Application Centric Lifecycle with Oracle Solaris 11

Peter Dennis
Oracle Solaris Engineering

ORACLE®

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

ORACLE®

Oracle Lifetime Support

Hardware and Operating Systems http://www.oracle.com/us/support/lifetime-support/lifetime-support-hardware-337183.html

- ## Premier Support
  - Provides maintenance for your Oracle hardware and integrated software (for example, firmware). Maintenance and ***software upgrades*** are included for Oracle operating systems and Oracle VM for ten years from their general availability date - ***extended to 20 years for Solaris 11 (2031)*** http://www.oracle.com/us/support/library/lifetime-support-hardware-301321.pdf on p.34 (37)

- ## Extended Support for Operating Systems
  - Puts you in control of your operating system upgrade strategy by providing additional maintenance and upgrades for Oracle Solaris operating system for an additional fee **(2034)**

- ## Sustaining Support for Operating Systems
 - Maximizes your investment protection by further extending support for operating systems and firmware. Features include access to Oracle online support tools, operating system upgrade rights, pre-existing fixes, patches and assistance from technical support experts

One Support Stream

11.0 → 11.1 → 11.2 → 11.3 → 11.next ⇢
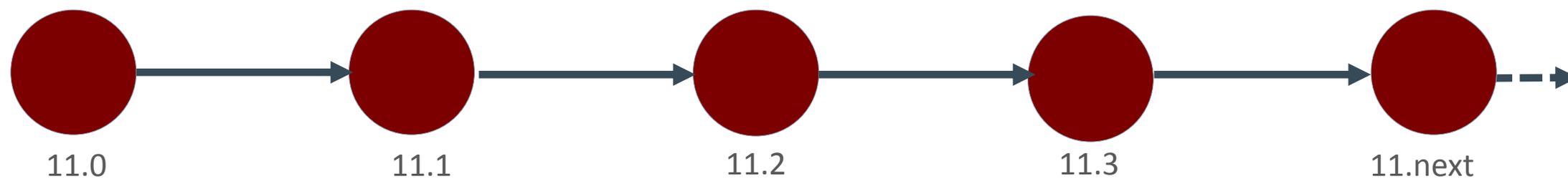
Monthly Support Repository Updates (SRUs)
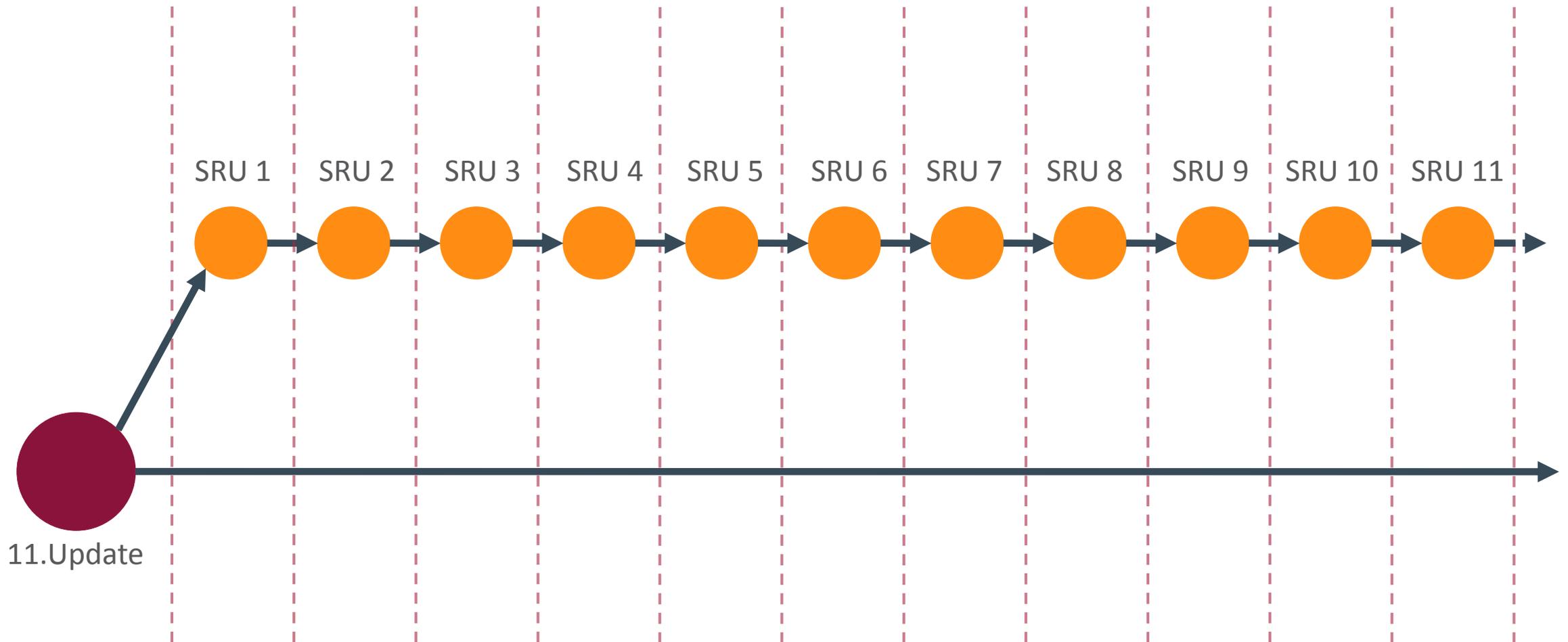
Quarterly Critical Patch Updates (CPUs)
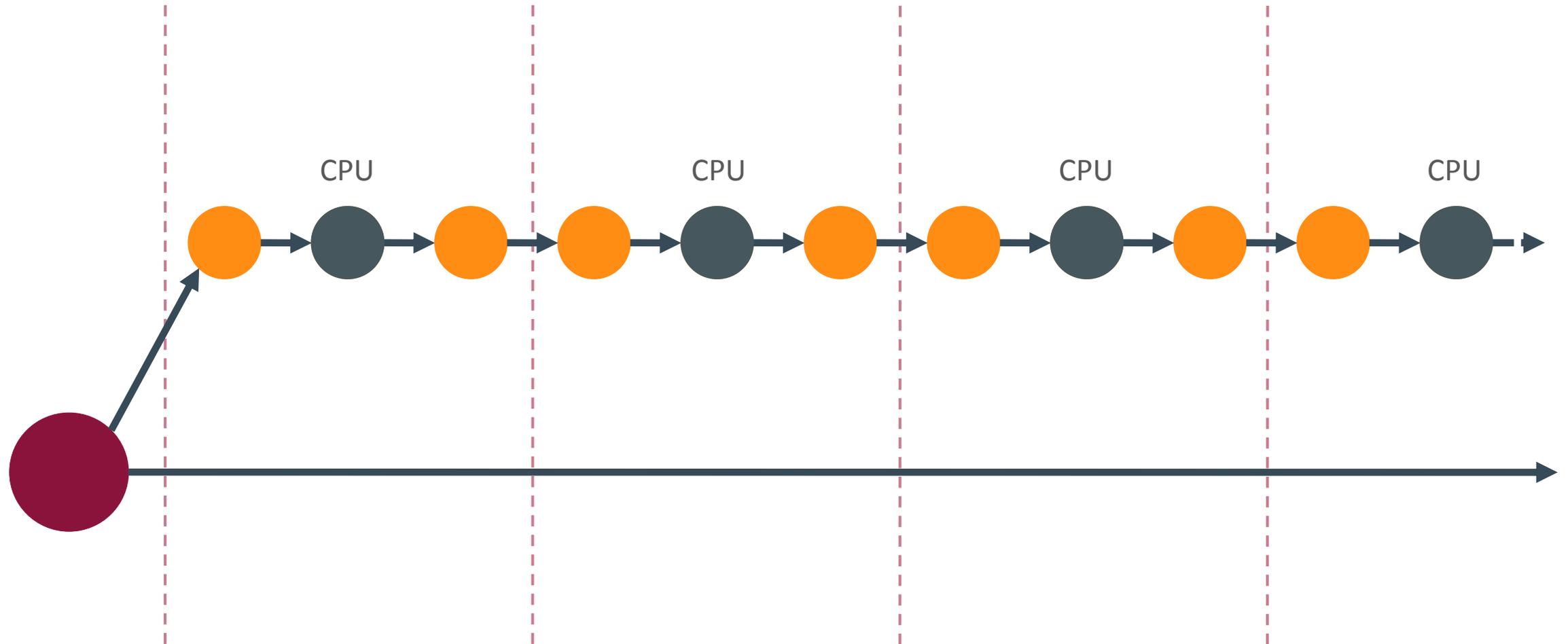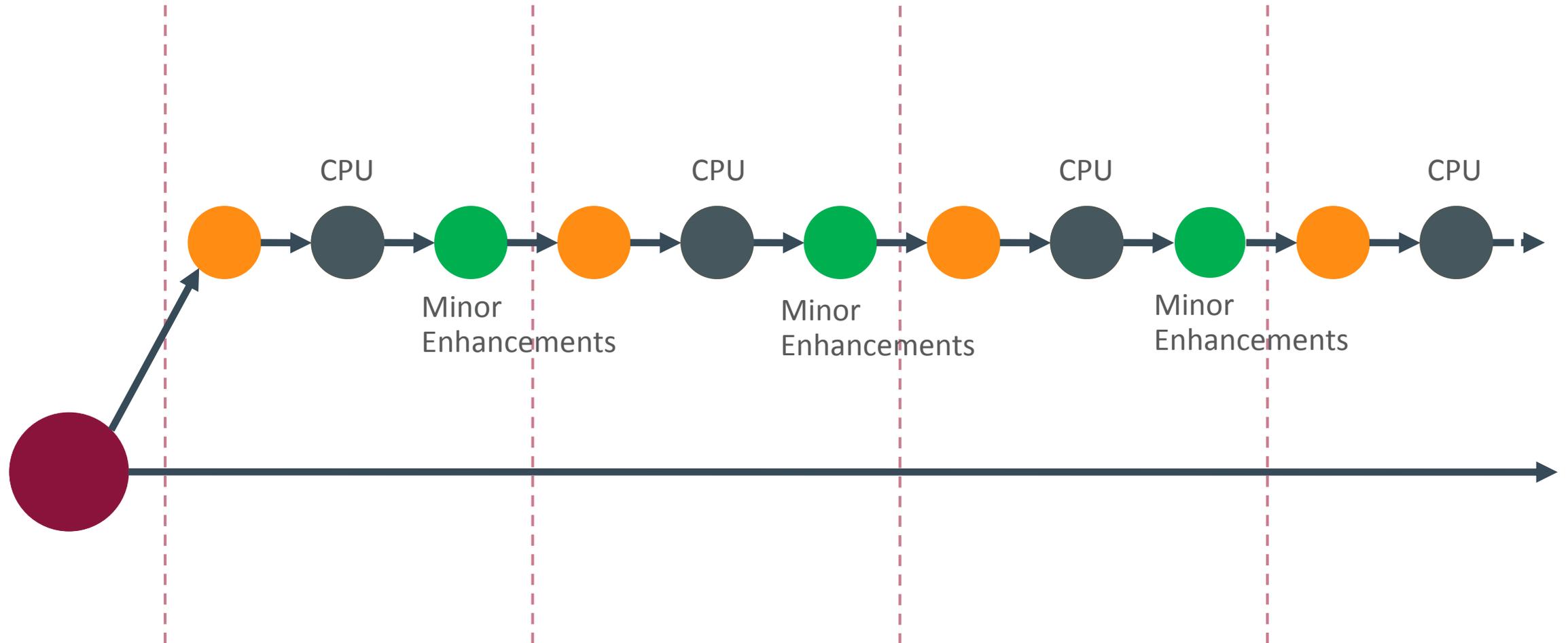
Oracle Solaris Installation

- Text Install ISO/USB images
  - Loaded via virtual disk (ilom, virtualbox) or usb devices
  - Basic install questions using a simple text interface
- For scaling install use AutoInstall images (for SPARC, x86)
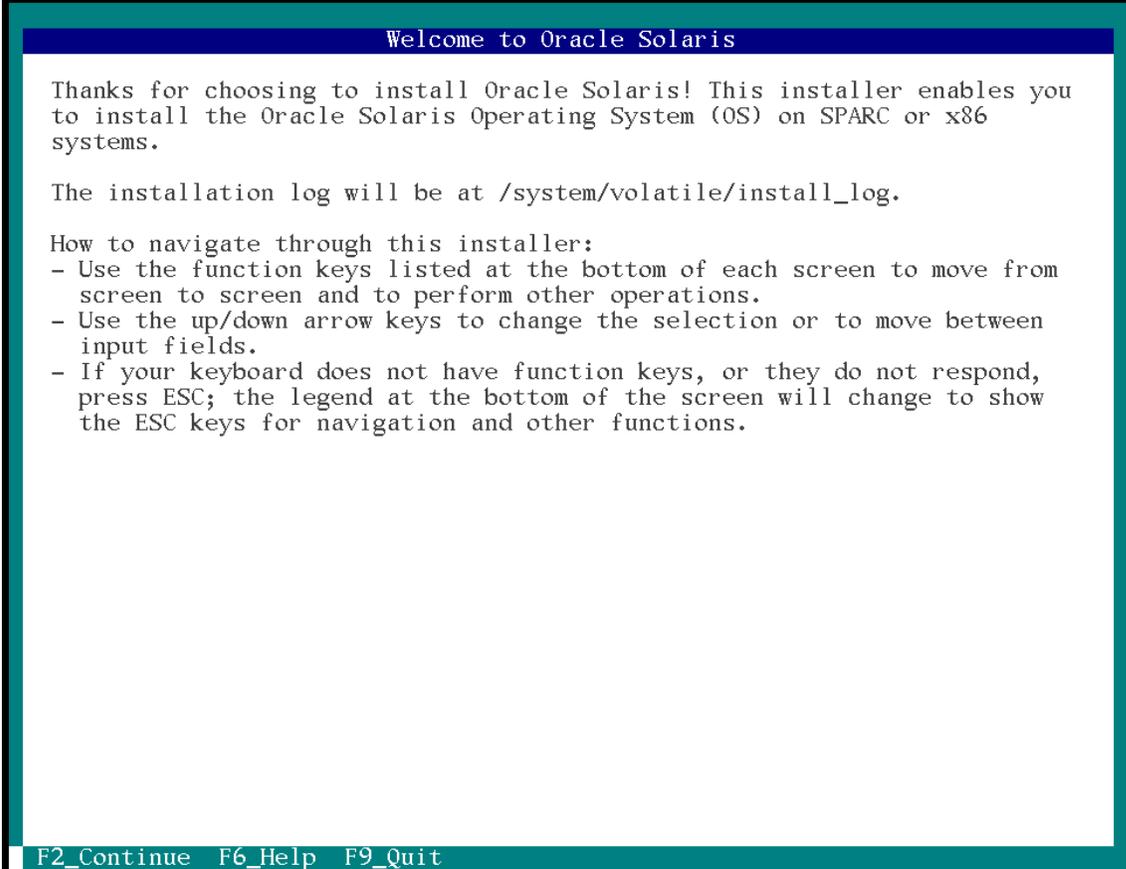
```
                    Welcome to Oracle Solaris

  Thanks for choosing to install Oracle Solaris! This installer enables you
  to install the Oracle Solaris Operating System (OS) on SPARC or x86
  systems.

  The installation log will be at /system/volatile/install_log.

  How to navigate through this installer:
  - Use the function keys listed at the bottom of each screen to move from
    screen to screen and to perform other operations.
  - Use the up/down arrow keys to change the selection or to move between
    input fields.
  - If your keyboard does not have function keys, or they do not respond,
    press ESC; the legend at the bottom of the screen will change to show
    the ESC keys for navigation and other functions.


  F2_Continue  F6_Help  F9_Quit
```

AutoInstall: Installing Oracle Solaris Instances

- Provides a scalable install service for multiple client systems

- Requirements:
  - DHCP server
  - AI install images
  - AI server
  - IPS repository

- Create client manifests

- Create profiles

- Associate with install services

Automated Installations Over the Network
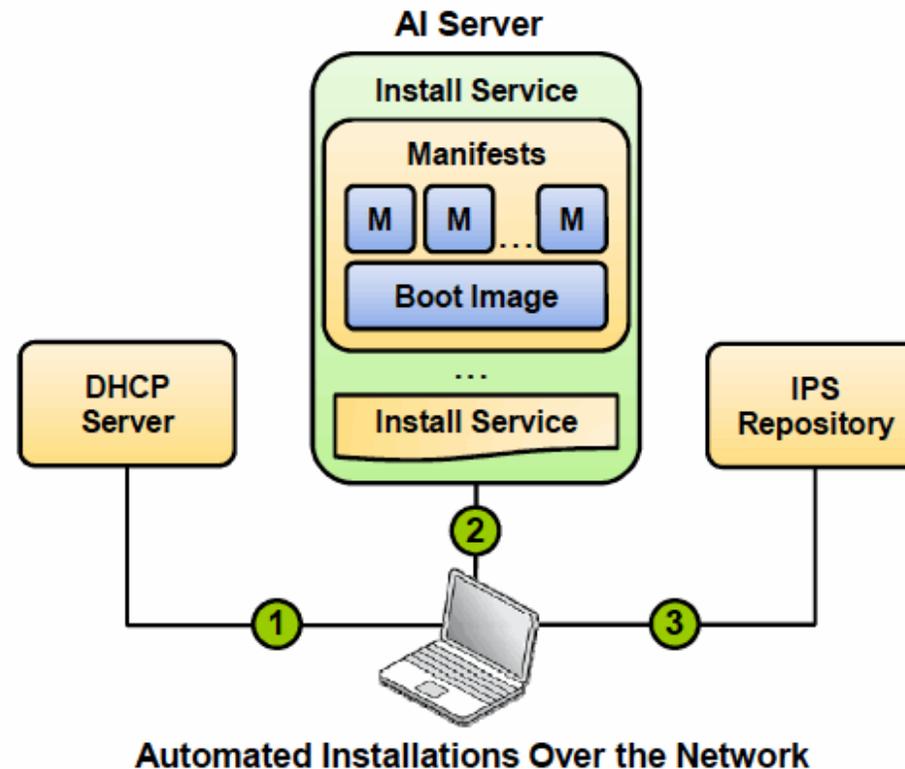
AutoInstall: Manifests

Client configuration

- Manifest describe important client configuration settings
- Web interface (port 5555 on localhost)

Steps | **Help**

Introduction
Root Pool
Data Pools
Disks
Repositories
✓ Software
Zones
Review

Preview XML

Review

Your manifest **default** will be saved locally when you press **Save** below.

Manifest Settings

AI Manifest Name: default

Root Pool Name: rpool
BE Name: solaris
Swap Device: Auto
Dump Device: Auto

Pool Name	Mountpoint	Redundancy	Disk Property	Property Value
rpool	null	None	Auto	

Publisher: solaris
Origin: http://pkg.oracle.com/solaris/release

Package: pkg:/entire@11.4-11.4
pkg:/group/system/solaris-minimal-server

Back   Save   Cancel

Interactive installadm

- Installadm(8) is interactive

```
installadm> list
Service Name Status Arch Type Secure Alias Aliases Clients Profiles
Manifests
------------ ------ ---- ---- ------ ----- ------- ------- -------- -------
---
default-i386 on      i386 iso  no      yes   0       0       0        1
s11_4beta    on      i386 iso  no      no    1       0       0        1
installadm> help list
list            [-a|--all | -s|--server -c|--client -m|--manifest -p|--
profile]
                [-v|--verbose] [-n|--service <svcname>]
list            [-v|--verbose] -e|--macaddr <macaddr>
```

First boot service

- A first boot service is one that runs once post the initial install

- Involves the following step
  - Write the first boot scripts
  - Create an SMF manifest (with the correct property: `config/completed`)
    - Could use svcbundle
  - Create a package manifest
  - Create a repository for the package
  - Publish the package
  - Modify the AI manifest to include the repository and the package to install

ORACLE®

Oracle Solaris 11.4 Beta: `svc-create-first-boot`

- Takes all the leg work out of creating the first boot service

- Can be run manually or interactively

```
svc-create-first-boot -s /first/setup-hosts.sh \
-d /files/first/first-boot.p5p \
-o package-fmri=setup-etc-hosts \
-o package-publisher=firstboot
```

- Resultant p5p file is a 'complete' repository and can be added to the AI manifest

Oracle Solaris 11.4 Beta x86 WAN Boot for Automated Installer

Installation and Software Management Features

- Enable x86 AI Installation via WAN
  - Secure from early Boot through Install

- Requires
  - UEFI-enabled x86 System
  - HMAC-256 protocols used by default

- Benefits
  - AI server can verify identity of client
  - Data encryption on network
  - Only authenticated clients can access data

- ToDo:
  - Set HMAC policy to hmac-sha256 for AI
  - Set credential for AI server and service
  - Set service authentication policy
  - Generate Keys
  - Configure AI Client in UEFI BIOS Setup
    - Set SHA256 HMAC Key
    - Set AES Encryption Key

Small is beautiful

Oracle Solaris Minimization

- install systems using the group package: `solaris-minimal-server`
  - Less installed software ➔ less need to update
  - Add the `solaris-11-cpu` and use that to update the system
  - Add extra software as required.
    - Oracle database requires a set of packages – use the prerequisite group package:
      - `oracle-rdbms-server-18c-preinstall`
      - `oracle-rdbms-server-12cR1-preinstall`
      - `oracle-ebs-server-R12-preinstall`

System Identity

- Oracle Solaris 11.3

```
$ uname –a
SunOS Coptic 5.11 11.3 i86pc i386 i86pc
$ pkg list entire
NAME (PUBLISHER)           VERSION                    IFO
entire (solaris)           0.5.11-0.175.3.29.0.5.0    i--
```

- Oracle Solaris 11.4

```
$ uname –a
SunOS eraser 5.11 11.4.0.12.0 i86pc i386 i86pc
$ pkg list entire
NAME (PUBLISHER)           VERSION                    IFO
entire (solaris)           11.4-11.4.0.0.0.12.1       i--
```

ORACLE®

System Identity

- The output of uname –v will now change when an SRU is updated

Uname –v output	Decoding
11.4.1.4.0	11.4 SRU 1 Build 1 Respin 0
11.4.5.7.0	11.4 SRU 5 Build 7 Respin 0

- The output of uname –r will remain as 5.11

Maintenance: addressing vulnerabilities

- Using the 'support/critical-patch-update/solaris-11-cpu' package

- Released for each Support Repository Update (SRU)

- Simply contains metadata

```
$ pkg contents -mr solaris-11-cpu
….
set name=CVE-2018-5095
value=pkg://solaris/mail/thunderbird@52.6.0,5.11-0.175
.3.29.0.4.0
set name=CVE-2018-5091
value=pkg://solaris/web/browser/firefox@52.6.0,5.11-
0.175.3.29.0.3.0
```

ORACLE®

Querying the CPU package

- Finding out if a particular CVE is addressed

Query	Command	Result
Is a particular CVE fixed ?	pkg search –r CVE-2018-5095	Returns a list of solaris-11-cpu packages which, will if installed, will ensure the issue is fixed
What package does a CVE apply too ?	pkg search –r :CVE-2018-5095:	Returns a list of packages, and their versions which have the fix applied

- If the CPU package is installed it will ensure packages are updated.

ORACLE®

Oracle Solaris 11.4 Beta using the CPU package

Compliance(1) report
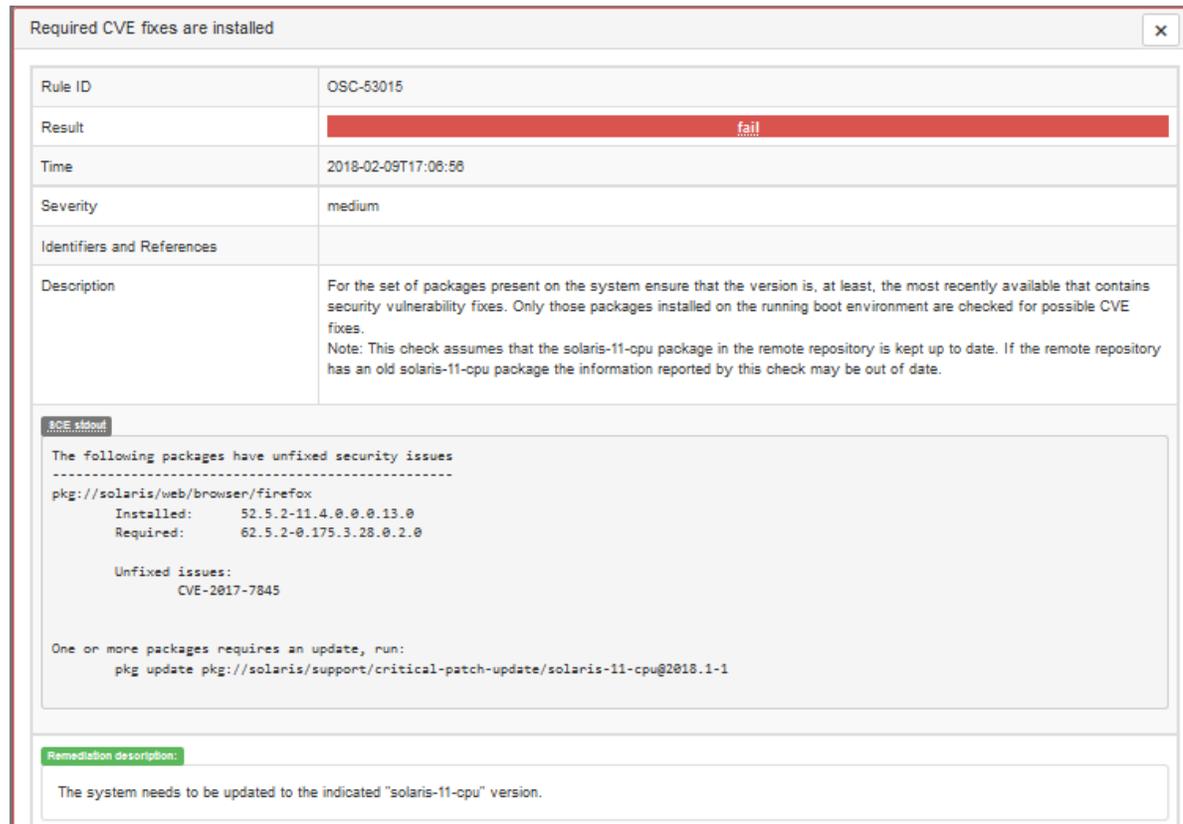
Required CVE fixes are installed

Rule ID	OSC-53015
Result	**fail**
Time	2018-02-09T17:06:56
Severity	medium
Identifiers and References	
Description	For the set of packages present on the system ensure that the version is, at least, the most recently available that contains security vulnerability fixes. Only those packages installed on the running boot environment are checked for possible CVE fixes. Note: This check assumes that the solaris-11-cpu package in the remote repository is kept up to date. If the remote repository has an old solaris-11-cpu package the information reported by this check may be out of date.

SCE stdout

```
The following packages have unfixed security issues
------------------------------------------------
pkg://solaris/web/browser/firefox
        Installed:      52.5.2-11.4.0.0.0.13.0
        Required:       62.5.2-0.175.3.28.0.2.0

        Unfixed issues:
                CVE-2017-7845


One or more packages requires an update, run:
        pkg update pkg://solaris/support/critical-patch-update/solaris-11-cpu@2018.1-1
```

Remediation description:

The system needs to be updated to the indicated "solaris-11-cpu" version.

- Uses two pieces of data:
  - The installed packages on the system
  - Metadata in the `solaris-11-cpu` packaging (uses the package that is in the defined repository)
- `solaris-11-cpu` package can be used to update system (as opposed to 'entire')

Oracle Solaris – Continuously Better Than Other Platforms

Simple and Error Free

Seamless update from SRU to SRU

Maximum Availability

Non destructive system update and rollback

Continuously Compatible

Application investment Protection

Always Secure

Install what you expect with end-to-end security

ORACLE®

System Updates

- Designed to be very simple

```
# pkg update
```

- Safe and quick
  - pkg(1) client will only update what needs to be updated
  - Will create, as needed, new boot environments or backup boot environments.
  - Package signing verification (only trust signed packages)

- Integrated with Solaris Technologies
  - ZFS (boot environments – live upgrade for free)
  - SMF (service management facility, as part of an update services can be stopped, restarted, disabled)
  - Audit history

- An easy development environment allowing for 3rd party packages

Reducing Application Downtime

- Oracle Solaris provides a Fault Management service
  - Diagnosis and report issues on the system
    - Hardware and software
  - Report issues to a variety of places: email/SNMP enabling proactive addressing of issues before they become critical
    - Use of Auto Service Request (asradm(8)) to log service requests (for example replace defect hardware)

- Administrative interface via: fmadm (fmdump to list FMA logs on a system)

- Set email notifications via SMF

```
#svccfg setnotify problem-diagnosed mailto:person@email.com
```

Oracle Solaris 11.4 Beta: Identifying System Issues

- Extends the Fault Management to identify software issues
  - When a Solaris process dies (core dumps) this triggers a software FMA event
  - The event triggers a software diagnosis engine to examine the produced core file
  - It will match the stack in the core with known stacks and produce an FMA report as to a possible issue

```
Description : A diagnostic core file was dumped in
              /var/diag/ec27ca6b-1e53-49d1-8d85-9f2324e6def2 for RESOURCE
              /usr/lib/ssm/hwmgmtd whose ASRU is
              svc:/system/sp/management:default. The ASRU is the Service FMRI
              for the resource and will be NULL if the resource is not part of
              a service. The following are potential bugs.
              stack[6] - 25121328
```

ORACLE®

More Metadata

- The package: `pkg:/system/diagnostic/stackdb` delivers a database of known stack traces and associated bug ids

- This package should be kept up to date on all systems, irrespective of updating the system as a whole:

```
# pkg update stackdb
```

- Find out if the reported bug id is fixed and what it is fixed in:

```
$ pkg search -r 25148407
INDEX                           ACTION VALUE      PACKAGE
com.oracle.service.bugid set    25148407
pkg:/system/ldoms@0.5.11-0.175.3.29.0.4.0
```

Maintenance Summary

- **Proactive**
  - Ensuring security vulnerabilities are addressed
  - Compliance framework – new CVE check
  - SRU documentation giving indication of important issues Doc ID: 2076753.1
  - SRU Readmes Doc ID: 2045311.1
  - Software Minimization – install only what is needed

- **Reactive**
  - Bugs occur, software fails – service calls – for known problems Fault Management can be used to match failures against known issues

Service Management Facility (SMF)

- Provides a rich mechanism to control services on a system
  - A service is a persistently running application (example: svc:/system/cron:default)
  - Services can be controlled via svcadm(8): enable, disable, restart, refresh, clear
  - Installation / removal of packages can interact with SMF services via 'actuators'
  - Applications can be controlled via such services
    - Quick service definitions can be created via the use of svcbundle(8) – lots of examples in the man page

```
# svcbundle -s service-name=site/pete \
        -s start-method=/lib/svc/method/pete.sh \
        -s model=daemon -o svc-pete.xml
```

Oracle Solaris 11.4 Beta: SMF Goal Services

- Many application services could be defined for a system

- System is only considered 'UP' when all application services are up and running

- Prior to Oracle Solaris 11.4 – had to check each service

- Goal Services (see svcadm(8))
  - Allows for the linking of application services under one service (a goal service)
  - A goal is only online when all the dependent services are online
  - Therefore only need to monitor the goal service as opposed to individual application services
  - Ability to define own goal service

ORACLE®

Using the goals service

- One goal service is provided and can be linked too

```
# svcs goals
STATE              STIME    FMRI
online             9:07:23  svc:/milestone/goals:default
# svcs -d goals
STATE              STIME    FMRI
online             9:07:22  svc:/milestone/multi-user-server:default
# svcadm goals site/pete svc:/milestone/multi-user-server:default
# svcs -d goals
STATE              STIME    FMRI
online             9:07:22  svc:/milestone/multi-user-server:default
online            10:17:40  svc:/site/pete:default
```

ORACLE®

Goals service

- Application service goes offline, then goal service goes offline

```
# svcs goals
STATE              STIME    FMRI
online             10:25:03 svc:/milestone/goals:default
# svcadm disable pete
# svcs goals
STATE              STIME    FMRI
maintenance        10:25:43 svc:/milestone/goals:default
```

- End result it means a standard goal could be defined across many systems running different applications

ORACLE®

Unified Archives

- Mechanism to create system archives
  - System backups
  - System cloning

```
# archiveadm create -D rpool/archives full.uar
```

- Do not include the dataset that is going to store the archive

- Specify the archive when installing

```
# zoneadm -z z2 install -a full.uar -z z1
```

Oracle Solaris 11.4 Beta: dehydrated archives

- Archives can be large (remember small is beautiful)

- Why copy around 'standard' binaries ? Only need to know changes....

- Create dehydrated archives

```
# archiveadm create -D rpool/export -dehydrate dfull.uar
# ls -lh
total 14184642
-rw-r--r--    1 root  root        1.2G Mar  2 22:14 dfull.uar
-rw-r--r--    1 root  root        5.6G Mar  2 21:20 full.uar
# zoneadm -z z3 install -a dfull.uar -z z1
```

- Note it is better to rehydrate the archive before installing from it

Summary: Oracle Solaris

- **Continuous Delivery Model**
  - Innovation and through dot releases
  - Regularly updated widely used open source packages
  - Quarterly Critical Patch Updates
  - Monthly Support Repository Updates

- **Secure, Stable, Virtualized**
  - Integrated security and Virtualization
  - Availability Features
  - Simplify Deployments and Operations

- **Best for Oracle Database and Java**
  - Data/Systems management
  - Networking Features
  - Performance Features

- **Long Term Investment Protection**
  - Oracle Solaris 11 Support through at least 2034
  - Lifetime Support for Oracle Solaris Legacy environments
  - Application Binary Compatibility

Mission Critical Operating System

References

- Solaris 11.4Beta Blog Index
  https://blogs.oracle.com/solarium/public-oracle-solaris-114-beta

- Solaris 11.4Beta Doc Library (**What's New**, Release Notes, ...)
  https://docs.oracle.com/cd/E37838_01/

- EOF Announcement Link
  http://www.oracle.com/technetwork/systems/end-of-notices/index.html

- Critical Patch Updates, Security Alerts and Bulletins
  https://www.oracle.com/technetwork/topics/security/alerts-086861.html

- Reference Index of CVE IDs and Solaris Patches (Doc ID 1448883.1)

Integrated Cloud

Applications & Platform Services

ORACLE®