ORACLE
SOLARIS

Oracle Solaris Immutable Zones for SAP Installation

ORACLE WHITE PAPER | FEBRUARY 2016

ORACLE

Introduction

This paper provides instructions and best practices on how to create and manage an SAP installation on an Oracle Solaris Immutable Zone. An Immutable Zone is a security mechanism that can be used to control the way users access files, protect system databases and applications, allow read-only virtual machines, and freeze the operating system and hardware configuration to prevent changes. An Oracle Solaris Immutable Zone obtains the zone's configuration by implementing read-only `root` file systems for non-global zones, global zones and kernel zones.

The goal of this document is to increase security features on the Oracle Solaris operating system by defining a non-global zone, global zone or kernel zone as an Immutable Zone and running the SAP application on this read-only zone. With this strategy, the system is made safer. The procedure is tested by simply setting the `zonecfg file-mac-profile` property for various SAP releases with Oracle Database 11*g* and 12*c*.

Motivation

Security and compliance are, definitely, the top concerns of organizations today. Data breaches are commonplace, with sensitive data getting into the hands of unknown groups and causing unrecoverable damage, such as the loss of customer confidence, the high costs of remediation, and credit rating downgrades. Attacks can come through a variety of channels—from denial of service to SQL injection, stolen user credentials, social engineering, and more. Oracle Solaris 11 offers a variety of proven security features that, when used in a "defense-in-depth" architecture, provide a sophisticated network-wide security system that controls the way users access files, protects system databases, and controls the use of system resources. Oracle Solaris 11 addresses security requirements at every layer. It is installed "secure by default" as a minimal-protection profile upon which the user can add additional protection. This helps to reduce the chance of intrusion by disabling all network services other than Secure Shell (SSH).

Oracle Solaris provides integrated compliance management and reporting tools to meet compliance obligations and also, more importantly, to help maintain change control through simple instructions for mitigating any compliance failure. For more information about Oracle Solaris Compliance tools for SAP installation, please refer to the last section of this whitepaper, "Running Oracle Solaris Compliance Reporting on an Immutable Zone" on page 6.

Using Immutable Zones is one technique that can protect applications and the system from malicious attacks by applying read-only protection to the host global zone, kernel zones and non-global zones. Oracle Solaris Zones technology is the recommended approach for deploying application workloads in an isolated environment—no process in one zone can monitor or affect processes running in another zone. Immutable Zones extend this level of isolation and protection by enabling a read-only file system, preventing any modification to the system or system configuration.

A simple example that employs Immutable Zones might involve locking down a zone running an application server so it is read-only. Figure 1 shows this example architecture.

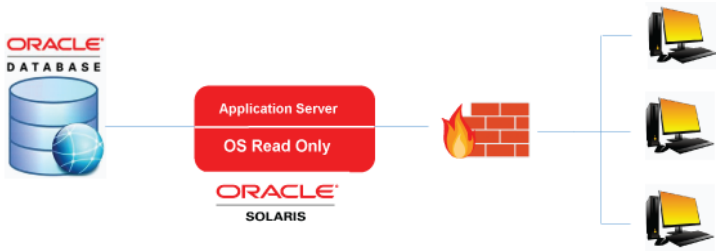

Figure 1. A typical architecture that leverages Oracle Solaris Immutable Zones.

Installing SAP Application on an Oracle Solaris Immutable Zone

Immutable Zones are Oracle Solaris zones with read-only root file systems. Both global and non-global zones can be Immutable Zones. A read-only zone can be configured simply by setting the `zonecfg file-mac-profile` property to one of the values `strict`, `fixed-configuration`, `flexible-configuration` or `dynamic-zones` (configuration is writeable but binaries and such or not). The mandatory write access control (MWAC) kernel policy is used to exact file system write privilege through a `zonecfg file-mac-profile` property. Because the global zone is not subject to MWAC policy, the global zone can write to a non-global zone's file system for installation, image updates, and maintenance.

By default, the `zonecfg file-mac-profile` property is not set in a non-global zone. A zone is configured to have a writable root dataset. In a `solaris` read-only zone, the `file-mac-profile` property is used to configure a read-only zone root. A read-only root restricts access to the runtime environment from inside the zone. Through the `zonecfg` utility, the `file-mac-profile` can be set to one of the following values (see Table 1). All profiles except `none` will cause the `/var/pkg` directory and its contents to be read-only from inside the zone.

TABLE 1. DIFFERENT VALUES OF FILE-MAC-PROFILE PROPERTY

Value of `file-mac-profile` Property	Description
`none`	Allows full read-write access. This is the default behavior for newly created zones and is equivalent to not setting `file-mac-profile` property.
`fixed-configuration`	Allows read-write access to files located in `/var` except for the following locations: » `/var/ld` » `/var/lib/postrun` » `/var/pkg` » `/var/spool/cron` » `/var/spool/postrun` » `/var/svc/manifest` » `/var/svc/profiles`
`flexible-configuration`	Same as `fixed-configuration`, but also allows read-write access on files located in `/etc`
`dynamic-zones`	Same as `fixed-configuration`, but allows for the creation of non-global or kernel zones. Applies only to the global zone (or the global zone of a kernel zone).
`strict`	Provides a full read-only file system. System logs and audit trails need to be sent off to another centralized system. » IPS packages cannot be installed. » Persistently enabled SMF services are fixed. » SMF manifests cannot be added from the default locations. » Logging and auditing configuration files are fixed. Data can only be logged remotely.

Another feature, the Trusted Path, can be used to securely enable modification of protected files. When logged in through the Trusted Path using the `-T` option to `zlogin`, a user can modify protected files from within the zone. This is much safer as the user no longer needs to be given root access in the global zone nor does the user need to boot the Immutable non-global zones in writeable mode.

Immutable Non-Global Zone

As an SAP system requires write access to some directories, it is not possible to install SAP inside an Immutable Zone without further configuration. The only method to give write access to directories within an Immutable Zone is to create ZFS file systems in the global zone and then add these ZFS file systems to the Immutable Zone via the `zonecfg add dataset` command.

The following steps have to be performed to define the non-global zone as an Immutable Zone.

1. Start by simply creating a new non-global zone without setting the `file-mac-profile` property as `fixed-configuration`, `flexible-configuration` or `strict`, because the default behavior for newly created zones for `file-mac-profile` is `none`.
2. SAP application and Oracle Database need write access to following directories:
   - `/export/home/daaadm`
   - `/export/home/sapadm`
   - `/export/home/oracle`
   - `/export/home/<SID>adm`
   - `/export/home/ora<SID>`
   - `/oracle`
   - `/sapmnt`
   - `/usr/sap`
   - `/var/tmp`

   a. This means that for each of these directories, a new ZFS file system must be created in the global zone. For example, to create a ZFS files system for `/oracle`, first execute the `zfs create` command in the global zone:

```
root@blade9:~# zfs create rpool/immuzone-oracle
```

   b. Then, add the newly created ZFS file system to the Immutable Zone with the `zonecfg` command:

```
root@blade9:~# zonecfg -z immuzone
zonecfg:immuzone> add dataset
zonecfg:immuzone:dataset> set name=rpool/immuzone-oracle
zonecfg:immuzone:dataset> end
zonecfg:immuzone> verify
zonecfg:immuzone> commit
zonecfg:immuzone> exit
```

c. Repeat these steps for all other directories until each directory has its own ZFS file system:

```
root@blade9:~# zfs list
NAME                                  USED  AVAIL  REFER  MOUNTPOINT
rpool/immuzone-exporthomedaaadm        31K  5.06G    31K  /zones/immuzone/root/export/home/daaadm
rpool/immuzone-exporthomeoracle        31K  5.06G    31K  /zones/immuzone/root/export/home/oracle
rpool/immuzone-exporthomeorasid       155K  5.06G   155K  /zones/immuzone/root/export/home/oraqo1
rpool/immuzone-exporthomesapadm        31K  5.06G    31K  /zones/immuzone/root/export/home/sapadm
rpool/immuzone-exporthomesid          254K  5.06G   254K  /zones/immuzone/root/export/home/qo1adm
rpool/immuzone-oracle                34.1G  5.06G  34.1G  /zones/immuzone/root/oracle
rpool/immuzone-sapmnt                1.67G  5.06G  1.67G  /rpool/immuzone-sapmnt
rpool/immuzone-usrsap                3.93G  5.06G  3.93G  /zones/immuzone/root/usr/sap
rpool/immuzone-vartmp                33.5K  5.06G  33.5K  /zones/immuzone/root/var/tmp
```

d. After adding these ZFS file systems as datasets to the Immutable Zone, it will contain the following datasets:

```
root@blade9:~# zonecfg -z immuzone info
dataset:
        name: rpool/immuzone-exporthomedaaadm
        alias: immuzone-exporthomedaaadm
dataset:
        name: rpool/immuzone-exporthomeoracle
        alias: immuzone-exporthomeoracle
dataset:
        name: rpool/immuzone-exporthomeorasid
        alias: immuzone-exporthomeorasid
dataset:
        name: rpool/immuzone-exporthomesapadm
        alias: immuzone-exporthomesapadm
dataset:
        name: rpool/immuzone-exporthomesid
        alias: immuzone-exporthomesid

dataset:
        name: rpool/immuzone-oracle
        alias: immuzone-oracle
dataset:
        name: rpool/immuzone-sapmnt
        alias: immuzone-sapmnt

dataset:
        name: rpool/immuzone-usrsap
        alias: immuzone-usrsap
dataset:
        name: rpool/immuzone-vartmp
        alias: immuzone-vartmp
```

e. Now log into the zone and mount the ZFS file systems at the appropriate paths. For example, the ZFS dataset `rpool/immuzone-oracle` should be mounted under `/oracle`:

Note: The empty directory has to be created and the mount point has to be set to that directory for the ZFS file system.

```
root@immuzone:~# mkdir /oracle
root@immuzone:~# zfs set mountpoint=/oracle immuzone-oracle
```

f. Repeat the process for each ZFS file system which was created for the SAP installation. The mount points of the ZFS file system are set as follows:

```
root@immuzone:~# zfs list | grep immuzone
immuzone-exporthomedaaadm          31K  5.06G    31K  /export/home/daaadm
immuzone-exporthomeoracle          31K  5.06G    31K  /export/home/oracle
immuzone-exporthomeorasid         155K  5.06G   155K  /export/home/oraqo1
immuzone-exporthomesapadm          31K  5.06G    31K  /export/home/sapadm
immuzone-exporthomesid            254K  5.06G   254K  /export/home/qo1adm
```

```
immuzone-oracle                 34.1G  5.06G  34.1G  /oracle
immuzone-usrsap                 3.93G  5.06G  3.93G  /usr/sap
immuzone-vartmp                 33.5K  5.06G  33.5K  /var/tmp
immuzone-sapmnt                  1.67G  5.06G  1.67G  /sapmnt
```

3. Install the SAP system: Now all directories are prepared for the SAP installation with Oracle Database.
4. Change the non-global zone to "Immutable Zone": After installing the SAP system with Oracle Database, log into the global zone and set the `file-mac-profile` to one of the values described in the Table 1. The configuration explained in this whitepaper works with all levels of the `file-mac-profile` property, but in this example the parameter is set to `strict` to create a fully read-only zone.

```
root@blade9:/export/home/sun# zonecfg -z immuzone set file-mac-profile=strict
```

5. Reboot the system and start the SAP with `startsap`: After rebooting the zone, use the `zoneadm list -p` command to check if the zone is configured as a read-only zone. In this example, there is the letter `R` in the second-last column of the output, which means the zone is booted as a read-only zone.

```
root@blade9:/export/home/sun# zoneadm -z immuzone reboot
root@blade9:/export/home/sun# zoneadm list -p
26:immuzone:running:/zones/immuzone:77e73de5-f94b-461b-baba fb1b70516922:solaris:excl:R:strict:
```

Now the zone is configured as an Immutable Zone with a read-only file system. However, only the ZFS file systems, which are created in the global zone and mounted within the Immutable Zone, are writeable.

Immutable Kernel Zone

Installing an SAP system with Oracle Database is also possible within immutable kernel zones.

1. After creating and installing a kernel zone, log into the kernel zone and create ZFS file systems for the directories required by the SAP and Oracle Database installation (as described in the previous section) within the kernel zone. Then, add these as datasets to the kernel zone. Do this by calling the `zonecfg -z global` command within the kernel zone and adding the dataset. The following datasets should be part of the zone:

```
root@kzimmu:~# zonecfg -z global info
file-mac-profile: strict
pool:
fs-allowed:
dataset:
        name: rpool/immuzone-exporthomedaaadm
dataset:
        name: rpool/immuzone-exporthomeoracle
dataset:
        name: rpool/immuzone-exporthomeorsid
dataset:
        name: rpool/immuzone-exporthomesapadm
dataset:
        name: rpool/immuzone-exporthomesid
dataset:
        name: rpool/immuzone-oracle
dataset:
        name: rpool/immuzone-sapmnt
dataset:
        name: rpool/immuzone-usrsap
dataset:
        name: rpool/immuzone-vartmp
```

2. After the ZFS file systems are added to the kernel zone, create the empty directories for the mount points and set the mount points for theses ZFS file systems. The output of `zfs list` should look as follows:

```
root@kzimmu:~# zfs list | grep immuzone
rpool/immuzone-exporthomedaaadm    31K  59.0G    31K  /export/home/daaadm
rpool/immuzone-exporthomeoracle    31K  59.0G    31K  /export/home/oracle
```

```
rpool/immuzone-exporthomeorasid   120K  59.0G   120K  /export/home/oraqo1
rpool/immuzone-exporthomesapadm    31K  59.0G    31K  /export/home/sapadm
rpool/immuzone-exporthomesid      278K  59.0G   278K  /export/home/qo1adm
rpool/immuzone-oracle            24.1G  59.0G  24.1G  /oracle
rpool/immuzone-sapmnt            1.60G  59.0G  1.60G  /sapmnt
rpool/immuzone-usrsap            3.98G  59.0G  3.98G  /usr/sap
rpool/immuzone-vartmp            35.5K  59.0G  35.5K  /var/tmp
```

3. The kernel zone is now properly configured to install an SAP system with Oracle Database. When the installation is finished successfully, set the `file-mac-profile` property to `strict` and reboot the kernel zone. To set the `file-mac-profile` property for a kernel zone, use the `zonecfg -z global` command within the global zone and then reboot the zone.

```
root@kzimmu:~# zonecfg -z global set file-mac-profile=strict
root@kzimmu:~# reboot
```

4. When the kernel zone has successfully rebooted, log into the kernel zone and use the command `zoneadm list -p` to check if the kernel zone is configured correctly as an Immutable Zone.

```
root@kzimmu:~# zoneadm list -p
0:global:running:/::solaris:shared:R:strict:
```

Running Oracle Solaris Compliance Reporting on an Immutable Zone

Since release 11.2, Oracle Solaris provides scripts that assess and report the compliance of Oracle Solaris with the command `compliance(1M)`. This command is used to run system assessments against security/compliance benchmarks and to generate HTML reports from those assessments. For more information about this topic, please refer to the white paper "Using the Oracle Solaris Compliance Tool for SAP Installation" (located at oracle.com/us/solutions/sap/solaris-compliance-tool-wp-2745025.pdf) and SAP note 2214056.

The user can run the compliance report on Immutable Zones for the four values of the `file-mac-profile` property: `strict, fixed-configuration, flexible-configuration` and `dynamic zones`. The compliance report on Immutable Zones set with `flexible-configuration` and `fixed-configuration` as well as `dynamic zones` can run normally. The `file-mac-profile=fixed-configuration` permits updates to `/var/*` directories, with the exception of directories that contain system configuration components. The `file-mac-profile=flexible-configuration` permits modification of files in `/etc/*` directories, changes to root's home directory, and updates to `/var/*` directories.

However, `file-mac-profile=strict` is a read-only file system with no exceptions. Because the compliance tool tries to write the `report.html` file in the path `/var/share/compliance/assessments`, the user should create a new ZFS file system and add it as a dataset for this folder. If the user has any other compliance reports saved under the folder `assessments`, it is recommended to change the name of the assessments and create the new ZFS file system as follows:

```
root@immuzone:/var/share/compliance/assessments# compliance assess -b solaris -a strict
compliance assess: Cannot create assessment repository: /var/share/compliance/assessments/strict: [Errno
30] Read-only file system: '/var/share/compliance/assessments/strict'

root@immuzone:/var/share/compliance# mv assessments/ old_assessments
root@immuzone:/var/share/compliance# ls -la
total 15
drwxr-xr-x   5 root     root           5 Jan 15 18:23 .
drwxr-xr-x  10 root     sys           10 Aug 28 15:33 ..
drwxr-xr-x   2 root     root          10 Nov  2 14:03 guides
drwx--x--x   5 root     root           5 Jan 15 16:36 old_assessments
root@blade9:~# zfs create rpool/immuzone-varcompliance
root@blade9:~# zfs set mountpoint=/immuzone/var/share/compliance/assessments rpool/immuzone-varcompliance
```

```
root@blade9:~# zfs list

NAME                              USED  AVAIL  REFER  MOUNTPOINT
rpool/immuzone-varcompliance     299K  5.06G   299K  /zones/immuzone/root/var/share/compliance/assessments


root@blade9:~# zonecfg -z immuzone
zonecfg:immuzone> add dataset
zonecfg:immuzone:dataset> set name=rpool/immuzone-complianceassess
zonecfg:immuzone:dataset> end
zonecfg:immuzone> verify
zonecfg:immuzone> commit
zonecfg:immuzone> exit

root@immuzone:~# zfs set mountpoint=/var/share/compliance/assessments immuzone-varsharecompliance
```

About the Authors

This document is based on Motahareh Kardeh's and Marc Nesello's experience with Oracle Solaris Immutable Zones with the SAP application. Motahareh Kardeh and Marc Nesello are Senior Software Engineers in Oracle's ISV Engineering teams for SAP.

References

For more information about Oracle Solaris Immutable Zones, see the following documents:

- How to Apply Read-Only Protection with Oracle Solaris Immutable Zones. https://community.oracle.com/docs/DOC-919614
- Oracle Solaris Administration: Configuring Read-Only Zones. https://docs.oracle.com/cd/E23824_01/html/821-1460/croz.html#scrolltoc
- Oracle Solaris Administration: Read-Only Zone Overview. https://docs.oracle.com/cd/E23824_01/html/821-1460/glhdg.html
- Solaris 11.2: Immutable Global Zone, by Casper Dik. https://blogs.oracle.com/casper/entry/solaris_11_2_immutable_global
- Immutable Zones on Encrypted ZFS, by Darren Moffat. https://blogs.oracle.com/darren/entry/immutable_zones_on_encrypted_zfs
- Solaris 11.2 Security: Part 1 – Security 101 and Checking your security. http://talesfromthedatacenter.com/archives/195
- SAP note 2214056—Solaris Compliance tool for SAP installation.
- SAP note 2260420—Oracle Solaris Immutable Zone with SAP installation.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com/SAP

Integrated Cloud Applications & Platform Services

Oracle Solaris Immutable Zones for SAP Installation
February 2016
Authors: Motahareh Kardeh and Marc Nesello