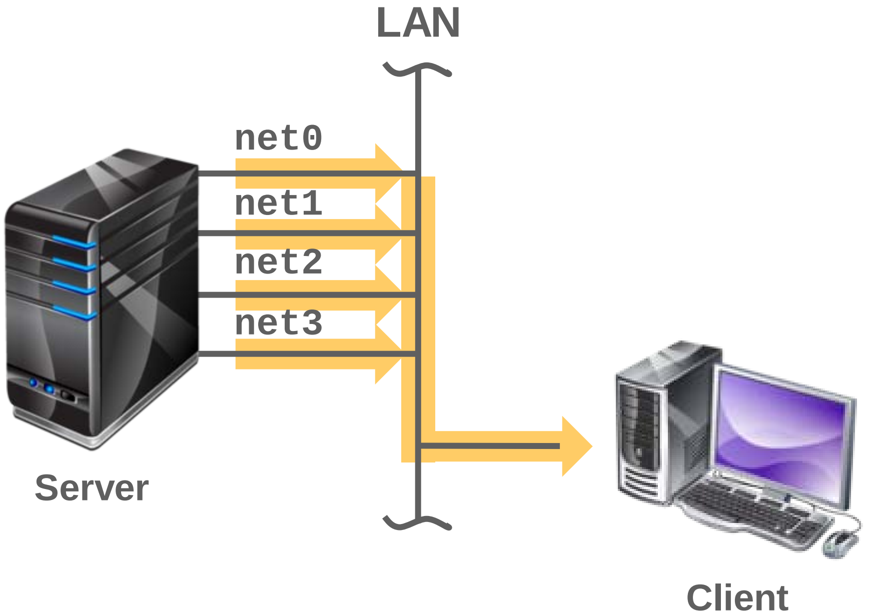
ORACLE

Agenda

- Configuring virtual switches
- Configuring link aggregation for high performance
- Configuring IPMP for IP high availability
- Configuring Packet Filter to control network access

IPMP: Introduction

- Performance advantages:
  - Fault tolerance
  - Load spreading
  - Increased bandwidth
  - Transparent redundancy
- IPMP groups:
  - Active-active
  - Active-standby

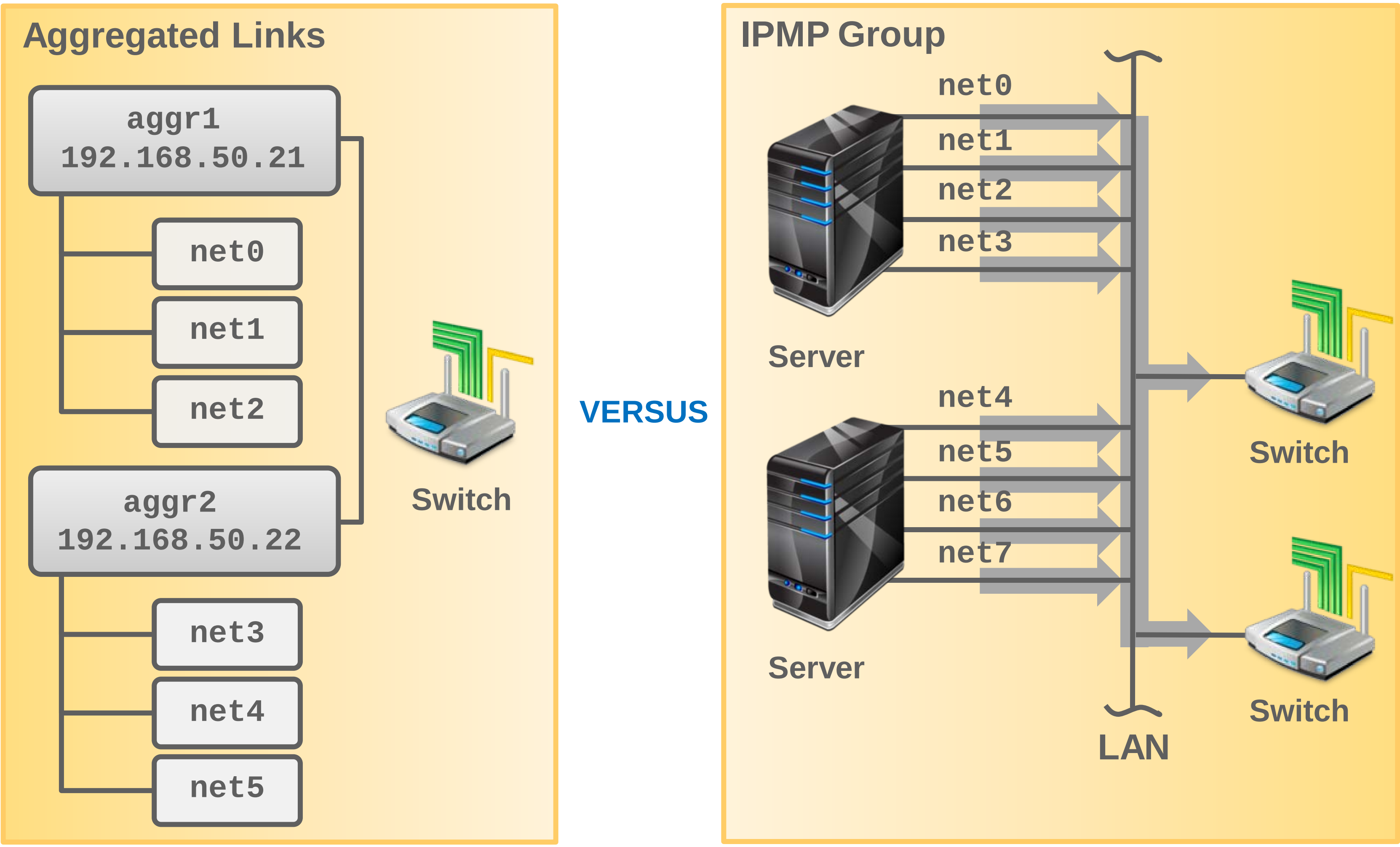


IPMP Components

Component	Description
IPMP daemon: `in.mpathd`	Detects interface failures and repairs
IPMP service: `svc:/network/ipmp`	Sets IPMP properties, such as enabling or disabling transitive probing
Configuration file: `/etc/default/mpathd`	Defines the daemon's behavior
IPMP administration command: `ipadm`	Configures IP network interfaces that are part of an IPMP group
IPMP display information command: `ipmpstat`	Provides information about the status of IPMP as a whole
IP kernel module	Manages outbound load spreading

ORACLE

Comparing Link Aggregation and IPMP



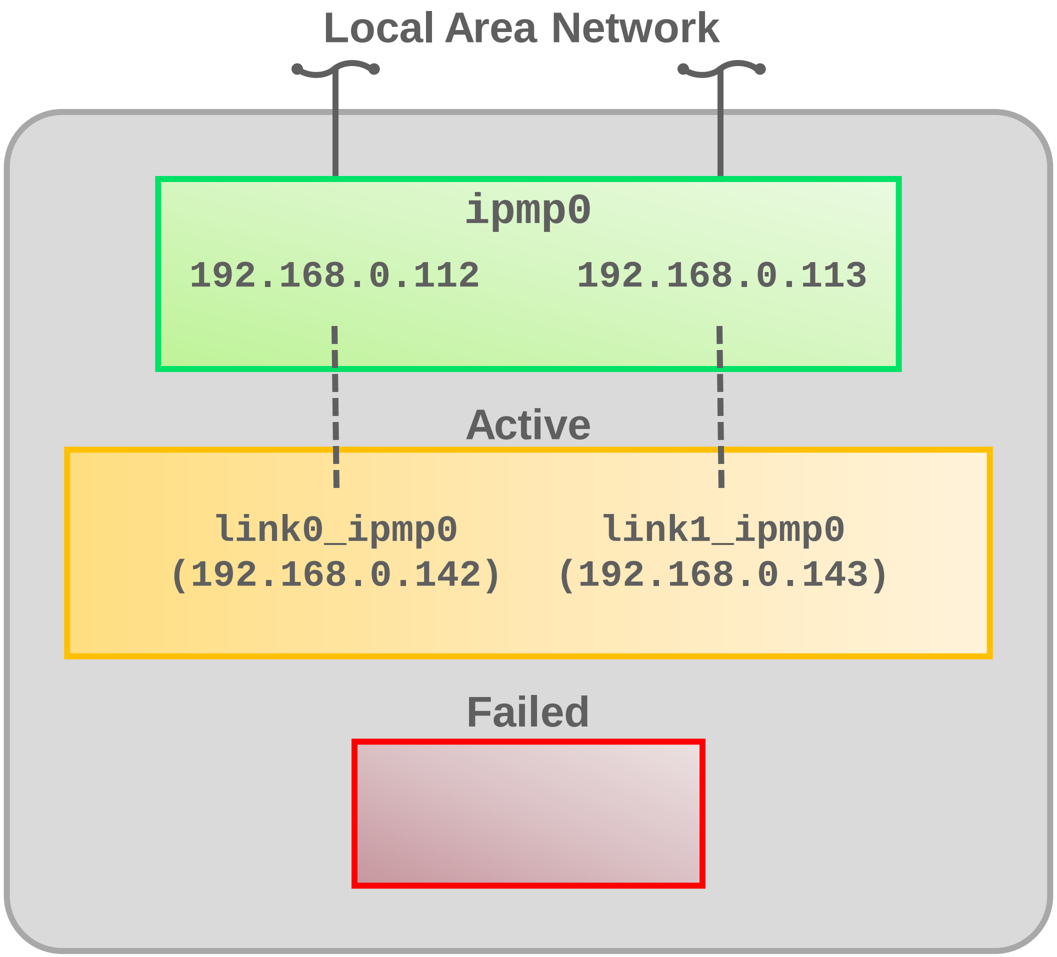
Failure and Repair Detection in IPMP

- To ensure continuous availability, IPMP performs failure detection on the IPMP group's underlying IP interfaces.
- Failed interfaces remain unusable until they are repaired.
- The remaining active interfaces continue to function, while any existing standby interfaces are deployed as needed.
- The `in.mpathd` daemon handles the following types of failure detection:
  - Probe-based failure detection
    - No test addresses are configured.
      - ICMP probes
      - Transitive probes
    - Test addresses are configured.
  - Link-based failure detection

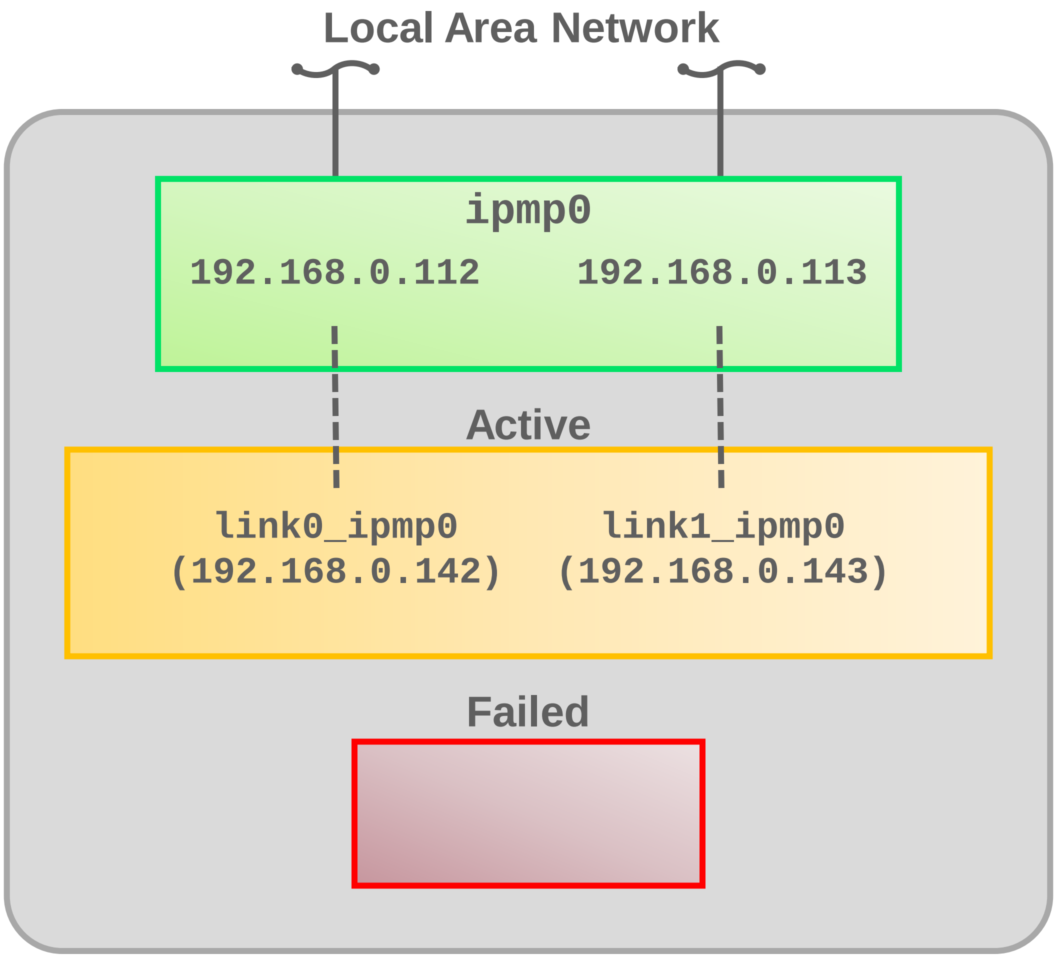
IPMP Configurations

- An IPMP configuration consists of two or more physical interfaces on the same system that are attached to the same network.
- These interfaces can belong to an IPMP group in either of the following configurations:
  - Active-active
  - Active-standby

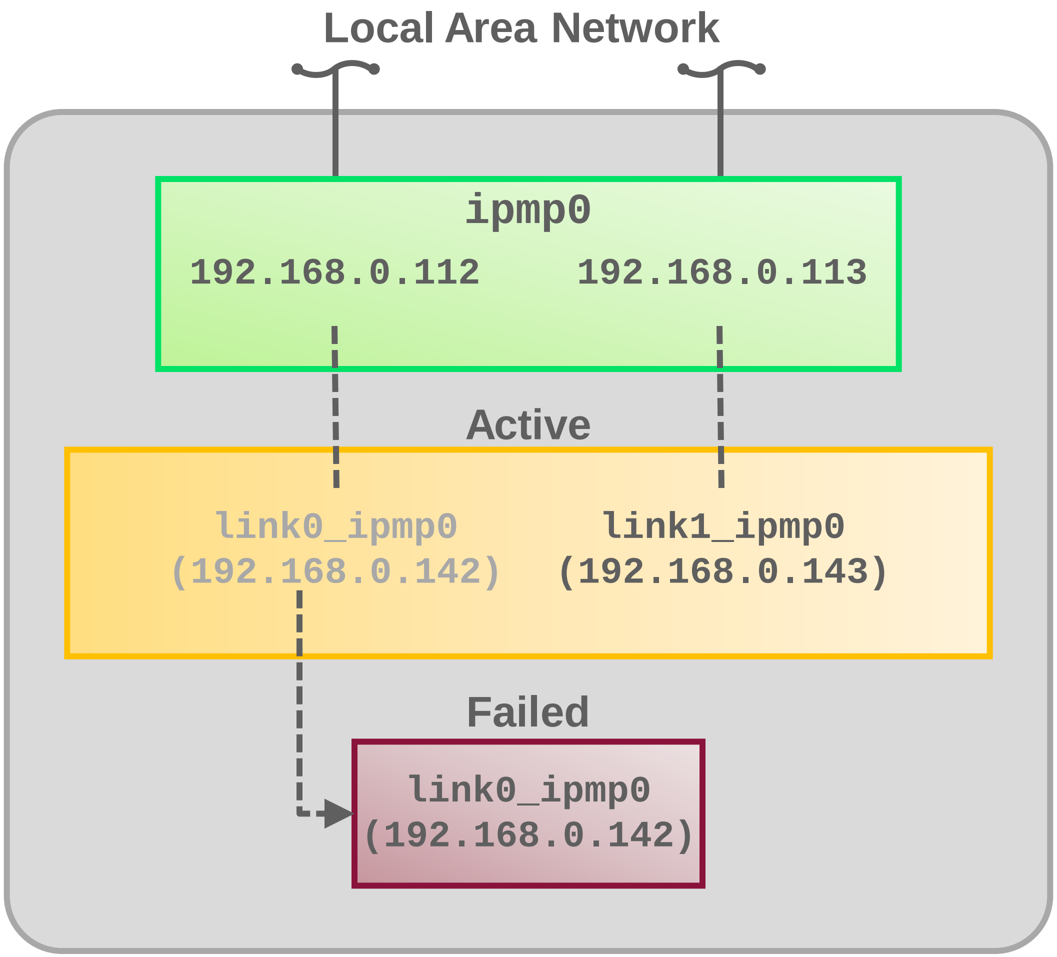
How IPMP Works: Active-Active



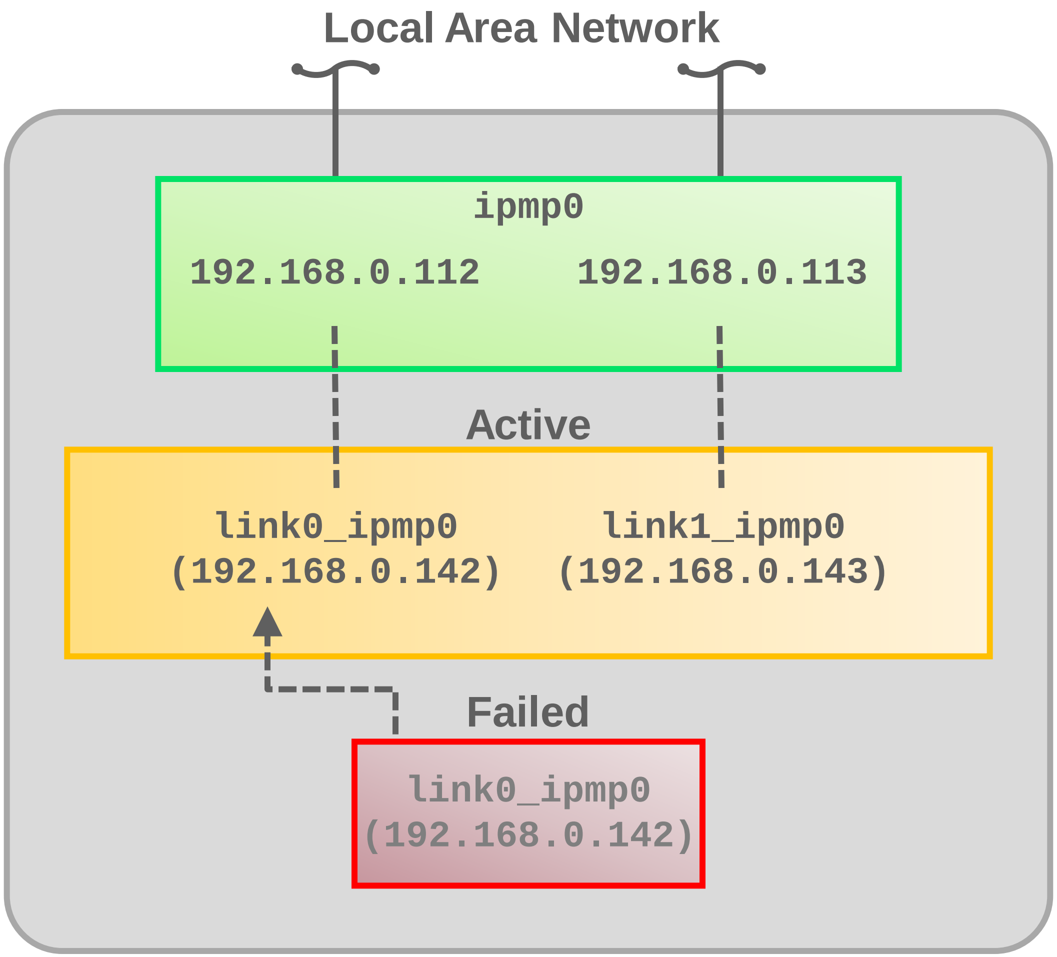
How IPMP Works: Active-Active



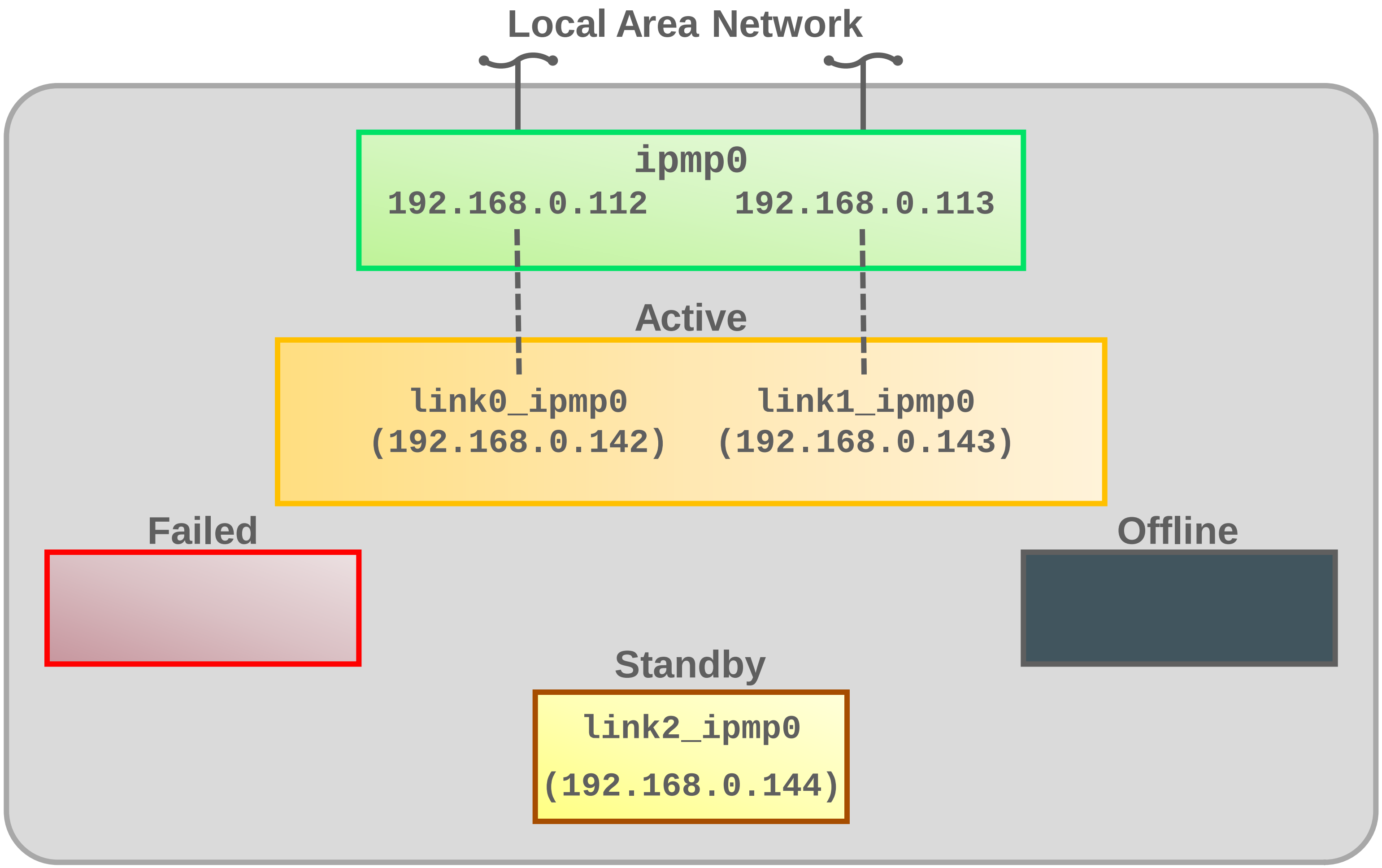
How IPMP Works: Active-Active



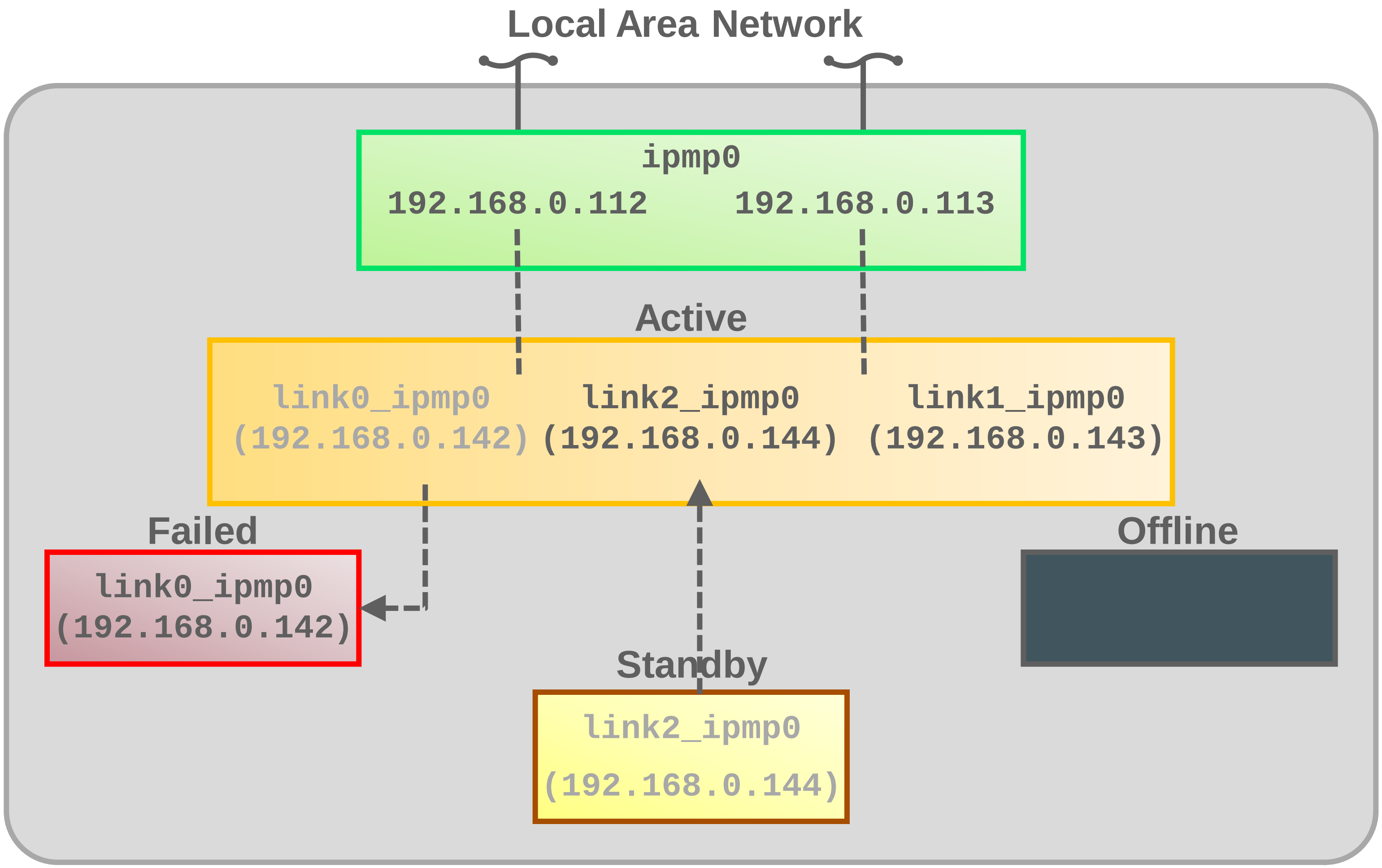
How IPMP Works: Active-Active



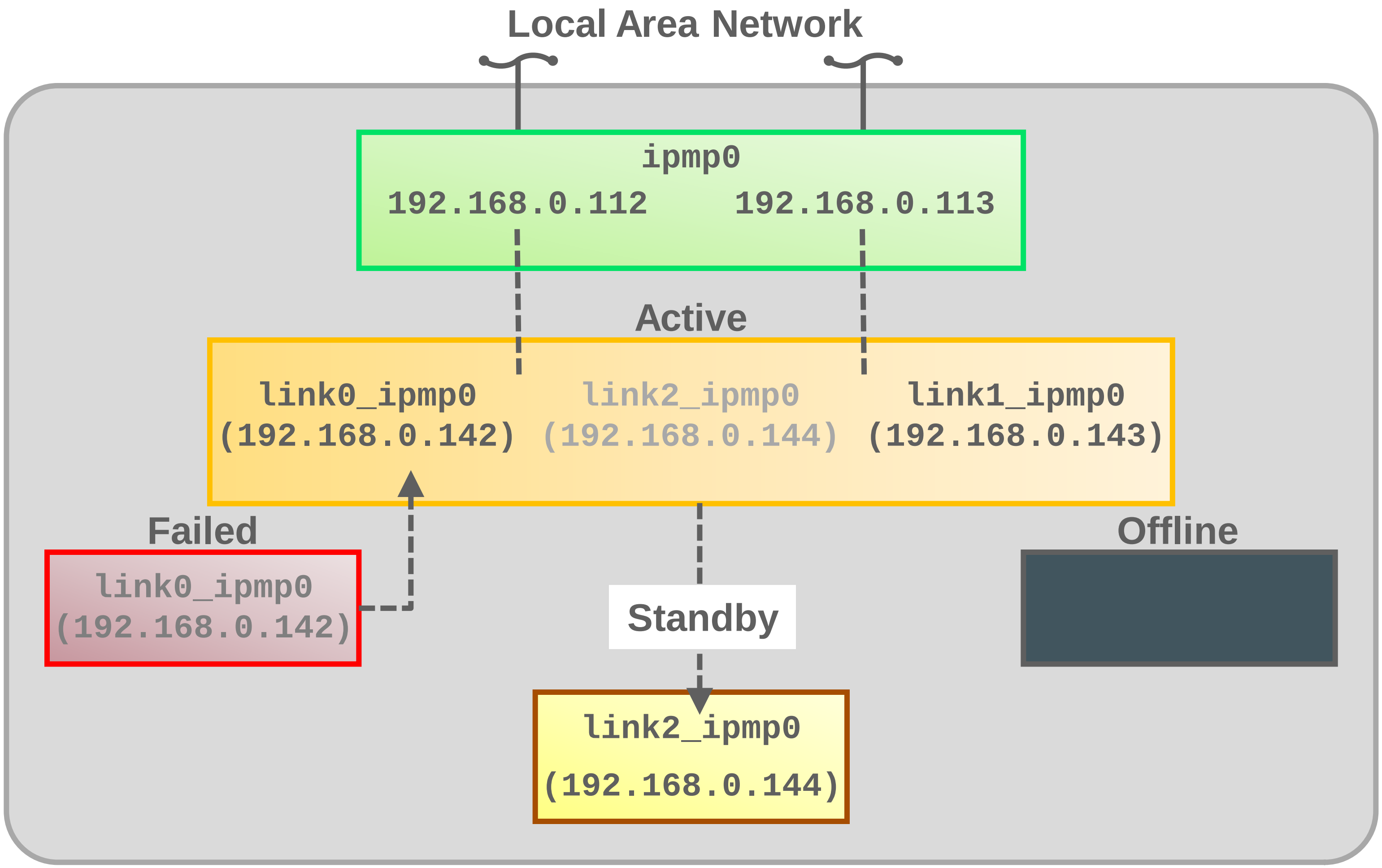
How IPMP Works: Active-Standby



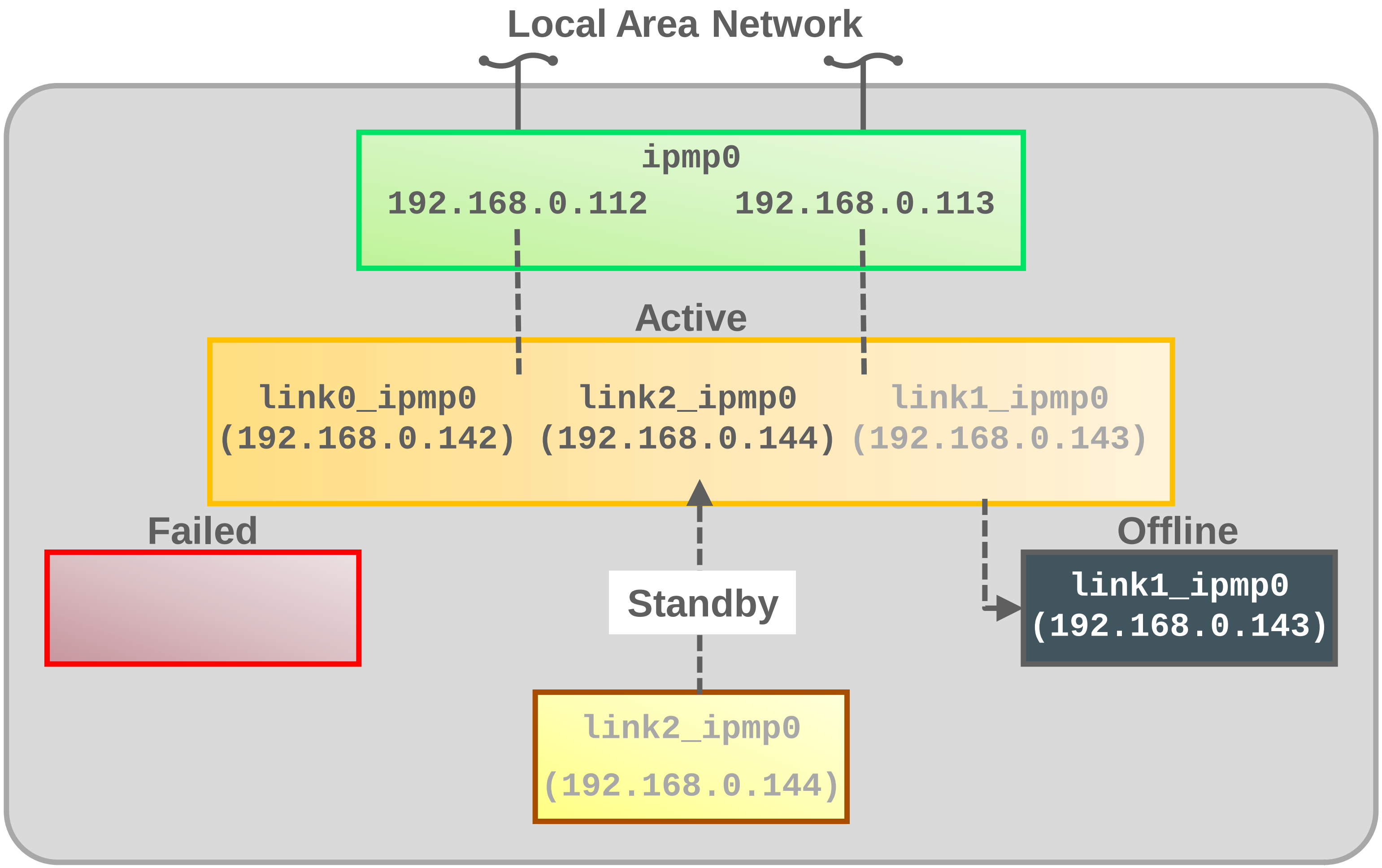
How IPMP Works: Active-Standby



How IPMP Works: Active-Standby



How IPMP Works: Active-Standby



Configuring an IPMP Group

This section covers the following topics:

- Creating an IPMP group
- Adding IP addresses to an IPMP group
- Moving an interface from one IPMP group to another
- Deleting or disabling an IPMP group

ORACLE

Creating an IPMP Group

1. Create IP interfaces for the datalinks to use in the IPMP group by using the `ipadm create-ip` command.
2. Create the IPMP group by using the `ipadm create-ipmp` command.

```
# dladm rename-link net0 link0_ipmp0
# dladm rename-link net1 link1_ipmp0
# ipadm create-ip link0_ipmp0
# ipadm create-ip link1_ipmp0
# ipadm create-ipmp ipmp0
# ipadm add-ipmp -i link0_ipmp0 -i link1_ipmp0 ipmp0
# ipmpstat -g
GROUP     GROUPNAME   STATE    FDT      INTERFACES
ipmp0     ipmp0       ok       --       link1_ipmp0 link0_ipmp0
```

Adding IP Addresses to an IPMP Group

1. Add addresses to an IPMP group by using the `ipadm create-addr` command.
2. Verify the results with the `ipadm show-addr` command.

```
# ipadm create-addr -T static -a 192.168.0.112/24 ipmp0/v4add1
# ipadm create-addr -T static -a 192.168.0.113/24 ipmp0/v4add2
# ipadm show-addr
ADDROBJ                 TYPE      STATE      ADDR
ipmp0/v4add1            static    ok         192.168.0.112/24
ipmp0/v4add2            static    ok         192.168.0.113/24
```

Moving an Interface from One IPMP Group to Another Group

1. Remove the interface from the IPMP group by using the `ipadm remove-ipmp` command.
2. Add the interface to another group by using the `ipadm add-ipmp` command.

```
# ipadm remove-ipmp -i link0_ipmp0 ipmp0
# ipadm add-ipmp -i link0_ipmp0 ipmp1
```

Deleting and Disabling an IPMP Group

To delete an IPMP group, use the `ipadm delete-ip` command.

```
# ipadm delete-ipmp ipmp0
```

To disable an IPMP group, use the `ipadm disable-if` command.

```
# ipadm disable-if -t ipmp0
```

ORACLE

Implementing Link Failover by Using IPMP

This section covers the configuration of:

- An active-active IPMP group
- An active-standby IPMP group

Configuring an Active-Active IPMP Group

1. Create IP interfaces by using `ipadm`.
2. Create an IPMP group and add the interfaces to the group.
3. Create static IP addresses for data access.

```
# dladm rename-link net0 link0_ipmp0
# dladm rename-link net1 link1_ipmp0
# ipadm create-ip link0_ipmp0
# ipadm create-ip link1_ipmp0
# ipadm create-ipmp ipmp0
# ipadm add-ipmp -i link0_ipmp0 -i link1_ipmp0 ipmp0
# ipadm create-addr -T static -a 192.168.0.112/24 ipmp0/v4add1
# ipadm create-addr -T static -a 192.168.0.113/24 ipmp0/v4add2
# ipadm show-addr
ADDROBJ          TYPE     STATE        ADDR
lo0/v4           static   ok           127.0.0.1/8
ipmp0/v4add1     static   ok           192.168.0.112/24
ipmp0/v4add2     static   ok           192.168.0.113/24
lo0/v6           static   ok           ::1/128
```

ORACLE

Assigning Test Addresses

To assign test addresses to an IPMP subinterface, use `ipadm create-addr -T static -a IP_address link/test`.

```
# ipadm create-addr -T static -a 192.168.0.142/24 link0_ipmp0/test
# ipadm create-addr -T static -a 192.168.0.143/24 link1_ipmp0/test
# ipadm show-addr
ADDROBJ            TYPE      STATE        ADDR
lo0/v4             static    ok           127.0.0.1/8
link0_ipmp0/test   static    ok           192.168.0.142/24
link1_ipmp0/test   static    ok           192.168.0.143/24
ipmp0/v4add1       static    ok           192.168.0.112/24
ipmp0/v4add2       static    ok           192.168.0.113/24
lo0/v6             static    ok           ::1/128
```

Configuring an Active-Standby IPMP Group

1. Set at least one interface's property to `standby` by using the `ipadm set-ifprop` command.
2. Confirm the results.

```
# ipadm show-ifprop -p standby link2_ipmp0
IFNAME      PROPERTY  PROTO PERM  CURRENT   PERSISTENT  DEFAULT POSSIBLE
link2_ipmp0 standby   ip    rw    off       --          off     on,off
# ipadm set-ifprop -p standby=on -m ip link2_ipmp0
# ipadm show-ifprop -p standby link2_ipmp0
IFNAME      PROPERTY  PROTO PERM  CURRENT   PERSISTENT  DEFAULT POSSIBLE
link2_ipmp0 standby   ip    rw    on        on          off     on,off
```

ORACLE

Monitoring an IPMP Group

This section covers the following topics:

- Displaying IPMP group information
- Obtaining IPMP address information
- Verifying IPMP interface information
- Obtaining probe target information
- Checking probe information

Displaying IPMP Group Information

To display IPMP group information, use `ipmpstat -g`.

```
# ipmpstat -g
GROUP GROUPNAME STATE FDT    INTERFACES
ipmp0     ok    10.00s link1_ipmp0 link0_ipmp0 (link2_ipmp0)
```

Obtaining IPMP Address Information

To display IPMP address information, use `ipmpstat -an`.

```
# ipmpstat -an
ADDRESS          STATE  GROUP  INBOUND     OUTBOUND
::               down   ipmp0  --          --
192.168.0.113    up     ipmp0  link1_ipmp0 link0_ipmp0
192.168.0.112    up     ipmp0  link0_ipmp0 link1_ipmp0 link0_ipmp0
```

Verifying IPMP Interface Information

To verify IPMP interface information, use `ipmpstat -i`.

```
# ipmpstat -i
INTERFACE     ACTIVE  GROUP      FLAGS     LINK    PROBE    STATE
link2_ipmp0   yes     ipmp0      -s-----   up      ok
link1_ipmp0   yes     ipmp0      --mbM--   up      ok
link0_ipmp0   no      ipmp0      -------   up      failed
```

Obtaining Probe Target Information

To display information about test address targets, use `ipmpstat -nt`.

```
# ipmpstat -nt
INTERFACE   MODE       TESTADDR            TARGETS
link1_ipmp0 multicast  192.168.0.143       192.168.0.100 192.168.0.111
link0_ipmp0 multicast  192.168.0.142       192.168.0.100 192.168.0.111
```

ORACLE

Checking Probe Information

To check probe information, use `ipmpstat -pn`.

```
# ipmpstat -pn
TIME      INTERFACE   PROBE  NETRTT  RTT       RTTAVG    TARGET
0.06s     link2_ipmp0 i163   0.26ms  0.49ms    0.33ms    192.168.0.100
0.90s     link1_ipmp0 i162   0.26ms  0.39ms    0.31ms    192.168.0.100
0.92s     link2_ipmp0 i164   0.19ms  0.36ms    0.34ms    192.168.0.100
0.49s     link0_ipmp0 i161   --      --        --        192.168.0.100
-0.49s    link0_ipmp0 i160   --      --        --        192.168.0.100
2.52s     link2_ipmp0 i165   0.23ms  0.39ms    0.34ms    192.168.0.100
2.74s     link1_ipmp0 i163   0.24ms  0.38ms    0.32ms    192.168.0.100
3.69s     link1_ipmp0 i164   0.25ms  0.45ms    0.34ms    192.168.0.100
2.31s     link0_ipmp0 i162   --      --        --        192.168.0.100
…
…
…
<Ctrl+C>
```

Quiz

What is the default policy for link aggregation?

a. L2 (Networking): MAC header

b. L3 (Addressing): IP header

c. L4 (Communication): TCP/UDP or other ULP header

Quiz

IPMP can be configured for both IPv4 and IPv6.

a. True

b. False

Quiz

Which IPMP component is responsible for detecting failures?

a. IPMP daemon
b. IPMP service
c. DHCP

Quiz

Link aggregation and IPMP cannot be deployed together.

a. True

b. False

Practice 5-3 Overview: Configuring IPMP

This practice covers the following topics:

- Configuring an active-active IPMP configuration
- Configuring an active-standby IPMP configuration
- Removing the IPMP configuration

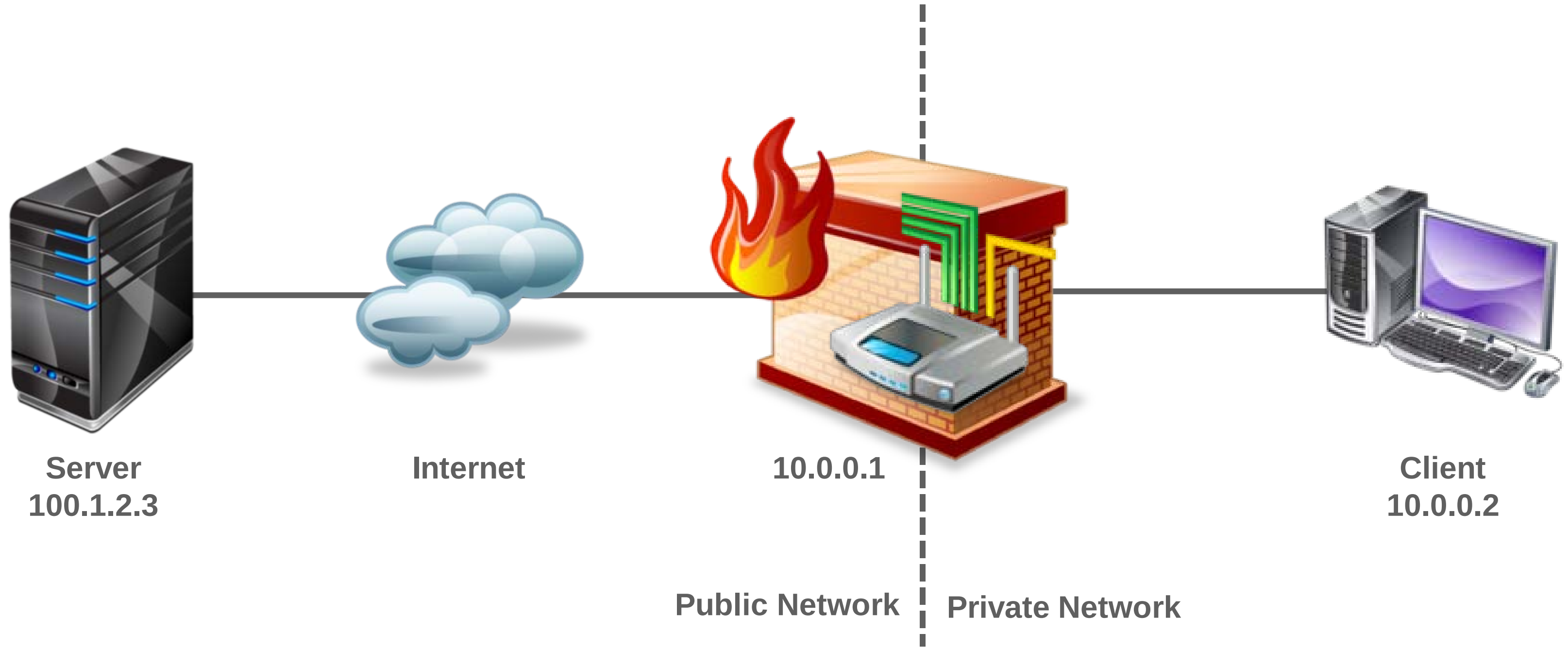
ORACLE

Agenda

- Configuring virtual switches
- Configuring link aggregation for high performance
- Configuring IPMP for IP high availability
- Configuring Packet Filter to control network access

Need for a Firewall

A firewall is a facility that restricts access between a protected network and an unprotected network (such as the Internet) or between other sets of networks based on the security policy of the organization.



Packet Filter: Overview

- The Packet Filter (PF) feature of Oracle Solaris is a network firewall that:
  - Is based on OpenBSD PF version 5.5
  - Captures incoming packets and evaluates them for entry to and exit from the system
  - Provides stateful packet inspection
  - Matches packets by IP address and port number as well as by the receiving network interface
- Both PF and IP Filter features are available for filtering packets in Oracle Solaris 11.3.
- **Note:** Because PF is a more robust filtering module, you should transfer your firewall policy from IP Filter rules to PF.

ORACLE

Comparison of IP Filter and PF

Firewall Feature	IP Filter	PF
Configuration files	Several, such as `ippool.conf`, `ipnat.conf`, and `ipv6.conf`	One `pf.conf` file
Package name	`ipfilter`	`firewall`, not installed by default
pass rules	Stateless by default	Stateful by default
Rights profile	Network Security	Network Firewall Management
SMF service name	`ipfilter`, enabled by default	`firewall`
IPv4 and IPv6 packet fragments	IP reassembly must be explicitly turned on	IP reassembly is on by default
Loopback interface protection	Must be enabled by `set intercept_lopback true;`	Firewall always intercepts packets on loopback interface
OS signature file	None	`pf.os`

ORACLE

Behavior of PF Firewall

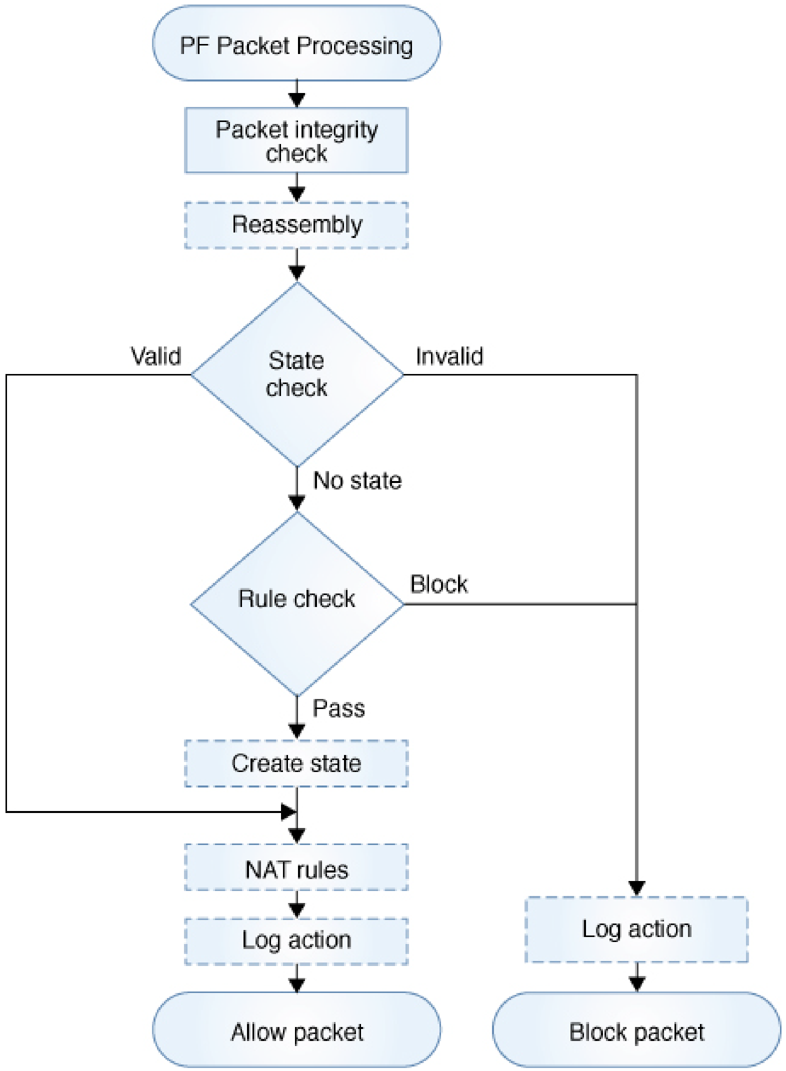
- The PF firewall is controlled by the `svc:/network/firewall` SMF service that loads the rules from the `/etc/firewall/pf.conf` configuration file.
- A rule helps process packets and determine whether they are accepted or dropped.
- You can use the `pfconf` script to edit the PF configuration file.
- When you save the file, the script verifies the syntax of the firewall rules and then refreshes the firewall service to put the new rules in effect.

PF Rules

- A rule in the `/etc/firewall/pf.conf` configuration file contains the following parts:
  - Actions: Define the action that applies to the packet if the packet matches the rule.
  - Match parameters: Define criteria that determine whether a packet matches the rule.
  - Optional actions: Define additional optional actions.
- You write a rule by using the following elements in order:
  - Begin the rule with an action.
  - Match desired parameters.
  - Include desired optional actions.
- PF rule syntax:

```
# action match-parameter optional-action-1 optional-action-2…
```

Packet Flow in the PF Firewall



Configuring PF Firewall

1. Install the PF package.

```
# pkg install firewall
```

2. Create or update the packet filtering rule set.

```
# pfconf
```

   The `pfconf` script uses the service property rules for the location of the PF configuration file.

3. Disable the `ipfilter` service first, then enable the PF.

```
# svcadm disable network/ipfilter
# svcadm enable network/firewall
```

4. (Optional) Disable the PF service.

```
# svcadm disable network/firewall
```

   This command removes all rules from the kernel and disables the PF service.

Monitoring PF Firewall

- Examine the status of the `firewall` service.

```
# svcs -x firewall:default
svc:/network/firewall:default (Network Firewall)
 State: disabled since Fri Apr 10 10:10:50 2015
Reason: Disabled by an administrator.
   See: http://oracle.com/msg/SMF-8000-05
   See: pf.conf(5)
   See: /var/svc/log/network-firewall:default.log
Impact: This service is not running.
```

- List the configuration file names and locations for PF service.

```
# svccfg -s firewall:default listprop | grep firewall
firewall                       application
firewall/fingerprints          astring     /etc/firewall/pf.os
firewall/rules                 astring     /etc/firewall/pf.conf
firewall/value_authorization   astring     solaris.smf.value.network.firewall
restarter/logfile              astring     /var/svc/log/network-firewall:default.log
```

ORACLE

Monitoring PF Firewall

- Examine the current rules of the PF firewall.

```
# pfctl -s rules
empty list for firewall(out)
pass in quick on net1 from 192.168.1.0/24 to any
pass in all
block in on net1 from 192.168.1.10/32 to any
```

- Verify the PF firewall configuration.

```
# pfctl -n -f /test/firewall/pf.conf
```

Summary

In this lesson, you should have learned how to configure:

- A virtual switch
- Link aggregation for high performance
- IPMP for IP high availability
- Packet Filter to control network access

6

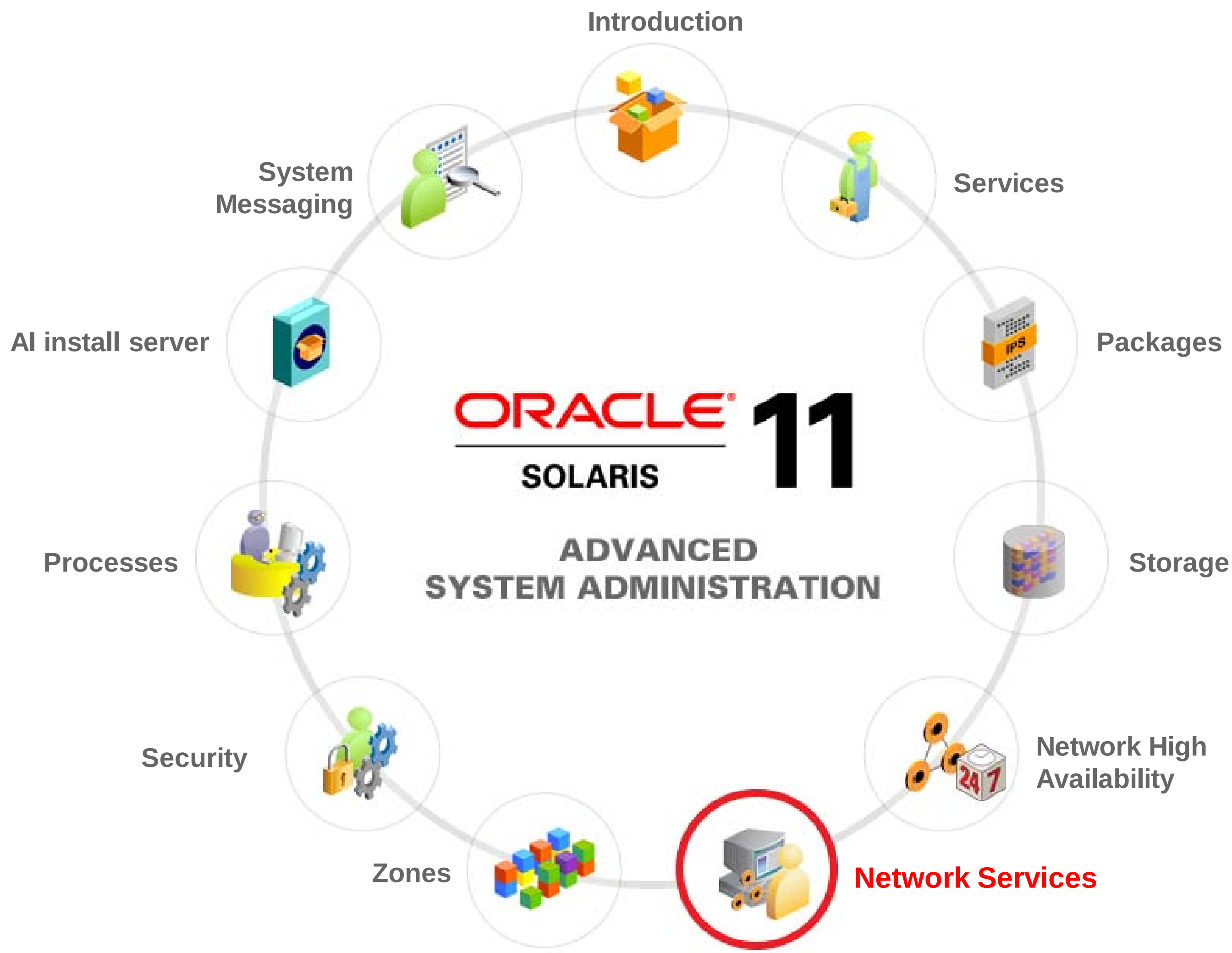
Administering Network Services

Objectives

After completing this lesson, you should be able to configure:

- Network File System (NFS)
- A Domain Name System (DNS) client
- A Lightweight Directory Access Protocol (LDAP) client

Job Workflow



Agenda

- Configuring the Network File System (NFS)
- Configuring a Domain Name System (DNS) client
- Configuring a Lightweight Directory Access Protocol (LDAP) client

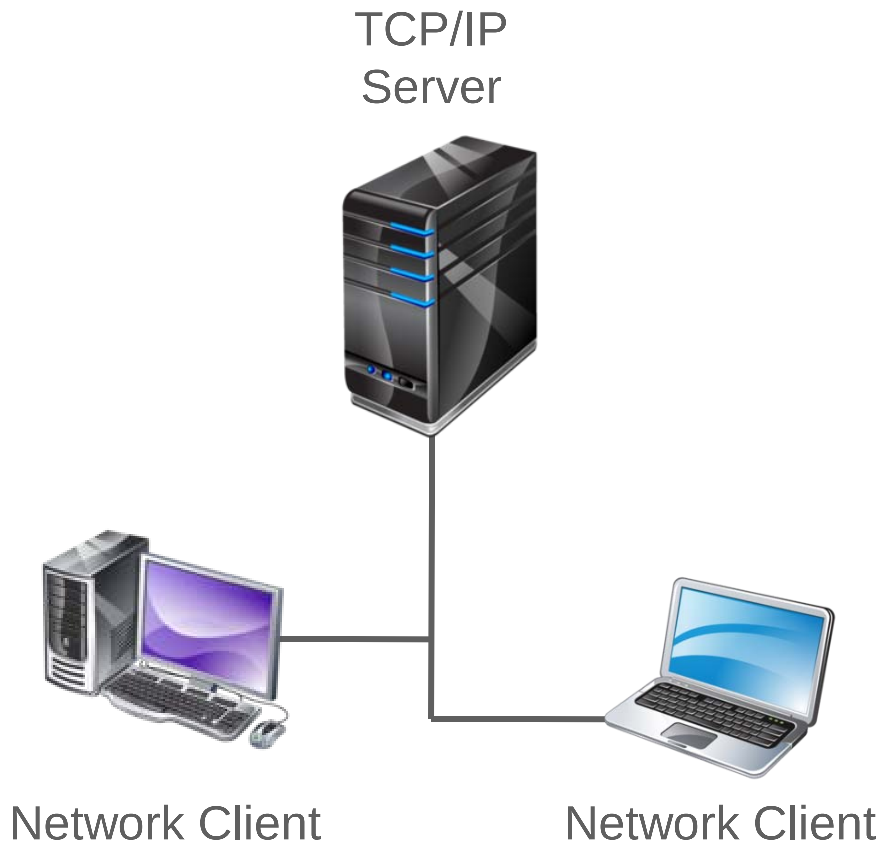
Importance of Network Services

Network services are required to ensure the following:

- Computers of different architectures that run different operating systems are able to share file systems across a network.
- You can look up IP addresses for:
  - Internet host names
  - Host names for IP addresses that are distributed across the network
- You have a directory structure that:
  - Includes details of various resources and identities
  - Can be accessed across networks

Configuring Network Services

- RARP/ARP
- TFTP
- NFS
- Name service
  - NIS, LDAP, DNS



Network File System: Overview

The Network File System (NFS):

- Allows access to file systems over the network
- Enables any system to access any other system's file systems
- Has the following advantages:
  - Accesses the same data
  - Reduces storage costs
  - Provides data consistency and reliability
  - Provides transparency
  - Reduces administration overhead
  - Provides heterogeneous environments
  - Enables automatic file sharing

Configuring NFS

This section covers the following topics:

- Configuring the NFS server
- Checking the NFS services status
- Configuring the NFS client
- Selecting a different version of NFS on a server
- Enabling the automount service
- Displaying NFS server and client statistics

Configuring the NFS Server

1. Create a ZFS file system for the files you want to share.
2. To share the file system:
   a. Set the ZFS `share` property.
   b. Set the ZFS `share.nfs` property to on.
3. Use the `share` command to verify what is being shared.

```
# zfs create rpool/export/home/docs
# zfs set share=name=docs,path=/export/home/docs,prot=nfs \
rpool/export/home/docs
name=docs,path=/export/home/docs,prot=nfs
# zfs set share.nfs=on rpool/export/home/docs
# zfs set compression=on rpool/export/home/docs
# share
docs    /export/home/docs  nfs sec=sys,rw
```

ORACLE

Checking the NFS Services Status

To check the status of the NFS services, use `svcs -a | grep nfs`.

```
# svcs -a | grep nfs
disabled          7:01:37 svc:/network/nfs/cbd:default
disabled          7:01:37 svc:/network/nfs/client:default
online            7:01:37 svc:/network/nfs/fedfs-client:default
online            7:01:37 svc:/network/nfs/mapid:default
online           16:31:11 svc:/network/nfs/status:default
online           16:31:12 svc:/network/nfs/nlockmgr:default
online           16:31:15 svc:/network/nfs/rquota:default
online           16:31:17 svc:/network/nfs/server:default
```

Configuring the NFS Client

1. Run `dfshares` *`server`* to verify that you can view the shared resource.
2. Create a directory to use as the mount point.
3. Run `mount -F nfs -o ro` *`server`*`:`*`resource`* *`/directory`* to specify the resource to be mounted.
4. Verify that the files in the shared resource can be shared.

```
# dfshares server1
RESOURCE                              SERVER     ACCESS     TRANSPORT
server1:/export/home/docs             server1    -          -
# mkdir /docs
# mount -F nfs -o ro server1:/export/home/docs /docs
# cd /docs
server1:/docs# ls
assetlist
```

Selecting a Different Version of NFS on a Server

To select a different version of NFS on a server or client, use the `sharectl` set command.

Example:

To set a server or client to provide only NFS version 3:

```
Server:
# sharectl set -p server_versmax=3 nfs
# sharectl set -p server_versmin=3 nfs

Client:
# sharectl set -p client_versmax=3 nfs
# sharectl set -p client_versmin=3 nfs
```

Enabling the Automount

To enable or disable the automount service, use the `svcadm` command.

```
Enable service:
# svcadm enable autofs

Mount file system:
# cd /net/server1/export/share/local

Disable service:
# svcadm disable autofs
```

ORACLE

Displaying NFS Server and Client Statistics

To display statistics about the NFS service on the client or server, use the `nfsstat` command.

```
# nfsstat -c
Client rpc:
Connection oriented:
calls     badcalls  badxids   timeouts newcreds  badverfs   timers
1595799   1511      59        297      0         0          0
cantconn nomem      interrupts
1198      0         7
Connectionless:
calls     badcalls  badxids   timeouts newcreds  badverfs   timers
1595799   1511      59        297      0         0          0
. . . . .
Client nfs:
calls     badcalls  clgets    cltoomany
1640097   3112      1640097   0
. . . . .
Client nfs_acl:
Version 2: (3105 calls)
null      getacl    setacl    getattr   access    getxattrdir
0 0%      0 0 %     0 0%      3105 100% 0 0%      0 0%
```

ORACLE

Practice 6-1 Overview: Configuring the NFS

This practice covers the configuration of the following:

- NFS server
- NFS client

Agenda

- Configuring the Network File System (NFS)
- Configuring a Domain Name System (DNS) client
- Configuring a Lightweight Directory Access Protocol (LDAP) client

ORACLE

Domain Name System: Overview

The Domain Name System (DNS) is:

- A hierarchical, distributed database that is implemented on a TCP/IP network
- Primarily used to look up IP addresses for Internet host names and host names for IP addresses
- Used to store other Internet-related host information, such as mail exchange routing information, location data, and available services

How DNS Works

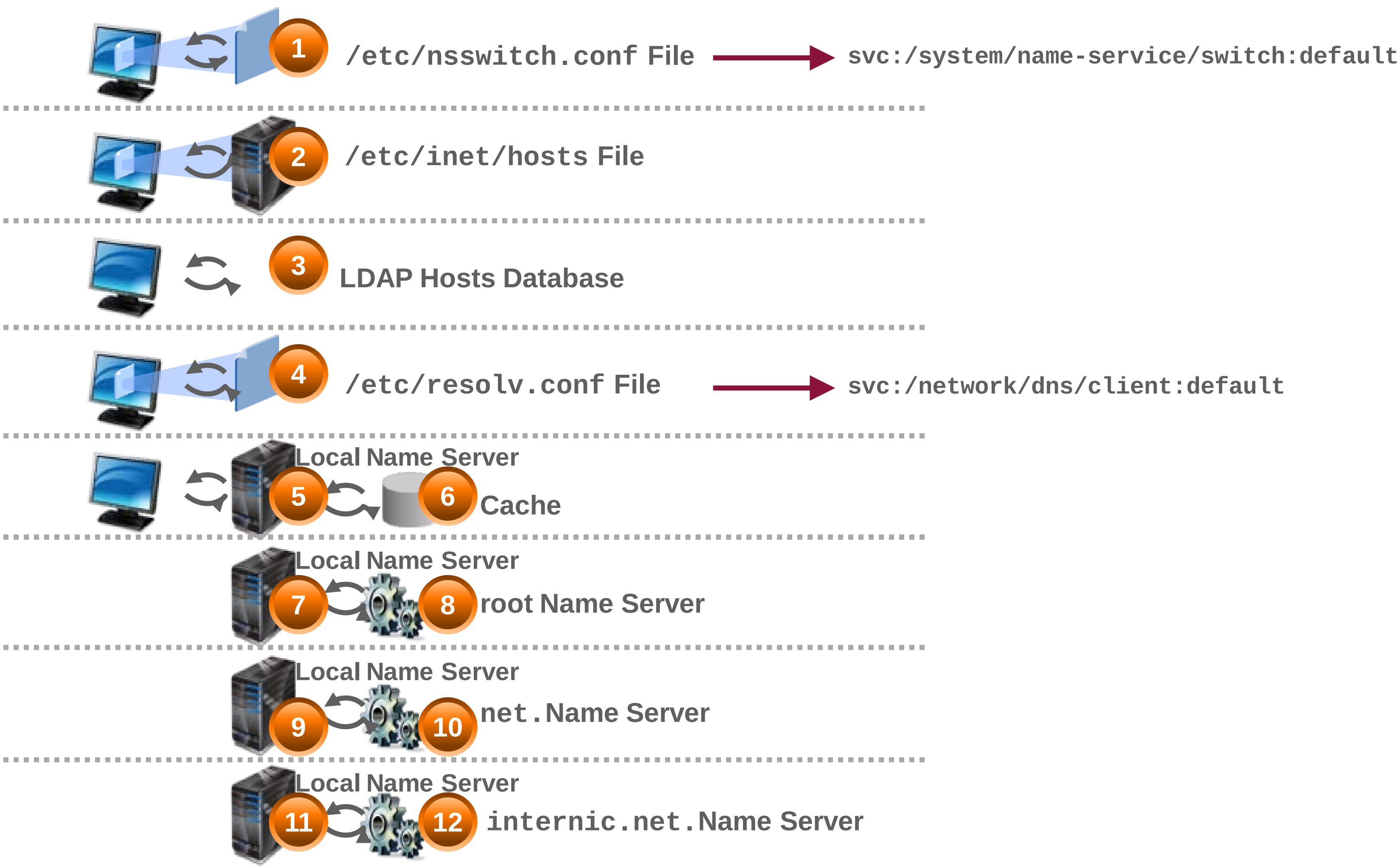
1. A DNS client requests information about a host name from one or more name servers and then waits for a response.
2. DNS servers respond to requests after looking up one of the following:
   - Information cache that was loaded from file or a third-party database on a DNS master
   - Network from a cooperating DNS slave server
3. If found, the host name is resolved.
4. If there is no response and the server is not responsible for the domain in question, the service recursively requests (if permitted) the host name from other servers and caches that response.

ORACLE

DNS Name Resolution

- *Name resolution* is the process of translating a domain name to an IP address (and vice versa).
- The name resolution process in Oracle Solaris 11 is implemented through SMF services.
  - The `/etc/resolv.conf` file (which determines the name resolution search list and the address of the DNS servers) is now an SMF service: `svc:/network/dns/client:default`
  - The `/etc/resolv.conf` file is activated by a reference to the DNS entry in the `/etc/nsswitch.conf` file.
  - The `/etc/nsswitch.conf` file is also an SMF service: `svc:/system/name-service/switch:default`

Name Resolution Process



Checking the Connection to the DNS Server

To check the connectivity, use `nslookup host_IP_address`.

```
# nslookup 192.168.0.100
Server:   192.168.0.100
Address:  192.168.0.100#53

100.0.168.192.in-addr.arpaname = s11-server1.mydomain.com
```

Practice 6-2 Overview: Configuring a DNS Client

In this practice, you configure a DNS client.

Note: The DNS server is already set up for you because setup is usually the job of a network administrator.

Agenda

- Configuring the Network File System (NFS)
- Configuring a Domain Name System (DNS) client
- Configuring a Lightweight Directory Access Protocol (LDAP) client

Lightweight Directory Access Protocol: Overview

Lightweight Directory Access Protocol (LDAP):

- Allows access to directory servers for distributed naming and other directory services
- Supports a hierarchal database structure
- Can be used to provide naming services in both UNIX and multiplatform environments

Preparing for LDAP Client Setup

The requirements for an Oracle Solaris client to use LDAP as a naming service are:

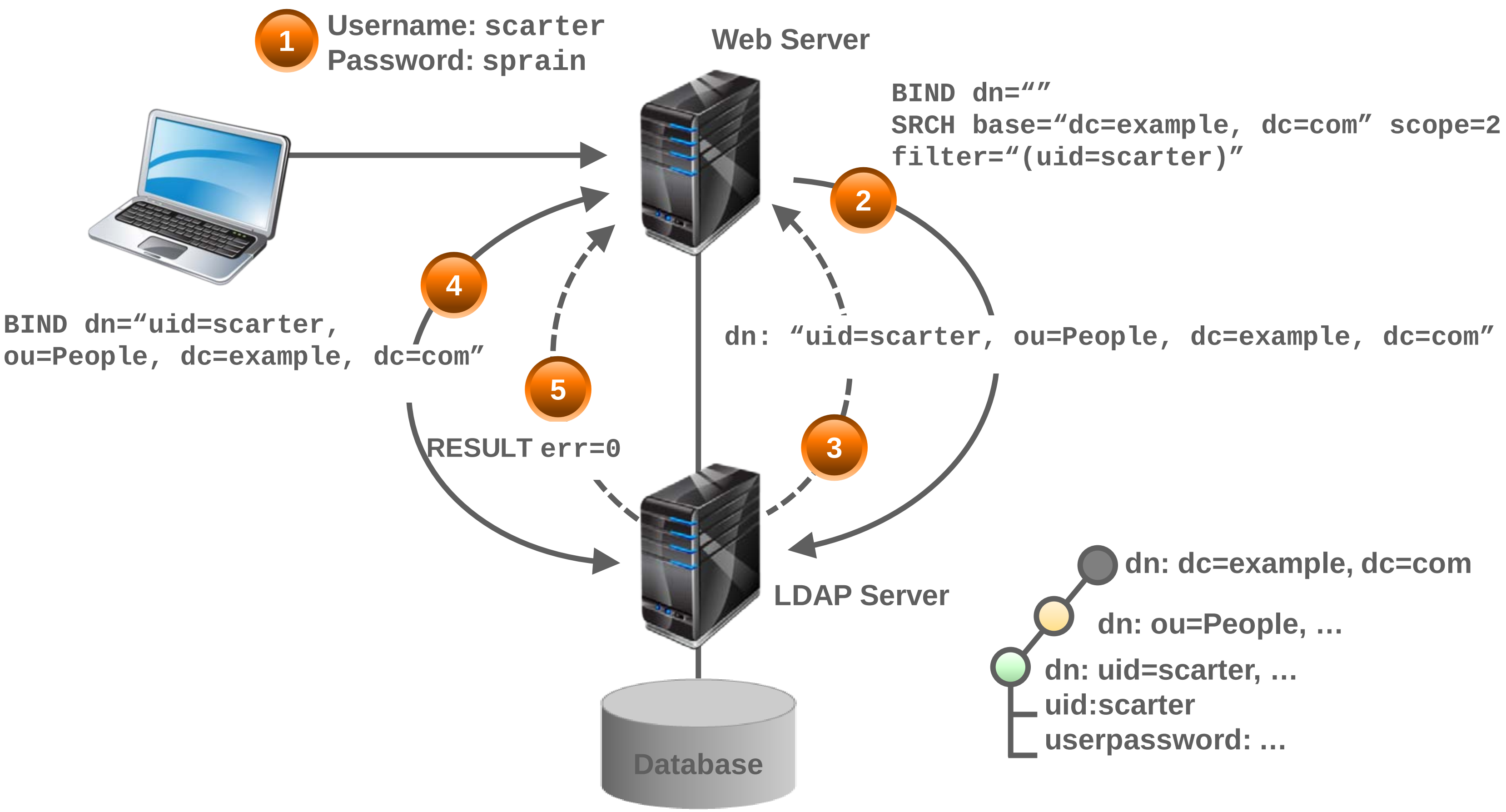
- The client's domain name must be served by the LDAP server.
- The name service switch must point to LDAP for the required services.
- The client must be configured with all the parameters that define its behavior.
- `ldap_cachemgr` must be running on the client.
- At least one server for which a client is configured must be running.

LDAP and the SMF

SMF manages the LDAP client service.

SMF Feature	LDAP Client Service
`svcadm`	Used to enable, disable, or restart the LDAP client service
`svc:/network/ldap/client`	The fault management resource identifier (FMRI) for the LDAP client service
`network/nis/domain`	During the configuration process, this service is also enabled to supply the domain name to be used by the `network/ldap/client` service
`svcs`	Used to query the status of the LDAP client and the `ldap_cachemgr` daemon

How LDAP Works



Practice 6-3 Overview: Configuring an LDAP Client

In this practice, you configure an LDAP client.

Note: The LDAP server is already set up for you because setup is usually the job of a network administrator.

ORACLE

Summary

In this lesson, you should have learned how to configure:

- Network File System (NFS)
- A Domain Name System (DNS) client
- A Lightweight Directory Access Protocol (LDAP) client

7

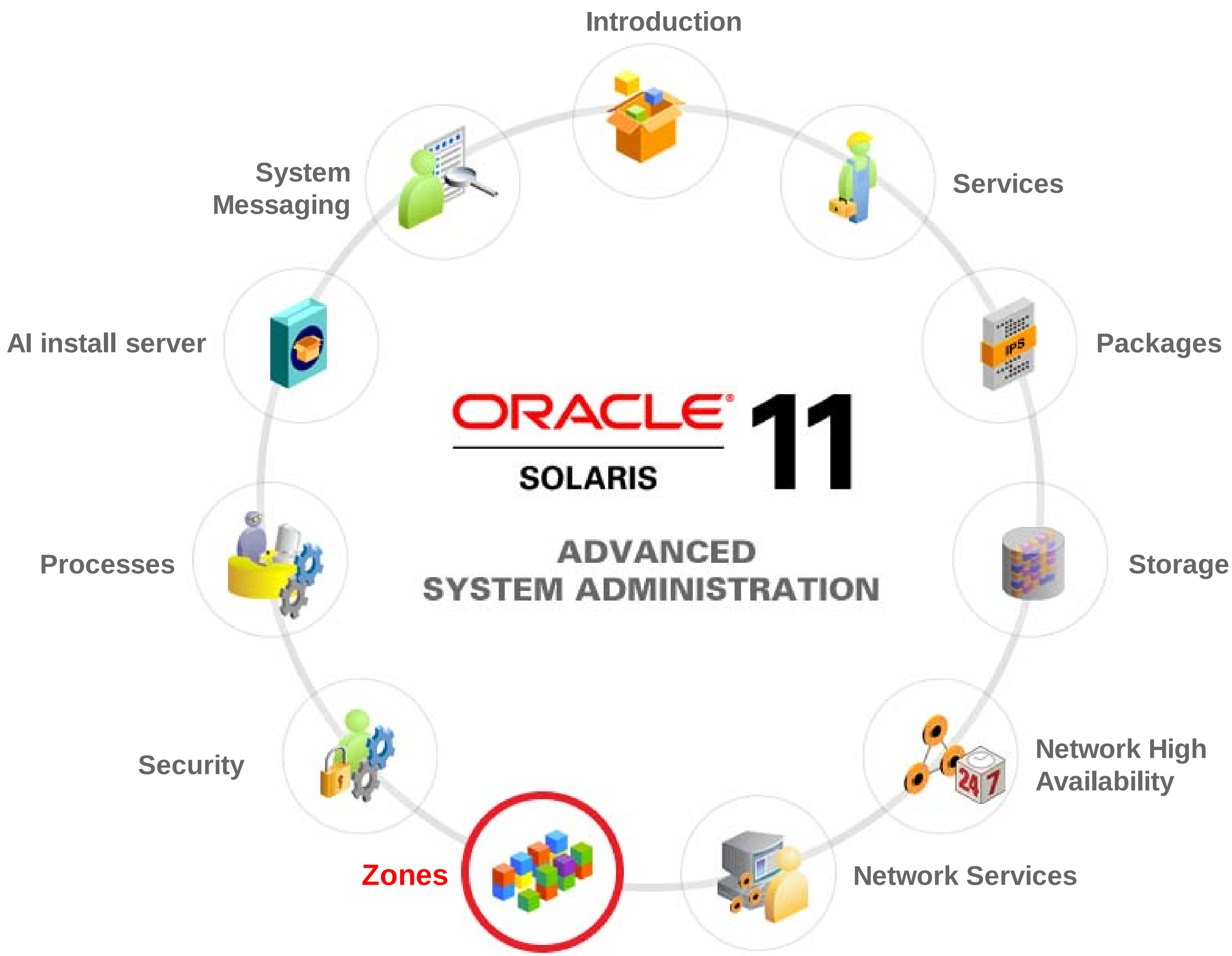
Advanced Administration of Zones

Objectives

After completing this lesson, you should be able to:

- Explain the fundamentals of Oracle Solaris 11 zones
- Manage system resources in a zone
- Migrate Oracle Solaris 10 systems
- Configure kernel zones
- Work with Unified Archives

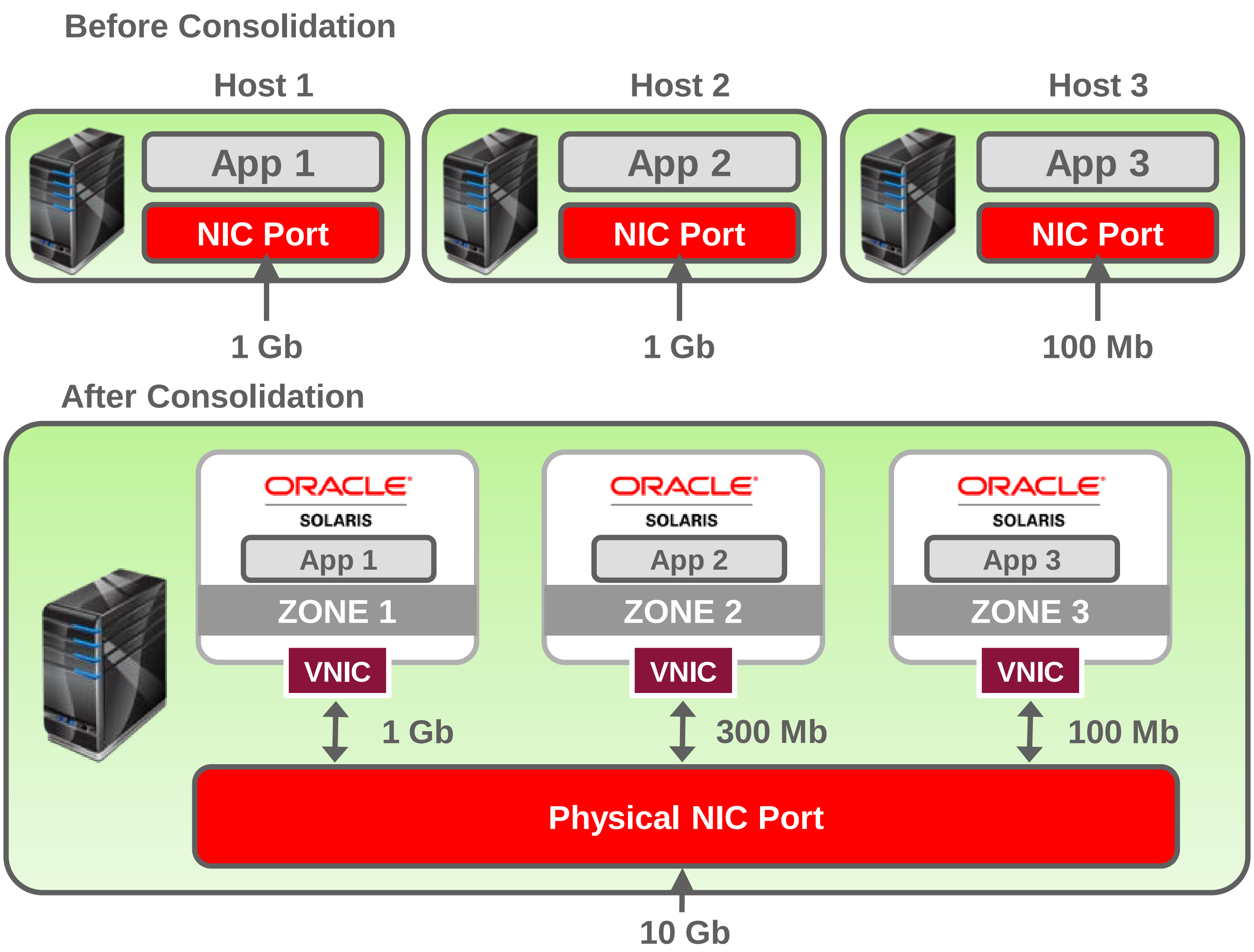
Workflow Orientation



Agenda

- Explaining the fundamentals of Oracle Solaris 11 zones
- Managing system resources in a zone
- Migrating Oracle Solaris 10 systems
- Configuring Kernel Zones
- Working with Unified Archives

Oracle Solaris Zones



ORACLE

Oracle Solaris Zone Brands

Oracle Solaris 11.3 supports the following zone brands:

- Oracle Solaris Zones (`solaris`):
  - Introduced in Oracle Solaris 10
  - Commonly called nonglobal zones, native, or just zones
  - A complete runtime environment for applications
- Oracle Solaris 10 Zones (`solaris10`):
  - Known as `solaris10` branded, nonglobal zones
  - Uses the BrandZ technology to run Oracle Solaris 10 applications on the Oracle Solaris 11 OS
- Oracle Solaris Kernel Zones (`solaris-kz`):
  - Introduced in Oracle Solaris 11.2
  - A feature enhancement that extends the functionality of the existing zones technology

ORACLE

Oracle Solaris 11 Zones: Features

Zones Feature	Description
Solaris 10 Zones	Solaris 10 Zones host Solaris 10 user environments inside zones on Oracle Solaris 11.
Boot environments for zones	Boot environments are integrated with Oracle Solaris Zones.
IPS integration	Oracle Solaris Zones have been integrated with the new IPS package management tools in Oracle Solaris 11.
Zone resource monitoring	Oracle Solaris 11 features a robust zones resource monitoring utility, `zonestat`.
Delegated administration	Delegate common zone administration tasks for specific zones to different administrators by using Role-Based Access Control.
Zones on shared storage	Configure, install, and run Oracle Solaris Zones hosted directly on arbitrary storage device objects, such as Fibre Channel, iSCSI targets, or kernel zone storage devices.
NFS server in nonglobal zones	Nonglobal zones now support NFS servers.
`unavailable` zone state	This state indicates that the zone has been installed, but cannot be verified, made ready, booted, attached, or moved.

ORACLE

Oracle Solaris 11 Zones: Features

Zones Feature	Description
Live zone reconfiguration	This feature enables configuration changes in a running nonglobal zone or kernel zone without the need to reboot, eliminating down time in service availability within the zone when configuration changes are made.
Live migration for kernel zones	This feature enables you to migrate a running kernel zone to a target system, without causing an outage.
Datalinks creation in nonglobal zones from the global zone	This feature enables administrators to dynamically create VNICs, VLANs, and IP-over-InfiniBand partitions directly in the nonglobal zone's namespace from the global zone.
Virtualized clocks	Set time values in nonglobal zones that are different from the value in the global zone. If you change the time in the global zone, the nonglobal zone time is offset by the same amount.

ORACLE

Agenda

- Explaining the fundamentals of Oracle Solaris 11 zones
- Managing system resources in a zone
- Migrating Oracle Solaris 10 systems
- Configuring Kernel Zones
- Working with Unified Archives

ORACLE

Importance of Resource Management

With the Oracle Solaris resource management facility, you can manage your system's application workloads by:

- Restricting access to a specific resource
- Offering resources to workloads on a preferential basis
- Isolating workloads from each another
- Preventing an application from consuming resources indiscriminately
- Changing an application's priority based on external events

Zone Resource Management

- Align resource management control boundaries with those of the zones.
- Zone resources that can be controlled include:
  – Resource pools or assigned CPUs
  – Resource controls
  – Scheduling classes

Managing System Resource Allocation to a Zone

System resource allocation to a zone can be controlled by:

- **Resource pools:** Used primarily to manage CPU usage
- **Resource capping:** Used to regulate physical memory consumption
- **Process scheduling:** Used to control the allocation of available CPU resources to processes

Resource Pool Allocation

- SMF supports two resource pool services:
  - Default resource pool service
    `svc:/system/pools:default`
  - Dynamic resource pool service
    `svc:/system/pools/dynamic:default`
- Resource pool services are disabled by default.
- To allocate a resource pool to a zone, you must:
  - Enable the two resource pool services
  - Create a pool configuration file and save it in the default configuration file `/etc/pooladm.conf`
  - Modify the pool configuration file to specify a subset of the system’s processors that should be dedicated to a zone
  - Bind the resource pool to the zone

ORACLE

How Resource Pools Work

- Oracle Solaris software boots.
- The initialization SMF service checks for the `/etc/pooladm.conf` file.
- If the file exists, `pooladm` makes the configuration the active pools' configuration.
- The system creates the dynamic configuration.
- Resources are allocated and monitored by the pools' resource controller (`poold`).

Memory Resource Capping

- Resource capping is controlled by the `rcapd` daemon.
- The `rcapd` daemon repeatedly samples the resource utilization of projects that have physical memory caps.
- The sampling interval is specified by the administrator.
- When physical memory utilization thresholds are exceeded, the daemon reduces the resource consumption with memory caps.

ORACLE

Specifying Resource Capping Within a Zone

- The `capped-memory` resource sets limits for physical, swap, and locked memory.
- At least one limit must be set.
- The `rcapd` daemon and `rcap` service must be up and running.

ORACLE

Allocating System Resources to a Zone

To allocate system resources to a zone, perform the following:

- Specify a subset of the system's processors that should be dedicated to a zone while it is running.
- Limit the amount of CPU resources that can be consumed by a zone.
- Control the allocation of available CPU resources among zones, based on their importance.
- Limit the amount of physical memory.

Live Zone Reconfiguration

- It allows you to reconfigure or report on the live configuration of `solaris` brand and `solaris10` brand nonglobal zones while the zones are running, without requiring to reboot.
- You can use this feature to make the following changes in running nonglobal zones:
  - Change resource controls
  - Change network configuration
  - Change the CPU resource pool
  - Add or remove file systems
  - Add or remove virtual and physical devices

ORACLE

Determining a Zone's Resource Utilization

To determine a zone's resource utilization, use the `zonestat` utility.

```
# zonestat -r summary 5
Collecting data for first interval...
Interval: 1, Duration: 0:00:05
SUMMARYInterval: 3, Duration: 0:00:15
SUMMARY                  Cpus/Online: 1/1   PhysMem: 1023M  VirtMem: 2047M
                    ---CPU----  --PhysMem-- --VirtMem-- --PhysNet--
               ZONE  USED %PART  USED %USED  USED %USED PBYTE %PUSE
            [total]  1.00  100%  658M 64.3%  839M 41.0%  1431 0.00%
           [system]  0.18 18.9%  373M 36.5%  521M 25.4%     -     -
           choczone  0.68 68.8% 44.0M 4.30% 49.6M 2.42%     0 0.00%
             global  0.11 11.0%  133M 13.0%  167M 8.16%  1431 0.00%
                 QA  0.00 0.40% 53.5M 5.23% 50.3M 2.46%     0 0.00%
        grandmazone  0.00 0.81% 53.3M 5.21% 51.4M 2.51%     0 0.00%


...
...
...
```

ORACLE

Determining a Zone’s Kernel File System Statistics

```
# fsstat -z s10 -z s10u9 zfs tmpfs
  new  name  name  attr attr lookup rddir  read  read write write
 file remov  chng   get  set    ops   ops   ops bytes   ops bytes
   93    82     6  163K  110   507K   148 69.7K 67.9M 4.62K 13.7M zfs:s10
  248   237   158  188K  101   612K   283 70.6K 68.6M 4.71K 15.2M zfs:s10u9
12.0K 1.90K 10.1K 35.4K   12  60.3K     4 25.7K 29.8M 36.6K 31.0M tmpfs:s10
12.0K 1.90K 10.1K 35.6K   14  60.2K     2 28.4K 32.1M 36.5K 30.9M tmpfs:S10u9
# fsstat -A -Z zfs tmpfs
  new  name  name  attr  attr lookup rddir  read  read write write
 file remov  chng   get   set    ops   ops   ops bytes   ops bytes
 360K 1.79K 20.2K 4.20M 1.02M  25.0M  145K 5.42M 2.00G 1.07M 8.10g zfs
 359K 1.48K 20.1K 4.04M 1.02M  24.5M  144K 5.31M 1.88G 1.06M 8.08G zfs:global
   93    82     6 74.8K   107   250K   144 54.8K 60.5M 4.61K 13.7M zfs:s10
  248   237   158 90.2K   101   336K   283 53.0K 58.3M 4.71K 15.2M zfs:s10u9
60.0K 41.9K 17.7K  410K   515   216K   426 1022K 1.02G  343K  330M tmpfs
49.4K 38.1K 11.0K  366K   489   172K   420  968K  979M  283K  273M tmpfs:global
5.28K 1.90K 3.36K 21.9K    12  21.7K     4 25.7K 29.8M 29.9K 28.3M tmpfs:s10
5.25K 1.90K 3.34K 22.1K    14  21.6K     2 28.4K 32.1M 29.8K 28.2M tmpfs:s10u9
```

ORACLE

Allocating and Managing System Resources in a Zone

This section covers allocating and managing the following:

- CPU resources with resource pools
- Physical memory resources with resource capping

ORACLE

Allocating and Managing CPU Resources with Resource Pools

To manage CPU consumption in a zone, perform the following steps by using resource pools:

1. Enabling services for resource pools
2. Configuring a persistent resource pool
3. Binding the zone to a persistent resource pool
4. Removing the resource pool configuration

Enabling Services for Resource Pools

To activate the resource pool services, run `svcadm enable -r pools/dynamic`.

```
# svcadm enable -r pools/dynamic
```

To verify that the service pools and the `poold` daemon are up, run `svcs *pools*` and `pgrep -lf poold`, respectively.

```
# svcs *pools*
STATE          STIME    FMRI
online         16:08:10 svc:/system/pools:default
online         16:08:11 svc:/system/pools/dynamic:default
# pgrep -lf poold
 2283 /usr/lib/pool/poold
```

Configuring a Persistent Resource Pool

To create the pool configuration file, use `pooladm -s`.

```
# pooladm –s
```

To verify that the file has been created, use `ls -l /etc/pool*`.

```
# ls -l /etc/pool*
-rw-r--r-- 1 root root 1298 Dec 14 16:13 /etc/pooladm.conf
# file /etc/pooladm.conf
/etc/pooladm.conf:      XML document
```

ORACLE

Displaying the Resource Pool Configuration File

To display the resource pool configuration file, use `poolcfg -c info`.

```
# poolcfg -c info
system default
        string  system.comment
        int     system.version 1
        boolean system.bind-default true
        string  system.poold.objectives wt-load
```

<Complete output presented in the Notes>

Modifying the Resource Pool Configuration File

To create the pset, use `poolcfg -c 'create pset pset_`*`psetname`*` (uint pset.min = x; uint pset.max = x)'`.

```
# poolcfg -c 'create pset pset_1to2 (uint pset.min = 1; uint
pset.max = 2)'
```

To create the pool, use `poolcfg -c 'create pool pool_`*`poolname’`*.

```
# poolcfg -c 'create pool pool_hrzone'
```

To associate the pset with the pool, use `poolcfg -c 'associate pool pool_`*`poolname`*` (pset pset_`*`psetname`*`) '`.

```
# poolcfg -c 'associate pool pool_hrzone (pset pset_1to2)'
```

ORACLE

Displaying and Committing the Modified Resource Pool Configuration File

To display the modified resource pool configuration, use `poolcfg -c info`.

```
# poolcfg -c info

<Output presented in the Notes>
```

To validate and commit the modified configuration, use `pooladm -n -c`, and then `pooladm -c`.

```
# pooladm -n -c
# pooladm -c
```

Displaying the Resource Pool Configuration That Is Currently in Use

To display the resource pool configuration that is currently in use, use `poolcfg -dc info`.

```
# poolcfg -dc info

system default
        string  system.comment
        int     system.version 1
        boolean system.bind-default true
        string  system.poold.objectives wt-load

        pool pool_hrzone
                int     pool.sys_id 1
                boolean pool.active true
                boolean pool.default false
                int     pool.importance 1
                string  pool.comment
                pset    pset_1to2
```

Displaying All Active Resource Pools

To display all the active resource pools on the system, use `poolstat -r all`.

```
# poolstat -r all
 id pool                 type rid rset                  min  max size used load
  1 pool_hrzone          pset   1 pset_1to2               1    2    1 0.00 0.00
  0 pool_default         pset  -1 pset_default            1  66K    1 0.00 0.17
```

Binding the Zone to a Persistent Resource Pool

This section covers the following steps:

1. Listing the current state of the zones
2. Allocating the pool to the zone and confirming the allocation
3. Rebooting the zone to activate the resource pool binding
4. Confirming the availability of the resource pool

Listing the Current State of the Zones

To list the current state of the zones on the system, use `zoneadm list -iv`.

```
# zoneadm list -iv
   ID NAME       STATUS      PATH                BRAND     IP
   0 global      running     /                   solaris   shared
   1 hrzone      running     /zones/hrzone       solaris   excl
   2 itzone      running     /zones/itzone       solaris   excl
```

ORACLE

Allocating the Pool to the Zone and Confirming the Allocation

To allocate the pool to the zone, use `zonecfg -z` followed by the zone name and set `pool=pool_poolname`.

```
# zonecfg -z hrzone set pool=pool_hrzone
```

To confirm that the allocation has been made, use `zonecfg -z zonename info pool`.

```
# zonecfg -z hrzone info | grep pool
pool: pool_hrzone
```

Confirming the Availability of the Resource Pool

To confirm the availability of the resource pool, log in by using `zlogin zonename`, and then use `poolcfg -dc info`.

```
# zlogin hrzone
[Connected to zone 'hrzone' pts/2]
Oracle Corporation  SunOS 5.11    11.3   September 2015

# poolcfg -dc info

<Output presented in the Notes>

# exit
Logout
[Connection to zone 'hrzone' pts/2 closed]
```

Removing the Resource Pool Configuration

This section covers the following steps:

1. Removing the pool configuration from the zone
2. Rebooting the zone
3. Checking the resource pool configuration for the zone
4. Deleting the resource pool
5. Displaying all active resource pools

Removing the Pool Configuration from the Zone

To remove the resource pool configuration from the zone, use `zonecfg -z zonename clear pool`.

```
# zonecfg -z hrzone clear pool
```

Rebooting the Zone

To reboot the zone, use `zlogin hrzone init 6` command.

```
# zlogin hrzone init 6
```

Checking the Resource Pool Configuration for the Zone

To check the resource pool configuration for the zone, log in by using `zlogin zonename`, and then use `poolcfg -dc info`.

```
# zlogin hrzone
[Connected to zone 'hrzone' pts/2]
Oracle Corporation  SunOS 5.11    11.3   September 2015

# poolcfg -dc info
        <Output presented in the Notes>
# exit
Logout
[Connection to zone 'hrzone' pts/2 closed]
```

Deleting the Resource Pool

To delete the resource pool, use `pooladm -x`.

```
# pooladm -x
```

Displaying All Active Resource Pools

To display all the active resource pools on the system, use `poolstat -r all`.

```
# poolstat -r all
 id pool           type rid rset           min  max size used load
  0 pool_default   pset  -1 pset_default   1    66K    2 0.00 0.73
```

Allocating and Managing Physical Memory Resources with Resource Capping

To add a memory cap to a zone, perform the following steps:

1. Configure the zone by using `zonecfg -z zone`.
2. Add the memory cap resource and set each memory cap type as appropriate: physical, swap, and locked.
3. Verify, commit, and exit the zone.

```
# zonecfg -z itzone
zonecfg:itzone> add capped-memory
zonecfg:itone:capped-memory> set physical=50m
zonecfg:itzone:capped-memory> set swap=100m
zonecfg:itzone:capped-memory> set locked=30m
zonecfg:itone:capped-memory> end
zonecfg:itzone> verify
zonecfg:itzone> commit
zonecfg:itzone> exit
```

Quiz

To display the resource pool configuration that is currently in use, which of the following commands will you use?

a. `poolstat -r all`
b. `poolcfg -c info`
c. `poolcfg –r all`
d. `poolcfg -dc info`
e. `poolstat –c info`
f. `poolstat –dc info`

Quiz

The `pooladm –c` command validates and commits the modified resource pool configuration file.

a. True

b. False

Practice 7-1 Overview: Allocating Resources to Zones

This practice covers the following topics:

- Enabling services for resource pools
- Configuring a persistent resource pool
- Binding the zone to a persistent resource pool
- Removing the resource pool configuration

Agenda

- Explaining the fundamentals of Oracle Solaris 11 zones
- Managing system resources in a zone
- Migrating Oracle Solaris 10 systems
- Configuring Kernel Zones
- Working with Unified Archives

Migrating Oracle Solaris 10 Systems

- Migrating Oracle Solaris 10 zones
- Migrating Oracle Solaris 10 global zones

Migrating Oracle Solaris 10 Zones

1. Assess the Oracle Solaris 10 zone to be migrated.
2. Create an archive of the Oracle Solaris 10 zone to be migrated.
3. Prepare the Oracle Solaris 11 target system.
4. Migrate the Oracle Solaris 10 zone.

Migrating Oracle Solaris 10 Global Zones

1. Assess the global zone to be migrated.
2. Create an archive of the global zone to be migrated.
3. Prepare the Oracle Solaris 11 target system.
4. Migrate the Solaris 10 global zone.

Practice 7-2: Overview

- 7-2: Migrating an Oracle Solaris 10 Global Zone to Oracle Solaris 11

Agenda

- Explaining the fundamentals of Oracle Solaris 11 zones
- Managing system resources in a zone
- Migrating Oracle Solaris 10 systems
- Configuring Kernel Zones
- Working with Unified Archives

ORACLE

Kernel Zones Overview

- New in Oracle Solaris 11.2 release
- Is managed by from the global zone by using the existing tools
- Is a new zone brand with brand name as “`solaris-kz`” and pronounced as “kernel zones”.
- Is managed by using existing tools such as `zonecfg`, `zoneadm`, and `zlogin`
- Provides a full kernel and user environment within a zone
- Increases kernel separation between the host and the global zone
- Provides greater flexibility in configuring and managing the zone than a default `solaris` zone
- Requires installing the `brand-solaris-kz` package

Why Kernel Zones?

From a technology perspective, in a nonglobal zone:

- The OS software layer must match across all instances on the same host
- Differing SRU/update levels for zones on the same host is not possible
- Suspending, resuming, and live migrating is not possible
- Managing ZFS pools and running a Common Internet File System (CIFS) server is not possible

From a customer perspective, in nonglobal zones:

- Aligning outage window to virtual environments is problematic
- Consolidating applications that require different OS versions is not possible
- Performing hardware maintenance on a system is not possible

ORACLE

Capabilities of Kernel Zones

The capabilities of kernel zones are derived from the following major design principles:

- Full zones integration
- Cross-platform implementation
- Emulation free
- Security
- Isolation
- Virtualization
- Granularity
- Transparency

System Requirements for Using Oracle Solaris Kernel Zones

To use kernel zones, your host hardware and host operating system must meet the following requirements:

- Operating system version of Oracle Solaris 11.2 or higher.
  - For SPARC systems:
    - A T4 SPARC system with System Firmware 8.5.0 or later
    - A T5, M5, or M6 system with System Firmware 9.2.0 or later
  - For X86 systems:
    - Nehalem+(Intel) or Barcelona+(AMD) based machines with:
      - CPU virtualization (for example, VT-x) enabled in the BIOS
      - Extended/Nested Page Table support, also referred to as EPT, NPT, or Rapid Virtualization Indexing (RVI)

In addition, both SPARC and x86 systems require:

- Minimum of 8 GB of RAM
- Kernel zone brand package, `brand/brand-solaris-kz`
- ZFS ARC tuning on the host

Auxiliary States

- Kernel zones use auxiliary states to communicate supplementary state information to the global zone.
- A kernel zone does not have an auxiliary state set by default.
- Auxiliary states are set only when you initiate debugging and kernel maintenance operations.
- The available kernel zone auxiliary states are:
  - `suspended`
  - `debugging`
  - `panicked`
- To view the global zone current state and the kernel zone auxiliary states, use the `zoneadm list –s` command.

```
global# zoneadm list -s
NAME    STATUS              AUXILIARY          STATE
global  running
kzone1  running
kzone2  running
kzone3  running            debugging
```

Configuring Kernel Zones

1. Install and verify whether kernel zone packages are installed on the global zone.

```
# pkg install brand/brand-solaris-kz
# pkg list brand/brand/brand-solaris-kz
```

2. Create a new kernel zone configuration.
3. Add any additional kernel zone resources such as CPUs, memory, storage devices, and network devices.
4. Install the kernel zone by using the `zoneadm -z` <*zonename*> `install` command.
5. Boot the kernel zone by using the `zoneadm -z` <*zonename*> `boot` command.
6. Log in to the zone by using the `zlogin -C` <*zonename*> command.

ORACLE

Configuring Kernel Zones

```
globalzone# zonecfg -z kzone1
Use 'create' to begin configuring a new zone.
zonecfg:kzone1> create -t SYSsolaris-kz
zonecfg:kzone1> add virtual-cpu
zonecfg:kzone1:virtual-cpu> set ncpus=8
zonecfg:kzone1:virtual-cpu> end
zonecfg:kzone1> info virtual-cpu
virtual-cpu:
ncpus: 8
zonecfg:kzone1> add device
zonecfg:kzone1:device> set match=/dev/rdsk/c9t0d0
zonecfg:kzone1:device> set id=4
zonecfg:kzone1:device> end
zonecfg:kzone1> info device
device:
match not specified
    storage.template: dev:/dev/zvol/dsk/%{global-
      rootzpool}/VARSHARE/zones/%{zonename}/disk%{id}
    storage: dev:/dev/zvol/dsk/rpool/VARSHARE/zones/kzone1/disk0
    id: 0
```

Configuring Kernel Zones

```
(continued...)

    bootpri: 0
device:
    match: /dev/rdsk/c9t0d0
    storage not specified
    id: 4
    bootpri not specified
zonecfg:kzone1> select capped-memory
zonecfg:kzone1:capped-memory> set physical=2048m
zonecfg:kzone1:capped-memory> end
zonecfg:kzone1> add anet
zonecfg:kzone1:anet> set id=3
zonecfg:kzone1:anet> end
zonecfg:kzone1> verify
zonecfg:kzone1> commit
zonecfg:kzone1> exit
# zoneadm -z kzone1 install
# zoneadm -z kzone1 boot
# zlogin -C kzone1
```

Host Data and Host ID

- Each kernel zone bootable device contains state information known as host data.
- A kernel zone's host data monitors kernel zone state information including:
  - Zone usage
  - Zone suspends
  - Time of day offset between the kernel zone clock and the global zone clock
  - OpenBoot variables (SPARC only)

Host Data and Host ID

- If the boot storage is in use, the kernel zone enters the `unavailable` state and displays an error message.
- If it is not in use, the kernel zone can be repaired by using the `zoneadm attach -x force-takeover` command.

```
global# zoneadm -z kzone1 attach
zone 'kzone1': error: ERROR: zone kzone1 is in use by host with
hostid 848611d4
zone 'kzone1': error: last known state: installed
zone 'kzone1': error: hostname: global2
zone 'kzone1': error: boot environment name: solaris-1
zone 'kzone1': error: boot environment uuid:
69ed2e6a-e25a-6d36-e022-ed7261ed8899
zone 'kzone1': error: last update time: Sun Apr 13 20:08:13 2014
zone 'kzone1': error: To fix, detach the zone from the other host then
attach it to this host
zone 'kzone1': error: If the zone is not active on another host,
attach it with
zone 'kzone1': error: zoneadm -z kzone1 attach -x force-takeover
```

ORACLE

Boot Loader

- The kernel zone boot loader manages booting operations on the kernel zone.
- To invoke the boot loader, the kernel zone must be in the `ready` or `installed` state.
- You can use the kernel zone boot loader to perform the following operations:
  - List alternative BEs
  - Boot the zone to an alternative BE
- To invoke the kernel zone boot loader, use the `zoneadm boot` command.

ORACLE

Boot Loader

To specify an alternative BE in a kernel zone:

1. Log in to the zone console.

```
# zlogin -C zonename
```

2. In a separate terminal window, list the available kernel zone BEs.

```
# zoneadm -z zonename boot -- -L
```

3. Boot to a selected BE.

```
# zoneadm -z zonename boot -- -Z boot-environment
```

ORACLE

Cloning a Kernel Zone

- Cloning allows you to make copies of an existing configured and installed zone.
- The cloned zone includes any changes that were made to customize the existing zone.
- Cloning a zone is an efficient way to add additional zones with a similar customized zone configuration.
- You can clone a kernel zone in the following ways:
  - By using the `zoneadm clone` command
  - By using Unified Archives

ORACLE

Cloning by Using `zoneadm clone`

In the following example, the kernel zone `kzone1` is cloned to the kernel zone `kzone2` on the host `global`:

1. To create a clone, you need to first halt that zone.

```
global# zoneadm -z kzone1 halt
```

2. Create a new zone configuration.

```
global# zonecfg -z kzone2 create -t kzone1
```

3. Clone the zone by using the `zoneadm clone` command.

```
global# zoneadm -z kzone2 clone kzone1
```

ORACLE

Cloning by Using Unified Archives

Cloning by using Unified Archives is recommended for large deployments.

Note: You will learn more about cloning by using Unified Archives in the next section “Working with Unified Archives.”

Suspending and Resuming a Kernel Zone

- The suspend operation is unique to kernel zones.
- You can suspend a kernel zone to disk by means of the `zoneadm suspend` command.
- The `zoneadm suspend` command places a kernel zone in the `suspended` state.
- You can resume a suspended zone by invoking the `zoneadm boot` command.
- Suspend and resume are supported only if a kernel zone has the `suspend` resource property in its configuration.

```
global# zonecfg -z kzone1 info suspend
suspend:
path: /system/zones/kzone1/suspend
storage not specified
```

Warm Migrating a Kernel Zone

The following example warm migrates the `kzone1` zone onto the new host:

1. On the global zone, suspend the file system on the kernel zone to be migrated.

```
global# zoneadm -z kzone1 suspend
```

2. Detach the kernel zone file system on the global zone.

```
global# zoneadm -z kzone1 detach
```

3. Export the zone configuration and transfer the file onto the new host.

```
global# zonecfg -z kzone1 export | ssh root@global2 \
zonecfg -z kzone1 -f -
```

Warm Migrating a Kernel Zone

4. Attach the zone on the new host.

```
global2# zoneadm -z kzone1 attach
```

5. Boot the kernel zone on the new host to resume the migrated zone.

```
global2# zoneadm -z kone1 boot
```

Quiz

To migrate a Kernel zone, you need to first halt it, detach it, and then attach it on the remote machine.

a. True

b. False

Quiz

Which are the following are the available kernel zone auxiliary states?

a. panicked

b. detached

c. configured

d. suspended

e. debugged

Practice 7-3 Overview: Configuring Kernel Zones (Demonstration)

This practice provides steps to access a demonstration on the Kernel zones feature as part of which you will get to observe the following:

- Configuring Kernel zones
- Cloning a Kernel zone
- Warm migration of a Kernel zone

Note: This practice is only a demonstration.

ORACLE

Agenda

- Explaining the fundamentals of Oracle Solaris 11 zones
- Managing system resources in a zone
- Migrating Oracle Solaris 10 systems
- Configuring Kernel Zones
- Working with Unified Archives

Archival Before Oracle Solaris 11

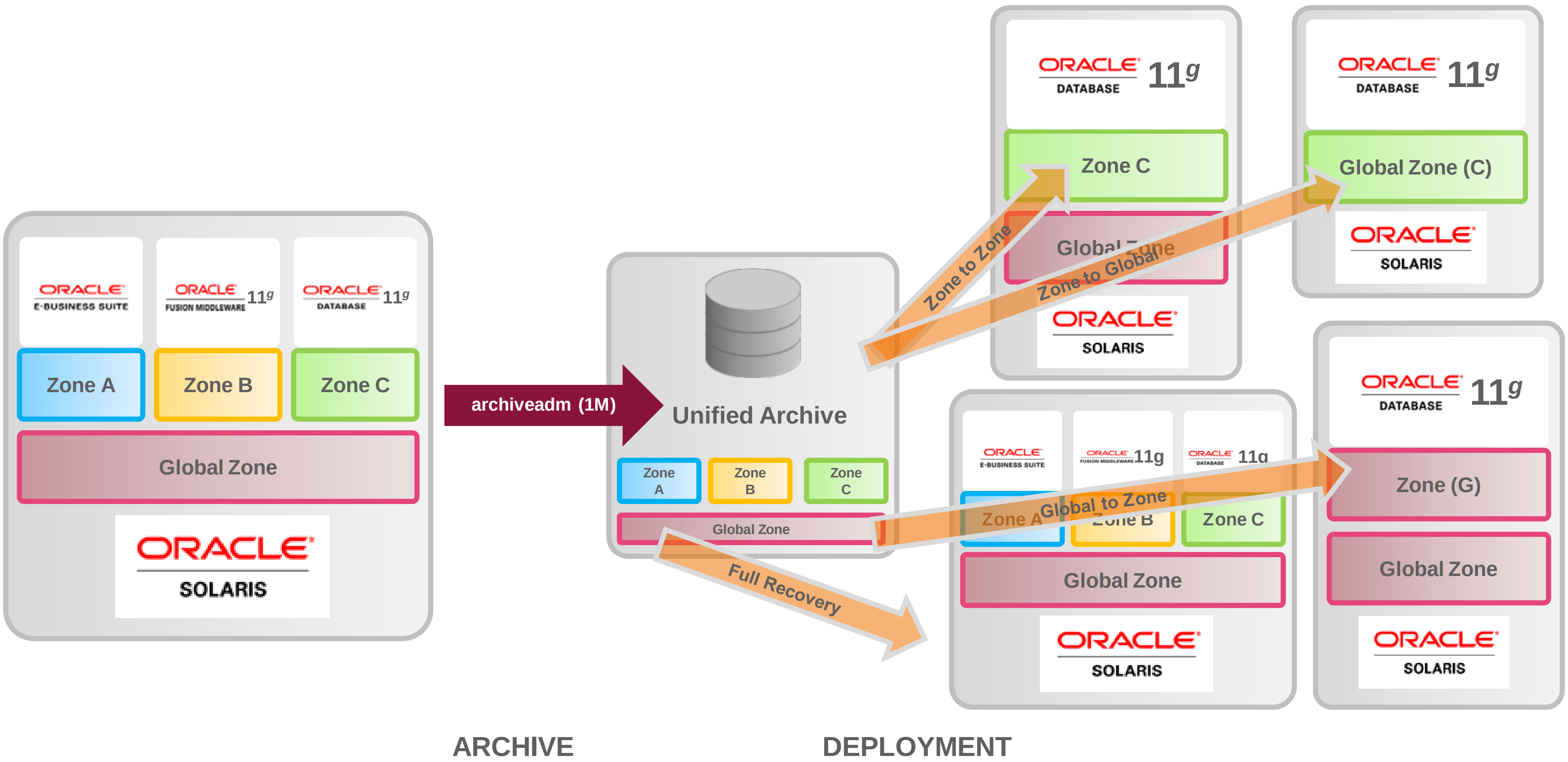
- Before Oracle Solaris 11, the default archive solution was the Oracle Solaris Flash Archive.
- Flash archives were designed to create and deploy OS instances of and to bare metal systems.
- With the introduction of BEs, IPS, and virtualization technologies, a more robust archive solution became possible.
- Unified Archives employs these technologies and provides a much more flexible and extensible solution.

Oracle Solaris Unified Archives Overview

- A new native archive type for Oracle Solaris, which may contain a global zone, a nonglobal zone, or a kernel zone
- Allows multiple system instances to be archived in a single unified file format
- Allows deploying the archives to recover a system by using one of the following methods:
  - Automated Installer (AI)
  - Zones utilities
  - Bootable media
- Provides `archiveadm` command-line utility to create the archive
- Provides the following main functions:
  - System recovery
  - System cloning
  - System migration

ORACLE

Oracle Solaris Unified Archives Overview



Key Terms

Terms	Description
System	A single deployed instance of an operating environment.
Archive	Set of system data and metadata which describes it and the system(s)
System Image	A specific system's data within an archive or elsewhere
Unified Archive	One or more system images bundled into a single archive. More specifically, an OVF-compliant OVA file with a nontraditional stream-based payload.

ORACLE

Unified Archives Types

Following are the two types of Unified Archives:

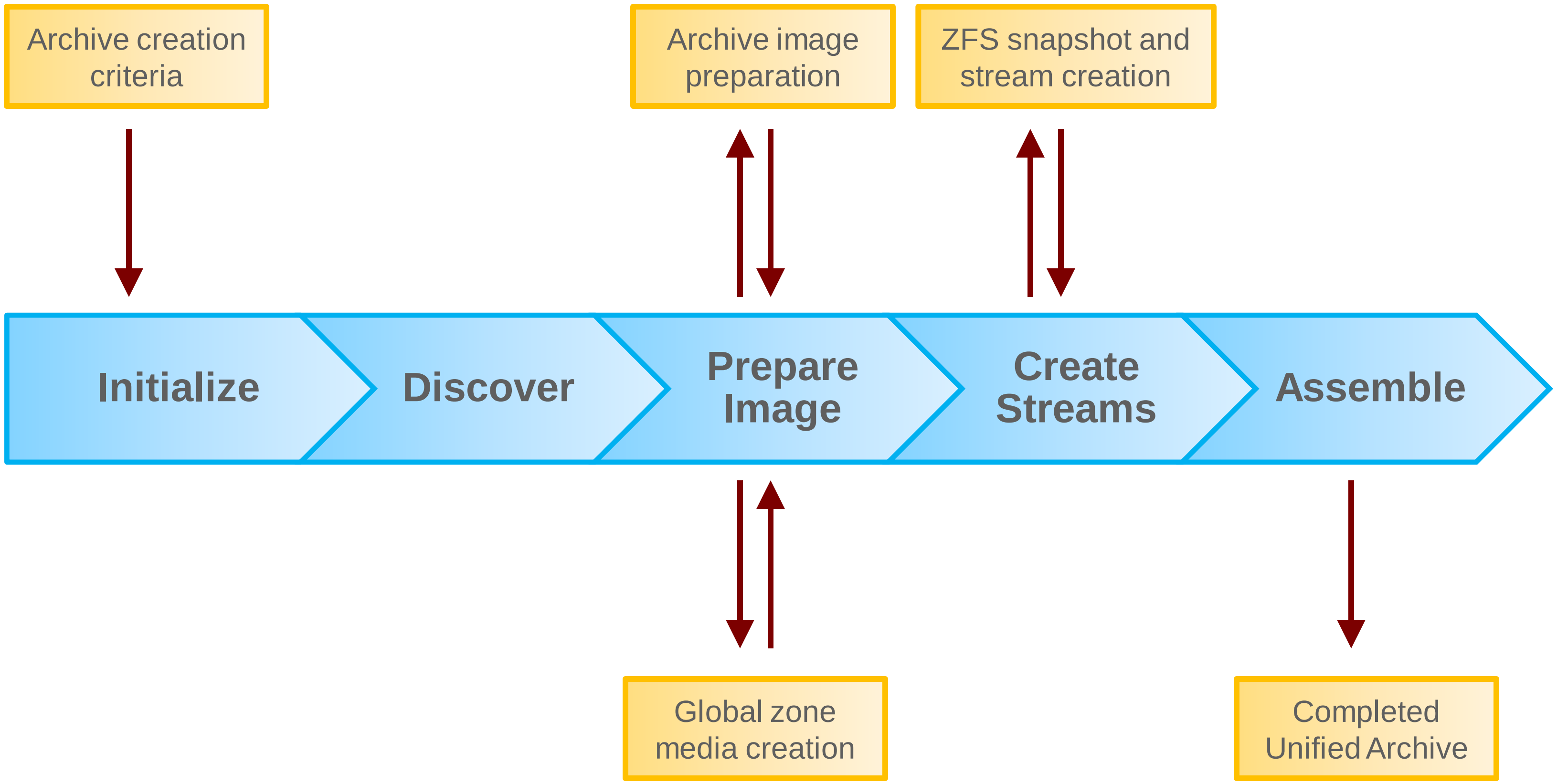
Unified Archive Types	**Description**
Clone archive	Allows archiving only one BE at a time
Recovery archive	Allows creating a full-system archive containing all boot environments from all included instances

Clone Archive	**Recovery archive**
Individually deployable systems	Single deployable system
Active BEs only	Active and Inactive BEs
Used for cloning	Used for recovery and migration

Platform Portability

- The requirement for platform compatibility is that the systems be of the same instruction set architecture (ISA).
- Unified Archives also enable image transforms.
- However, there are some systems that cannot be transformed, such as:
  - Oracle Solaris 10 brand zones
  - Trusted Solaris or labeled zone archives

Unified Archives Creation



Creating a Clone Archive

- By default, a clone archive is created.
- Use the `archiveadm create <archive-name>` command to create a clone archive.

```
# archiveadm create -z kzone1 /var/tmp/kzone1.uar
Initializing Unified Archive creation resources...
Unified Archive initialized: /var/tmp/kzone1.uar
Logging to: /system/volatile/archive_log.29929
Executing dataset discovery...
Dataset discovery complete
Creating install media for zone(s)...
Media creation complete
Preparing archive system image...
Beginning archive stream creation...
Archive stream creation complete
Beginning final archive assembly...
Archive creation complete
# archiveadm info /var/tmp/kzone1.uar
Archive Information
          Creation Time:  2014-05-28T10:16:01Z
            Source Host:  t4-1ou
           Architecture:  sparc
       Operating System:  Oracle Solaris 11.3 SPARC
      Deployable Systems: kzone1
```

Creating a Recovery Clone

Use the `archiveadm create -r <archive-name>` command to create a recovery clone.

```
# archiveadm create -r -z global /var/tmp/globalrecovery.uar
Initializing Unified Archive creation resources...
Unified Archive initialized: /var/tmp/globalrecovery.uar
Logging to: /system/volatile/archive_log.11234
Executing dataset discovery...
Dataset discovery complete
Preparing archive system image...
Beginning archive stream creation...
Archive stream creation complete
Beginning final archive assembly...
Archive creation complete
# archiveadm info globalrecovery.uar
Archive Information
             Creation Time: 2013-10-03T18:13:21Z
               Source Host: example
              Architecture: i386
          Operating System: Oracle Solaris 11.3 X86
        Deployable Systems: global
```

Deploying Unified Archives

- After an archive is created, you can store it as a file until it needs to be deployed.
- Deployment scenarios include:
  - System recovery
  - System cloning
  - System migration
- Archive deployment modes are:
  - Oracle Solaris Automated Installer (AI)
  - Oracle Solaris Zones utilities
  - Bootable media

ORACLE

Deploying a Zone from Unified Archives by Using Zones Utilities

1. Select a zone configuration to use or create one.
   - If you have already created a zone configuration, skip to Step 2.
   - If you need to create a zone configuration from an existing archive, use the following steps.
     A. Clone the zone configuration using the archive.

```
# zonecfg -z new-zone create -a archive
```

     B. Verify that the zone configuration was created.

```
# zoneadm list -cv
```

2. Install and boot the zone.

```
# zoneadm -z new-zone install –a archive
# zoneadm -z new-zone boot
```

Deploying an Archive Using AI

To deploy an archive by using AI:

- You must have a compatible AI service and AI manifest
  - For example, if the archived system is Oracle Solaris 11.3 FCS, any Oracle Solaris 11.3 version AI service is compatible.
- You have to modify the AI manifest to include the following information:
  - The location of the archive
  - The name of the systems the archive should be deployed to

Note: Each archive does not require its own service. The specific archive deployed is determined by the manifest used for a specific deployment.

Deploying a System from Unified Archives by Using AI

1. If required, create a new install service.

```
# installadm create-service -n new-service -s <ISO_source_or_FMRI_location>
```

2. Edit the default manifest XML file to reference the Unified Archive or create a new manifest with the updated manifest XML file.

```
# installadm create-manifest -n svcname -m manifest -f file
```

3. Confirm whether the service was created and the new manifest was applied to the service.

```
# installadm list -n new-service
# installadm list –m manifest-file
```

ORACLE

Deploying an Archive Using Bootable Media

1. Create a media image from an existing archive.

```
# archiveadm create-media archive-name
```

   – For example, to create an ISO image, you must include the `-f` option.

```
# archiveadm create-media -f iso archive.uar
```

2. Create bootable media.
   – ISO images: Burn the `.iso` file to a CD or DVD.
   – USB images: Use the `usbcopy` utility to copy the image to a USB flash drive.
3. Boot from the media.

Troubleshooting Cloning and Archiving

- Issues may be encountered when creating and deploying Unified Archives.
- Most issues related to archive creation involve system configuration, available space for archive storage, and connectivity to the package repositories, which are used to prepare the image for redeployment.
- Common deployment issues include target configuration and selection problems and failure to configure the deployed system.
- In the case of archive creation or deployment errors, logging files are created. These files contain detailed data regarding the errors encountered.

Note: With Solaris Kernel Zones, some log files may be within the specific zone.

ORACLE

Practice 7-4 Overview: Working with Unified Archives (Demonstration)

Note: This practice is only a demonstration.

Summary

In this lesson, you should have learned how to:

- Explain the fundamentals of Oracle Solaris 11 zones
- Manage system resources in a zone
- Migrate Oracle Solaris 10 systems
- Configure kernel zones
- Work with Unified Archives

8

Securing the Oracle Solaris 11 OS

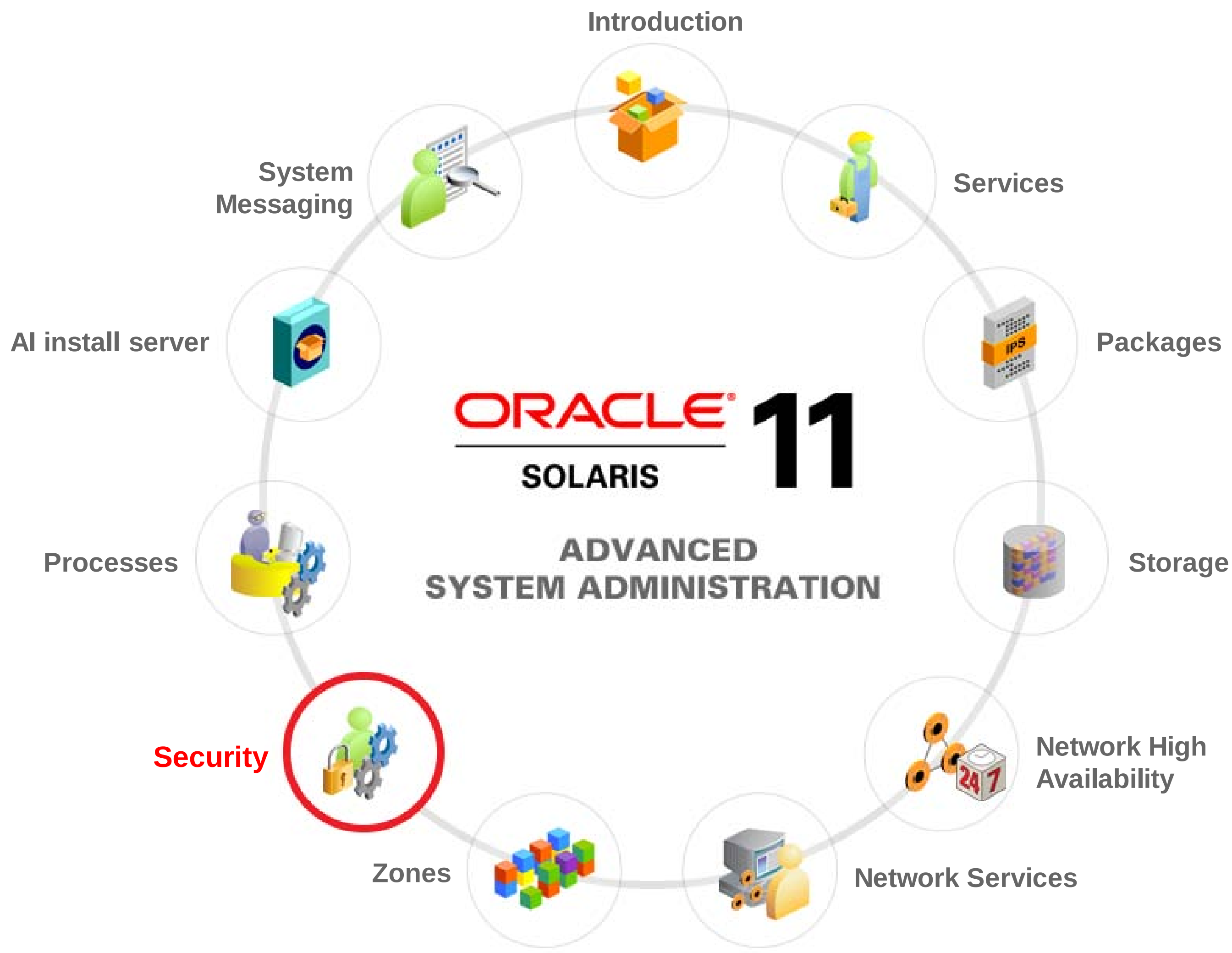
ORACLE

Objectives

After completing this lesson, you should be able to:

- Implement user privileges and roles
- Manage privileges
- Manage user rights
- Verify file integrity by using BART
- Monitor the audit service
- Assess the compliance of an Oracle Solaris system

Workflow Orientation



Agenda

- Implementing privileges, rights, and roles
- Managing privileges
- Managing user rights
- Verifying file integrity by using BART
- Monitoring the audit service
- Assessing the compliance of an Oracle Solaris system

ORACLE

Importance of Assigning User Privileges and Roles

It is important to assign user privilege and roles to ensure that:

- Processes and users have the appropriate level of access they need to perform their functions
- A company's requirements for process rights management and role-based access control are met

Process Rights Management and Privileges

- Process rights management is implemented by *privileges.*
- Privileges:
  - Enable processes to be restricted at the command, user, role, or system-specific resource level
  - Decrease the security risk associated with one user or one process having full superuser capabilities on a system
  - Enable gradation between user capabilities and root capabilities
  - Restrict programs and processes to only the capabilities that the program requires (the principle of “least privilege”)

Privilege Descriptions

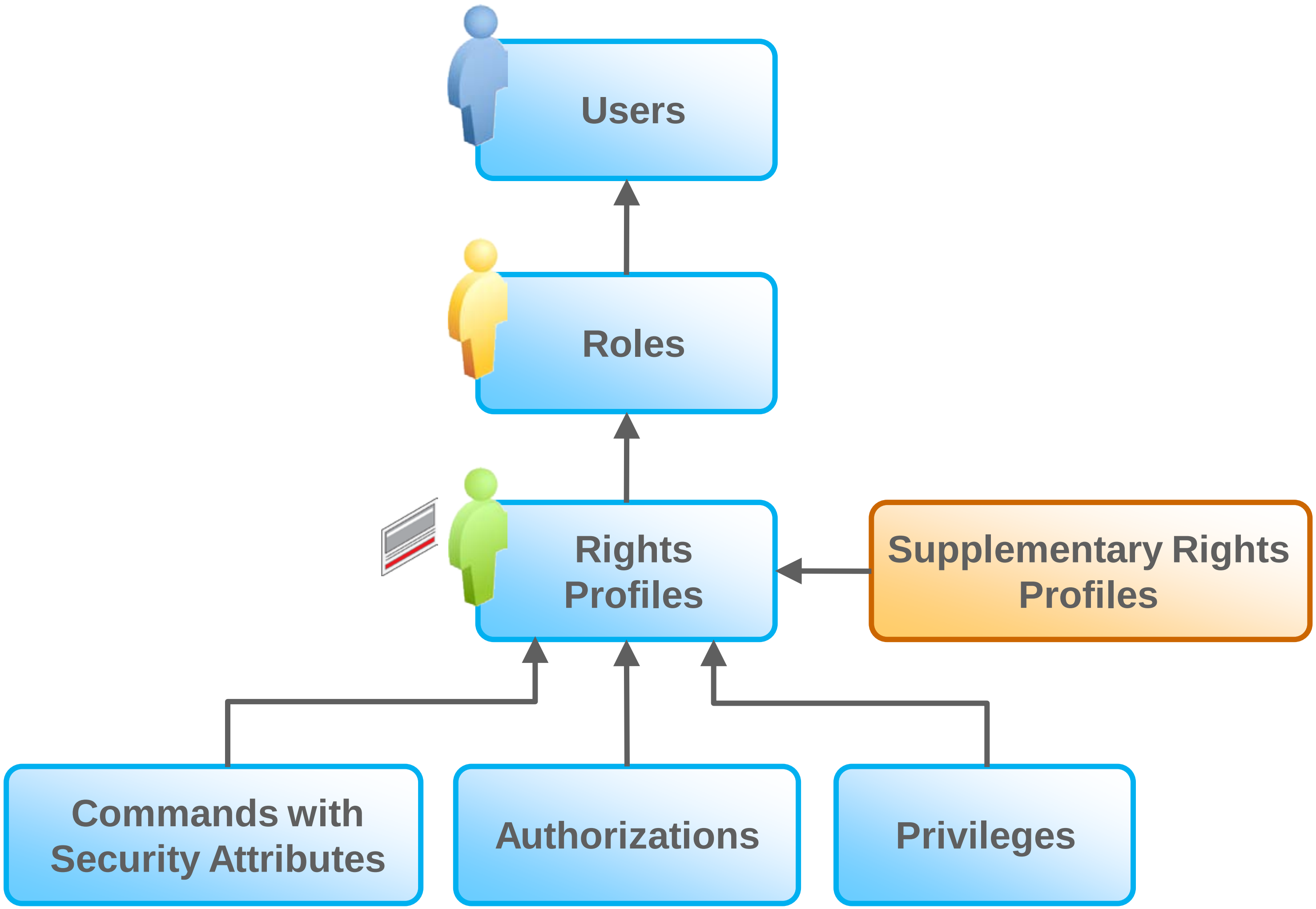
Area of Privilege	Description
`FILE` privileges	Privileges that begin with the string `file` operate on file system objects.
`IPC` privileges	Privileges that begin with the string `ipc` override IPC object access controls.
`NET` privileges	Privileges that begin with the string `net` give access to specific network functionality.
`PROC` privileges	Privileges that begin with the string `proc` allow processes to modify restricted properties of the process itself.
`SYS` privileges	Privileges that begin with the string `sys` give processes unrestricted access to system properties.

Implementing Privileges

Privilege Set	Description
Effective privilege set (E)	Set of privileges that are currently in effect
Inheritable privilege set (I)	Set of privileges that a process can inherit across a call to `exec()`
Permitted privilege set (P)	Set of privileges that are available for use
Limit privilege set (L)	Outside limit of the privileges that are available to a process and its children. By default, the limit set is `all` privileges

```
E (Effective): basic
I (Inheritable): basic
P (Permitted): basic
L (Limit): all
```

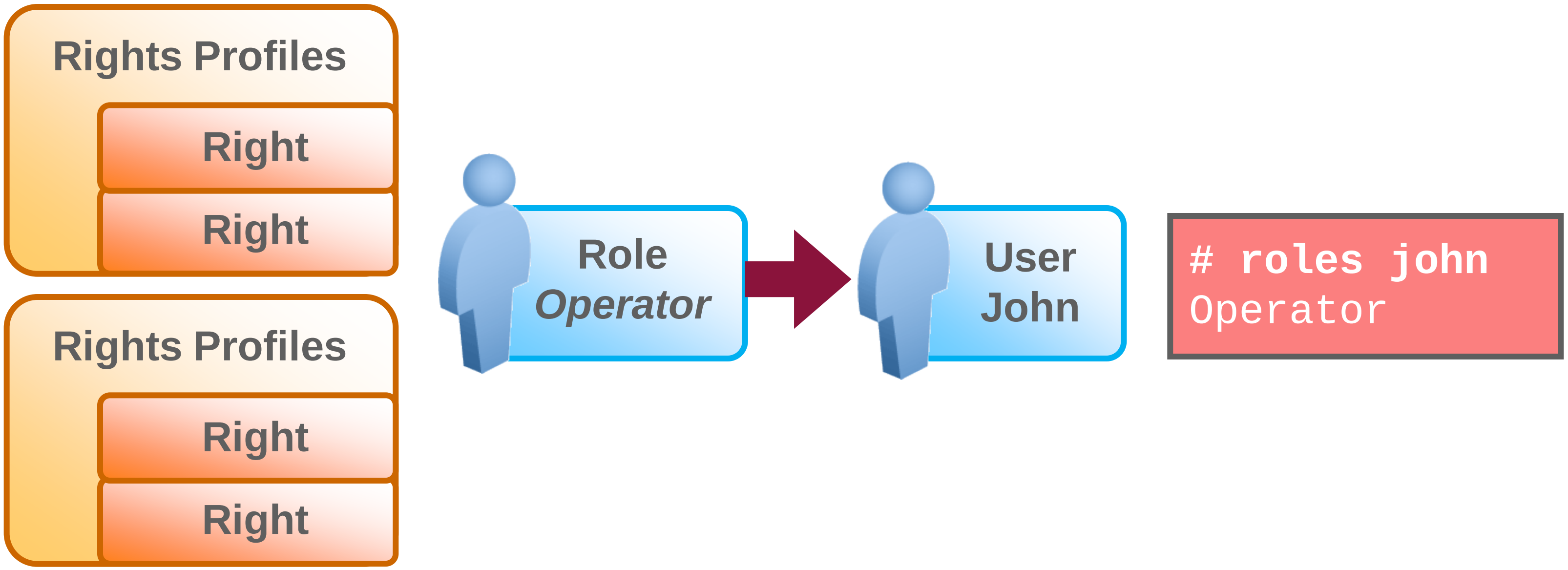
User Rights Management



Roles

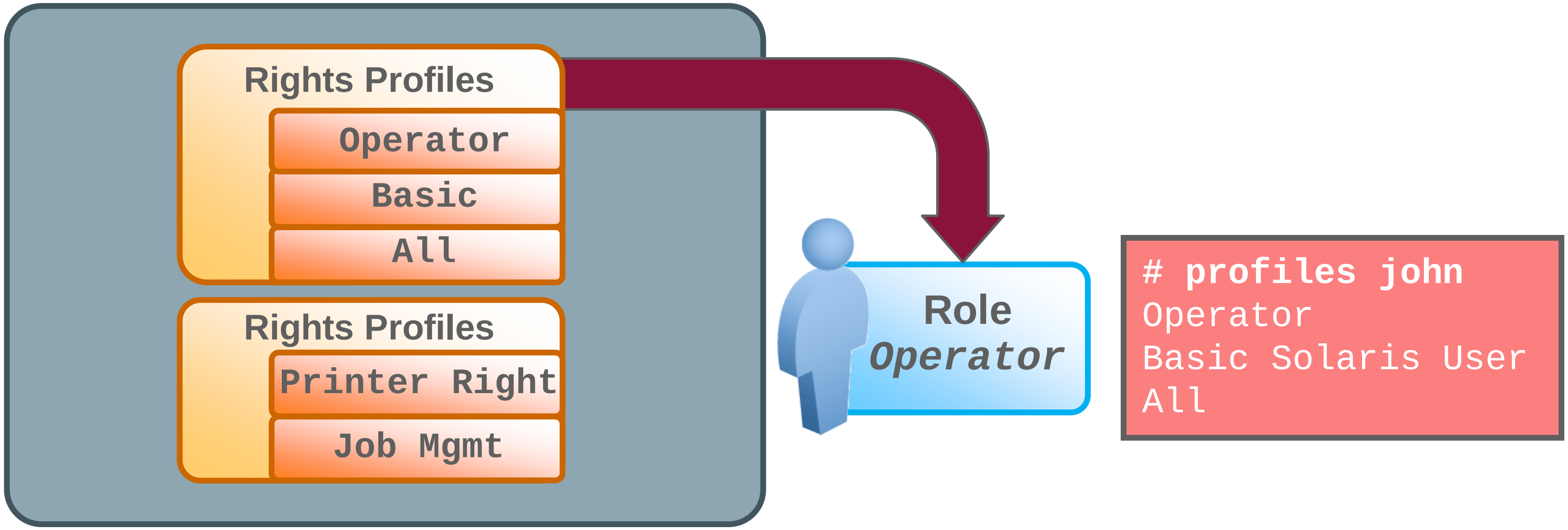
A role:

- Is a special type of user account that performs a set of administrative tasks
- Contains one or more rights profiles
- Provides access to restricted functionality



Rights Profile

- Is a collection of rights that can be assigned to a user or role
- Rights are commands or scripts that are run with special security attributes.



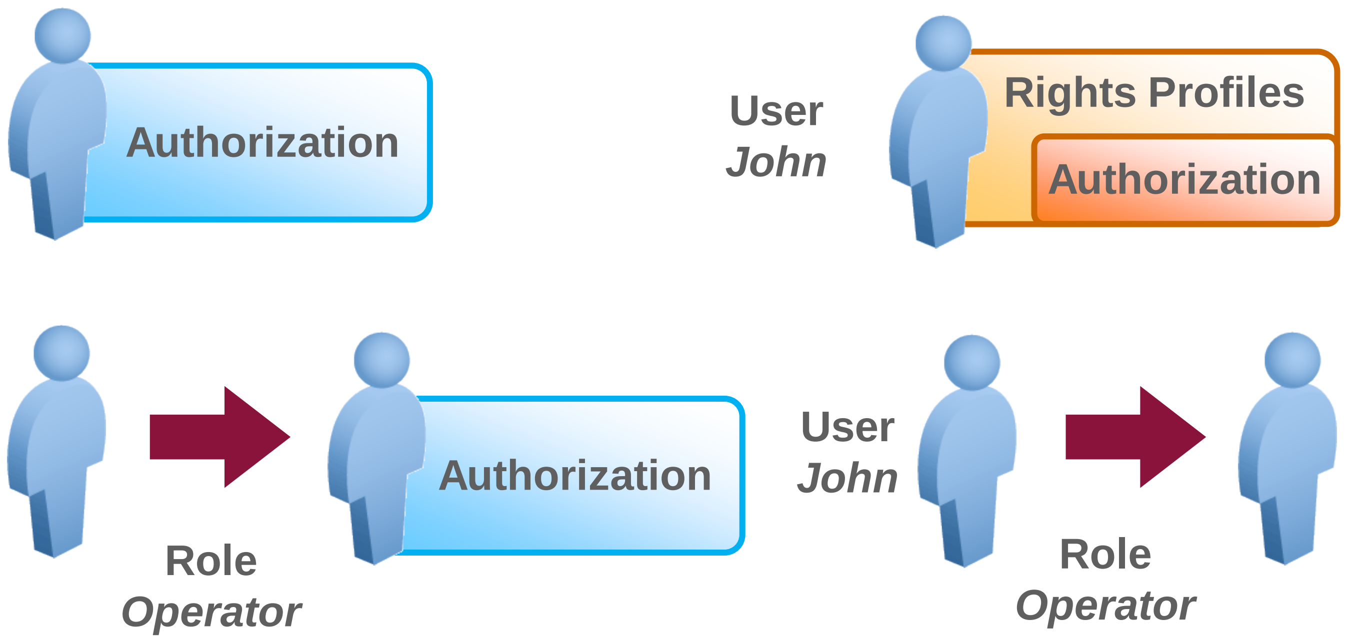
Basic Solaris User Rights Profile

```
# getent prof_attr | grep ‘Basic Solaris User’
Basic Solaris User:RO::Automatically assigned
rights:auths=solaris.mail.mailq,solaris.network.autoconf.read,solaris.ad
min.wusb.read;profiles=All;help=RtDefault.html
```

Interpreting the `/etc/security/policy.conf` File

```
# cat /etc/security/policy.conf
<header and copyright output omitted>
#
AUTHS_GRANTED=
PROFS_GRANTED=Basic Solaris User
AUTH_PROFS_GRANTED=
CONSOLE_USER=Console User
#PAM_POLICY=
# crypt(3c) Algorithms Configuration
#
# CRYPT_ALGORITHMS_ALLOW specifies the algorithms that are allowed to
# be used for new passwords. This is enforced only in crypt_gensalt(3c).
#
CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6
<output omitted>
#CRYPT_ALGORITHMS_DEPRECATE=__unix__
...
CRYPT_DEFAULT=5
#PRIV_DEFAULT=basic
#PRIV_LIMIT=all
#
# LOCK_AFTER_RETRIES specifies the default account locking policy for local
# user accounts (passwd(4)/shadow(4)). The default may be overridden by
# a user's user_attr(4) "lock_after_retries" value.
# YES enables local account locking, NO disables local account locking.
# The default value is NO.
#
#LOCK_AFTER_RETRIES=NO
```

Authorizations and Privileges

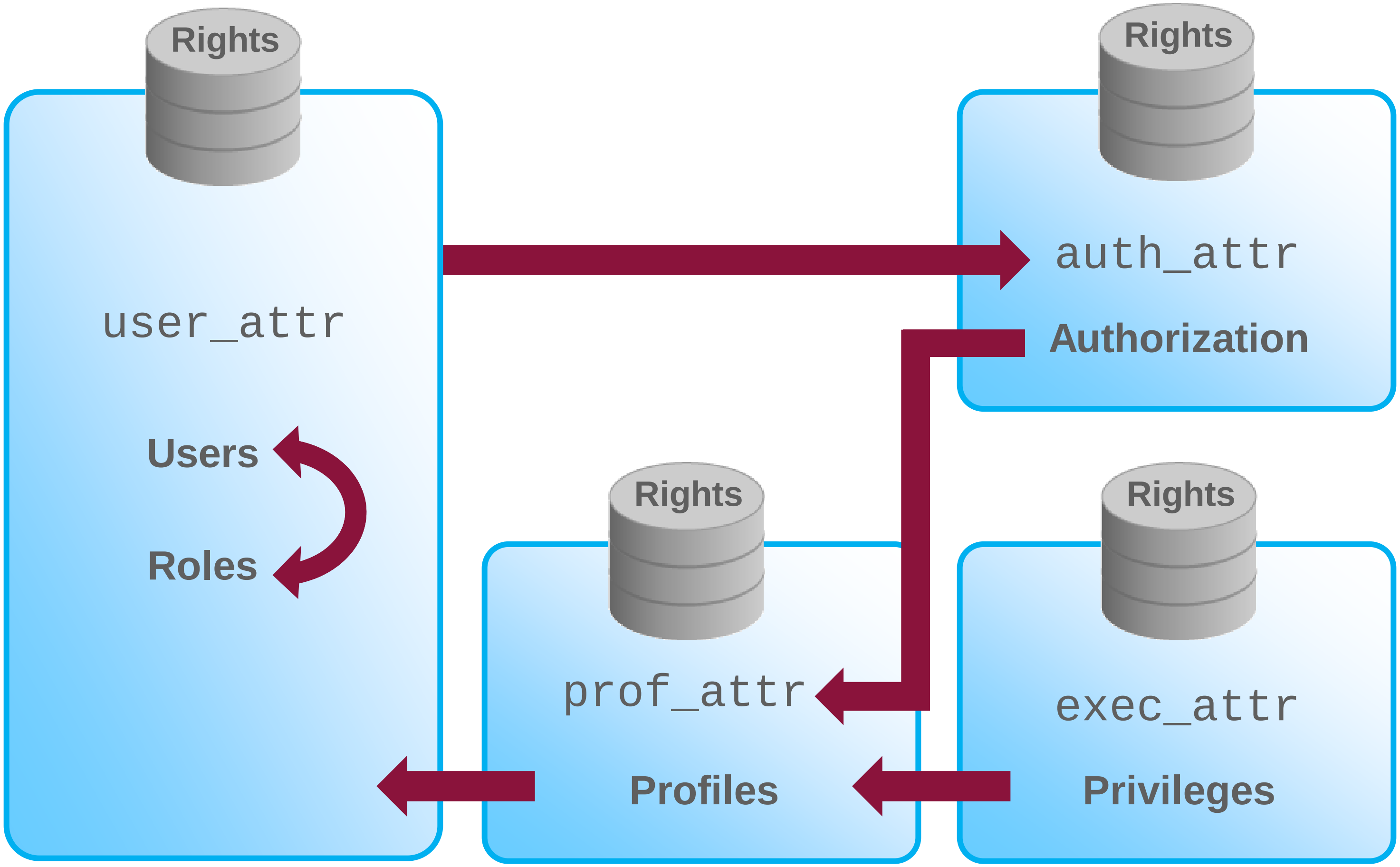



```
# auths john
solaris.admin.wusb.read,solaris.mail.mailq,sola
ris.network.autoconf.read
```

Security Attributes

- Enable a process to perform an operation that is otherwise forbidden to regular users
- Include authorizations, privileges, and `setuid` and `setgid` programs
- Can be assigned to a user

Key Rights Databases



Interpreting the `user_attr` Database

```
# getent user_attr | grep chris
chris::::profiles=Printer Management
```

Interpreting the `auth_attr` Database

```
# getent auth_attr | more
solaris.smf.read.ocm:::Read permissions for protected Oracle Configuration Manager
Service Properties::
solaris.smf.value.ocm:::Change Oracle Configuration Manager System Repository
Service values::
solaris.smf.manage.ocm:::Manage Oracle Configuration Manager System Repository
Service states::
solaris.smf.manage.dbus:::Manage D-BUS Service States::help=SmfDBUSStates.html
solaris.:RO::All Solaris Authorizations::help=AllSolAuthsHeader.html
solaris.account.:RO::Account Management::help=AccountHeader.html
solaris.account.setpolicy:RO::Change the account policy
settings::help=AccountSetPolicy.html
solaris.account.activate:RO::Sets the initial password for a newly created
account::help=AccountActivate.html
solaris.admin.edit:RO::Edit Administrative Files::help=AdminEdit.html
solaris.admin.idmap.rules:RO::Manage Identity Mapping Rules::help=IdmapRules.html
solaris.admin.wusb.:RO::Administer Wireless USB::help=WUSBHeader.html
solaris.admin.wusb.read:RO::Read Wireless USB Host and Device
Information::help=WUSBread.html
solaris.admin.wusb.modify:RO::Add or delete information of Wireless USB
Device::help=WUSBmodify.html
solaris.admin.wusb.host:RO::Manage Wireless USB Host::help=WUSBhost.html
solaris.audit.:RO::Audit System-wide Management::help=AuditHeader.html
<output omitted>
```

ORACLE

Interpreting the exec_attr Database

```
# getent exec_attr | grep 'Network Management'
Network
Management:solaris:cmd:RO::/usr/sbin/dladm:euid=dladm;egid=netadm;privs=sys_dl_conf
ig,net_rawaccess,proc_audit
Network Management:solaris:cmd:RO::/usr/sbin/dlstat:euid=dladm;egid=sys
Network
Management:solaris:cmd:RO::/usr/sbin/flowadm:euid=dladm;egid=sys;privs=sys_dl_confi
g,net_rawaccess,proc_audit
Network Management:solaris:cmd:RO::/usr/sbin/flowstat:euid=dladm;egid=sys
Network
Management:solaris:cmd:RO::/usr/sbin/ipadm:euid=netadm;egid=netadm;privs=sys_ip_con
fig,net_rawaccess
Network Management:solaris:cmd:RO::/usr/bin/ipstat:privs=dtrace_kernel
Network Management:solaris:cmd:RO::/usr/bin/netstat:uid=0
Network Management:solaris:cmd:RO::/usr/bin/rup:euid=0
Network Management:solaris:cmd:RO::/usr/bin/ruptime:euid=0
Network Management:solaris:cmd:RO::/usr/bin/setuname:euid=0
Network Management:solaris:cmd:RO::/usr/bin/tcpstat:privs=dtrace_kernel
Network Management:solaris:cmd:RO::/usr/sbin/asppp2pppd:euid=0
Network Management:solaris:cmd:RO::/usr/sbin/ifconfig:uid=0
Network Management:solaris:cmd:RO::/usr/sbin/ipaddrsel:euid=0
Network Management:solaris:cmd:RO::/usr/sbin/ipqosconf:euid=0
Network Management:solaris:cmd:RO::/usr/sbin/rndc:privs=file_dac_read
Network Management:solaris:cmd:RO::/usr/sbin/route:privs=sys_ip_config
...
<output truncated>
```

ORACLE

Interpreting the prof_attr Database

```
# getent prof_attr | more
TPM Administration:RO::Administer Privileged TPM
Operations:auths=solaris.smf.manage.tcsd,solaris.smf.value.tcsd
Desktop Configuration:RO::Configure graphical desktop
software:auths=solaris.smf.manage.x11,solaris.smf.manage.font,solaris.smf.manage.op
engl,solaris.smf.manage.dt.login
D-BUS Management:RO::Manage D-
BUS:auths=solaris.smf.manage.dbus;help=RtDBUSMngmnt.html
CUPS Administration:RO:::auths=solaris.smf.manage.cups
DTrace Toolkit::::
Software Installation:RO::Add application software to the
system:auths=solaris.smf.manage.servicetags;profiles=ZFS File System
Management;help=RtSoftwareInstall.html
Device Security:RO::Manage devices and Volume
Manager:auths=solaris.smf.manage.dt.login,solaris.device.*,solaris.smf.manage.vt,so
laris.smf.manage.allocate,solaris.smf.value.keymap;help=RtDeviceSecurity.html
NTP Management:RO::Manage the NTP
service:auths=solaris.smf.manage.ntp,solaris.smf.value.ntp
...
...
Audit Configuration:RO::Configure Solaris
Audit:auths=solaris.smf.value.audit;help=RtAuditCfg.html
Audit Control:RO::Control Solaris
Audit:auths=solaris.smf.manage.audit;help=RtAuditCtrl.html
Audit Review:RO::Review Solaris Auditing logs:help=RtAuditReview.html
<output omitted>
```

ORACLE

Relationships Among the Four Rights Databases

From the user_attr database:

```
sysadmin::::type=role;profiles=Device Management,File System Management,Printer
Management;roleauth=role

johndoe::::type=normal;auths=solaris.system.date;roles=sysadmin
```

From the prof_attr database:

```
Device Management:RO::Control Access to Removable
Media:auths=solaris.device.*;help=RtDeviceMngmnt.html
```

From the auth_attr database:

```
solaris.device.:RO::Device Allocation::help=DevAllocHeader.html
solaris.device.allocate:RO::Allocate Device::help=DevAllocate.html
solaris.device.config:RO::Configure Device Attributes::help=DevConfig.html
solaris.device.revoke:RO::Revoke or Reclaim Device::help=DevRevoke.html
solaris.device.cdrw:RO::CD-R/RW Recording Authorizations::help=DevCDRW.html
<output truncated>
```

From the exec_attr database:

```
Device Management:solaris:cmd:RO::/usr/sbin/allocate:uid=0
Device Management:solaris:cmd:RO::/usr/sbin/add_drv:uid=0
Device Management:solaris:cmd:RO::/usr/sbin/deallocate:uid=0
Device Management:solaris:cmd:RO::/usr/sbin/rem_drv:uid=0
Device Management:solaris:cmd:RO::/usr/sbin/update_drv:uid=0
```

Profile Shells

- Enable access to the privileged rights that are assigned to the rights profile
- Are assigned to a specific user as a login shell or through the `su` command to assume a role
- Users must be assigned one of the profile shells: `pfsh` for Bourne shell (`sh`), `pfcsh` for C shell (`csh`), or `pfksh` for Korn shell (`ksh`).
- When a user executes a command, the profile shell:
  1. Searches the role's rights profiles and associated rights
  2. Uses the first matching entry if the same command appears in more than one profile
  3. Executes the command with the attributes specified in the RBAC configuration files

ORACLE

Implementing the User Privileges and Roles Plan

In the next section, you learn how Oracle Solaris 11:

- Supports process rights management
- Supports user rights management to grant appropriate privileges to users

Quiz

Oracle Solaris implements process rights management through privileges.

a. True

b. False

Quiz

Which letter indicates a set of privileges being used during a process execution?

a. E

b. I

c. P

d. L

Quiz

Which of the following rights databases contains rights profiles?

a. `user_attr`

b. `auth_attr`

c. `exec_attr`

d. `prof_attr`

Quiz

A profile shell is a special type of shell that enables access to the privileged rights that are assigned to the rights profile.

a. True

b. False

Agenda

- Introducing privileges, rights, and roles
- Managing privileges
- Managing users rights
- Verifying file integrity by using BART
- Monitoring the audit service
- Assessing the compliance of an Oracle Solaris system

ORACLE

Configuring and Managing Privileges

This section covers the following topics:

- Examining process privileges
- Managing user privileges

Examining Process Privileges

You first cover the following topics:

- Determining the privileges available to the shell
- Determining the privileges available to a process
- Displaying the description of a privilege

Determining the Privileges Available to the Shell

To determine which privileges are available to your processes, run `ppriv $$` to list the process privileges that are available to your shell.

```
# ps
 PID TTY     TIME CMD
 990 pts/4   0:01 bash
 991 pts/4   0:00 su
 993 pts/4   0:00 ps
# ppriv $$
990:  -bash
flags = <none>
    E: all
    I: basic
    P: all
    L: all
```

Determining the Process Privileges Available to a Shell

To display the names of the privileges in each privilege set, use `ppriv -v $$`.

```
# ppriv -v $$
990:bash
flags = <none>
     E: contract_event,contract_identity,contract_observer,cpc_cpu,dtrace_kernel,
     dtrace_proc,dtrace_user,file_chown,file_chown_self,file_dac_execute,
<output omitted>
     I: file_link_any,file_read,file_write,net_access,proc_exec,proc_fork,
     proc_info, proc_session
     P: contract_event,contract_identity,contract_observer,cpc_cpu,dtrace_kernel,
     dtrace_proc,dtrace_user,file_chown,file_chown_self,file_dac_execute,
<output omitted>
     L: contract_event,contract_identity,contract_observer,cpc_cpu,dtrace_kernel,
     dtrace_proc,dtrace_user,file_chown,file_chown_self,file_dac_execute,
<output omitted>
```

Determining the Privileges Available to a Process

To determine which privileges are available to a process, use `ppriv -v pid`.

```
# ppriv -v 476
476:  /usr/sbin/cron
flags = <none>
 E: contract_event,contract_identity,contract_observer,cpc_cpu,
    dtrace_kernel,dtrace_proc,dtrace_user,file_chown,
<output omitted>
 I: file_link_any,file_read,file_write,net_access,proc_exec,
    proc_fork,proc_info,proc_session
 P: contract_event,contract_identity,contract_observer,cpc_cpu,
    dtrace_kernel,dtrace_proc,dtrace_user,file_chown,
<output omitted>
 L: contract_event,contract_identity,contract_observer,cpc_cpu,
    dtrace_kernel,dtrace_proc,dtrace_user,file_chown,
<output omitted>
```

Displaying the Description of a Privilege

To display a privilege definition, use `ppriv -vl privilege`.

```
# ppriv -vl contract_event
contract_event
     Allows a process to request critical events without
     limitation.
     Allows a process to request reliable delivery of all
     events on any event queue.
# ppriv -vl proc_exec
proc_exec
     Allows a process to call execve().
```

ORACLE

Managing User Privileges

- Determining the privileges directly assigned to you
- Determining the privileged commands you can use
- Assigning privileges to a user or role
- Limiting privileges of a user or role
- Determining the privileges needed by a program by using the `ppriv` debugging command
- Using the `ppriv` debugging command to examine privilege use in a profile shell
- Using the `truss` command to examine privilege use in a regular shell

ORACLE

Determining the Privileges Directly Assigned to You

To view the privileges that have been directly assigned to your user account, use `ppriv -v $$`.

```
$ ppriv -v $$
990:  bash
flags = <none>
    E: file_link_any,proc_clock_highres,proc_session
    I: file_link_any,proc_clock_highres,proc_session
    P: file_link_any,proc_clock_highres,proc_session
    L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,sys_time
$ ppriv -vl proc_clock_highres
    Allows a process to use high resolution timers.
```

ORACLE

Determining the Privileged Commands That You Can Use

To determine which rights profiles you have been assigned, use `profiles`.

```
$ profiles
All
Basic Solaris User
$ profiles -l
All
          *
Basic Solaris User
     auths=solaris.mail.mailq,solaris.network.autoconf.read,solaris.admin.wusb.read
     profiles=All
       /usr/bin/cdrecord.bin
privs=file_dac_read,sys_devices,proc_lock_memory,proc_priocntl,net_privaddr
       /usr/bin/readcd.bin        privs=file_dac_read,sys_devices,net_privaddr
       /usr/bin/cdda2wav.bin
privs=file_dac_read,sys_devices,proc_priocntl,net_privaddr
```

Assigning Privileges to a User or Role

To assign privileges to a user, use `usermod -K key=value loginname`.

```
# usermod -K defaultpriv=basic,proc_clock_highres jjones
# getent user_attr | grep jjones
jjones:::defaultpriv=basic,proc_clock_highres
```

To assign privileges to a role, use `rolemod -K key=value rolename`.

```
# rolemod -K defaultpriv=basic,proc_clock_highres realtime
# getent user_attr | grep realtime
realtime:::defaultpriv=proc_clock_highres
```

ORACLE

Limiting Privileges of a User or Role

1. Determine the privileges in a user's (or role's) basic set and limit set.
2. Remove one of the privileges from the basic set or from the limit set.
3. Test that the user (or role) can still perform other assigned functions as required.

```
# usermod -K limitpriv=all,!sys_linkdir jjones
# getent user_attr | grep jjones
jjones:::defaultpriv=basic;limitpriv=all,!sys_linkdir
```

```
# rolemod -K limitpriv=all,!sys_linkdir realtime
# getent user_attr | grep realtime
realtime:::defaultpriv=basic;limitpriv=all,!sys_linkdir
```

ORACLE

Determining Privileges Needed by a Program by Using the `ppriv` Debugging Command

1. Enter the command that is failing as an argument to the `ppriv` debugging command.

```
$ ppriv -De touch /etc/acct/yearly
touch[1298]: missing privilege "file_dac_write"
   (euid = 60004, syscall = “openat64”) for “/etc/acct/yearly
    at zfs_zaccess+0x245
touch: cannot create /etc/acct/yearly: Permission denied
```

2. If only the `syscall` ID is displayed in the output, you can determine which system call is failing by finding the `syscall` ID in the `/etc/name_to_sysnum` file.

Using the `ppriv` Debugging Command to Examine Privilege Use in a Profile Shell

```
jjones:~$ ls -l useful.script
-rw-r--r-- 1 aloe staff 2303 Dec 15 10:10 useful.script
jjones:~$ chown objadmin useful.script
chown: useful.script: Not owner
jjones:~$ ppriv -eD chown objadmin useful.script
chown[11444]: missing privilege "file_chown"
      (euid = 130, syscall = 16) needed at zfs_zaccess+0x258
chown: useful.script: Not owner
```

Using the `truss` Command to Examine Privilege Use in a Regular Shell

```
$ truss touch /etc/acct/yearly
...
...
(output truncated)

open64("/etc/acct/yearly", O_WRONLY|O_CREAT|O_TRUNC, 0666) Err#13 EACCES
[file_dac_write]
open("/usr/lib/locale/en_US.UTF-8/LC_MESSAGES/SUNW_OST_OSCMD.mo",
O_RDONLY) Err#2 ENOENT
open("/usr/lib/locale/en_US.UTF-8/LC_MESSAGES/SUNW_OST_OSLIB.mo",
O_RDONLY) Err#2 ENOENT
fstat64(2, 0xF5165980)                                   = 0
touchwrite(2, " t o u c h", 5)                           = 5
: cannot create write(2, " :   c a n n o t   c r e".., 16)  = 16
/etc/acct/yearlywrite(2, " / e t c / a c c t / y e".., 16)  = 16
: write(2, " :  ", 2)                                    = 2
Permission deniedwrite(2, " P e r m i s s i o n   d".., 17) = 17

write(2, "\n", 1)                               = 1
_exit(1)
```

Practice 8-1 Overview: Delegating Privileges to Users and Processes

This practice covers the following topics:

- Examining process privileges
- Managing user privileges

Agenda

- Introducing privileges, rights, and roles
- Managing privileges
- Managing user rights
- Verifying file integrity by using BART
- Monitoring the audit service
- Assessing the compliance of an Oracle Solaris system

ORACLE

Configuring and Using Role-Based Access Control RBAC

This section covers the following topics:

- Creating a role
- Creating, cloning, or changing a rights profile
- Assigning a rights profile to a role
- Assigning a role to a user
- Assuming a role
- Restricting an administrator to explicitly assigned rights
- Assigning a rights profile to a user
- Delegating authorization to a user
- Assigning authorization to a role
- Modifying a systemwide RBAC policy

Creating a Role

To create a role, use `roleadd -m -d dir rolename`.

```
# roleadd -u 3000 -g 10 -m -d /export/home/level1 -c "Level 1 Support“ \ -P
"Printer Management,Media Backup,Media Restore" level1
64 blocks
# passwd level1
New Password: <Type role password>
Re-enter new Password: <Type role password>
passwd: password successfully changed for level1
# getent passwd | grep level1
level1:x:3000:10:Level 1 Support:/export/home/level1:/usr/bin/pfbash
# grep level1 /etc/shadow
level1:$5$3jauLOtl$YDVdoH6q03m3YrOGZloql/MSrVaw0U7UgdNbiYEVbj8:16043::::::416
# getent user_attr | grep level1
level1:::profiles=Printer Management,Media Backup,Media
Restore;roleauth=role
```

Creating a Rights Profile

1. Create a rights profile.
2. Set the profile properties:
   - Use the `set` subcommand for profile properties that have a single value, such as `set desc`.
   - Use the `add` subcommand for properties that have more than one value, such as `add cmd`.

Creating a Rights Profile: Example

```
# profiles -p -S LDAP “New Users"
profiles:New Users> set desc="For all users of LDAP"
profiles:New Users> add profiles=“New Basic User"
profiles:New Users> set defaultpriv="basic,!proc_info"
profiles:New Users> set limitpriv="basic,!proc_info"
profiles:New Users> end
profiles:New Users> exit
#
# profiles -p “New Users"
Found profile in LDAP repository.
profiles:New Users> info
        name=New Users
        desc=For all users of LDAP
        defaultpriv=basic,!proc_info,
        limitpriv=basic,!proc_info,
        profiles=New Basic User
```

ORACLE

Cloning and Modifying a Rights Profile

1. Create a new rights profile from an existing profile.

```
# profiles -p [-S repository] existing-profile-name
```

   – To enhance an existing rights profile:
      a. Create a new profile.
      b. Add the existing rights profile as a supplementary rights profile.
      c. Add the enhancements.
   – To remove content from an existing rights profile, clone the profile, rename it, and then modify it.
2. Continue to modify the new rights profile by adding or removing supplementary rights profiles, authorizations, and other security attributes.

ORACLE

Cloning and Modifying a Rights Profile: Example

```
# profiles -p "Network IPsec Management"
profiles:Network IPsec Management> add auths="solaris.admin.edit/etc/hosts"
Cannot add. Profile cannot be modified
#
# profiles -p "Total IPsec Mgt"
Total IPsec Mgt> set desc="Network IPsec Mgt plus edit authorization"
Total IPsec Mgt> add profiles="Network IPsec Management"
Total IPsec Mgt> add auths="solaris.admin.edit/etc/hosts"
Total IPsec Mgt> add auths="solaris.admin.edit/etc/inet/ipsecinit.conf"
Total IPsec Mgt> add auths="solaris.admin.edit/etc/inet/ike/config"
Total IPsec Mgt> add auths="solaris.admin.edit/etc/inet/secret/ipseckeys"
Total IPsec Mgt> exit
#
# profiles -p "Total IPsec Mgt" info
        name=Total IPsec Mgt
        desc=Network IPsec Mgt plus edit authorization
        auths=solaris.admin.edit/etc/hosts,
              solaris.admin.edit/etc/inet/ipsecinit.conf,
              solaris.admin.edit/etc/inet/ike/config,
              solaris.admin.edit/etc/inet/secret/ipseckeys
        profiles=Network IPsec Management
```

Assigning a Rights Profile to a Role

To assign a rights profile to a role, use `rolemod [-P profile][-s shell] rolename`.

```
# rolemod -P profile1,profile2 -s /usr/bin/pfksh level1
```

Assigning a Role to a User

1. Assign the role to the user by using `usermod -u uid -g gid -m -d` *`dir`* `-R` *`role`* `-c` *`comment loginname`*.
2. Assign a password to the role by using `passwd` *`rolename`*.
3. Verify that an entry has been made in the `user_attr` database.

Assigning a Role to a User: Example

```
# useradd -u 4009 -g 10 -m -d /export/home/paul \
-R level1 -c “Paul” paul
64 blocks
# passwd paul
New Password: <Type rolename password>
Re-enter new Password: <Type rolename password>
passwd: password successfully changed for paul
# getent user_attr | grep paul
paul:::roles=level1
# roles paul
level1
# usermod -R level1 paul
# passwd -r repository level1
Password: <Type rolename password>
Confirm Password: <Retype rolename password>
# usermod -R "" paul
```

ORACLE

Assuming a Role

1. In a terminal window, determine which roles you can assume by using `roles`.
2. Use the `su` command to assume a role by using `su - rolename`.
3. Verify that you are now in a role by using `/usr/ucb/whoami`.
4. View the capabilities of your role by using `ppriv $$`.

```
# roles
sysadmin,oper,primaryadm
# su - sysadmin
Password: <Type sysadmin password>
$ /usr/ucb/whoami
sysadmin
$ ppriv $$
950:    bash
flags = <none>
    E: basic
    I: basic
    P: basic
    L: all
```

Restricting the Superuser

It is your responsibility to control and monitor system activity by performing the following tasks:

- Setting limits on who can use various resources
- Logging resource use
- Monitoring who is using the resources

Note: The system tracks real and effective user and group ID logins. To determine the real UID, use `who am i`. To determine the effective UID, user `whoami`.

Restricting an Administrator to Explicitly Assigned Rights

You can restrict a role or user to a limited number of administrative actions in either of the following ways:

- Use the Stop rights profile.
- Modify the `policy.conf` file on a system and require the role or user to use that system for administrative tasks.

```
# rolemod -P “Profile_Name,All,Stop" rolename
```

Assigning the Rights Profile to a User

```
# profiles chris
Basic Solaris User
All
# usermod -P "Printer Management" chris
# profiles chris
chris:
Printer Management
Basic Solaris User
All
# getent user_attr | grep chris
chris:::profiles=Printer Management
# profiles -l chris
Printer Management:
/etc/init.d/lp euid=0, uid=0
/usr/bin/cancel euid=lp, uid=lp
/usr/bin/lpset egid=14
/usr/bin/lpstat euid=0
/usr/lib/lp/local/accept uid=lp
/usr/lib/lp/local/lpadmin uid=lp, gid=8
/usr/lib/lp/lpsched uid=0
<output omitted>
All:
*
```

ORACLE

Delegating an Authorization to a User

1. Delegate the authorization to the user by using `usermod -A` *`authorization loginname`*.
2. Verify that an entry has been made in the `user_attr` database for the user.
3. View the authorizations for the user by using the `auths` command.

Delegating an Authorization to a User: Example

```
# su - chris
Oracle Corporation     SunOS 5.11  11.3     September 2015
chris:~$ crontab -l root
crontab: you must be super-user to access another user's crontab file
chris:~$ exit
# usermod -A solaris.jobs.admin chris
# getent user_attr | grep chris
chris::::auths=solaris.jobs.admin;profiles=Printer Management
# auths chris
solaris.admin.wusb.read,solaris.jobs.admin,solaris.mail.mailq,solaris.network.autoc
onf.read,solaris.print.*
# su - chris
Oracle Corporation     SunOS 5.11  11.3     September 2015
chris:~$ crontab -l root
#ident  "%Z%%M%   %I%  %E% SMI"
#
# The root crontab should be used to perform accounting data collection.
(output omitted)
chris:~$ exit
```

Assigning Authorization to a Role

1. Assign the authorization to a role by using `rolemod -A “authorization” rolename`.
2. Verify that an entry has been made in the `user_attr` database for the role.
3. View the authorizations for the role by using the `auths` command.

```
# rolemod -A “solaris.admin.usermgr.*” level1
# auths level1
solaris.admin.usermgr.*,solaris.admin.wusb.read,solaris.mail.ma
ilq,solaris.media.extract,solaris.network.autoconf.read,solaris
.print.*,solaris.smf.manage.ndmp,solaris.smf.read.ndmp,solaris.
smf.value.ndmp
```

Modifying a Systemwide RBAC Policy

1. Determine the privileges that you want to comment out for the basic user.
2. Using a text editor, modify the `PRIV_DEFAULT=basic` default entry and restart the system.
3. As a user, test the modification.

```
# pfedit /etc/security/policy.conf
# grep PRIV_DEFAULT /etc/security/policy.conf
# There are two different settings; PRIV_DEFAULT determines the default
# Similarly, PRIV_DEFAULT=basic,!file_link_any takes away only the
PRIV_DEFAULT=basic,!proc_info,!proc_session
# init 6
<log in to the system>
# su - jjones
Oracle Corporation    SunOS 5.11      11.3     September 2015
$ ps -A -o user -o pid -o comm | grep jjones
   USER  PID COMMAND
 jjones 1935 -bash
 jjones 1941 grep
 jjones 1942 ps
```

ORACLE

Practice 8-2 and Practice 8-3: Overview

Practice 8-2 covers the following topics:

- Managing roles and profiles
- Configuring a rights profile
- Working with individual authorizations
- Creating a systemwide RBAC policy

Practice 8-3 covers monitoring and restricting the superuser.

ORACLE

Agenda

- Implementing privileges, rights, and roles
- Managing privileges
- Managing user rights
- Verifying file integrity by using BART
- Monitoring the audit service
- Assessing the compliance of an Oracle Solaris system

BART: Overview

BART is a file verification and reporting tool that:

- Performs a file-level check of the software contents of a system
- Enables you to determine what file-level changes have occurred on a system
- Compares changes to a known baseline

BART: Example

```
# vi bartrules
IGNORE all
/export/home/oracle1
CHECK all

# bart create -r bartrules > bart-`hostname`-`date '+%d%m%Y-%H:%M:%S'`

# ls bart*
bart-s11-server1-21092015-01:11:08  bartrules

# touch /export/home/oracle1/newfile

# bart create -r bartrules > bart-`hostname`-`date '+%d%m%Y-%H:%M:%S'`

# ls bart*
bart-s11-server1-21092015-01:11:08  bartrules
bart-s11-server1-21092015-01:11:50

# bart compare -r bartrules bart-s11-server1-21092015-01\:11\:08     \
bart-s11-servr1-21092015-01\:11\:50
/export/home/oracle1:
  size  control:5  test:6
  dirmtime  control:55f55ee4  test:55ffc9c6
/export/home/oracle1/newfile:
  add
```

BART: Example

```
# vi /export/home/oracle1/newfile
This is a test.

# bart create -r bartrules > bart-`hostname`-`date '+%d%m%Y-%H:%M:%S'`

# ls bart*
bart-s11-server1-21092015-01:11:08  bart-s11-server1-21092015-01:15:42
bart-s11-server1-21092015-01:11:50  bartrules

# bart compare -r bartrules bart-s11-server1-21092015-01\:11\:50      \
bart-s11-servr1-21092015-01\:15\:42
/export/home/oracle1:
  dirmtime  control:55ffc9c6  test:55ffcaa9
/export/home/oracle1/newfile:
  size  control:0  test:16
  mtime  control:55ffc9c6  test:55ffcaa9
  contents  control:e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
test:11586d2eb43b73e539caa3d158c883336c0e2c904b309c0c5ffe2c9b83d562a1
```

Practice 8: Overview

- 8-4: Verifying file integrity by using BART

Agenda

- Implementing privileges, rights, and roles
- Managing privileges
- Managing user rights
- Verifying file integrity by using BART
- Monitoring the audit service
- Assessing the compliance of an Oracle Solaris system

Auditing in Oracle Solaris

Auditing is the process of collecting data about the use of system resources. Auditing in Oracle Solaris 11:

- Is enabled by default
- Records security-related system events
- Records events in a network-wide audit trail
- Detects misuse or unauthorized activity
- Reviews patterns of access and the access histories of users and objects
- Discovers attempts to bypass protection mechanisms
- Discovers extended use of privileges

Oracle Solaris 11 Auditing Features

Following are the enhancements in the Oracle Solaris Auditing feature in Oracle Solaris 11:

- Oracle Solaris Auditing and Device Allocation replace “BSM.”
- `bsmconv` and `bsmunconv` commands, and the need to restart have been removed.
- `bsmrecord` is renamed `auditrecord`.
- `/etc/security/audit` directory and symlink no longer exist. `/var/audit` is now the official audit directory.
- By default, Oracle Solaris Auditing is configured and enabled. `lo` events are the default configured events.
- By using the Audit Configuration rights profile, all global configurations can be performed by `auditconfig`. `audit_startup` and `audit_control` no longer exist.

Oracle Solaris 11 Auditing Features

- By using the `useradd`, `roleadd`, `usermod`, and `rolemod` commands, you can place the per-user `audit_flags` security attribute in the `user_attr` database.
- You can use the `profiles` command to place the desired per-user audit flags for the rights profiles in the `prof_attr` database.
- By using the Audit Control rights profile, you can control the Oracle Solaris audit service with `audit` to refresh, change audit files, disable, and re-enable.
- Global zone auditing need not be enabled for per-zone auditing.

ORACLE

Default Configuration of the Audit Service

- The audit service has a default configuration and is immediately operational on the global zone after you install Oracle Solaris 11.
- No additional action is required to enable or configure the service to become usable.
- With its default configuration, the audit service records the following operations:
  - Login and logout operations
  - Use of the `su` command
  - Screen lock and screen unlock operations

ORACLE

Displaying Audit Service Defaults

- Displaying the default audit policy

```
# auditconfig -getpolicy
configured audit policies = cnt
active audit policies = cnt
```

- Displaying default class for attributable events

```
# auditconfig -getflags
active user default audit flags = lo(0x1000,0x1000)
configured user default audit flags = lo(0x1000,0x1000)
```

- Displaying the default class for non-attributable events

```
# auditconfig -getnaflags
active non-attributable audit flags = lo(0x1000,0x1000)
configured non-attributable audit flags = lo(0x1000,0x1000)
```

Displaying Audit Service Defaults

- Displaying the default audit plugins

```
# auditconfig -getplugin
Plugin: audit_binfile
Attributes: p_age=0h;p_dir=/var/audit;p_fsize=4M;p_minfree=1;

Plugin: audit_syslog (inactive)
Attributes: p_flags=;

Plugin: audit_remote (inactive)
Attributes: p_hosts=;p_retries=3;p_timeout=5;
```

- Displaying the audit queue controls

```
# auditconfig -getqctrl
no configured audit queue hiwater mark
no configured audit queue lowater mark
no configured audit queue buffer size
no configured audit queue delay
active audit queue hiwater mark (records) = 100
active audit queue lowater mark (records) = 10
active audit queue buffer size (bytes) = 8192
active audit queue delay (ticks) = 20
```

Enabling and Disabling the Audit Service

- Use the `audit -s` command to enable the audit service if it is not running or to refresh the service if it is currently running.

  Note: Auditing is enabled by default.

```
# audit -s
```

- Verify that auditing is enabled.

```
# auditconfig -getcond
audit condition = auditing
```

- Use the `audit –t` command to disable the service.

```
# audit -t
```

Viewing Contents of Binary Audit Files

```
# cd /var/audit
# ls
...
20150901132110.20150901190523.s11-server1  20150915172913.20150915181644.s11-server1
20150906173827.20150906180719.s11-server1  20150915181840.20150921092344.s11-server1
20150913113111.20150913113321.s11-server1  20150921092353.not_terminated.s11-server1

# praudit 20150915181840.20150921092344.s11-server1 more
file,2015-09-15 10:18:40.951 -08:00,
header,52,2,system booted,na,s11-server1,2015-09-15 10:17:20.708 -08:00
text,booting kernel
header,42,2,init(1m),na,s11-server1,2015-09-15 10:18:51.640 -08:00
text,booted
return,success,0
header,32,2,su,na,s11-server1,2015-09-15 10:19:01.833 -08:00
return,success,0
header,32,2,su logout,na,s11-server1,2015-09-15 10:19:04.667 -08:00
return,success,0
header,69,2,login - ssh,,s11-server1,2015-09-15 10:21:53.234 -08:00
subject,oracle1,oracle1,staff,oracle1,staff,1059,1249775782,3696 136704 s11-desktop
return,success,0
header,69,2,role login,,s11-server1,2015-09-15 10:21:56.902 -08:00
subject,oracle1,root,root,root,root,1064,1249775782,3696 136704 s11-desktop
return,success,0
...
```

Agenda

- Implementing privileges, rights, and roles
- Managing privileges
- Managing user rights
- Verifying file integrity by using BART
- Monitoring the audit service
- Assessing the compliance of an Oracle Solaris system

Compliance in Oracle Solaris OS

- The Oracle Solaris 11 OS provides the `compliance` command to assess system compliance and generate reports against the following security benchmarks:
  - Solaris security policy benchmark
  - Payment Card Industry Data Security Standard (PCI DSS) security policy benchmark
- The compliance report indicates which tests failed and which tests passed, and provides remediation steps.
- You must examine the compliance report and then perform additional tasks to comply with the standard.
- Oracle Solaris also supports creating tailorings from existing security benchmarks.

Solaris Security Policy Benchmark

- The Solaris security policy benchmark is a standard based on the “secure by default” (SBD) installation of Oracle Solaris.
- The benchmark provides two profiles:
  - `Baseline`: Matches closely with the default SBD installation of Oracle Solaris
  - `Recommended`: Satisfies organizations with stricter security requirements than the `Baseline` profile

ORACLE

PCI DSS Security Policy Benchmark

- The PCI DSS security policy benchmark is a security standard for organizations that handle cardholder information for major debit and credit cards.
- The standard is defined by the PCI Security Standards Council to offer robust and secure payments by cards.
- The key intent of the PCI DSS security benchmark is to reduce credit card fraud.

ORACLE

Assessing the Security Compliance of an Oracle Solaris System

1. Install the `compliance` package.

```
# pkg install compliance
```

2. List the benchmarks and profiles that are available.

```
# compliance list –p
```

3. Create an assessment.

```
# compliance assess -p Solaris_PCI-DSS -b pci-dss -a pci-dss
```

4. List the assessments in the compliance directory.

```
# compliance list -v -a pci-dss
```

5. Locate the assessments in the compliance directory.

```
# compliance report -a pci-dss
# compliance report -f log -a pci-dss
# compliance report -f xccdf -a pci-dss
```

6. View the assessments.
7. Fix any failures that your security policy requires to pass.

Tailorings for Security Benchmarks

Tailorings customize the benchmark assessments to verify the security policy of a particular system.

- To create customized assessments, you include or exclude rules from an existing benchmark, profile, or tailoring.
- To use a tailoring to assess systems, you must install the source benchmark as well as the tailoring.

Creating Tailorings for Security Benchmarks

1. Open the compliance editor to create a tailoring.

```
# compliance tailor -t baselinecustom
*** compliance tailor: No existing tailoring 'baselinecustom', initializing
tailoring:baselinecustom> info
Properties:
        tailoring=baselinecustom
        benchmark: not set
        profile: not set
```

2. Set the benchmark and exclude all rules.

```
tailoring:baselinecustom> set benchmark=solaris
tailoring:baselinecustom> set profile=Baseline
tailoring:baselinecustom> info
Properties:
        tailoring=baselinecustom
        benchmark=solaris
        profile=Baseline
tailoring:baselinecustom> exclude -a
Discard existing rule selections (y/N)? y
```

ORACLE

Creating Tailorings for Security Benchmarks

3. Open the pick screen, navigate, and include particular rules.

```
tailoring:baselinecustom> pick
...
> _   OSC-53005  The OS version is current
> _   OSC-16005  All local filesystems are ZFS
> _   OSC-61510  root login by using ssh(1) is disabled
> _   OSC-46014  Passwords require at least 14 characters
> _   OSC-59000  root is a role
> _   OSC-04511  Booting the system should require a password
...
```

4. Commit the changes and exit the compliance editor.

```
tailoring:baselinecustom> commit
tailoring:baselinecustom> exit
```

5. List the tailoring.

```
# compliance tailor list
        baselinecustom
```

ORACLE

Creating Tailorings for Security Benchmarks

6. Test the tailoring on a system and evaluate the output.

```
# compliance assess -t baselinecustom
```

7. Locate the assessment.

```
# compliance report
/var/share/compliance/assessments/baselinecustom.2015-09-11,12:04/report.html
```

8. Display the assessment in a web browser.

Quiz

BART is a tool that performs a file-level check of the software contents of a system and enables you to determine what file-level changes have occurred on a system.

a. True

b. False

Practice 8: Overview

- 8-5: Assessing the compliance of an Oracle Solaris System

Summary

In this lesson, you should have learned how to:

- Describe privileges, rights, and roles
- Manage privileges
- Manage user rights
- Verify file integrity by using BART
- Monitor the audit service
- Assess the compliance of an Oracle Solaris system

9

Managing Processes and Priorities

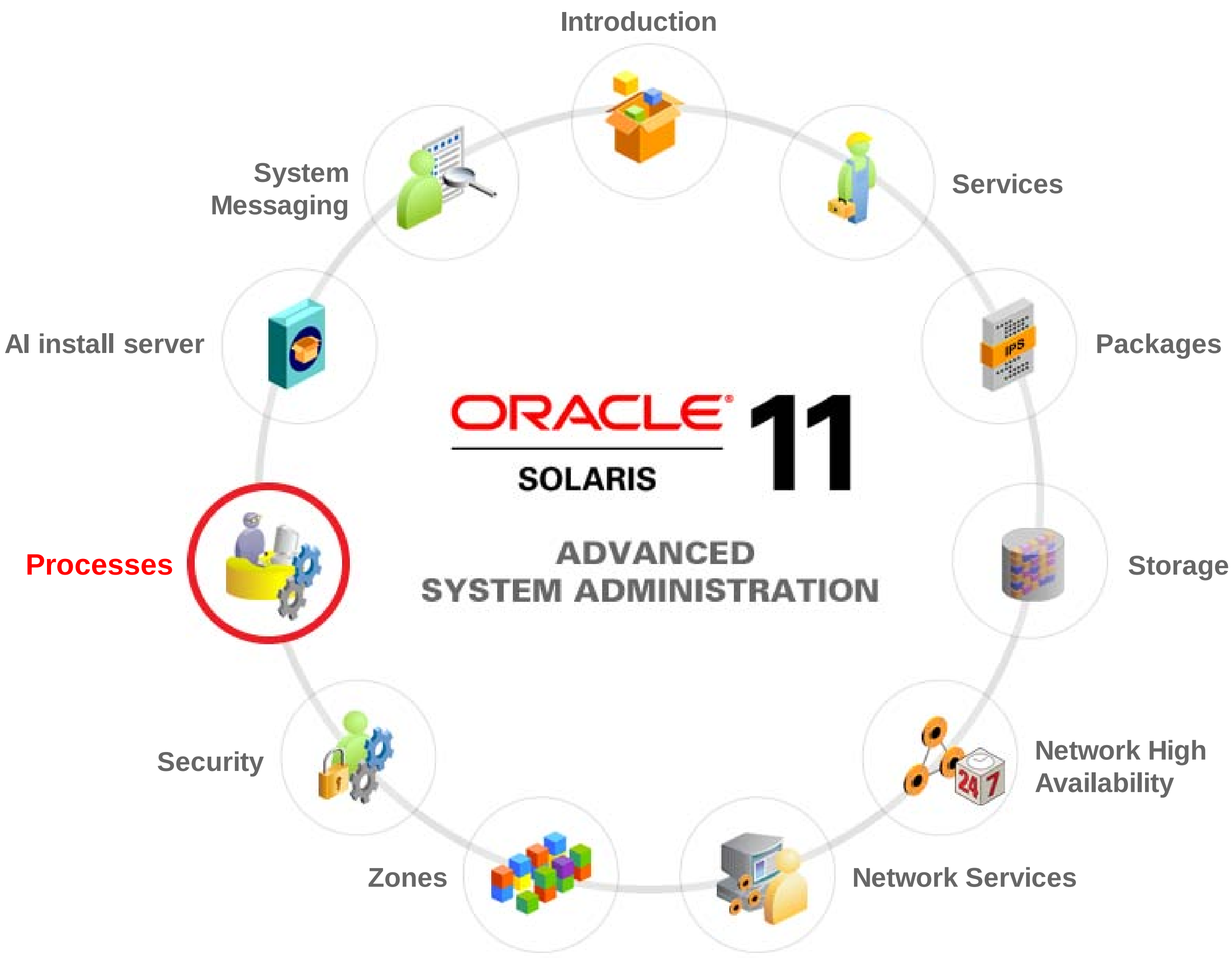
Objectives

After completing this lesson, you should be able to:

- Implement process execution in an appropriate scheduling class
- Manage process scheduling priority
- Manage the scheduling class of zones
- Configure the fair share scheduler
- Monitor the fair share scheduler

ORACLE

Job Workflow



Agenda

- Implementing process execution in an appropriate scheduling class
- Managing process scheduling priority
- Configuring the fair share scheduler
- Managing the scheduling class of zones

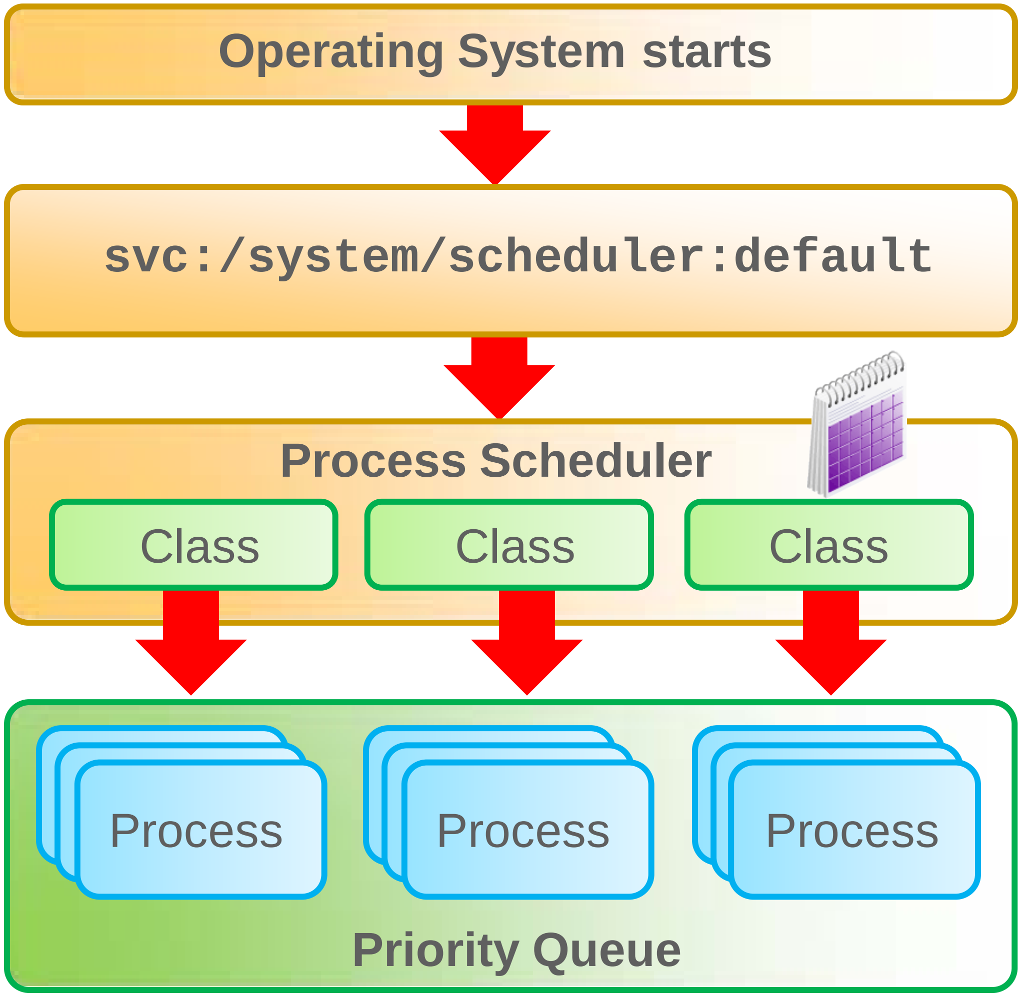
Importance of Process Execution in an Appropriate Scheduling Class

The process execution in an appropriate scheduling class plan ensures that:

- System resources are used appropriately
- Processes are prioritized in accordance with business needs and requirements
- Process workload distribution is controlled
- Processes are assigned to the appropriate scheduling class

ORACLE

Process Scheduler



Process Priority

- Global priority:
  - It is based on scheduling class.
- Designated priority:
  - Designating a priority affects global priority assignment and position in a priority queue.
  - Both scheduling class and user priority can be designated.
  - User priority is based on the assigned priority range of the scheduling class.

Process Scheduling Classes

Scheduling Class	Description
Time sharing (TS)	Default class for processes and their associated kernel threads. Priorities in this class are dynamically adjusted in an attempt to allocate processor resources evenly.
Interactive (IA)	Enhanced version of the TS class that applies to the in-focus window in the GUI. Its intent is to give extra resources to processes associated with that specific window.
Fair share scheduler (FSS)	This class is share based rather than priority based. Threads managed by FSS are scheduled based on their associated shares and the processor's utilization.
Fixed priority (FX)	Priorities for threads associated with this class are fixed. That is, they do not vary dynamically over the lifetime of the thread.
System (SYS)	Used to schedule kernel threads. Threads in this class are “bound” threads, which means that they run until they block or complete.
System Duty-Cycle Class (SDC)	This class is a variant of the SYS class. SDC adjusts its threads’ priority to give them a specified percentage of the processor. It also gives them a scheduling quantum, which gives other threads at the same priority on the same CPU a chance to run.
Real-Time (RT)	Threads in the RT class are fixed priority, with a fixed-time duration called quantum.

ORACLE

Priority Ranges for Scheduling Classes

Scheduling Class	Priority Range
Real-time (RT)	100 through 159
System (SYS)	60 through 99
Fair share scheduler (FSS)	0 through 59
Fixed priority (FX)	0 through 59
Interactive (IA)	0 through 59
Time sharing (TS)	0 through 59

Combining FSS with Other Scheduling Classes

- Ensure that the FSS, TS, IA, and FX scheduling classes do not share the same processor set (pset).
- All processes that run on a processor set must be in the same scheduling class so that they do not compete for the same CPUs.
- To avoid starving applications in the FSS class, use processor sets for FSS class and FX class applications.
- The following classes can be in the same processor sets:
  - TS and IA classes
  - FSS and RT classes

    Note: FSS has no control over the RT class processes.

ORACLE

Using CPU Shares with the FSS

- The FSS uses CPU shares to control the allocation of available CPU resources among workloads.
- Assigning a greater number of CPU shares to a project gives that project more CPU resources from the FSS.
- CPU share allocation and CPU resource usage are not the same.
  - CPU shares define the relative importance of workloads in relation to other workloads.
  - Resource utilization is the percentage of CPU capacity being used.
- When allocating CPU shares, you should know:
  - How many shares the project has in comparison with other projects
  - How many of the other projects are competing for CPU resources

Scheduling Class on a System with Zones Installed

- Nonglobal zones use the system’s default scheduling class.
- For a new default scheduling class setting, nonglobal zones obtain the new setting when booted or rebooted.
- To ensure that all zones get a fair share of the system CPU resources, set the FSS as the system default scheduling class.

Implementing the Process Execution in an Appropriate Scheduling Class

You will next learn how to:

- Determine the scheduling priorities and classes for the process running on the system
- Modify scheduling priorities
- Set the FSS as the default scheduler
- Configure CPU shares for zones

Quiz

For the operating system to prioritize processes, all processes must have the same scheduling class.

a. True

b. False

Quiz

Which scheduling class has the highest range of user priority designations?

a. Fair share scheduler (FSS)
b. Real-time (RT)
c. System (SYS)
d. Time sharing (TS)

Quiz

What is the purpose of CPU shares?

a. To control the allocation of available CPU resources among workloads
b. To increase CPU capacity
c. To change the global priority of a project in the priority queue
d. To cap the CPU resource usage of a process

Quiz

Nonglobal zones use the default system scheduling class for the system.

a. True

b. False

Agenda

- Implementing process execution in an appropriate scheduling class
- Managing process scheduling priority
- Configuring the fair share scheduler
- Managing the scheduling class of zones

Managing Process Scheduling Priority

This section covers the following topics:

- Displaying processes by using the `top` command
- Displaying process class information
- Determining the global priority of a process
- Designating a process priority
- Modifying a process priority

Displaying Processes by Using the `top` Command

To display the top 10 processes that are using the most CPU resources, use `top 10 –s 10`.

```
# top 10 -s 10
last pid:  1121;  load avg:  0.20,  0.14,  0.12;  up 0+01:50:30        14:10:30
87 processes: 83 sleeping, 3 running, 1 on cpu
CPU states: 81.8% idle,  5.1% user, 13.1% kernel,  0.0% iowait,  0.0% swap
Kernel: 609 ctxsw, 9 trap, 327 intr, 1935 syscall, 4 flt
Memory: 1024M phys mem, 84M free mem, 977M total swap, 977M free swap

   PID USERNAME NLWP PRI NICE  SIZE   RES STATE    TIME    CPU COMMAND
   991 oracle      2  59    0   87M   19M sleep    0:11  4.03% gnome-terminal
   733 oracle      3  59    0   65M   53M run      0:23  3.82% Xorg
   929 oracle     20  59    0  160M  140M run      2:01  1.75% java
   934 oracle      1  56    0   12M 5552K run      0:06  1.46% xscreensaver
  1120 root        1  59    0 4296K 2480K cpu      0:00  0.25% top
   917 oracle      1  49    0  107M   36M sleep    0:01  0.22% nautilus
   913 oracle      1  59    0   27M   15M sleep    0:01  0.08% metacity
    11 root       18  59    0   12M   11M sleep    0:41  0.06% svc.configd
```

ORACLE

Displaying Process Class Information

To display information about process classes, use `priocntl -l`.

```
# priocntl -l
CONFIGURED CLASSES
==================
SYS (System Class)

TS (Time Sharing)
Configured TS User Priority Range: -60 through 60

SDC (System Duty-Cycle Class)

FSS (Fair Share)
     Configured FSS User Priority Range: -60 through 60

FX (Fixed priority)
Configured FX User Priority Range: 0 through 60
IA (Interactive)
Configured IA User Priority Range: -60 through 60
```

Determining the Global Priority of a Process

To determine the global priority of a process, use `ps -ecl`.

```
$ ps -ecl
 F S UID PID  PPID CLS PRI  ADDR      SZ  WCHAN    TTY       TIME   CMD
19 T 0   0    0    SYS 96   f00d05a8   0           ?          0:03  sched
 8 S 0   1    0    TS  50   ff0f4678 185  ff0f4848 ?         36:51   init
19 S 0   2    0    SYS 98   ff0f4018   0  f00c645c ?          0:01 pageout
19 S 0   3    0    SYS 60   ff0f5998   0  f00d0c68 ?        241:01 fsflush
 8 S 0   269  1    TS  58   ff0f5338 303  ff49837e ?          0:07    sac
 8 S 0   204  1    TS  43   ff2f6008  50  ff2f606e console    0:02     sh
```

Designating a Process Priority

1. Start a process with a designated priority by using `priocntl -e -c` *`class`* `-m` *`user-limit`* `-p` *`user-priority`* *`command-name`*.
2. Verify the process status by using `ps -ecl | grep` *`command-name`*.

```
# priocntl -e -c TS -m 60 -p 60 find . -name core -print
# ps -ecl | grep find
 0 S      0  2959  2771   TS  60    ?   1865        ? pts/1       0:01 gfind
ps -ecl | grep find
 0 S      0  2959  2771   TS  60    ?   1961        ? pts/1       0:01 gfind
ps -ecl | grep find
 0 R      0  2959  2771   TS  59    ?   1985          pts/1       0:02 gfind
```

Modifying a Process Priority

1. Change the priority of the process by using `priocntl -s -p` *`user-priority pid`*.
2. Verify the process status by using `ps -ecl | grep` *`command-name`*.

```
# priocntl -s -p 30 3093
# ps -ecf | grep myprog
    root  3093  2909   RT 130 09:09:34 pts/3   0:00 /bin/bash /root/myprog
    root  3124  2771   IA  32 09:15:25 pts/1   0:00 grep myprog
```

ORACLE

Agenda

- Implementing process execution in an appropriate scheduling class
- Managing process scheduling priority
- Configuring the fair share scheduler
- Managing the scheduling class of zones

ORACLE

Configuring the Fair Share Scheduler (FSS)

This section covers the following topics:

- Making the FSS the default scheduling class
- Manually moving processes from other classes into the FSS class
- Manually moving a project's processes into the FSS class
- Tuning scheduler parameters

Making FSS the Default Scheduling Class

To set the default scheduler for the system to be FSS, use `dispadmin -d FSS`.

```
# dispadmin -d FSS
# dispadmin -d
FSS     (Fair Share)
```

```
# dispadmin -l
CONFIGURED CLASSES
==================

SYS     (System Class)
TS      (Time Sharing)
SDC     (System Duty-Cycle Class)
FSS     (Fair share)
FX      (Fixed Priority)
IA      (Interactive)
FSS     (Fair Share)
```

Manually Moving the `init` Process into the FSS Class

To move the `init` process into the FSS class, use `priocntl -s -c FSS -i pid 1`.

```
# ps -ecf | grep init
    root     1     0   TS  59 07:42:52 ?        0:00 /usr/sbin/init
    root  4564  1262  FSS   1 10:01:48 pts/1    0:00 grep init
# priocntl -s -c FSS -i pid 1
# ps -ef -o class,zone,fname | grep init
 FSS   global init
```

Manually Moving Processes from Other Classes into the FSS Class

To move all processes into the FSS class, use `priocntl -s -c FSS -i all`.

```
# priocntl -s -c FSS -i all
```

```
# ps -ef -o class,zone,fname | grep -v CLS | sort -k2 | more
 FSS   global asr-noti
 FSS   global auditd
 FSS   global automoun
 FSS   global automoun
 FSS   global bash
 FSS   global bash
 FSS   global bonobo-a
 FSS   global clock-ap
 FSS   global console-
 FSS   global cron
 FSS   global dbus-dae
```

Manually Moving a Project's Processes into the FSS Class

To move the processes that run in a project to the FSS scheduling class, use `priocntl -s -c FSS -i projid projectID_number`.

```
# ps -o user,pid,uid,projid,project,class
    USER   PID   UID PROJID  PROJECT  CLS
    root  2771     0      1 user.root  TS
    root  3000     0      1 user.root  TS
# priocntl -s -c FSS -i projid 1
# ps -o user,pid,uid,projid,project,class
    USER   PID   UID PROJID  PROJECT  CLS
    root  2771     0      1 user.root FSS
    root  3015     0      1 user.root FSS
```

ORACLE

Changing Scheduler Parameters

To change the scheduler parameters, use `dispadmin -c scheduler -g [-r resolution]`.

```
$ dispadmin -c FSS -g
#
# Fair Share Scheduler Configuration
#
RES=1000
#
# Time Quantum
#
QUANTUM=110
$ dispadmin -c FSS -g -r 100
#
# Fair Share Scheduler Configuration
#
RES=100
#
# Time Quantum
#
QUANTUM=11
```

Practice 9-1 Overview: Modifying Process Scheduling Priority

This practice covers the following topics:

- Managing scheduling class and process priorities
- Configuring the fair share scheduler

Agenda

- Implementing process execution in an appropriate scheduling class
- Managing process scheduling priority
- Configuring the fair share scheduler
- Managing the scheduling class of zones

Managing the Scheduling Class of Zones

This section covers the following topics:

- Assigning CPU shares to the global zone
- Configuring CPU shares configuration in a nonglobal zone
- Measuring CPU performance in the zones
- Removing the CPU shares configuration from a zone

Assigning CPU Shares to the Global Zone

To assign CPU shares to the global zones, use `prctl -n zone.cpu-shares -v` *`number_of_shares`* `-r -i zone global`.

```
# prctl -n zone.cpu-shares -v 60 -r -i zone global
```

ORACLE

Configuring CPU Shares Configuration in a Nonglobal Zone

1. Add the CPU shares to the zone by using `zonecfg -z` *`zone`*.
2. Set the number of shares for the global zone by using `set cpu-shares=`*`number`*.
3. Exit `zonecfg`.
4. Verify the configuration change by using `zonecfg -z` *`zone`* `info`.

Configuring CPU Shares in a Nonglobal Zone: Example

```
# zonecfg -z hrzone
zonecfg:hrzone> set cpu-shares=80
zonecfg:hrzone> verify
zonecfg:hrzone> commit
zonecfg:hrzone> exit
# zonecfg -z hrzone info
zonename: hrzone
zonepath: /zones/hrzone
brand: solaris
autoboot: true
bootargs:
pool:
limitpriv:
scheduling-class:
ip-type: exclusive
hostid:
fs-allowed:
[cpu-shares: 80]
net:
address not specified
allowed-address not specified
physical: vnic1
defrouter not specified
rctl:
name: zone.cpu-shares
value: (priv=privileged,limit=80,action=none)
(output omitted)
```

Measuring CPU Performance in the Zones

To measure CPU performance in the zones, use `prstat -Z`.

```
# prstat -Z
…
…
…
ZONEID    NPROC  SWAP   RSS MEMORY      TIME  CPU ZONE
     0       98  348M  451M    44%   0:00:50 0.3% global
     1       27   34M   43M   4.2%   0:20:09 8.3% hrzone
     2       27   34M   43M   4.2%   0:16:15 2.4% itzone
```

Removing the CPU Shares Configuration from a Zone

1. Remove the CPU shares configuration from a zone by using `zonecfg -z` *`zone`* `clear cpu-shares`.
2. Verify the configuration change by using `zonecfg -z` *`zone`* `info`.
3. Reboot the zone to make the configuration effective.

Removing the CPU Shares Configuration from a Zone: Example

```
# zonecfg -z hrzone clear cpu-shares
# zonecfg -z hrzone info
zonename: hrzone
zonepath: /zones/hrzone
brand: solaris
autoboot: true
bootargs:
pool:
limitpriv:
scheduling-class:
ip-type: exclusive
hostid:
fs-allowed:
net:
    address not specified
    allowed-address not specified
     configure-allowed-address: true
    physical: vnic1
    defrouter not specified
…
…
```

ORACLE

Practice 9-2 Overview: Configuring the FSS in an Oracle Solaris Zone

This practice covers the following topics:

- Configuring CPU shares
- Monitoring FSS in two zones
- Removing the CPU shares configuration

Summary

In this lesson, you should have learned how to:

- Implement process execution in an appropriate scheduling class
- Manage process scheduling priority
- Manage the scheduling class of a zone
- Configure the fair share scheduler
- Monitor the fair share scheduler

10

Installing Oracle Solaris 11 on Multiple Hosts

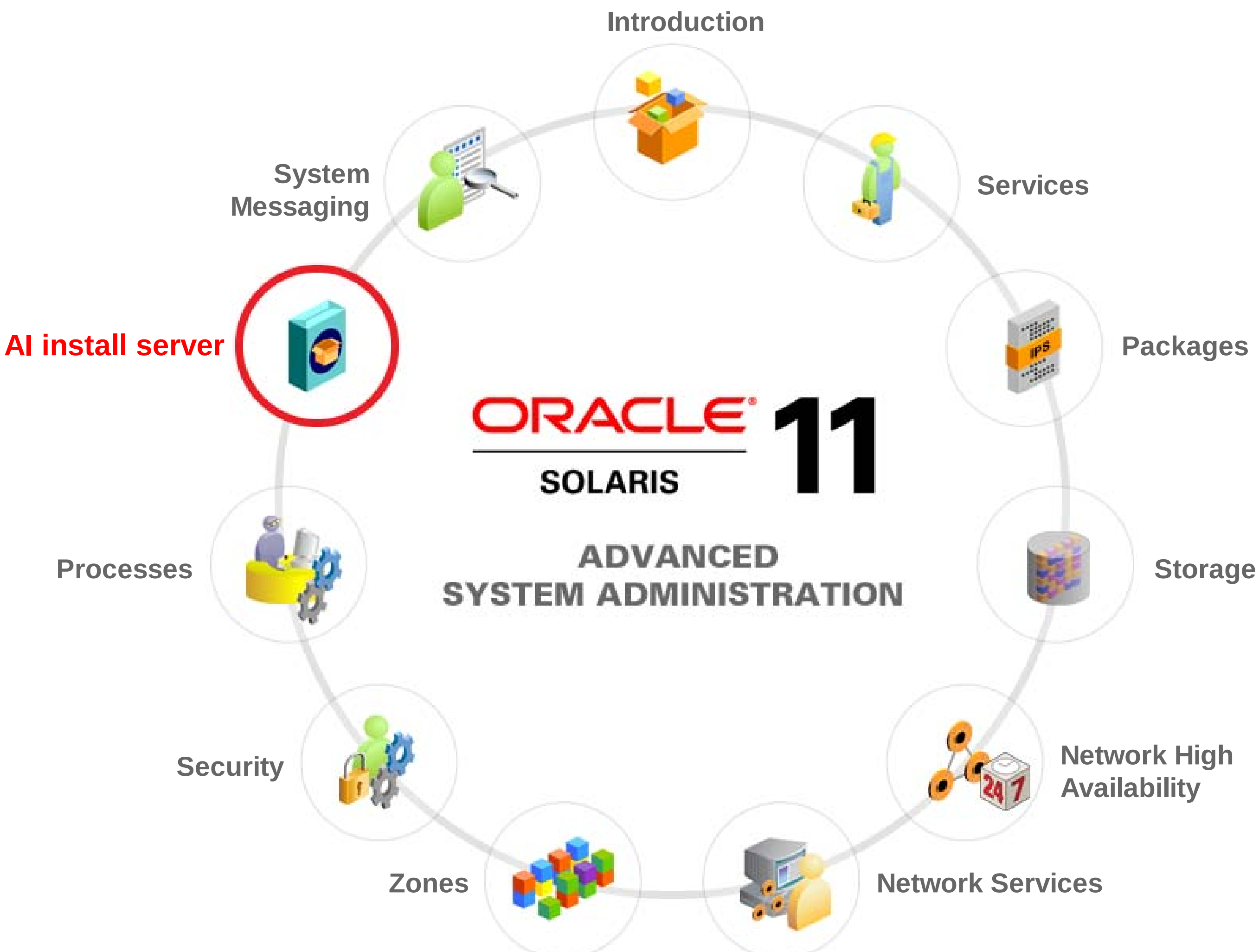
ORACLE

Objectives

After completing this lesson, you should be able to:

- Describe the Automated Installer (AI)
- Configure the AI install server
- Configure the AI client
- Build an Oracle Solaris image by using the distribution constructor

Job Workflow



Agenda

- Introducing the Automated Installer (AI)
- Configuring the AI install server
- Configuring the AI client
- Building an Oracle Solaris Image

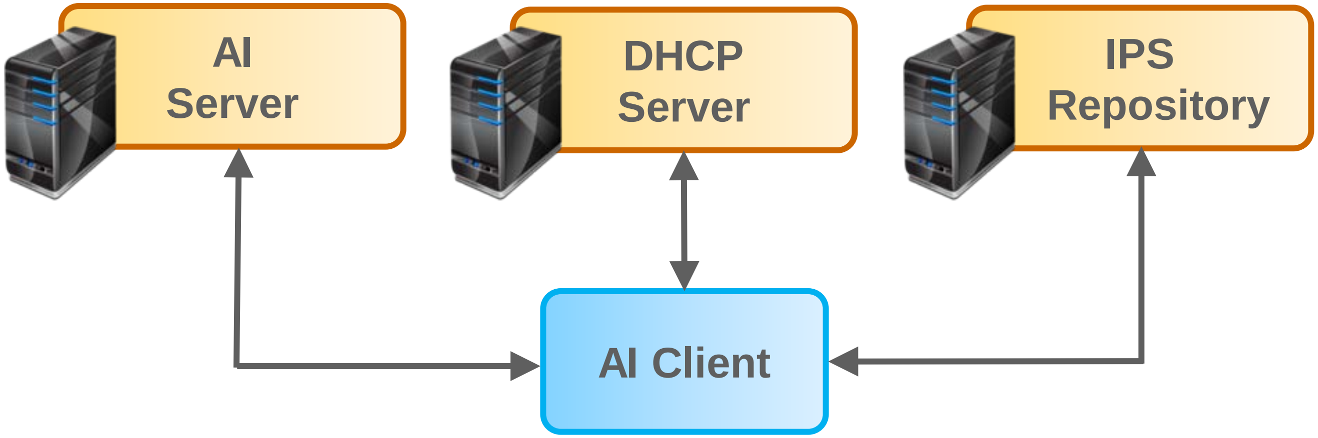
Advantages of Using the Automated Installer

The AI helps you achieve the following:

- Install the Oracle Solaris 11 OS.
- Update all Oracle Solaris x86/64 machines to Oracle Solaris 11.
- Allow flexible configuration of disk layout, Kerberos service and users, provisioning of zones, and software selection.
- Support unattended installation on multiple machines.
- Save significant installation time.

Automated Installation: Overview

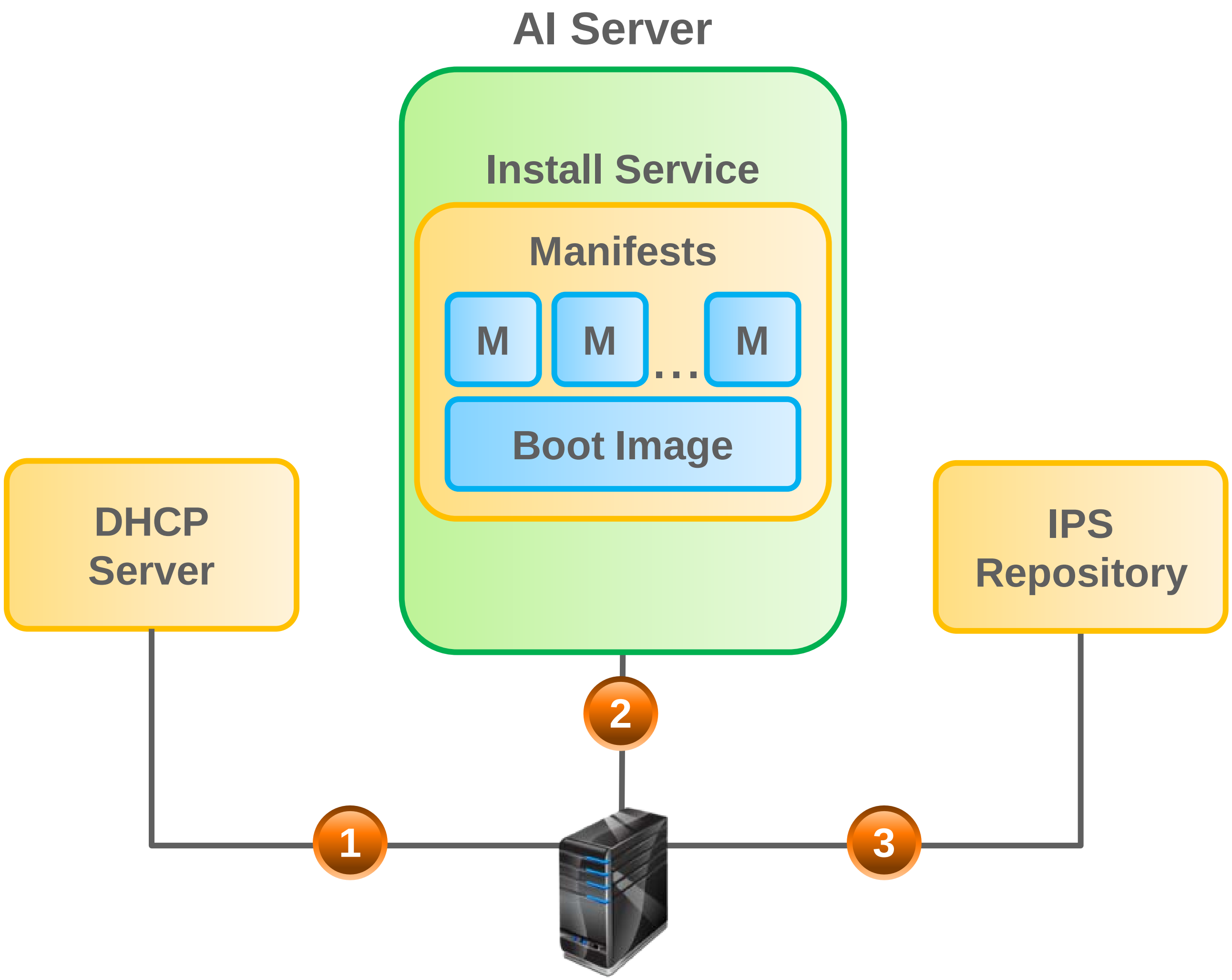
- The AI automates the installation of the OS on one or more SPARC and x86 systems over a network.
- The installations differ in architecture, software packages, disk capacity, network configuration, and other parameters.
- Automated installation requires an AI server, a DHCP server, an IPS repository, and a client system:



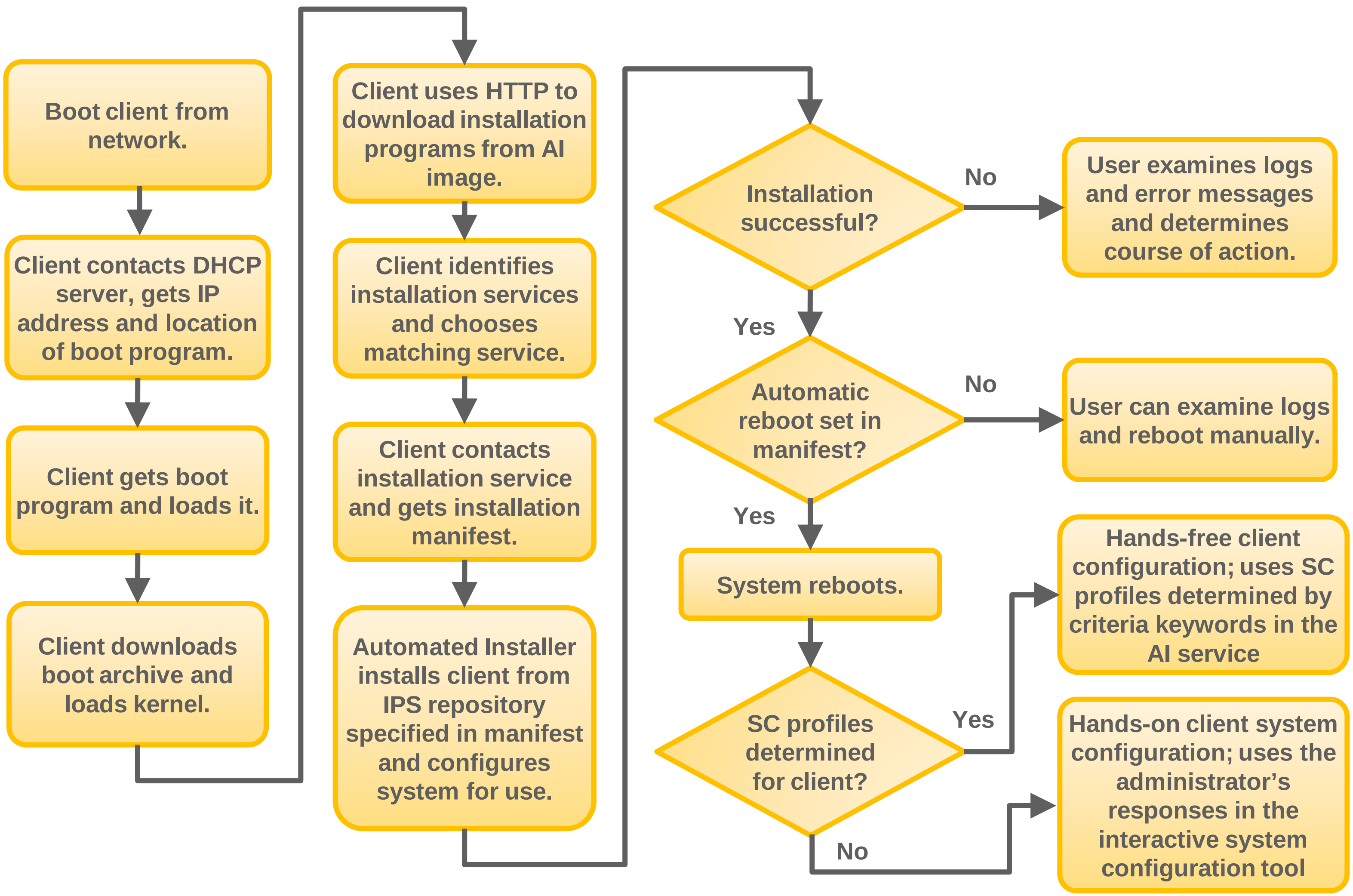
AI Environmental Requirements

- Network
- Client access to AI service and IPS repository
- AI service storage location
- Manifests and system configuration profiles
- Custom manifest and profile storage location

Automated Installation Process



How the AI Works



ORACLE

AI SMF Service

- The SMF service `svc:/system/install/server:default` represents the overall state of the AI server application and all the installation services.
- The AI SMF service is enabled when `installadm create-service` is run.
  - To enable the AI SMF service manually:

```
# svcadm enable svc:/system/install/server:default
```

  - To disable the AI SMF service manually:

```
# svcadm disable svc:/system/install/server:default
```

ORACLE

AI Manifest

- Part of the AI installation service
- XML file that contains installation and configuration instructions for one or more clients
- Default manifest included in each boot image
- Unpacked along with other files in the image

Identifying the Types of AI Manifests

Type	Description
Default AI manifest	Is an installation manifest that has no criteria associated with it
Custom AI manifest	Provides installation criteria for a specific client
Criteria manifest	Allows client-specific installation instructions to be associated with AI services

default.xml File

```
<!DOCTYPE auto_install SYSTEM "file:///usr/share/install/ai.dtd">
<auto_install>
  <ai_instance name="default">
    <target>
      <logical>
       <zpool name="rpool" is_root="true">
        <filesystem name="export" mountpoint="/export"/>
        <filesystem name="export/home"/>
        <be name="solaris"/>
       </zpool>
      </logical>
    </target>
    <software type="IPS">
      <source>
        <publisher name="solaris">
          <origin name="http://pkg.oracle.com/solaris/release"/>
        </publisher>
      </source>
      <software_data action="install">
        <name>pkg:/entire</name>
        <name>pkg:/group/system/solaris-large-server</name>
      </software_data>
    </software>
  </ai_instance>
</auto_install>
```

Criteria Manifest

- Associates client-specific installation instructions with AI services
- Uses an AI manifest selection algorithm
- Uses multiple nonoverlapping criteria
- Can be added using the `installadm create-manifest` command:

```
# installadm create-manifest -f  \  /export/manifests/manifest_x86.xml \
-n s11-x86 –C /export/manifests/criteria_x86.xml
```

ORACLE

Criteria Manifest: Examples

- `arch` criteria manifest file:

```
<ai_criteria_manifest>
        <ai_criteria name="arch">
                <value>i86pc</value>
        </ai_criteria>
</ai_criteria_manifest>
```

- `mac` criteria manifest file:

```
<ai_criteria_manifest>
   <ai_criteria name=“mac">
       <value>0:14:4F:20:53:94</value>
   </ai_criteria>
 </ai_criteria_manifest>
```

- `ipv4` criteria manifest file:

```
<ai_criteria_manifest>
  <ai_criteria name=“ipv4">
            <value>192.168.0.114/24</value>
  </ai_criteria>
</ai_criteria_manifest>
```

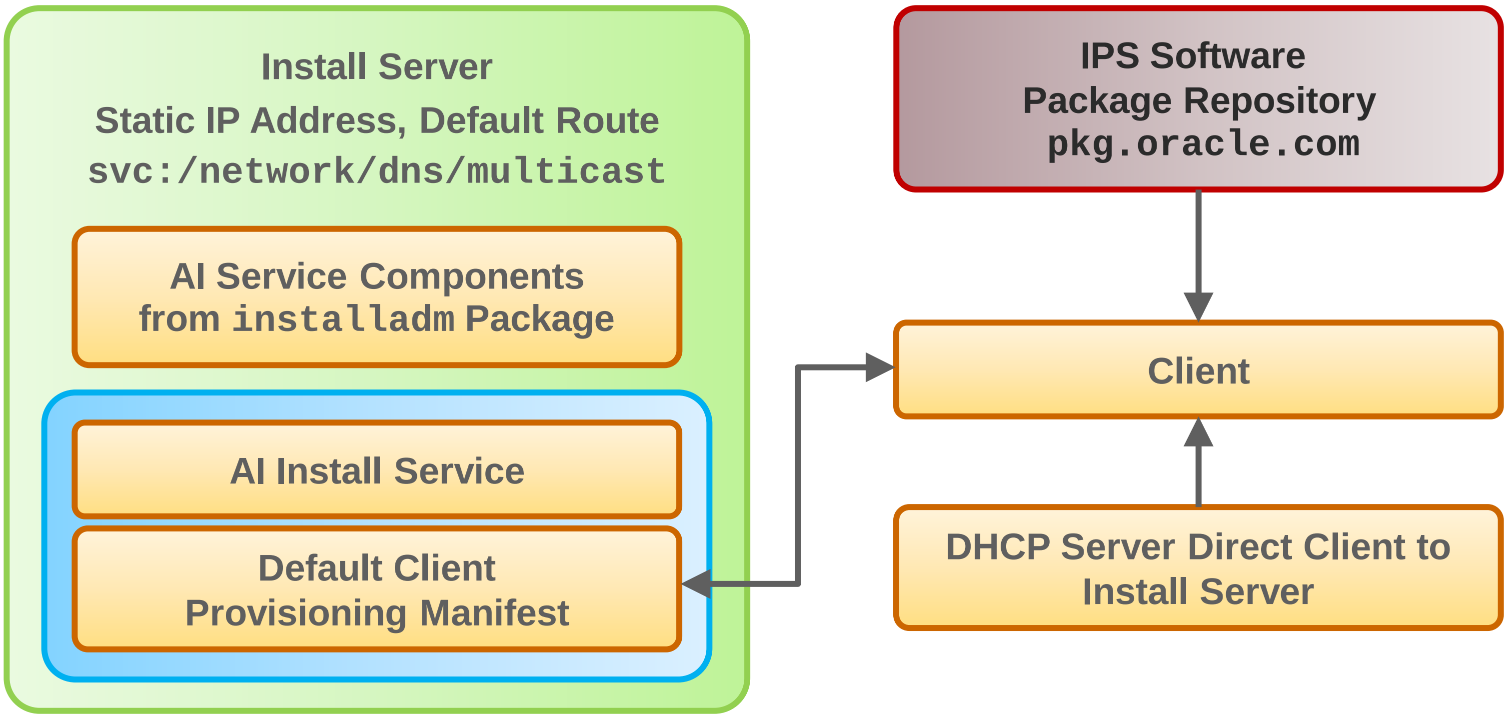
System Configuration Profiles

- SC profiles:
  - Specify client configuration
  - Set SMF properties for appropriate SMF services
  - Are applied during the first client boot after installation
  - Are created by using the `sysconfig create-profile` utility
- AI clients may have multiple SC profiles.
- If no SC profile is specified, the interactive system configuration tool is used at first client boot.

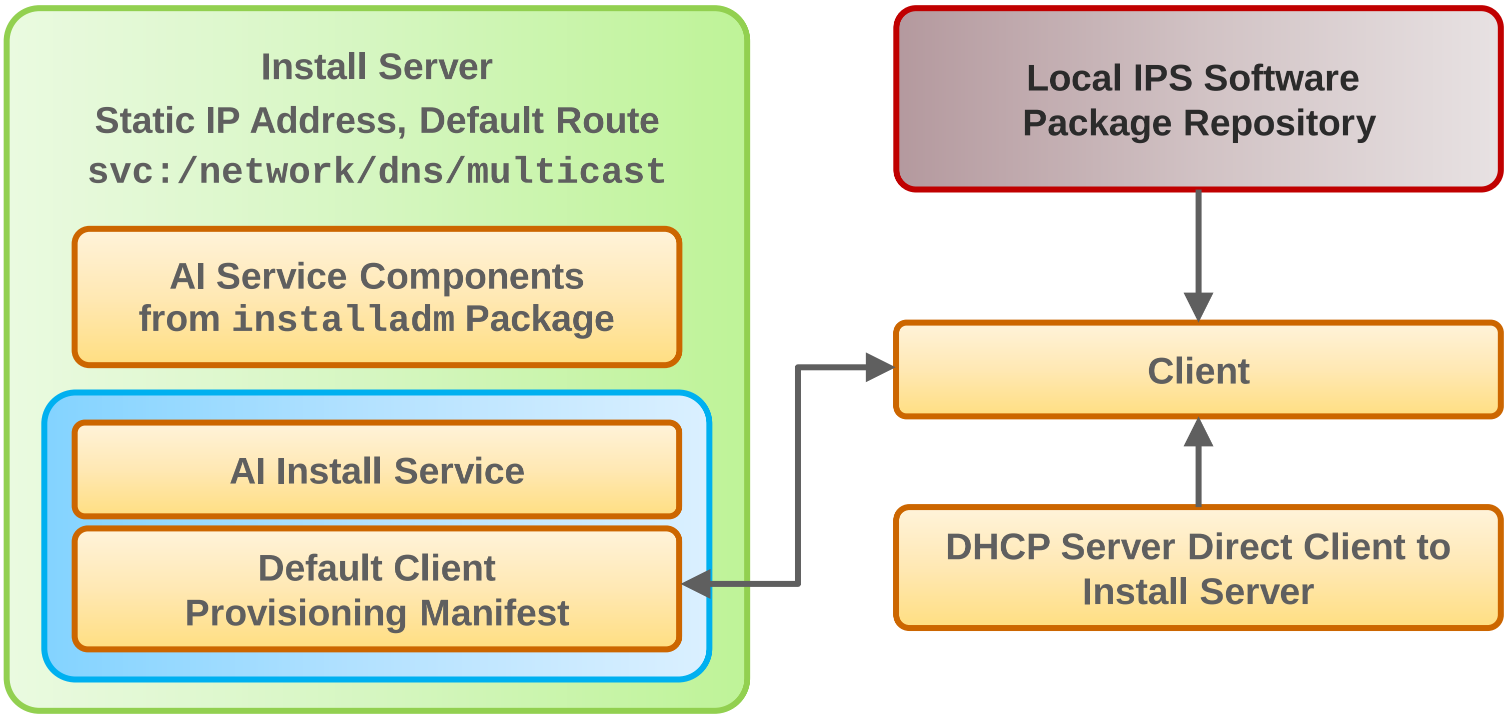
SC Profile: Example

```
<!DOCTYPE service_bundle SYSTEM "/usr/share/lib/xml/dtd/service_bundle.dtd.1">
<service_bundle type="profile" name="sysconfig">
  <service version="1" type="service" name="system/config-user">
    <instance enabled="true" name="default">
      <property_group type="application" name="root_account">
        <propval type="astring" name="login" value="root"/>
        <propval type="astring" name="password"
     value="$5$bypT4oRp$Dsy3J0FhJNBXqlxDtCJjlqk3k3ZHAg8cb98bPLs3kI9"/>
        <propval type="astring" name="type" value="role"/>
      </property_group>
      <property_group type="application" name="user_account">
        <propval type="astring" name="login" value="oracle1"/>
     ...
...
       <property type="astring" name="search">
        <astring_list>
          <value_node value="mydomain.com"/>
        </astring_list>
      </property>
    </property_group>
    <instance enabled="true" name="default"/>
  </service>
</service_bundle>
```

AI Use Case: Using Default Manifest

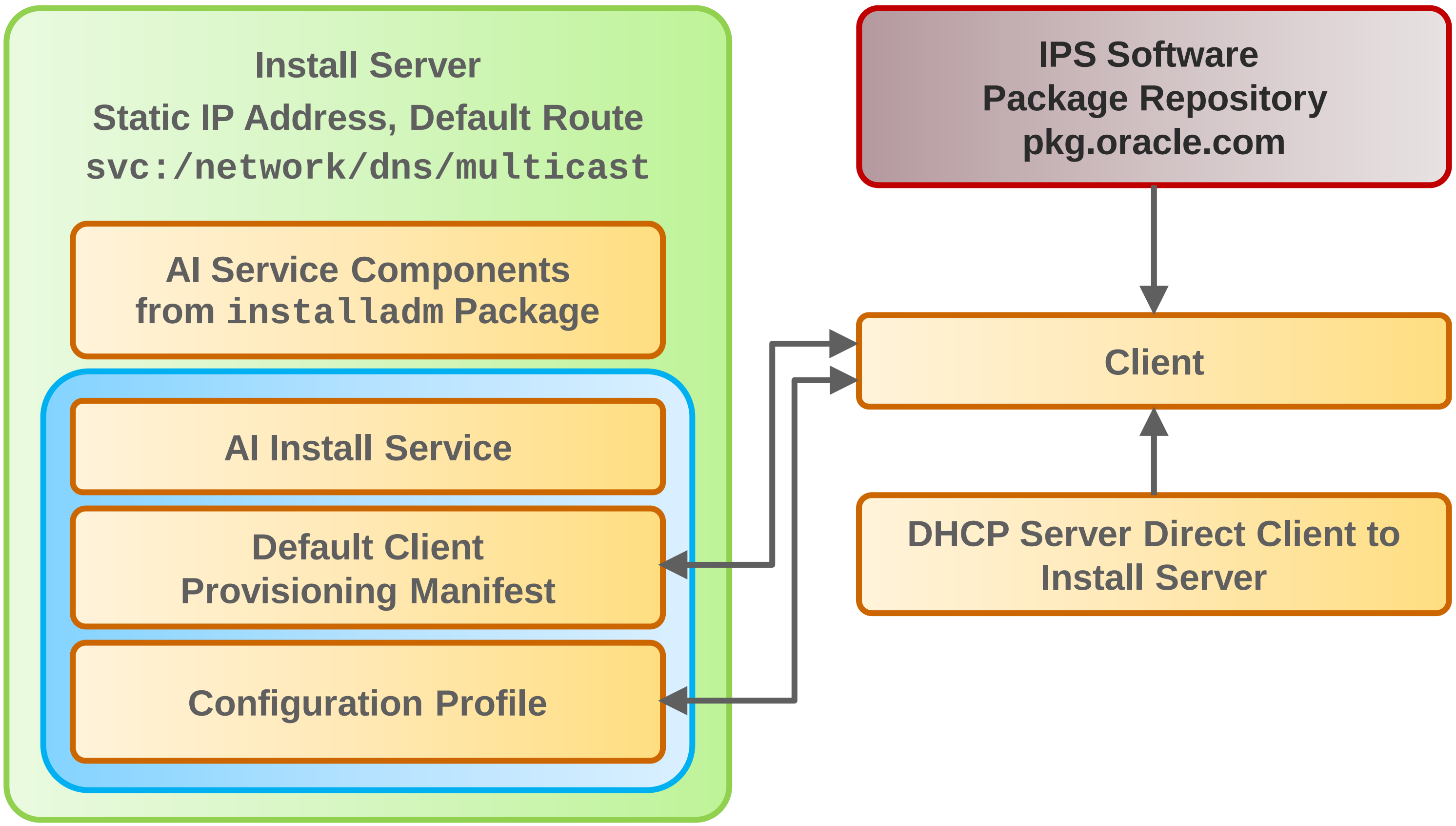


AI Use Case: Using Custom Manifest

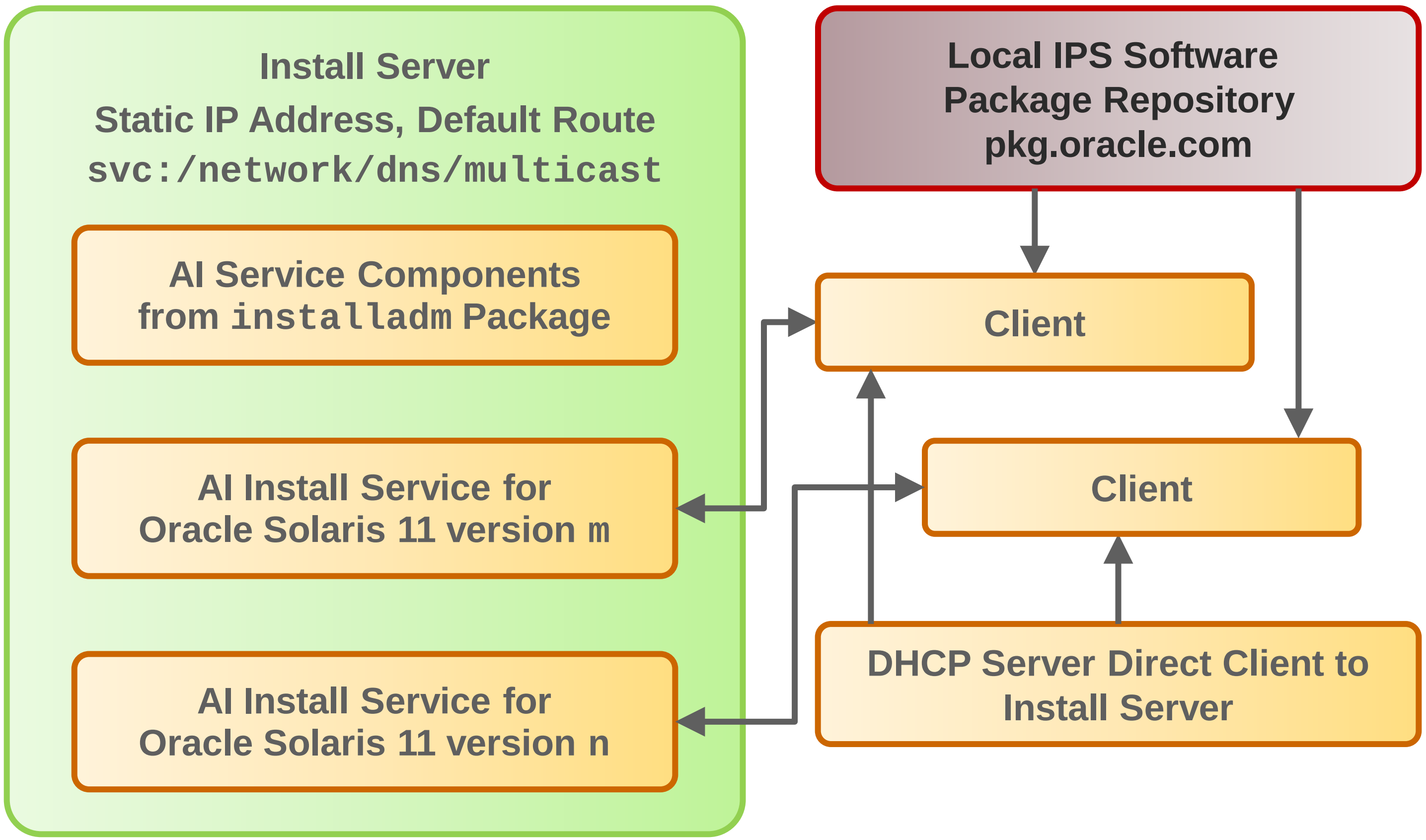


ORACLE

AI Use Case: Using an SC Profile



AI Use Case: Multiple AI Services



Quiz

Which AI component provides installation instructions to the client system?

a. AI server
b. DHCP server
c. IPS repository

Agenda

- Introducing the Automated Installer
- Configuring the AI install server
- Configuring the AI client
- Building an Oracle Solaris Image

Reviewing AI Install Server Requirements

Package Group	Memory	Recommended Minimum Disk Space
`solaris-desktop`	2 GB	13 GB
`solaris-large-server`		9 GB
`solaris-small-server`		8 GB
`solaris-minimal-server`		6 GB

Software	Requirement
Operating system	Oracle Solaris 11 must be installed.
IP address	A static IP address must be used.
Router	The default route must be set.
DHCP	DHCP must be set up.
IPS repository	The repository must be set up locally.

Verifying AI Install Server Software Requirements

Check the following to verify that the server is ready to be configured as an AI server:

- Static IP address configuration
- Operational DNS
- IPS configured and available from the AI server

Verifying the Static IP Address

To verify that the operating system is configured with a static IP address, run `svcs network/physical`, followed by `ipadm show-addr`.

```
# svcs network/physical:default
STATE          STIME    FMRI
online         15:02:57 svc:/network/physical:default
# ipadm show-addr
ADDROBJ            TYPE     STATE        ADDR
...
net0/v4            static   ok           192.168.0.100/24
...
#
```

Verifying That DNS is Operational

To verify that the DNS is operational, run `nslookup` *`server domain name`*.

```
# nslookup server1.mydomain.com
Server:         192.168.0.100
Address:        192.168.0.100#53

Name:   server1.mydomain.com
Address: 192.168.0.100
```

Verifying That IPS is Available Locally

To verify that the correct local IPS repository is available to your server, run `pkg publisher`.

```
# pkg publisher
PUBLISHER    TYPE      STATUS   P   LOCATION
solaris      origin    online   F   http://s11-server1.mydomain.com
```

To test IPS on the local server by searching for the entire package, run `pkg search entire`.

```
# pkg search entire
INDEX       ACTION    VALUE            PACKAGE
pkg.fmri    set       solaris/entire   pkg:/entire@0.5.11-0.175.3.0.0.30.0
```

Practice 10-1 Overview: Verifying System AI Requirements (Optional)

In this practice, you check the existing version of Oracle Solaris 11 to verify the system requirements for the AI installation.

Note: This practice is optional and must be completed *only* if you have not completed the Practice 3 tasks.

Configuring the AI Install Server

1. Enable the DNS multicast service.
2. Create a directory for the AI service.
3. Verify the `netmasks` file configuration.
4. Create an AI installation service:
   - With a DHCP setup
   - Without a DHCP setup
5. Review the default installation instructions.
6. Add installation criteria to an AI service.

ORACLE

Enabling the DNS Multicast Service

To enable the DNS multicast service, run `svcadm enable svc:/network/dns/multicast`.

```
# svcadm enable svc:/network/dns/multicast
# svcs network/dns/multicast
STATE          STIME    FMRI
online          1:32:27 svc:/network/dns/multicast:default
```

Installing the AI Installation Tools

1. Ensure that you are connected to an IPS repository that contains the `install/installadm` package .

```
# pkg publisher
PUBLISHER    TYPE     STATUS  P  LOCATION
solaris      origin   online  F  http://s11-server1.mydomain.com
# pkg list -a installadm
NAME (PUBLISHER)            VERSION                       IFO
install/installadm          0.5.11-0.175.3.0.0.30.0       ---
```

2. Determine whether the `installadm` package is already installed on this system.

```
# pkg list installadm
pkg list: no packages matching 'installadm' installed
```

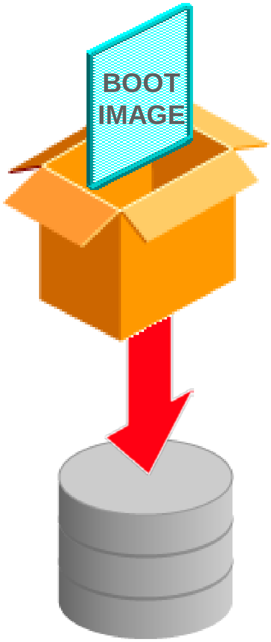
3. Install the `installadm` package by using the `pkg install` command.

```
# pkg install install/installadm
```

Setting Up the AI Boot Image

Download the AI boot image from:

http://www.oracle.com/technetwork/server-storage/solaris11/downloads/index.html

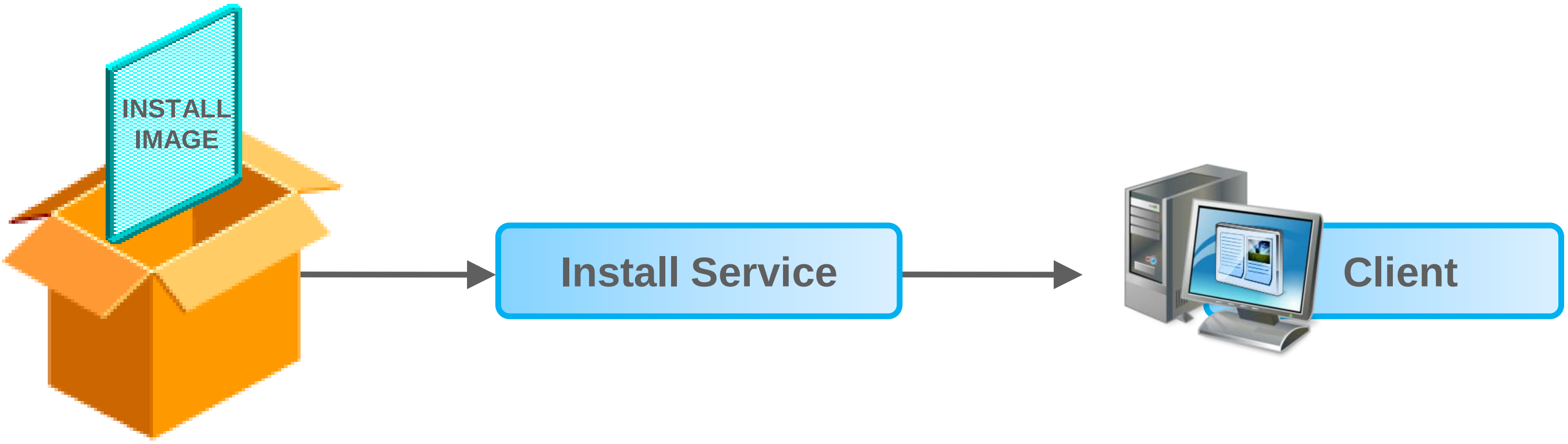


Note: The AI ISO image must be the same version as the Oracle Solaris OS that you plan to install on the client.

Configuring an AI Installation Service

The AI installation service:

- Associates an installation image with a named installation service
- Enables client systems to use the install service name to find the correct install image
- Is associated with only one boot image
- Can be created with or without a DHCP setup



Verifying the `netmasks` File Configuration

To verify the `netmasks` file configuration, run `getent netmasks` *`IP_Address`*.

```
# getent netmasks 192.168.0.0
```

If a network mask entry for the local subnet does not exist in `/etc/netmasks`, update the file.

```
# pfedit /etc/netmasks
 …
192.168.0.0 255.255.255.0
```

Creating an AI Installation Service with an ISC DHCP Server Setup

To create an AI installation service with an ISC DHCP server setup, run `installadm create-service`, followed by the service name, the path to the ISO image, the IP address range, and the path to where the ISO image should be unpacked.

```
# installadm set-server -i 192.168.0.130 -c 5
<output omitted>
# installadm create-service -n basic_ai \
-s /opt/ora/iso/sol-11_3-ai-x86.iso -d /export/ai/basic_ai
<output omitted>
# installadm list
Service Name Status Arch Type Secure Alias Alients Clients Profiles Manifests
------------ ------ ---- ---- ------ ----  ------- ------- -------- ---------
basic_ai     on     i386 iso  no     on    0       0       0        1
```

Creating an AI Installation Service Without a DHCP Setup

To create an AI installation service without a DHCP setup, run `installadm create-service`, followed by the service name, the path to the ISO image, and the path to where the ISO image should be unpacked.

```
# installadm create-service -n s11-sparc \
-s /var/tmp/images/sparc/sol-11_3-ai-sparc.iso -d /install/images/s11-sparc

Creating service: s11-sparc

Setting up the target image at /install/images/s11-sparc ...
Service discovery fallback mechanism set up
Creating SPARC configuration file
Refreshing install services

Creating default-sparc alias.

No local DHCP configuration found. This service is the default alias
for all SPARC clients. If not already in place, the following should be added to the DHCP
configuration:
            Boot file : http://10.80.238.5:5555/cgi-bin/wanboot-cgi

Service discovery fallback mechanism set up
Creating SPARC configuration file
Refreshing install services
```

Adding a Client to the AI Installation Service

To add a client to the AI installation service, run `installadm create-client -c`, followed by the client MAC address and the AI installation service name.

```
# installadm create-client -e 08:00:27:85:C7:D6 -n basic_ai
# installadm list -c
Service Name      Client Address        Arch   Image Path
------------      ---------------       ----   -----------
basic_ai          08:00:27:85:C7:D6     i386   /export/ai/default_ai
```

Adding an SC Profile to an Installation Service

Use the `installadm create-profile` command to add the *profile_filename* SC profile to the *svcname* installation service.

```
# installadm create-profile -n svcname -f profile_filename
```

Use the `installadm validate` command to validate SC profiles for syntactic correctness.

```
# installadm validate -n svcname -p profile_name
```

ORACLE

Creating a Custom AI Manifest

To create and apply a custom AI manifest, perform the following steps:

1. Create a directory to store your manifest files.
2. Copy the `default.xml` file to the `basic_ai.xml` file.
3. Modify the `basic_ai.xml` file.
4. Add the new custom AI manifest to the appropriate AI installation service.
5. Add the criteria file to associate the client host.

Selecting the AI Manifest

- The criteria file associates installation instructions with the client.
- The AI manifest selection algorithm is as follows:
  - The client does not match the criteria for any manifest: The client uses the default manifest.
  - The client matches the criteria for a single manifest: The client uses that manifest.
  - The client matches the criteria for multiple manifests: The criteria are evaluated based on ordering.
- The criteria file uses multiple nonoverlapping criteria.

Adding Installation Criteria to an AI Manifest

To create a manifest for a service and associate it with the installation criteria, run `installadm create-manifest`, followed by the service name, the manifest's file path name, and the criteria file's path name.

```
# installadm create-manifest -n basic_ai \
-f /var/tmp/manifests/basic_ai.xml \
-C /var/tmp/manifests/criteria_ai.xml
# installadm list -m
Service Name      Manifest           Status
------------      --------           ------
basic_ai            basic_ai
                    orig_default      Default
default-i386        orig_default      Default
# installadm list -m -n basic_ai
Manifest           Status   Criteria
--------           ------   --------
basic_ai                    mac = 08:00:27:85:C7:D6
orig_default       Default  None
```

Introducing the Automated Installer CLI Manifest Editor

- Administrators can edit AI manifests without any knowledge of XML by using enhancements to the existing `installadm(1M)` command.
- This interface provides the ability to interactively create and edit new manifests that can be associated with AI services.
  - The interface presents the AI manifest content as a set of objects and properties
  - The interface can be accessed from the create-manifest or update-manifest subcommands. For example:

```
# installadm create-manifest -n servicename -m new-manifest
```

Note: It brings up a manifest in the installadm interactive mode that is based on reasonable defaults.

```
# installadm update-manifest -n servicename -f file -m manifest
```

Note: It updates a manifest using the contents of the named file

ORACLE

Installing and Configuring Zones by Using AI

This section covers the following topics:

- How AI installs nonglobal zones
- Specifying nonglobal zones in the global zone AI manifest
- Nonglobal zone configuration and installation data

How AI Installs Nonglobal Zones

Nonglobal zones are installed and configured on the first reboot after the global zone is installed.

1. When a system is installed using AI, nonglobal zones can be installed on that system by using the configuration element in the AI manifest.
2. When the system first boots after the global zone installation, the zone's self-assembly SMF service (`svc:/system/zones-install:default`) configures and installs each nonglobal zone defined in the global zone AI manifest.
3. If the zone is configured with `autoboot=true`, the `system/zones-installservice` boots the zone after the zone is installed.

Specifying Nonglobal Zones in the Global Zone AI Manifest

```
<!DOCTYPE auto_install SYSTEM "file:///usr/share/install/ai.dtd.1">
<auto_install>
  <ai_instance>
    <target>
      <logical>
        <zpool name="rpool" is_root="true">
          <filesystem name="export" mountpoint="/export"/>
          <filesystem name="export/home"/>
          <be name="solaris"/>
        </zpool>
      </logical>
    </target>
    <software type="IPS">
      <source>
        <publisher name="solaris">
          <origin name="http://pkg.oracle.com/solaris/release"/>
        </publisher>
      </source>
      <software_data action="install">
        <name>pkg:/entire@latest</name>
        <name>pkg:/group/system/solaris-large-server</name>
      </software_data>
    </software>
    <configuration type="zone" name="zone1" source="http://server/zone1/config"/>
    <configuration type="zone" name="zone2" source="file:///net/server/zone2/config"/>
  </ai_instance>
</auto_install>
```

ORACLE

Nonglobal Zone Configuration and Installation Data

Required File	Description
`config` file	Required. The `config` file is the zone's configuration in file form from the output of the `zonecfg export` command.
AI manifest	Optional. This AI manifest for zone installation specifies packages to be installed in the zone, along with publisher information, and certificate and key files as necessary.
Configuration profile	Optional. You can provide zero or more configuration files for a nonglobal zone. These configuration profiles are similar to the system configuration profiles for configuring the global zone.

ORACLE

Practice 10-2 Overview: Configuring the AI Server

This practice covers the following topics:

- Enabling the DNS multicast service
- Verifying the `netmasks` file configuration
- Creating an AI installation service with a DHCP setup
- Adding installation criteria to an AI service
- Creating a directory to store the AI manifest files
- Modifying the AI manifest files

ORACLE

Agenda

- Introducing the Automated Installer
- Configuring the AI install server
- Configuring the AI client
- Building an Oracle Solaris Image

ORACLE

How a Client Is Installed

The client is booted from the network. After booting, the client system performs the following steps:

1. Contacts the DHCP server and retrieves the client's network configuration and the location of the installation server
2. Loads the net image
3. Completes its installation using the AI manifest
4. Reboots if `auto_reboot` is set in the AI manifest, or the client should be manually rebooted
   Note: During reboot, the client system is configured either by using system configuration profiles or by using the responses provided in the interactive system configuration tool.

Configuring the Client System

This section covers the following topics:

- Identifying the client system requirements
- Using Secure Shell to remotely monitor an installation
- Implementing the configuration
- Reviewing client installation messages

Identifying Client System Requirements

Client System	Requirement
Disk space	Recommended minimum: 13 GB
Memory	Recommended minimum: 2 GB
Architectures	• X86: 64-bit only • SPARC: Oracle Solaris M-series and T-series systems only
Network access	• DHCP server that provides network configuration information • AI install server • IPS repository that contains the packages to be installed on the client system

Additional SPARC client system requirements:

- WAN boot support
- Firmware that includes the current version of the OBP that contains the latest WAN boot support

Using Secure Shell to Remotely Monitor an Installation

- For x86 client installations, the `menu.lst` file is located in:
  - `/etc/netboot/menu.lst.01MAC_address` if `installadm create-client` was used
  - `/etc/netboot/<service_name>/menu.lst` if `installadm create-client` was not used
- For SPARC client installations, `system.conf` and `wanboot.conf` are in:
  - `/etc/netboot/<service_name>`

  For the `default-sparc` service, symlinks to these files are in `/etc/netboot`.

Implementing the Configuration

- To boot a SPARC client and start an installation, use the following command from the OBP prompt:
  `OK boot net:dhcp - install`
- To boot an x86 client from the network, from the GNU GRUB menu, select the `Oracle Solaris 11.3 Text Installer and command line` boot option.

Reviewing Client Installation Messages

If the client installation is successful, you see the following:

- Automated Installation started message:

```
Automated Installation started
   The progress of the Automated Installation will be
output to  the console
   Detailed logging is in the logfile at
/system/volatile/install_log
   Press RETURN to get a login prompt at any time.
```

- Automated Installation succeeded message:

```
Automated Installation finished successfully
The system can be rebooted now
Please refer to the /system/volatile/install_log file for
details
After reboot it will be located at
/var/sadm/system/logs/install_log
```

ORACLE

Practice 10-3, Practice 10-4, Practice 10-5, and Practice 10-6: Overview

You will now perform the following practices:

- Deploying the OS to a network client
- Configuring Oracle Solaris 11 instances
- Customizing the automated installation
- (Optional) Deploying a system by using a Unified Archive through the AI

Agenda

- Introducing the Automated Installer
- Configuring the AI install server
- Configuring the AI client
- Building an Oracle Solaris Image

Distribution Constructor: Introduction

- Is a command-line tool that is used to build:
  - Preconfigured custom Oracle Solaris images
  - An ISO image based on the XML manifest file
- Allows creation of the following Oracle Solaris image types:
  - x86 or SPARC Oracle Solaris text installer image
  - Oracle Solaris x86 Live Media image
  - x86 or SPARC ISO image for Automated Installations
  - SPARC USB images for AI and text installer
- Is distributed in the `distribution-constructor` package, which contains:
  - The `distro_const` command-line utility and its files
  - Sample manifest files

ORACLE

Identifying System Requirements for Using the Distribution Constructor

Requirement	Description
Disk space	Recommended minimum: 8 GB
Oracle Solaris release	• SPARC or x86 Oracle Solaris 11 operating system (OS) must be installed. • Network access to the IPS repositories specified in the manifest file is required. • SPARC images can be created only on a SPARC system. • x86 images can be created only on an x86 system. • The Oracle Solaris release version must match the release version of the image to be built with the distribution constructor.
Required packages	The distribution-constructor package must be installed.

ORACLE

Using Distribution Constructor Manifest Files

Manifest File	Manifest Type	Description
`/usr/share/distro_const/dc_text_x86.xml`	x86 text installer ISO image	Used to create an ISO image that you can boot to initiate a text installation of the Oracle Solaris OS on x86 machines
`/usr/share/distro_const/dc_text_sparc.xml`	SPARC text installer ISO image	Used to create an ISO image that you can boot to initiate a text installation of the Oracle Solaris OS on SPARC machines
`/usr/share/distro_const/dc_livecd.xml`	x86 Live Media ISO image	Used to create an ISO image that is comparable with the Oracle Solaris live media image
`/usr/share/distro_const/dc_ai_sparc.xml`	SPARC AI ISO image	Used to create a SPARC AI ISO image for automated installations of the Oracle Solaris OS to SPARC clients
`/usr/share/distro_const/dc_ai_x86.xml`	x86 AI ISO image	Used to create an x86 AI ISO image for automated installations of the Oracle Solaris OS to x86 clients

ORACLE

Image Creation Process

- The distribution constructor:
  - Contains sample manifests that can be used to create a custom x86 Live Media ISO, an x86 or SPARC Automated Install ISO image, or an x86 or SPARC text installation ISO image
  - Creates images based on settings specified in manifest files
- The manifest files contain specifications for the contents and parameters of the ISO images that you create using the distribution constructor.

Creating a Custom Image

To create a custom image, perform the following steps:

1. Install the `distribution-constructor` package, which contains the distribution constructor application and the sample manifests.

```
# pkg install distribution-constructor
```

2. Copy one of the sample manifests and create a custom manifest file with a new file name.
3. Optionally, you can edit the manifest elements to specify a different location for the build area or different publisher and repository location.
4. Create custom scripts to further modify the image.

Building an Image

- The build can be performed in one step:
  - `distro_const build manifest`
- Checkpointing is enabled by default.
- The build can be stopped and resumed at a specific checkpoint (step):
  - `distro_const build -p step manifest`
  - `distro_const build -r step manifest`

ORACLE

Quiz

The distribution constructor is used to create only Oracle Solaris SPARC text installer images.

a. True

b. False

Quiz

Which command enables you to build an OS image in one step?

a. `distro_const`

b. `distro_const build`

c. `distro_const build` *`manifest`*

Quiz

The process of stopping and restarting during the image build process is called ________.

a. checking
b. checkpointing
c. spotcheck

Summary

In this lesson, you should have learned how to:

- Describe the Automated Installer
- Configure the AI install server
- Configure the AI Client
- Build an Oracle Solaris Image

11

Implementing System Messaging and Diagnostic Facilities

ORACLE

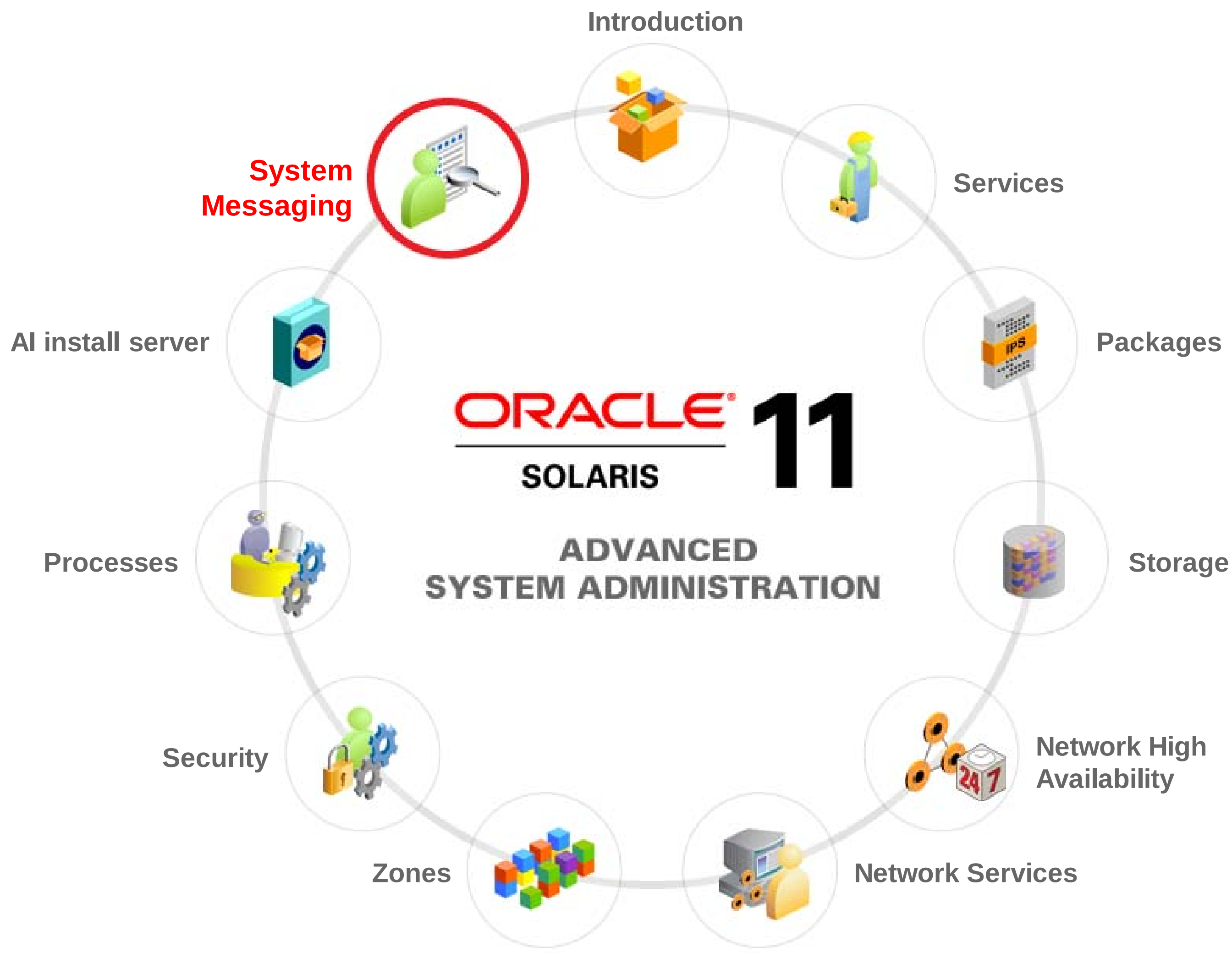
Objectives

After completing this lesson, you should be able to:

- Monitor system logs
- Identify a crash dump file
- Identify a core dump file
- Troubleshoot a script execution issue
- Troubleshoot a software update failure
- Troubleshoot a network connectivity issue
- Troubleshoot a directory access issue
- Troubleshoot a default shell issue
- Configure the following:
  - System messaging
  - System crash facilities
  - Dump facilities for business application failure
- Explain the role of DTrace in diagnosing system issues

ORACLE

Job Workflow



Agenda

- Managing System Logs
- Configuring System Messaging
- Configuring System Crash Facilities
- Configuring Dump Facilities for Business Application Failure
- Explaining the Role of DTrace in Diagnosing System Issues

Importance of Implementing System Messaging and Diagnostic Facilities

System messaging and diagnostic facilities implementation ensures that:

- Controls are in place to monitor system activities so that issues can be addressed quickly and efficiently
- System crashes and core dumps are captured and reported so that major problems can be analyzed and corrected

ORACLE

Monitoring System Logs

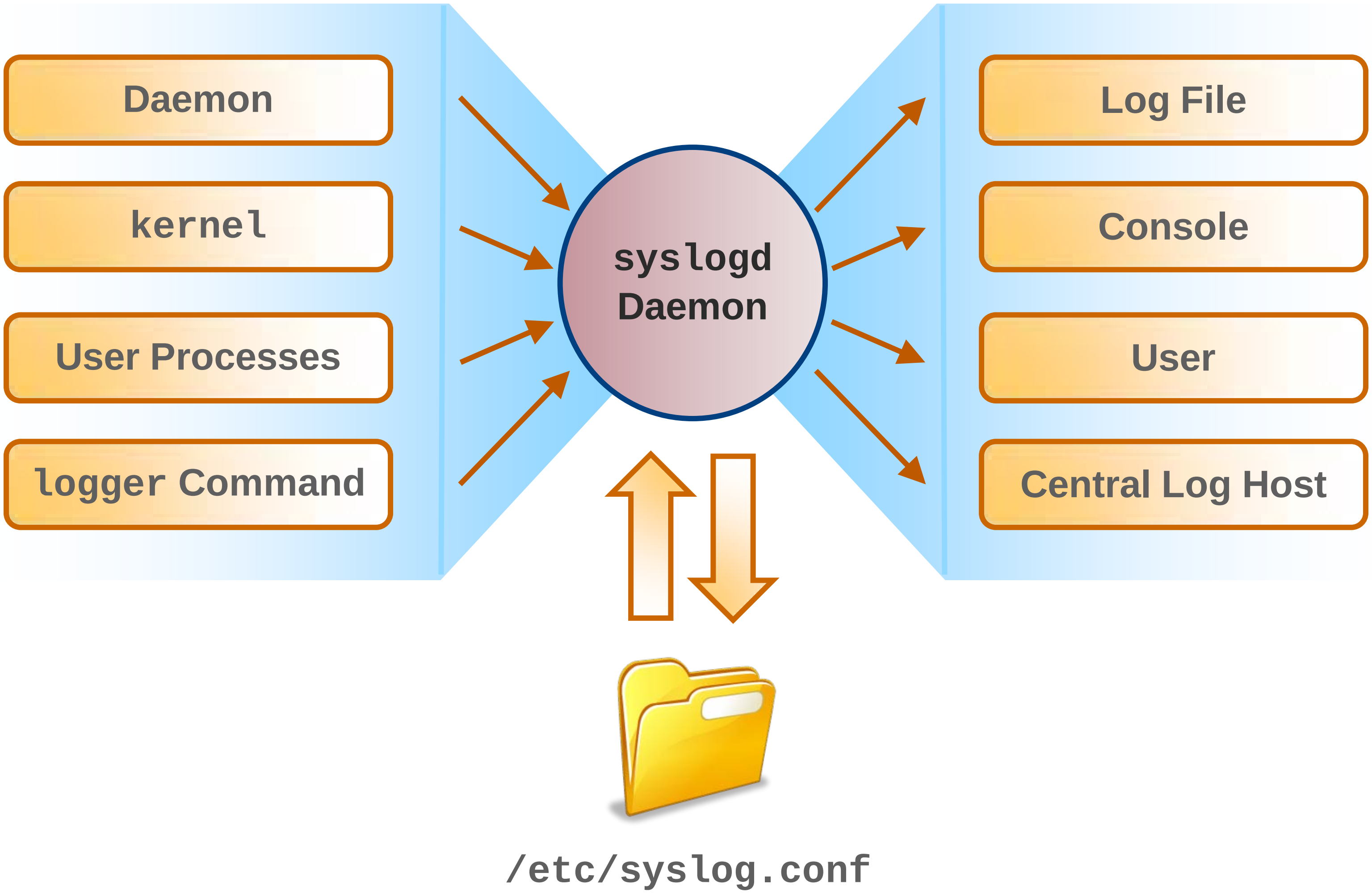
System messages are stored in the `/var/adm` directory.

```
client1:/var/adm# ls
acct         lastlog      messages     messages.2   sa           sulog
aculog       log          messages.0   messages.3   sm.bin       utmpx
exacct       loginlog     messages.1   pool         streams      wtmpx
```

- The `/var/adm` directory contains several message files:
  - Most recent messages: `/var/adm/messages`
  - Oldest messages: `messages.3`
- Message files are rotated about every 10 days:
  - `messages.0` is renamed `messages.1`.
  - `messages.1` is renamed `messages.2`.
  - `messages.2` is renamed `messages.3`.

ORACLE

syslogd Daemon



`/etc/syslog.conf` File

An `/etc/syslog.conf` file configuration entry consists of:

- The selector field, which contains two components:
  - ***`facility:`*** Category of system process that can generate messages
  - ***`facility.level:`*** Severity or importance of a message
- The action field, which determines where the message is sent

```
*.err                          /var/adm/messages
```

ORACLE

Interpreting the `/etc/syslog.conf` File Selector *`facility`* Field

Field	Description
`kern`	Messages generated by the kernel
`user`	Messages generated by user processes. This is the default priority for messages from programs or facilities that are not listed in this file.
`mail`	Messages generated by the mail system
`daemon`	Messages generated by system daemons, such as the `in.ftpd` and the `telnetd` daemons
`auth`	Messages generated by the authorization system, including the `login`, `su`, and `getty` commands
`lpr`	Messages generated by the line printer spooling system, such as the `lpr` and `lpc` commands

Interpreting the `/etc/syslog.conf` File Selector *`facility`* Field

Field	Description
`news`	Files reserved for the USENET network news system
`uucp`	Designated for the UNIX-to-UNIX copy (UUCP) system, which does not currently use the `syslog` function
`cron`	Designated for `cron/at` messages generated by systems that do logging through `syslog`. The current version of the Oracle Solaris Operating Environment does not use this facility for logging.
`audit`	Designated for audit messages generated by systems that audit by means of `syslog`
`local0-7`	Fields reserved for local use
`mark`	The time when the message was last saved
`*`	All facilities, except the `mark` facility

ORACLE

Interpreting the `/etc/syslog.conf` File Selector *`level`* Field

Level	Priority	Description
`emerg`	0	Panic conditions that are normally broadcast to all users
`alert`	1	Conditions that should be corrected immediately, such as a corrupted system database
`crit`	2	Warnings about critical conditions, such as hard device errors
`err`	3	Errors other than hard device errors
`warning`	4	Warning messages
`notice`	5	Nonerror conditions that might require special handling
`info`	6	Informational messages
`debug`	7	Messages that are normally used only when debugging a program
`none`	8	Messages not sent from the indicated facility to the selected file

ORACLE

Interpreting the `/etc/syslog.conf` File Action Field

Field	Description
`/pathname`	This indicates the full path name to the targeted file.
`@host`	The `@` sign denotes that messages must be forwarded to a remote host. Messages are forwarded to the `syslogd` daemon on the remote host.
`user1, user2`	The `user1` and `user2` entries receive messages if they are logged in.
`*`	All logged-in users receive messages.

Monitoring a `syslog` File in Real Time

To view messages sent to the `/var/adm/messages` file, use `tail -f /var/adm/messages`.

```
Jun 14 13:15:39 host1 inetd[2359]:[ID 317013 daemon.notice] telnet[2361]
from 192.9.200.1 45800
```

Number	Field	Result
1	Date/time	`Jun 14 13:15:39`
2	Local host name	`host1`
3	Process name/PID number	`inetd[2359]`
4	MsgID number/selector facility.level	`[ID 317013 daemon.notice]`
5	Incoming request	`telnet`
6	PPID number	`[2361]`
7	IP address	`192.9.200.1`
8	Port number	`45800`

Interpreting System Messages

```
# tail -f /var/adm/messages
Nov 9 09:25:53 server1 named[472]: [ID 873579 daemon.notice] running
Nov 9 09:26:24 server1 mac: [ID 736570 kern.info] NOTICE: net1
unregistered
#
```

```
# tail -f /var/adm/messages
Nov 9 09:40:03 client1 genunix: [ID 936769 kern.info] fssnap0 is
/pseudo/fssnap@0
Nov 9 09:40:07 client1 gnome-session[784]: [ID 702911 daemon.warning]
WARNING: IceListenForConnections returned 2 non-local listeners:
inet/client1:39166,inet6/client1:38708
#
```

Configuring the `/etc/syslog.conf` File

You configure this file to:

- Define target locations for the `syslog` message files
- Use a selector level of `err` to indicate that all events of priority error (and higher) are logged to the target defined in the action field

```
*.err;kern.notice;auth.notice                   /dev/sysmsg
*.err;kern.debug;daemon.notice;mail.crit   /var/adm/messages
*.alert;kern.err;daemon.err                      operator
*.alert                                          root
usr.emerg                                        *
```

Note: Whenever you make changes to this file, you must restart the `syslogd` daemon.

Stopping and Starting the `syslogd` Daemon

- The `syslogd` daemon can be started:
  - Automatically during boot
  - Manually from the command line
- Each time the `syslogd` daemon starts, the `/etc/syslog.conf` configuration file is read.
- After you have modified the configuration file, you can:
  - Manually stop or start the `syslogd` daemon
  - Send the `syslogd` daemon a `refresh` command

```
# svcadm disable svc:/system/system-log:default
# svcadm enable svc:/system/system-log:default
# svcadm refresh svc:/system/system-log:default
```

ORACLE

`logger` Command

- This command enables you to send messages to the `syslogd` daemon.
- You can write administrative shell scripts that report the status of backups or other functions.

```
logger [ -i ] [ -f file ] [ -p priority ] [ -t tag ] [ message ]
```

```
# logger System rebooted
```

```
# logger -p user.err System rebooted
```

Agenda

- Managing System Logs
- Configuring System Messaging
- Configuring System Crash Facilities
- Configuring Dump Facilities for Business Application Failure
- Explaining the Role of DTrace in Diagnosing System Issues

Configuring System Messaging

This section covers the following topics:

- TCP tracing
- Logging a message by using TCP trace
- Setting up message routing
- Restarting the message logging daemon
- Using TCP trace to log a message
- Monitoring message logging in real time

TCP Tracing

- You can use the inetadm command to enable the trace option on one or more services.
- The inetadm command uses the syslog command to record and log the following:
  - Client's IP address
  - TCP port number
  - Name of the service
- You can configure /etc/syslog.conf so that the syslogd daemon selectively distributes messages sent to it from the inetd daemon.

```
# grep daemon.notice /etc/syslog.conf
*.err;kern.debug;daemon.notice;mail.crit /var/adm/messages
```

ORACLE

Logging a Message by Using TCP Trace

```
# inetadm -m spray tcp_trace=TRUE
# inetadm -l svc:/network/rpc/spray:default
SCOPE    NAME=VALUE
         name="sprayd"
         endpoint_type="tli"
         proto="datagram_v"
         isrpc=TRUE
         rpc_low_version=1
         rpc_high_version=1
         wait=TRUE
         exec="/usr/lib/netsvc/spray/rpc.sprayd"
         user="root"
default  bind_addr=""
default  bind_fail_max=-1
default  bind_fail_interval=-1
default  max_con_rate=-1
default  max_copies=-1
default  con_rate_offline=-1
default  failrate_cnt=40
default  failrate_interval=60
default  inherit_env=TRUE
default  tcp_trace=TRUE
default  tcp_wrappers=FALSE
default  connection_backlog=10
default  tcp_keepalive=FALSE
```

ORACLE

Setting Up Message Routing

1. By using the `pfedit` utility, edit the contents of the `/etc/syslog.conf` file to append the following entry to the file:

   ```
   local0.notice                    @hostname
   ```

2. Restart the `syslogd` daemon to activate the new configuration.
3. On the local host, create the `/var/log/loca10.log` file.
4. Modify the `/etc/syslog.conf` file and add the entry as follows:

   ```
   local0.notice                    /var/log/local0.log
   ```

5. Restart the `syslogd` daemon to activate the new configuration.

Setting Up Message Routing: Example

```
root@host1:~# vi /etc/syslog.conf
<content omitted>
local0.notice             @host2
root@host1:~# svcadm refresh system/system-log
root@host2:~# touch /var/log/local0.log
root@host2:~# vi /etc/syslog.conf
root@host2:~# grep local0 /etc/syslog.conf
local0.notice                 /var/log/local0.log
root@host2:~# svcadm refresh system-log
```

Monitoring a `syslog` File in Real Time

To view the messages sent to the `/var/adm/messages` file, use `tail -f /var/adm/messages`.

```
# tail -f /var/adm/messages
…
…
Dec 20 06:10:05 client1 inetd[655]: [ID 317013 daemon.notice]
    ftp[3044] from 192.168.0.100 61017
```

Practice 11: Overview

You will perform the following practices:

- Practice 11-1: Troubleshooting a script execution issue
- Practice 11-2: Troubleshooting a software update failure
- Practice 11-3: Troubleshooting a network connectivity issue
- Practice 11-4: Troubleshooting directory access issues
- Practice 11-5: Using the man pages
- Practice 11-6: Setting up system messaging

Agenda

- Managing System Logs
- Configuring System Messaging
- Configuring System Crash Facilities
- Configuring Dump Facilities for Business Application Failure
- Explaining the Role of DTrace in Diagnosing System Issues

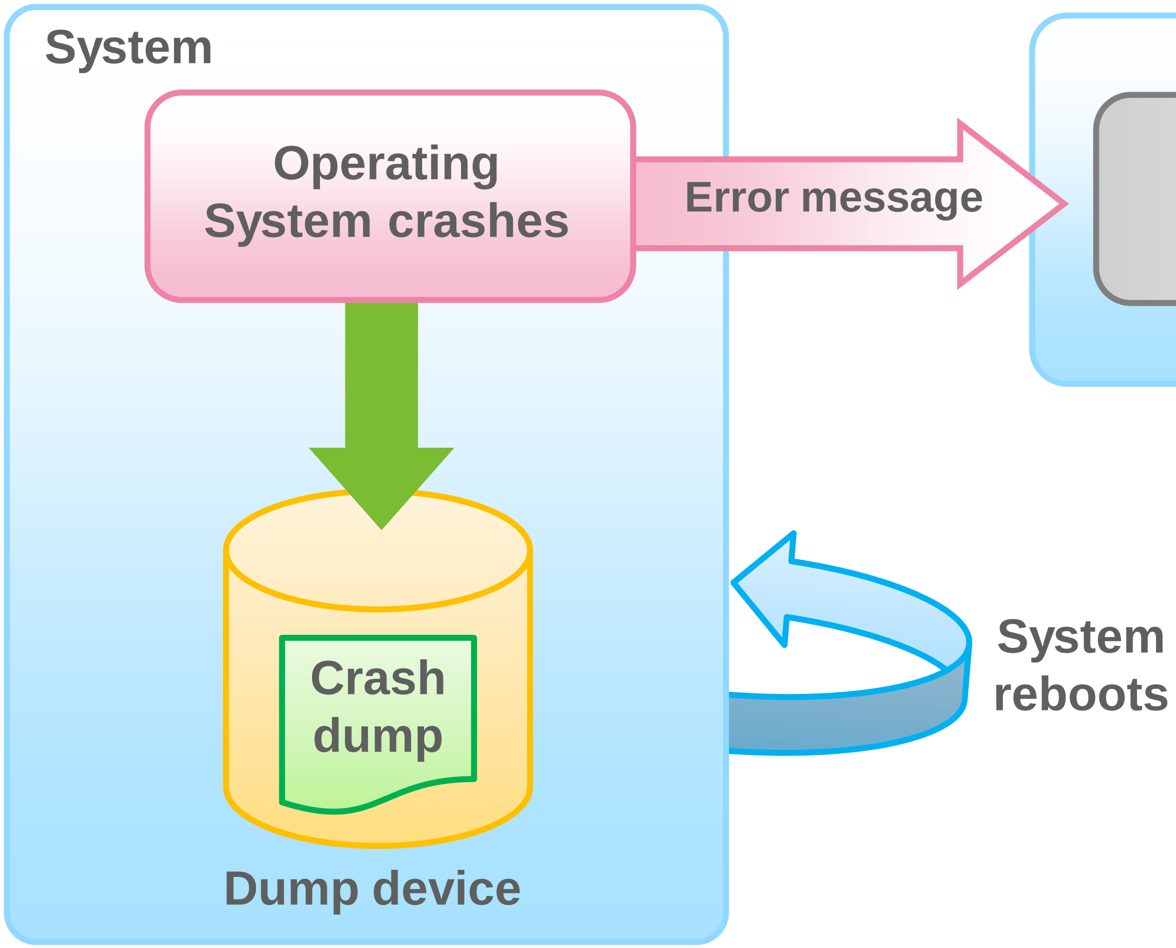
Configuring System Crash Facilities

This section covers the following topics:

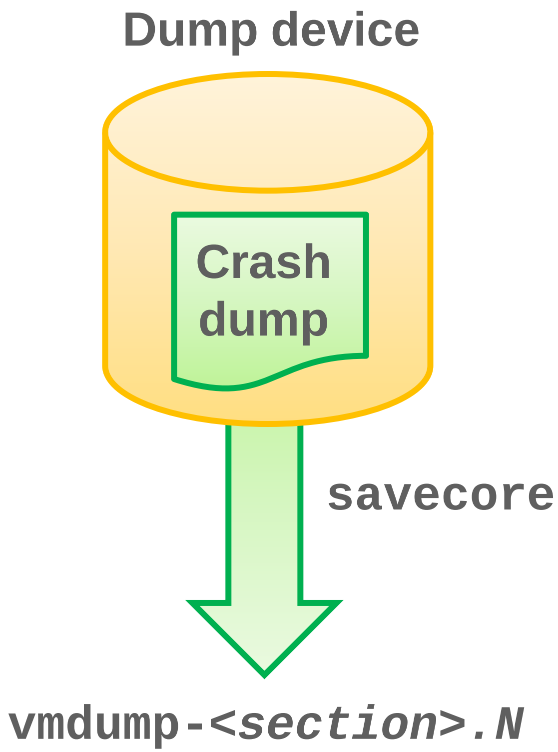
- Crash dump process: Overview
- How and where crash dump files are saved
- Displaying the current crash dump configuration
- Modifying the crash dump configuration
- Saving the crash dump file
- Uncompressing the crash dump file
- Displaying the crash dump file contents

ORACLE

Crash Dump Process: Overview



How and Where Crash Dump Files Are Saved



`/etc/dumpadm.conf` File

```
# cat /etc/dumpadm.conf
#
# dumpadm.conf
#
# Configuration parameters for system crash dump.
# Do NOT edit this file by hand -- use dumpadm(1m) instead.
#
DUMPADM_DEVICE=/dev/zvol/dsk/rpool/dump
DUMPADM_SAVDIR=/var/crash/client1
DUMPADM_CONTENT=kernel+zfs
DUMPADM_ENABLE=yes
DUMPADM_CSAVE=on
```

Displaying the Current Crash Dump Configuration

To display the current crash dump configuration, use `dumpadm`.

```
# dumpadm
Dump content        : kernel with ZFS metadata
Dump device         : /dev/zvol/dsk/rpool/dump (dedicated)
Savecore directory: /var/crash/client1
Savecore enabled    : yes
Save compressed     : on
```

ORACLE

Modifying the Crash Dump Configuration

To modify the crash dump configuration, use `/usr/sbin/dumpadm [-nuy] [-c content] [-d dump-device][-m mink | minm | min%] [-s savecore-dir] [-r root-dir] [-z on | off]`.

```
# dumpadm -y -d /dev/dsk/c0t1d0s1
Dump content       : kernel
Dump device        : /dev/dsk/c0t1d0s1 (dedicated)
Savecore directory: /var/crash/client1
Savecore enabled  : yes
Save compressed   : on
```

Saving the Crash Dump File

To save the crash dump file to the designated dump device, use `savecore -L`.

```
# savecore -L
dumping to /dev/zvol/dsk/rpool/dump, offset 65536, content: kernel
    sections: zfs
 0:02  91% done (kernel)
 0:02 100% done (zfs)
100% done: 142706 (kernel) + 13595 (zfs) pages dumped, dump succeeded
savecore: System dump time: Tue Jan  7 07:59:43 2014

savecore: Saving compressed system crash dump files in directory
    /var/crash/data/3e381450-d324-c553-a88a-a89bd42b6f7e
savecore: Decompress all crash dump files with '(cd
    /var/crash/data/3e381450-d324-c553-a88a-a89bd42b6f7e && savecore -v
    0)' or individual files with 'savecore -vf /var/crash/data/3e381450-
    d324-c553-a88a-a89bd42b6f7e/vmdump{,-<secname>}.0'
```

ORACLE

Uncompressing the Crash Dump File

To uncompress the crash dump file, use `savecore -vf /var/crash/hostname/vmdump.0`.

```
# savecore -vf /var/crash/data/3e381450-d324-c553-a88a-
a89bd42b6f7e/vmdump.0
savecore: System dump time: Tue Jan  7 07:59:43 2014

savecore: saving system crash dump in /var/crash/data/3e381450-d324-
c553-a88a-a89bd42b6f7e/vmcore.0
Constructing corefile /var/crash/data/3e381450-d324-c553-a88a-
a89bd42b6f7e/vmcore.0
 0:18 100% done: 142706 of 142706 pages saved
4874 (3%) zero pages were not written
dump decompression took 0 minutes and 18 seconds
```

Displaying the Crash Dump File Contents

To display the contents of the crash dump file, perform the following steps:

1. Change directories to the `/var/crash` directory.
2. List the files in the crash directory.
3. Use the `file` command to access the crash dump file, either `vmcore.0` or `vmdump.0`.
4. View the contents of the file by using the `string` command.

ORACLE

Displaying the Crash Dump File Contents: Example

```
# cd /var/crash/data/<UID>
root@client1:/var/crash/data/<UID># savecore –v 0
root@client1:/var/crash/data/<UID># ls
vmcore-zfs.0  vmcore.0      vmdump-zfs.0  vmdump.0
root@client1:/var/crash/data/<UID># file vmcore.0
vmcore.0:  SunOS 5.11 11.3 64-bit Intel live dump from ‘client1‘
root@client1:/var/crash/data/<UID># strings vmcore.0 | more
i86pc
3e381450-d324-c553-a88a-a89bd42b6f7e
SunOS
client1
5.11
11.3
i86pc
kernel
core kernel pages
ZFS metadata (ZIO buffers)
.symtab
.strtab
.shstrtab
...
...
```

Quiz

Saving of the crash dump file is enabled by default.

a. True

b. False

Agenda

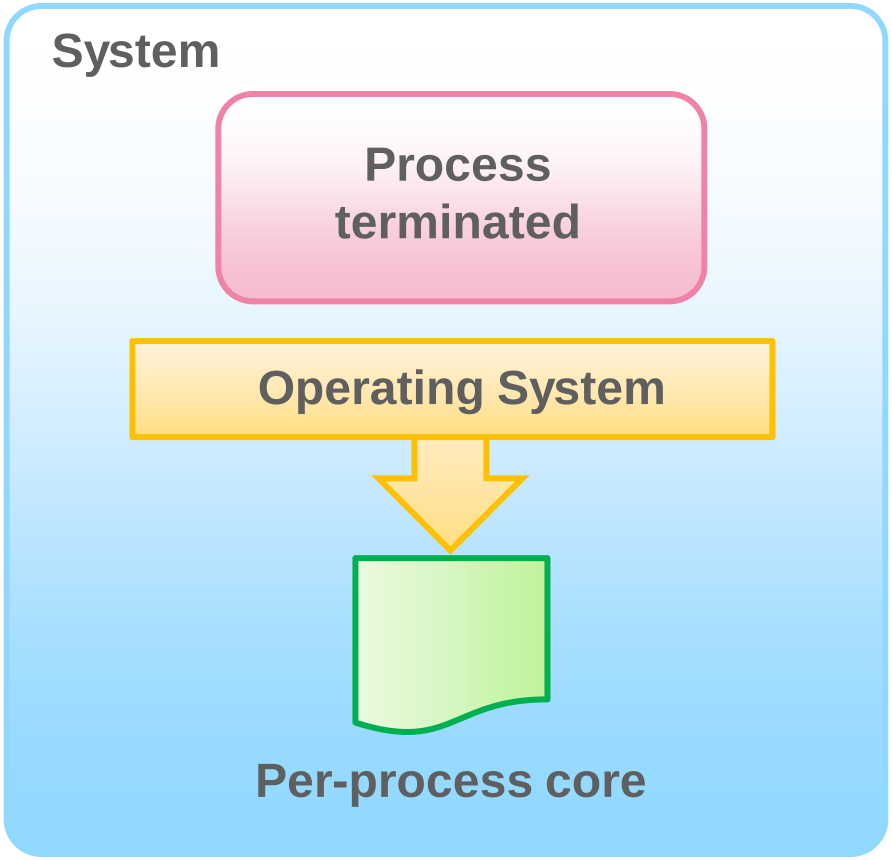
- Managing System Logs
- Configuring System Messaging
- Configuring System Crash Facilities
- Configuring Dump Facilities for Business Application Failure
- Explaining the Role of DTrace in Diagnosing System Issues

Configuring Dump Facilities for Business Application Failure

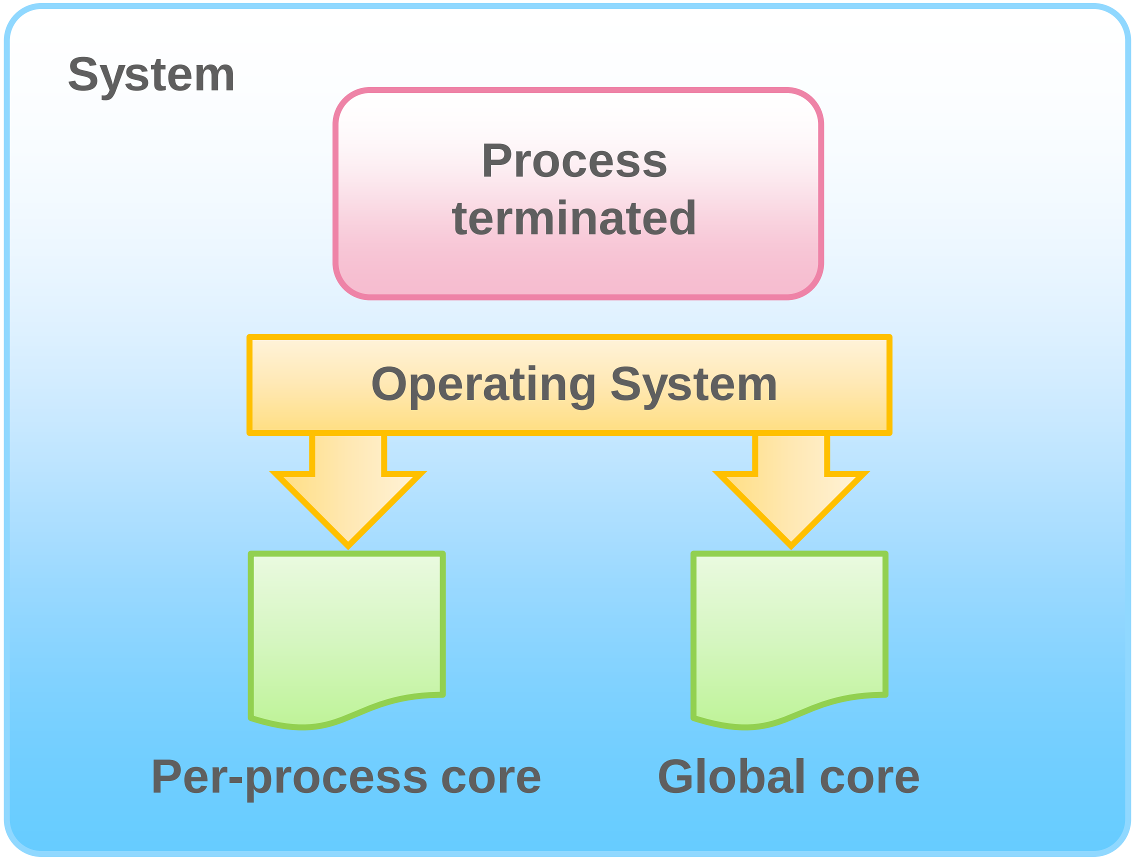
This section covers the following topics:

- Displaying the current core dump configuration
- Modifying the core dump configuration
- Setting a core file name pattern
- Enabling a core file path
- Displaying the contents of the core dump file

Core Dump Process: Overview



How and Where Core Dump Files Are Saved



Core Dump: Example

```
core:  ELF 32-bit LSB core file 80386 Version 1, from 'bash'
```

What Is a Core File?

- A file generated in response to fatal errors.
  - For the kernel, the file is referred to as a “crash dump.”
  - For an application or process, the file is referred to as a “core dump.”
- A fatal kernel error:
  - Results in a system crash (“panic”)
  - Generates a core file that contains a snapshot of the kernel’s memory space when the error occurred
- A fatal application or process error:
  - Results in abnormal termination
  - Generates a core file that contains a snapshot of the process’s memory space when the error occurred

ORACLE

Core File Generation: Advantages and Disadvantages

- Advantages
  - Core files are used to analyze and determine the root cause of a crash or core dump so that the problem can be resolved.
- Disadvantages
  - Core files take up a large amount of disk space.
  - Core files must be managed.

Core File Paths

- Per-process core file path:
  - Defaults to `core`
  - Is enabled by default
  - If enabled, produces a core file when a process terminates abnormally
  - Is inherited by a new process from its parent process
- Per-process files are owned and can be viewed only by the process owner.
- Global core file path:
  - Defaults to `core`
  - Is disabled by default
  - If enabled, produces an additional core file with the same content as the per-process core file
- Global core files are owned by the superuser. Nonprivileged users cannot read these files.

Displaying the Current Core Dump Configuration

To display the current core dump configuration, use `coreadm`.

```
# coreadm
     global core file pattern: /var/core/core.%f.%p
     global core file content: default
       init core file pattern: core
       init core file content: default
            global core dumps: disabled
       per-process core dumps: enabled
      global setid core dumps: disabled
 per-process setid core dumps: disabled
     global core dump logging: disabled
```

Modifying the Core Dump Configuration

To modify the core dump configuration, use `coreadm [-g pattern] [-i pattern] [-d option ... ] [-e option ... ]`.

```
# coreadm -e log
# coreadm
     global core file pattern: /var/core/core.%f.%p
     global core file content: default
       init core file pattern: core
       init core file content: default
            global core dumps: enabled
       per-process core dumps: enabled
      global setid core dumps: disabled
 per-process setid core dumps: disabled
     global core dump logging: enabled
```

Setting a Core File Name Pattern

- To set a per-process file name pattern, use `coreadm -p $HOME/corefiles/%f.%p $$`.

```
$ coreadm -p $HOME/corefiles/%f.%p $$
```

- To set a global file name pattern, use `coreadm -g /var/core/%f.%p`.

```
# coreadm -g /var/core/%f.%p
```

Enabling a Core File Path

- To enable the per-process core file path, use `coreadm -e process`.
- To enable the global core file path, use `coreadm -e global -g /var/core/core.%f.%p`.
- To verify the configuration, use `coreadm`.

```
# coreadm
     global core file pattern: /var/core/core.%f.%p
     global core file content: default
       init core file pattern: core
       init core file content: default
            global core dumps: enabled
       per-process core dumps: enabled
      global setid core dumps: disabled
 per-process setid core dumps: disabled
     global core dump logging: enabled
```

ORACLE

Displaying the Contents of the Core Dump File

To display the contents of the core dump file:

1. Change directories to the `/var/core` directory.
2. List the files in the core directory.
3. Use the `file` command to access the core file.
4. View the contents of the file by using the `string` command.

Displaying the Core Dump File Contents: Example

```
# cd /var/core
root@client1:/var/core# ls /var/core
core.bash.1554
root@client1:/var/core# file core*
core.bash.1554:ELF 32-bit LSB core file 80386 Version 1, from 'bash'
root@client1:/var/core# strings core.bash.1554 | more
CORE
bash
-bash
CORE
i86pc
CORE
CORE
CORE
CORE
bash
-bash
…
…
```

Quiz

In which directory are the system messages stored?

a. `/var/lib`
b. `/var/tmp`
c. `/var/adm`
d. `/var/log`

Quiz

What is the facility in the following `syslog` entry?

```
Aug 10 05:40:03 client1 genunix: [ID 936769
kern.info] fssnap0 is /pseudo/fssnap@0
```

a. `genunix`
b. `kern`
c. `info`

Quiz

What is the severity level for the following message?

```
Aug 10 05:40:00 client1 mac: [ID 469746
kern.info] NOTICE: net1 registered
```

a. alert
b. warning
c. notice
d. info

Quiz

A core dump is generated when the system experiences a fatal error.

a. True

b. False

Quiz

What is the result of a fatal application or process error? (Choose two.)

a. System panic
b. Abnormal termination of the application or process
c. A core dump being created on the designated dump device

Quiz

You can separately enable or disable two configurable `core` file paths: per-process and global.

a. True

b. False

Quiz

The global core file path is enabled by default.

a. True

b. False

Quiz

What is the default target destination for the following `syslog` message type?

`*.err;kern.debug;daemon.notice;mail.crit`

a. `/dev/sysmsg`

b. `/var/adm/messages`

c. `operator`

d. `root`

Quiz

You must always restart the `syslogd` daemon after you modify the `etc/syslog.conf` file.

a. True

b. False

Practice 11-7 Overview: Configuring System and Application Crash Facilities

This practice covers configuring:

- System crash facilities
- Dump facilities for business application failure

Agenda

- Managing System Logs
- Configuring System Messaging
- Configuring System Crash Facilities
- Configuring Dump Facilities for Business Application Failure
- Explaining the Role of DTrace in Diagnosing System Issues

ORACLE

DTrace: Overview

- A comprehensive, dynamic tracing facility that is built into the Oracle Solaris operating system
- An observability technology that helps you examine the behavior of user programs as well as the operating system in development and in production
- Features:
  - Examines the entire software stack
  - Determines the root cause of performance problems
  - Tracks the source of aberrant behavior

ORACLE

DTrace: Capabilities

- Analysis and observability
  - Provides a powerful new system and a process-centric framework for real-time analysis and observability
- Safety and comprehensive monitoring
  - Provides over 50,000 prebuilt data-monitoring points, inspection kernels, and user space levels
- Flexibility
  - Enables you to create custom programs to dynamically instrument the system
    - There is no need to instrument, stop, or restart your applications.
    - DTrace enables users to dynamically create as many monitoring points as required.

ORACLE

DTrace: Components

- Probes
- Providers
- Consumers
- D programming language

Probes

- *Probes* are programmable sensors or points of instrumentation placed all over the Oracle Solaris system.
- DTrace provides thousands of probes.
- Each probe is associated with an action.
- When the probe fires, certain defined actions are executed.
- A four-tuple (`provider:module:function:name`) uniquely identifies every probe.
  - **Example:** `fbt:zfs:arc_read:entry`

Providers

- Libraries of probes are called *providers*.
- Providers make probes available to the DTrace framework.
- These libraries instrument a specific area of the system or a mode of tracing.
- New providers are added with every release of the operating system.

Consumers

- *Consumers* are user mode programs that call in to the underlying DTrace framework.
- Four consumers are available in the current version of Oracle Solaris:
  - `DTrace(1M)`
  - `lockstat(1M)`
  - `plockstat(1M)`
  - `intrstat(1M)`

D Language

- Tracing programs, also referred to as *scripts*, are written in the D programming language.
- The language is a subset of C with added functions and variables that are specific to tracing.
- Additional capabilities of the D language include the following:
  - Supports ANSI C operators, strings, pointers, struct, and unions
  - Consists of expressions based on built-in variables: `pid`, `execname`, `timestamp`, and `curthread`
  - Performs arithmetic only on integers in D programs (floating-point arithmetic is not permitted in D)
  - Consists of CLI and scripting modes

DTrace Toolkit

- The DTrace Toolkit is a collection of over 230 DTrace scripts and one-liners for performance observability and troubleshooting.
- The toolkit contains:
  - Scripts
  - Man pages
  - Sample documentation
  - Notes files
  - Tutorials
- To install the DTrace toolkit:

```
# pkg install dtrace-toolkit
```

DTrace Toolkit: Important Scripts

Script Folder	Function
`Apps`	For certain applications (such as Apache and NFS)
`CPU`	Measuring CPU activity
`Disk`	Analyzing I/O activity
`Extra`	For other categories
`Kernel`	For kernel activity
`Locks`	Analyzing locks
`Mem`	Analyzing memory and virtual memory
`Net`	Analyzing activity of network interfaces and the TCP/IP stack
`Proc`	Analyzing activity of a process
`System`	Measuring systemwide activity
`User`	Monitoring activity by UID
`Zones`	Monitoring activity by zone

Before Using DTrace

Consider the following options before using DTrace:

- Perform a sanity check first.
  - `/var/adm/messages`
- Start with the "Big 5" stat tools.
  - `vmstat`, `mpstat`, `iostat`, `prstat`, and `netstat` for memory leaks
- Answer the following high-level questions for a quick initial diagnosis:
  - Is there a significant number of cache misses?
  - How much time is spent in user mode compared with system mode?
  - Is the system short on memory or other critical resources?
  - What are the system's I/O characteristics?

ORACLE

Launching DTrace

Before launching DTrace, consider the following facts:

- Only `root` is allowed to run DTrace by default.
- Non-`root` users need one or more of the following privileges to access DTrace:
  - `DTrace_kernel`
  - `DTrace_proc`
  - `DTrace_user`

```
% ppriv -l | grep Dtrace
DTrace_kernel DTrace_proc DTrace_user
```

DTrace: Example

Scenario: Your system processes are causing a massive number of system calls and subsequently having a negative effect on system performance. You want to investigate the number of system calls that the processes are making.

```
# dtrace –n 'syscall::read:entry {@[execname] = count()}'
dtrace: description 'syscall::read:entry ' matched 1 probe
^C
gnome-settings-d                                    1
in.mpathd                                           2
gnome-terminal                                      3
init                                                4
hald                                                72
hald-addon-acpi                                     72
Xorg                                                248
#
```

Summary

In this lesson, you should have learned how to:

- Monitor system logs
- Identify a crash dump file
- Identify a core dump file
- Troubleshoot a script execution issue
- Troubleshoot a software update failure
- Troubleshoot a network connectivity issue
- Troubleshoot a directory access issue
- Troubleshoot a default shell issue
- Configure the following:
  - System messaging
  - System crash facilities
  - Dump facilities for business application failure
- Explain the role of DTrace in diagnosing system issues

12

Introducing Oracle Solaris 11 on the Cloud

ORACLE®

Lesson Objectives

After completing this lesson, you should be able to:

- Explain Oracle Compute Cloud Service
- Subscribe to Oracle Compute Cloud Service
- Create an Oracle Solaris Instance on the Cloud
- Create an SSH-enabled User on an Oracle Solaris Instance
- Create a Virtualized Topology Using Orchestration JSONs

Agenda

- Explaining Oracle Compute Cloud service
- Subscribing to Oracle Compute Cloud service
- Creating an Oracle Solaris Instance on the cloud
- Creating an SSH-enabled user on an Oracle Solaris instance
- Creating a virtualized topology using Orchestration JSONs

Compute Cloud Service

Oracle Cloud is the industry’s broadest and most integrated public cloud. It offers the following services:

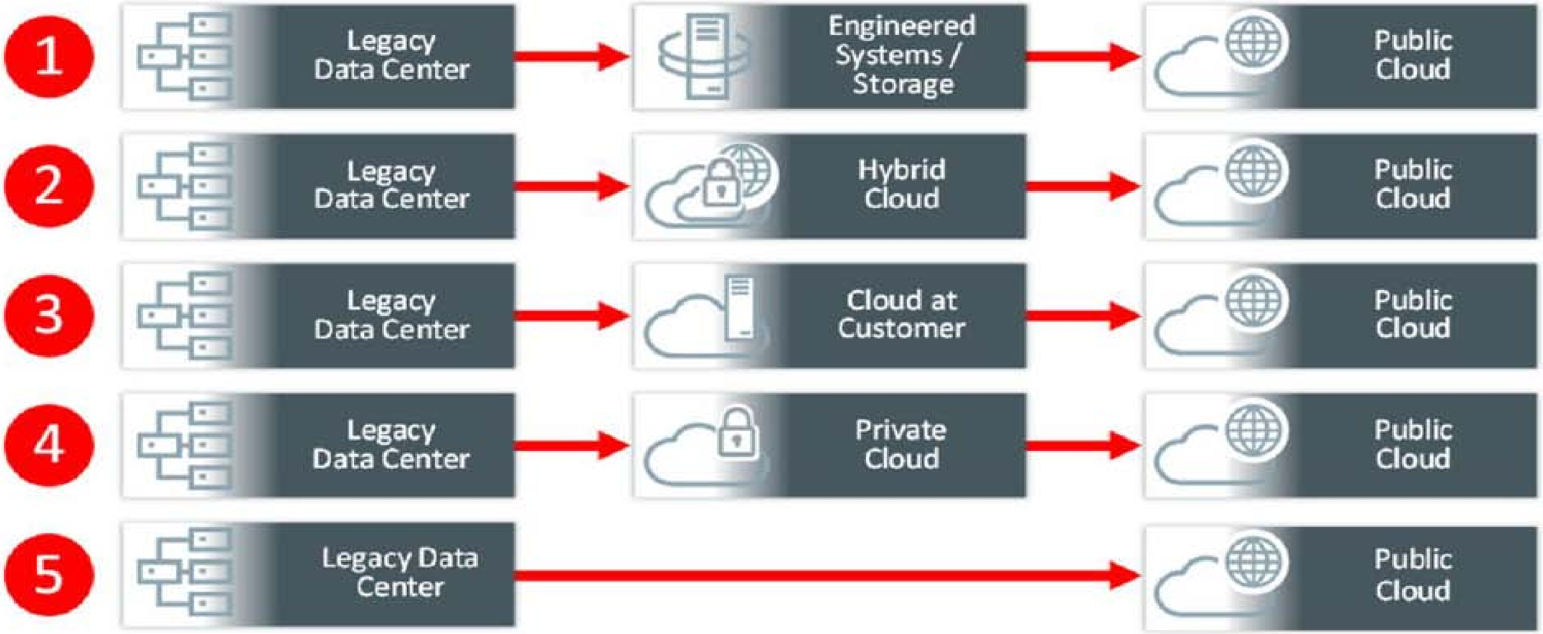
- Software as a service (SaaS)
- Platform as a service (PaaS)
- Infrastructure as a service (IaaS)

IaaS Compute Cloud Service

- Provides infrastructure services over the Internet.
- Enables users to perform the following:
  - Provision and monitor virtual machines quickly.
  - Create and attach block storage to virtual machines.
  - Capture virtual machines as reusable templates.
  - Attach virtual machines to multiple networks.
- Can be accessed through:
  - Graphical User Interface
  - Command line interface or REST API

ORACLE

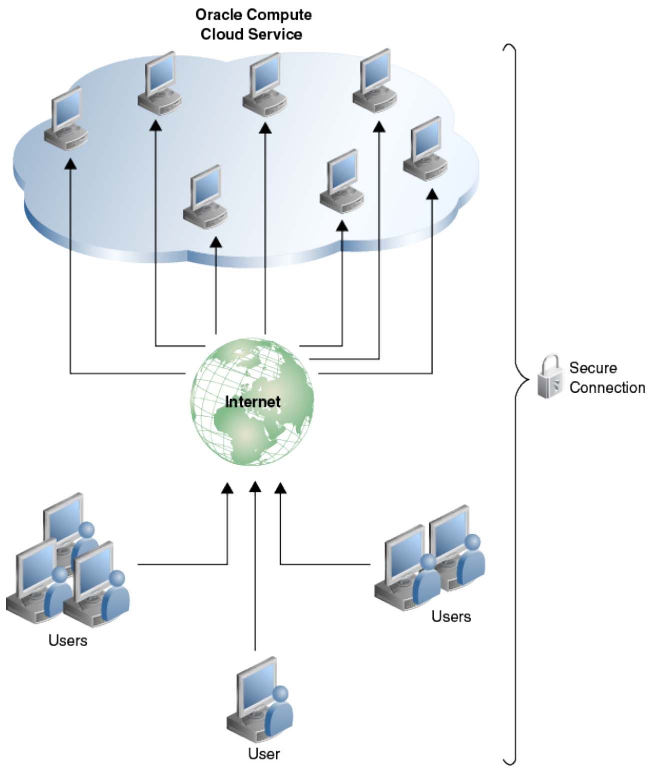
Five Oracle Journeys to the Public Cloud



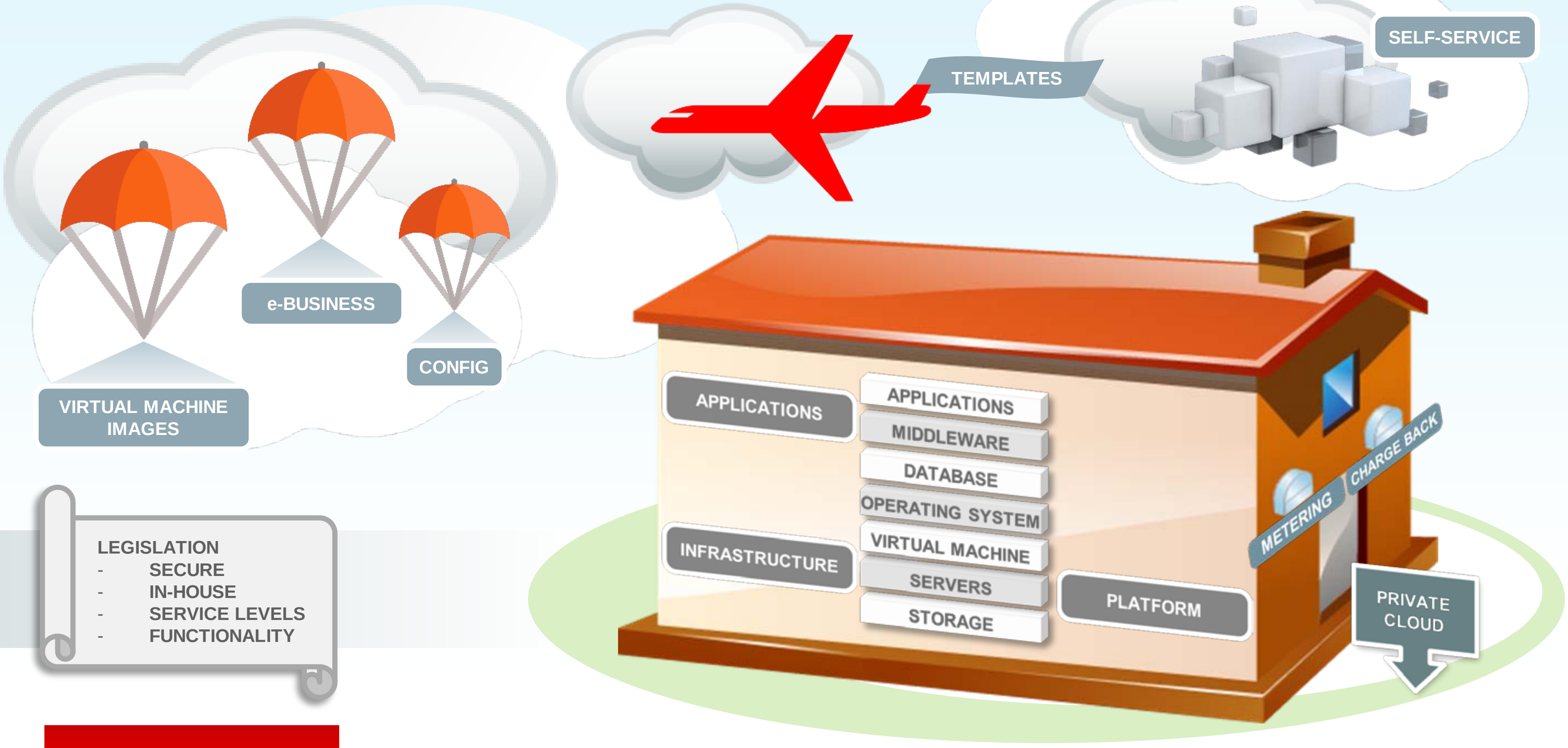
ORACLE®

What is Oracle Compute Cloud Service?

- Oracle Compute Cloud Service is a secure, reliable, low cost, infrastructure service.
- You can use Oracle Compute Cloud Service to do the following:
  – Rapidly provision virtual machines on Oracle Cloud with all the necessary storage and networking resources.
  – Manage and scale your virtual machine topology in the cloud easily.
  – Migrate your Oracle and third-party applications to Oracle Cloud.



Oracle Compute Cloud Service



ORACLE

Features of Oracle Compute Cloud Service

- Create virtual machines using Oracle-provided or custom machine images.
- Assign processor and memory resources from a range of resource profiles.
- Use persistent boot disks to start your instance.
- Attach high-capacity block storage to your instance.
- Practice fine-grained control over network traffic.
- Reserve a persistent public IP address and assign it to your instance.
- Ensure secure access to your instance.
- Monitor and manage your resources using a web console.
- Automate provisioning and management workflows using orchestrations.
- Migrate on-premise workloads and applications to the cloud.

Oracle Compute Cloud Service Terminology

Term	Definition
Image List	An **image list** is a collection of Oracle Compute Cloud Service machine images.
Instance	An **instance** is a virtual machine in Oracle Compute Cloud Service.
Instance Snapshot	An **instance snapshot** captures the current state of the non-persistent boot disk of an instance and creates a corresponding machine image.
IP Network	An **IP network** allows you to define an IP subnet in your account.
IP Network Exchange	An **IP network exchange** enables access between IP networks that have non-overlapping addresses, so that instances on these networks can exchange packets with each other without NAT.
IP Reservation	An **IP reservation** is a public IP address that you can attach to an Oracle Compute Cloud Service instance that requires access to or from the internet.
Launch Plan	A **launch plan** is a JavaScript Object Notation (JSON) script that defines the properties of one or more instances in Oracle Compute Cloud Service.

ORACLE

Oracle Compute Cloud Service Terminology

Term	Definition
Machine Image	A **machine image** is a template of a virtual hard disk of a specific size with an installed operating system.
Orchestration	An **orchestration** defines the attributes and interdependencies of a collection of compute, networking, and storage resources in Oracle Compute Cloud Service.
Route	A **route** specifies the IP address of the destination as well as a vNICset which provides the next hop for routing packets.
Security Application	A **security application** allows you to specify the protocol and port that you want to use to enable traffic between a source and a destination using security rules.
Security IP List	A **security IP list** is a list of IP subnets (in the CIDR format) or IP addresses that are external to instances in Oracle Compute Cloud Service.
Security List	A **security list** is a group of Oracle Compute Cloud Service instances that you can specify as the source or destination in one or more security rules.
Security Rule	A **security rule** is a firewall rule that you can define to control network access to Oracle Compute Cloud Service instances over a specified security application.

Oracle Compute Cloud Service Terminology

Term	Definition
Shape	A **shape** is a resource profile that specifies the number of OCPUs and the amount of memory to be allocated to an instance in Oracle Compute Cloud Service. The shape determines the type of disk drive that your instance uses.
Site	A **site** is a set of physical servers and the associated storage and networking resources in an Oracle Cloud data center. Each site has a distinct REST API endpoint.
Storage Volume	A **storage volume** is a virtual disk that provides persistent block storage space for instances in Oracle Compute Cloud Service.
Storage Volume Snapshot	A **storage volume snapshot** is a backup of all the data currently stored on a storage volume.
Virtual NIC	A **Virtual NIC**, or vNIC, is a virtual network interface card that enables an instance to be associated with a network.
Virtual NIC Set	A **Virtual NIC Set**, or **vNICset**, is a collection of one or more vNICs.
VPN Endpoint	A **VPN endpoint** represents a VPN tunnel between your data centre and your Oracle Compute Cloud Service site.

Agenda

- Explaining Oracle Compute Cloud service
- Subscribing to Oracle Compute Cloud service
- Creating an Oracle Solaris Instance on the cloud
- Creating an SSH-enabled user on an Oracle Solaris instance
- Creating a virtualized topology using Orchestration JSONs

Subscribing to Oracle Compute Cloud Service

1. Create and configure your account on Oracle Cloud
2. Request a trial or purchase a subscription
3. Activate the service
4. Verify activation
5. Create users and assign appropriate roles to each user

Agenda

- Explaining Oracle Compute Cloud service
- Subscribing to Oracle Compute Cloud service
- Creating an Oracle Solaris Instance on the cloud
- Creating an SSH-enabled user on an Oracle Solaris instance
- Creating a virtualized topology using Orchestration JSONs

About Oracle-Provided Solaris Images on the Cloud

- Oracle provides machine images for **Oracle Solaris 11.3 (x86, 64-bit).**
- Oracle-provided images include the essential packages for getting started using the instance that you create in Oracle Compute Cloud Service.
- Instances created by using any of the Oracle-provided Oracle Solaris images, a user named `opc` is preconfigured.
- The `opc` user is configured for remote access over the SSH v2 protocol using RSA keys.
- The images include a single disk that is mapped to the root ZFS storage pool (`rpool`).
- If you create instances by using an Oracle-provided Oracle Solaris image, then you can update packages from the support repository, file service requests to get support, and so on.

ORACLE

What is an Instance?

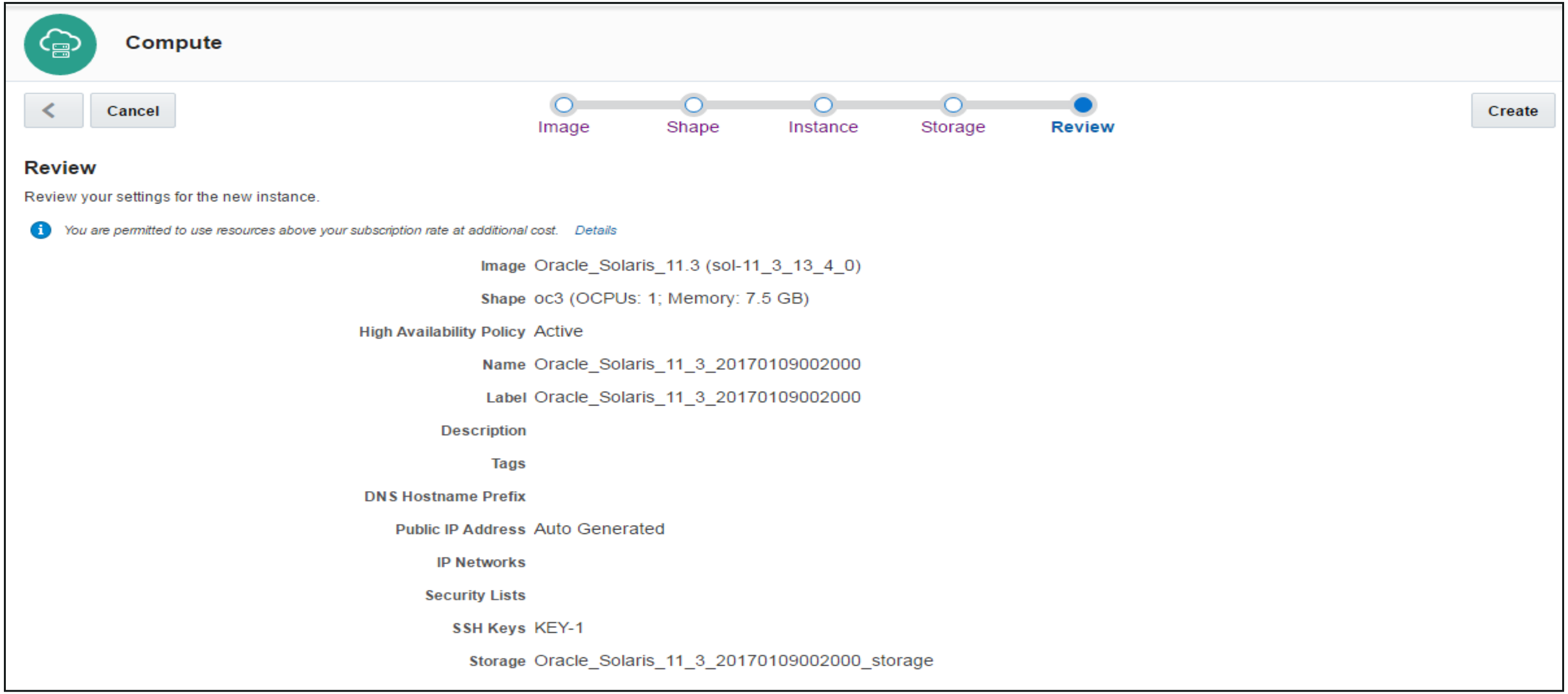
- An instance is a virtual machine running a specific operating system and having specified CPU and memory resources.
- An instance is defined by its machine image and shape.
    - **Machine image:** Is a virtual hard disk that has a specific operating system installed
    - **Shape:** Defines the number of CPUs and RAM available to an instance
- When you create an instance, the initial status is **Preparing.**
- After the image is installed and the instance starts, the status changes to **Running.**
- When an instance is in the **Running** status, you can connect to it, attach or detach storage volumes and security lists.

Workflow for Creating Your First Oracle Solaris 11.3 Instance on the Cloud

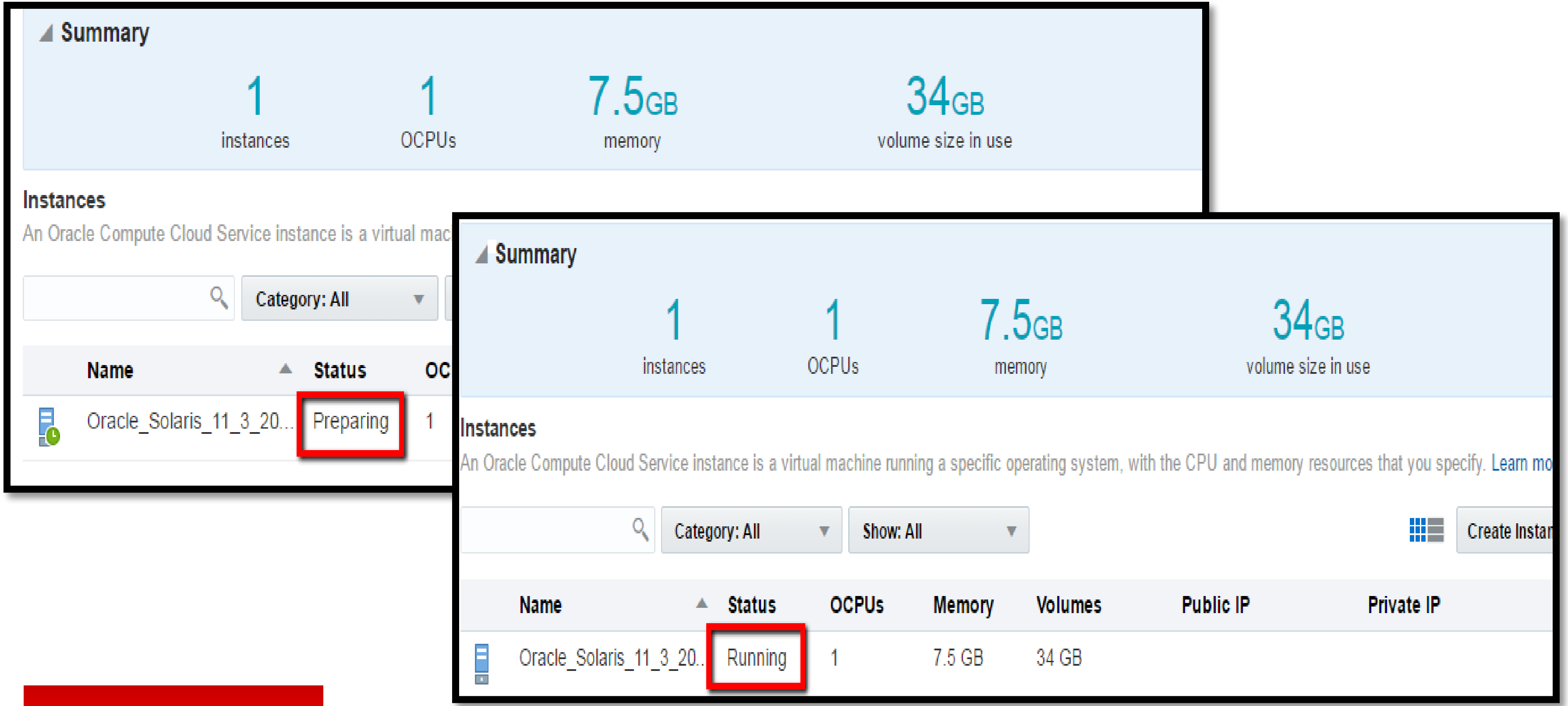
1. Generate SSH key pairs
2. Sign in to Oracle Compute Cloud Service
3. Add the SSH public keys
4. Create an instance using the web console
5. After creating the instance, you can do the following:
    a. Create and attach storage volumes
    b. Add your instance to a security list to control network access to the instance
6. Access your instance securely by using SSH

ORACLE

Create Instance Wizard



View Oracle Solaris Instance Status



ORACLE®

Agenda

- Explaining Oracle Compute Cloud service
- Subscribing to Oracle Compute Cloud service
- Creating an Oracle Solaris Instance on the cloud
- Creating an SSH-enabled user on an Oracle Solaris instance
- Creating a virtualized topology using Orchestration JSONs

ORACLE®

Creating an SSH-enabled User on an Oracle Solaris Instance

What Do You Need?

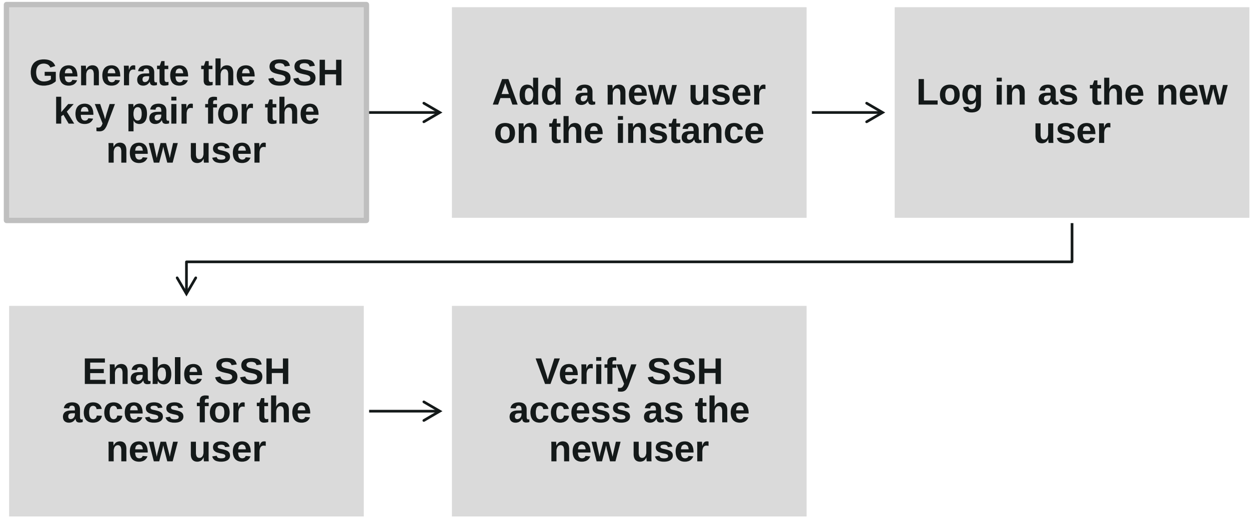
- An Oracle Compute Cloud Service Solaris instance
- Public IP address of the Oracle Compute Cloud Service Solaris instance on which you want to create new users.
- Your SSH private key to log in to the Oracle Compute Cloud Service Solaris instance.
- Root password for the Oracle Compute Cloud Service Solaris instance

Note:

Use `ssh` to log in to your instance as the `opc` user, with the SSH private key that corresponds to the SSH public key that you specified while creating the instance.

ORACLE

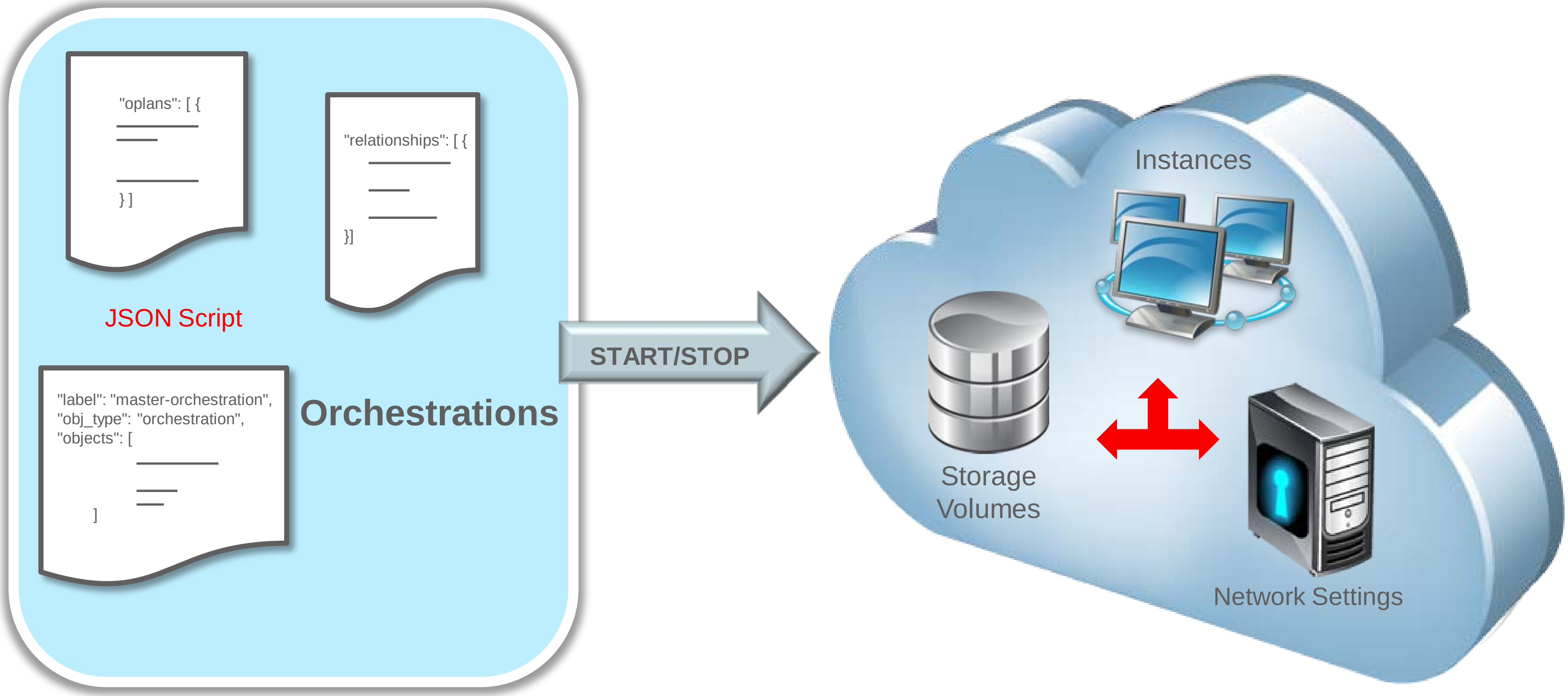
Workflow for Creating an SSH-Enabled User on an Oracle Solaris Instance



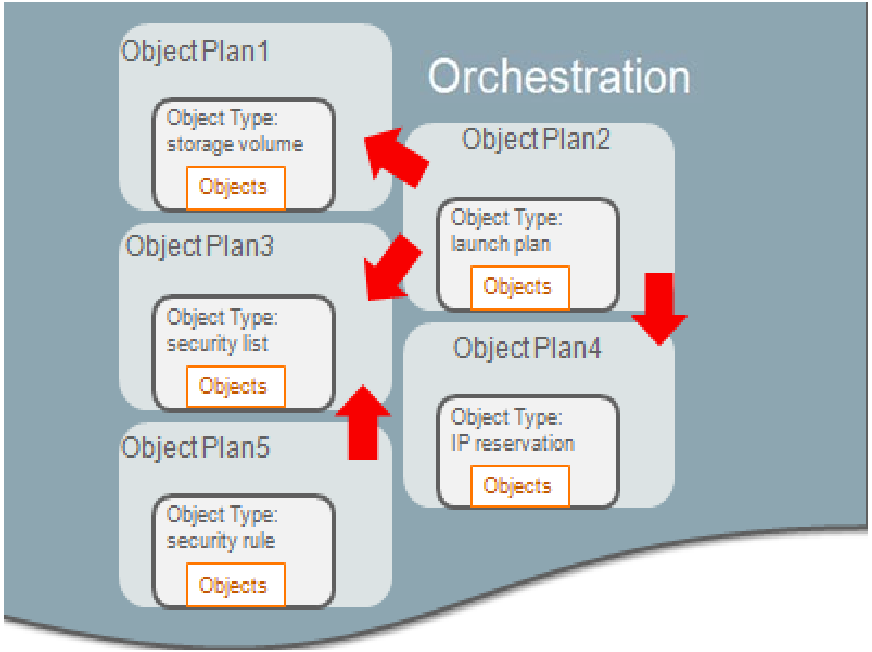
Agenda

- Explaining Oracle Compute Cloud service
- Subscribing to Oracle Compute Cloud service
- Creating an Oracle Solaris Instance on the cloud
- Creating an SSH-enabled user on an Oracle Solaris instance
- Create a virtualized topology using Orchestration JSONs

What Is an Orchestration?



What Does an Orchestration Look Like?

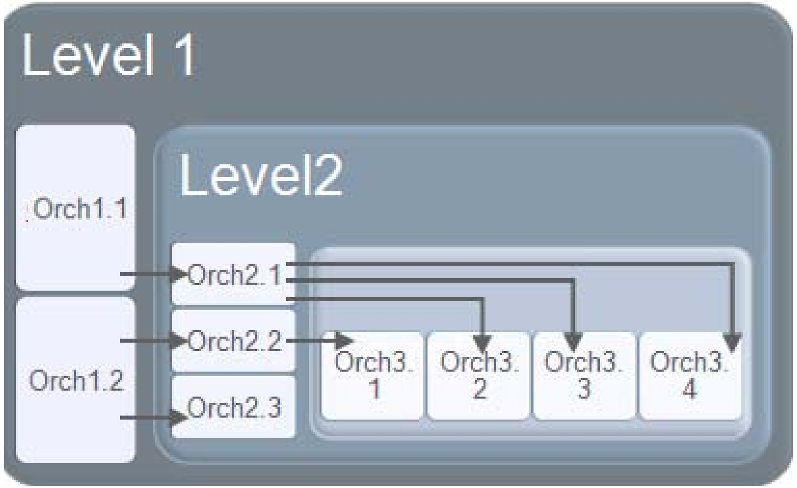


Why Should I Use Orchestrations?

- Simplify the process of provisioning and removing objects.
- Assign specified objects to specified instances.
- Define dependencies between objects.
- Specify a high availability policy for instances.

Which Objects Can I Create and How Can I Use them in My Orchestration?

Object Types	Description
`ip/reservation`	Reserves an IP address
`launchplan`	Creates an instance
`orchestration`	Starts a set of orchestrations
`storage/volume`	Creates a storage volume
`secapplication`	Creates a security application
`seciplist`	Creates a security IP list
`seclist`	Creates a security list
`secrule`	Creates a security rule



Creating an Instance Using Orchestration

1. Build your orchestration using JSON
2. Upload the orchestration to Oracle Compute Cloud Service
3. Check that the prerequisite objects are available
4. Start the orchestration

ORACLE

Refer to Oracle Cloud Computing Resources

Refer the following resources for further information on Oracle Cloud Computing:

- https://www.oracle.com/cloud
- https://docs.oracle.com/cloud/latest/stcomputecs/index.html
- https://education.oracle.com/cloud

Summary

In this lesson, you have learned how to:

- Explain Oracle Compute Cloud Service
- Subscribe to Oracle Compute Cloud Service
- Create an Oracle Solaris Instance on the Cloud
- Create an SSH-enabled User on an Oracle Solaris Instance
- Create a Virtualized Topology Using Orchestration JSONs