Oracle® Fusion Middleware

Patching Guide for Oracle Identity and Access Management

11*g* Release 2 (11.1.2.2.0)

E50311-03

April 2014

This document describes the process of patching an Oracle Fusion Middleware Identity and Access Management 11*g* Release 2 (11.1.2.2.0) deployment.

ORACLE

Oracle Fusion Middleware Patching Guide for Oracle Identity and Access Management, 11*g* Release 2 (11.1.2.2.0)

E50311-03

Primary Author: Rekha Kamath

Contributing Author: Gururaj B. S.

Contributor: Jeremy Banford

Contents

Preface

This document describes the process of patching an Oracle Fusion Middleware Identity and Access Management 11*g* Release 2 (11.1.2.2.0) deployment.

Audience

This document is intended for administrators who are responsible for patching Oracle Identity and Access Management.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documents:

- *Oracle Fusion Middleware Deployment Guide for Oracle Identity and Access Management*
- *Oracle Fusion Middleware Release Notes*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.

Convention	Meaning
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Understanding Oracle Identity and Access Management Patching Scenarios

This chapter provides an overview of the scenarios to patch an Oracle Identity and Access Management environment.

You can patch an Oracle Identity and Access Management environment using one of the following methods:

- **Manual patching**

  You can manually patch an existing Oracle Identity and Access Management environment using the OPatch tool.

  For information about manually patching an Oracle Identity and Access Management environment, see Chapter 3, "Manually Patching Oracle Identity and Access Management."

- **Automated patching**

  Automated patching involves using the new Identity and Access Management Lifecycle Tools. Note that this option is available only if you have created the Oracle Identity and Access Management environment using the Deployment Tool.

  For information about creating an Oracle Identity and Access Management environment using the Deployment Tool, see *Oracle Fusion Middleware Deployment Guide for Oracle Identity and Access Management*.

  To know more about automated patching, see Chapter 4, "Patching Oracle Identity and Access Management Using Lifecycle Tools."

2

Overview of Oracle Identity and Access Management Lifecycle Tools for Patching

This chapter introduces the patching tools that are part of the Oracle Identity and Access Management Lifecycle Tools. It also describes the concepts and terminology related to these tools.

This chapter contains the following sections:

2.1 Introduction to Patching Oracle Identity and Access Management Using Lifecycle Tools

The Oracle Identity and Access Management Lifecycle Tools can be used to patch an Oracle Identity and Access Management environment in an automated and orchestrated manner. The tools perform the following functions:

- Determine where and when, in an environment, each patch needs to be applied during a **patch session**.
- Generate a **patch plan** that lists in detail the steps of the session.
- Verify patch prerequisites against all hosts while servers are running.
- Stop servers to apply patches, apply the required patches, and restart the servers.
- Apply configuration or other artifact changes automatically for those patches that include these changes.

The following tools are used for automated patching of an Oracle Identity and Access Management environment:

- **Patch Manager**

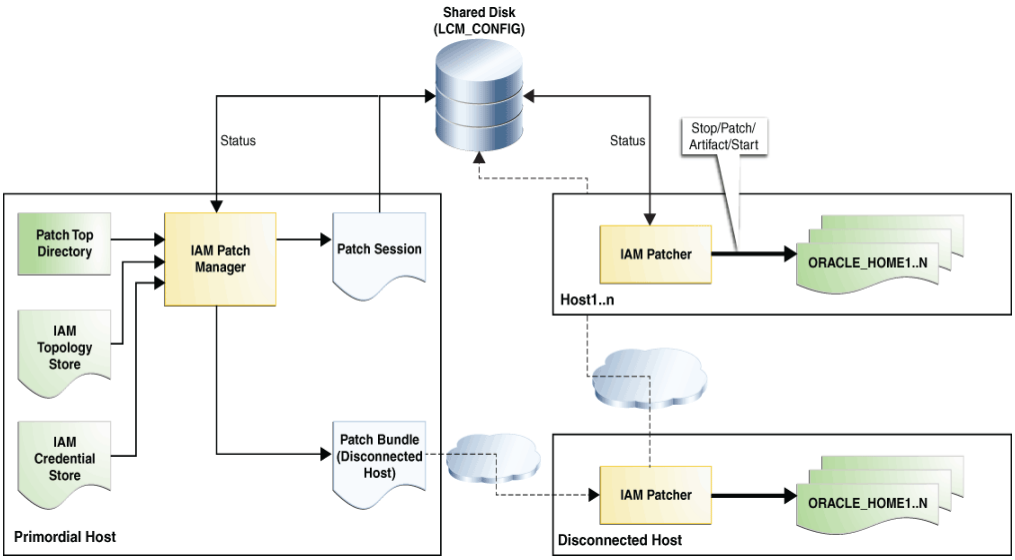
  The Oracle Identity and Access Management Patch Manager generates the patch plan, and controls and provides the status of the resulting patch session.

- **Patcher**

  The Oracle Identity and Access Management Patcher executes the steps in a patch session, as listed in the patch plan.

Figure 2–1 shows the process of patching an Oracle Identity and Access Management environment using the Lifecycle Tools.

Figure 2–1 Patching Oracle Identity and Access Management Using Lifecycle Tools



2.1.1 Products Supported

The Oracle Identity and Access Management Patcher patches all of the products that are supported by the Oracle Identity and Access Management Deployment Tool.

For the complete list of supported products, see "Products Deployed Using the Oracle Identity and Access Management Deployment Wizard" in *Oracle Fusion Middleware Deployment Guide for Oracle Identity and Access Management*.

2.2 Terminology

The following terms are used in the document:

Patch

A patch is a small collection of files that are applied over an existing installation. Patches are associated with particular versions of Oracle products. When applied to the correct version of an installed product, patches result in a slightly modified version of the product.

Interim patches make bug fixes available to customers, in response to specific bugs. They require a particular base release or patch set to be installed before you can apply them. These patches are not versioned, and the bug fixes they contain are made generally available in a future patch set as well as the next product release.

Tier

For patching an environment, an Identity and Access Management deployment is split into discrete tiers, each containing certain products, Oracle WebLogic Server domains, and server instances.

These tiers include:

- Directory

- Access
- Identity
- Web

During the generation of a patch plan, the patches provided are mapped to one or more tiers. Most products belong to a single tier, but there might be exceptions. For instance, Oracle WebLogic Server patches are applied across both the Access and Identity tiers, while common patches are applied across all tiers.

Topology Store

The topology store is an XML file that is generated by the Deployment Tool when the environment is created. It contains extensive physical and logical details about the environment, and is used by the Lifecycle Tools in applying patches.

IAM_TOP

The `IAM_TOP` directory contains the binary product installations. This directory is either located on a mounted network share or on a local disk, depending on how the Oracle Identity and Access Management environment is created. For information about creating an environment, see *Oracle Fusion Middleware Deployment Guide for Oracle Identity and Access Management*.

IAM_LCM_TOP

The `IAM_LCM_TOP` directory contains the installation of the Oracle Identity and Access Management Lifecycle Tools, including the Patch Manager and Patcher executables, and various configuration files that drive the behavior of the tools.

LCM_CONFIG

The `LCM_CONFIG` directory contains additional configuration files, including the topology store, runtime data, and log information for the Oracle Identity and Access Management Lifecycle Tools. This includes the patch session and the plan files that are human-readable.

Patch Top

A patch top directory (PATCH_TOP) contains unzipped patches that are sorted by product. The Patch Manager scans information in the `PATCH_TOP` directory to read the patches, validate the files, and after validating, include these patches in the patch plan generated.

2.3 Oracle Identity and Access Management Patch Manager

The Oracle Identity and Access Management Patch Manager is as administrative tool that generates a patch plan and controls the patch session. You can run the Patch Manager only from the primordial host of the deployment.

The Patch Manager does not execute any actions such as stopping or starting servers, and so on. All actions affecting a deployment are executed by the Patcher.

2.3.1 Patch Session

All automated patching occurs within a patch session. You can create a patch session to apply one or more patches, or to rollback patches that are already applied to a product.

Note: You can stop a patch session that is in progress, by executing the `abort` command.

The Patch Manager maintains a session file in the location `LCM_CONFIG/patch/session/` to track the patch process coordination with the Patcher. The session file contains the current status of the patch session. For more information about the status of a patch session, see Table 4–5.

At any given time, only one active patch session can exist in the deployment.

2.3.2 Patch Plan

A patch plan, which is created by the Patch Manager, consists of a set of comprehensive steps to patch the deployment.

2.3.2.1 Phases of a Patch Plan

A patch plan consists of the following three phases:

- Patch Apply Prerequisite Phase (all services running)

  The prerequisite checks are executed, but no changes are made to the deployment. This phase can be executed before you plan your system downtime, and apply patches. If any issue is found, it can be addressed immediately. This enables you to apply the patches smoothly during downtime.

- Patch Pre-Apply Phase (all services down)

  All servers that need to be shut down to apply patches are stopped. This action is deployment-aware. For example, if the patch top consists solely of an Oracle Access Manager patch, you need not stop every server instance. Only Oracle HTTP Server and Oracle Identity Manager, which depend on Oracle Access Manager, and Oracle Access Manager itself, are stopped. Oracle Unified Directory remains up during the execution of the plan. This ensures that the required downtime is minimized.

- Patch Apply Phase (limited services available)

  Patches are applied, any artifact changes related to the patches are executed, and servers are started.

2.3.2.2 Generating a Patch Plan

The Patch Manager generates the patch plan as follows:

1. A patch top directory containing patches, classified by each product subdirectory, is provided to the tool. Ensure that all downloaded patches have been unzipped, and that any zip files for those have been moved out of the patch top directory.
2. The patch top directory is scanned and initial validations are performed.
3. The deployment topology is read and analyzed.
4. The information obtained in Step 2 and Step 3 is combined, and a patch plan is generated using the `OPlan` utility. The patch plan is generated in HTML, plain-text and binary format, which is used for execution.
5. The log messages of the Patch Manager are written to the `log` directory in `LCM_CONFIG`:

The administrator needs to manually run the Patch Manager to begin a patching session. For information about how to run the Patch Manager, see Section 4.2.

2.4 Oracle Identity and Access Management Patcher

The Oracle Identity and Access Management Patcher is an execution engine that completes the steps in a patch session as listed in the patch plan, on each host in the deployment. The Patcher executes only those steps that are applicable to a specific host in a deployment. After completing the steps on a specific host, the Patcher displays a message indicating the next host on which the Patcher needs to be executed, and exits.

You need to execute the Patcher multiple times on a specific host, if required, during the execution of a patch plan, as different phases of the patch plan are executed.

3

Manually Patching Oracle Identity and Access Management

This chapter describes how to use the OPatch utility to patch an Oracle Identity and Access Management environment that is not created using the Deployment Tool.

For environments that are created using the Deployment Tool, OPatch is still used to patch the Identity and Access Management Lifecycle Tools themselves, when required.

This chapter contains the following topics:

3.1 About Manually Patching Oracle Identity and Access Management Using OPatch

OPatch is a Java-based utility that requires the installation of Oracle Universal Installer. It is platform independent, and runs on all supported operating systems.

As the first step to manually patch Oracle Identity and Access Management, obtain the latest version of the OPatch tool that is compatible with the product.

3.1.1 Products Supported

All of the products of the Oracle Identity and Access Management stack that are installed using Oracle Universal Installer can be patched manually using the OPatch utility.

Note:

- For information related to database patching requirements, see *Oracle Fusion Middleware Release Notes*.
- For information related to patching Oracle WebLogic Server, see *Oracle Smart Update Applying Patches to Oracle WebLogic Server*.

3.2 Steps for Manually Patching Oracle Identity and Access Management

The following table lists the steps that you need to complete to manually patch Oracle Identity and Access Management:

Note: To manually patch Oracle Identity and Access Management (11.1.2.2), follow the OPatch instructions provided in *Oracle Fusion Middleware Patching Guide* in the Oracle Fusion Middleware 11*g* Release 1 (11.1.1.7) Documentation Library.

Table 3–1 Tasks for Patching Oracle Identity and Access Management Using OPatch

Task	Description	More Information
Step 1: Obtain OPatch.	Obtain the latest version of OPatch from My Oracle Support.	"Getting OPatch" in *Oracle Fusion Middleware Patching Guide*
Step 2: Obtain the required patch(es).	Obtain the required patch(es) by specifying the patch ID in My Oracle Support.	"Getting Patches that Can be Applied with OPatch" in *Oracle Fusion Middleware Patching Guide*
Step 3: Review the information about system requirements, certification, and interoperability.	Ensure that the system environment and configuration meet the minimum requirements for patching the software.	"OPatch System Requirements" in *Oracle Fusion Middleware Patching Guide*
Step 4: Back up the Middleware home, domain home, and Oracle instances.	Back up the Middleware home directory (including the Oracle home directories inside the Middleware home), local Domain home directory, local Oracle instances, and also the Domain home and Oracle instances on any remote systems that use the Middleware home.	"Backup and Recovery Considerations for Patching" in *Oracle Fusion Middleware Patching Guide*
Step 5: Understand the Oracle Identity and Access Management environment that you need to patch manually.	Understand the environment in which you need to run the OPatch utility to manually patch Oracle Identity and Access Management.	"OPatch in a Fusion Middleware Environment" in *Oracle Fusion Middleware Patching Guide*.
Step 6: Run the OPatch utility to apply the required patch(es).	In the command-line interface, enter the command to run the OPatch utility.	"Running OPatch" in *Oracle Fusion Middleware Patching Guide*

Note: To troubleshoot issues that you might encounter while running the OPatch utility, see "Troubleshooting OPatch in a Fusion Middleware Environment" in *Oracle Fusion Middleware Patching Guide*.

4

Patching Oracle Identity and Access Management Using Lifecycle Tools

This chapter describes the procedure for patching the components of the Oracle Identity and Access Management software using the Lifecycle Tools.

It contains the following topics:

4.1 Before You Begin

Before patching your Oracle Identity and Access Management software using the Lifecycle Tools, ensure that you complete the following prerequisites:

4.1.1 Installing the Oracle Identity and Access Management Lifecycle Tools for Patching Supported Products

Obtain patching-related tools for patching an Oracle Identity and Access Management deployment by installing the Oracle Identity and Access Management Lifecycle Tools.

For information about installing the Oracle Identity and Access Management Lifecycle Tools, see *Oracle Fusion Middleware Deployment Guide for Oracle Identity and Access Management*.

When you deploy an Oracle Identity and Access Management environment using the Oracle Identity and Access Management Lifecycle Tools, patching-related directories `IAM_LCM_TOP` and `LCM_CONFIG`, are created.

IAM_LCM_TOP contains configuration files, executable files, scripts, and property files containing various environment variables that control the patching process. Figure 4–1 shows the contents of the IAM_LCM_TOP directory.

The LCM_CONFIG directory contains files such as logs, patch plans, topology store, credential store, and so on, that are used for some patching tasks. Figure 4–2 shows the contents of the LCM_CONFIG directory.

Table 4–1 describes the components of the IAM_LCM_TOP and LCM_CONFIG directories.

Figure 4–1 Directory Structure of IAM_LCM_TOP

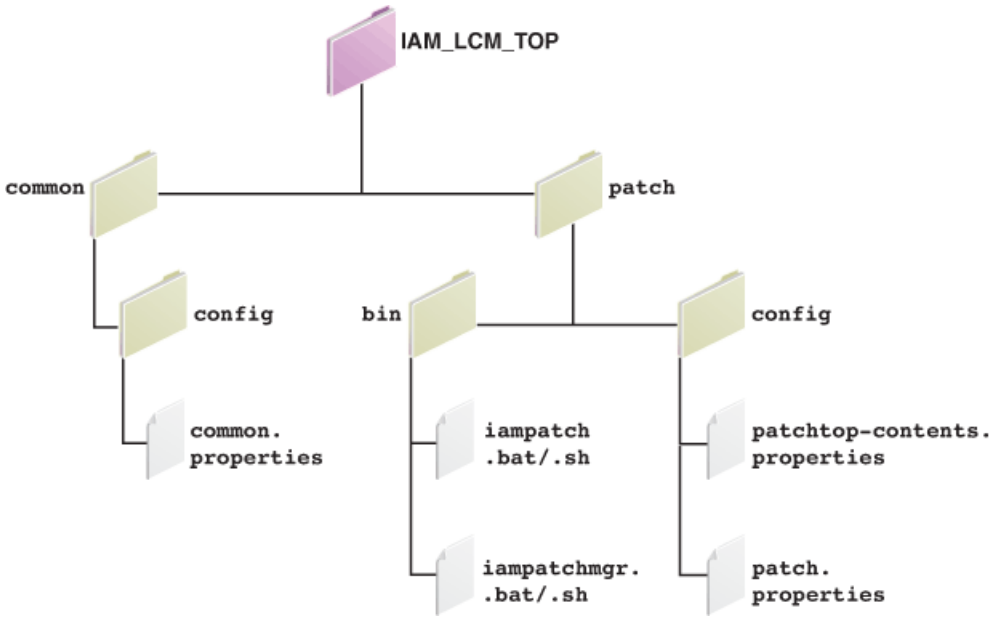


Figure 4–2 Directory Structure of LCM_CONFIG

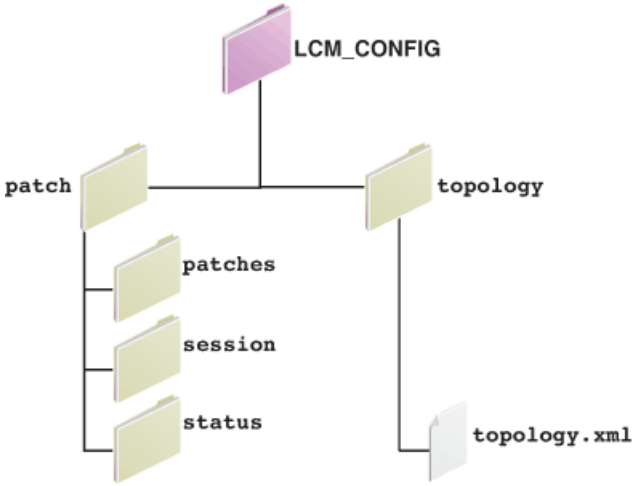


Table 4–1 Directory Structure of an Oracle Identity and Access Management Patching Deployment

Directory Structure	Description
IAM_LCM_TOP	
IAM_LCM_TOP/patch	Contains the configuration files and the executable files for patching the software.
IAM_LCM_TOP/patch/bin	Contains the Oracle Identity and Access Management Patch Manager and Oracle Identity and Access Management Patcher tools that can be executed on UNIX and Windows systems (.sh / .bat).
IAM_LCM_TOP/patch/config	Contains patch.properties, patchtop-contents.properties, iampatchmgr-logging.properties, iampatch-logging.properties that can be configured before running the patching tools. See Section 4.1.2 and Section 4.1.4.
IAM_LCM_TOP/common/config	Contains common.properties file that consists of information about JAVA_HOME, IAM_TOP, and LCM_CONFIG. See Section 4.1.3.
IAM_LCM_TOP/patch/script	Contains scripts and property files required by the Patcher to start or stop services and for applying artifacts.
LCM_CONFIG	
LCM_CONFIG/patch	Contains status files, logs, patches, and patch plan generated by Patch Manager when a patch session is started.
LCM_CONFIG/patch/patches	Contains set of patches read in from the provided patch top, and staged by the Patch Manager for use during the session. These patches are used by the Patch Manager to generate the patch plan.
LCM_CONFIG/patch/session	Contains the patch plan in a machine-readable format, and other information about the session in progress that Oracle Identity and Access Management Patcher uses to execute the patching steps.
LCM_CONFIG/patch/status	Contains host-based files tracking the execution state of each patch-plan step. Also contains all generated log files, and the patch plan in human-readable HTML and plain-text formats.
LCM_CONFIG/topology	Contains the topology store file topology.xml that provides detailed information about the Oracle Identity and Access Management deployment. Additionally, the provisioning.plan file, located in IAM_TOP/provisioning/plan, is also used for some patching tasks.

Note: Modify the values in the common.properties file and the patchtop-contents.properties file as required. Before modifying these files, ensure that you check the content of these files, and set correct values.

4.1.2 Verifying patchtop-contents.properties File

The patchtop-contents.properties file is located in *IAM_LCM_TOP*/patch/config/. It declares the relative paths within the patch top you provide, under which you place patches for each product supported by the Lifecycle Tools.

Open the patchtop-contents.properties file, and verify its content.

Example 4–1 shows the contents of the patchtop-contents.properties file.

Example 4–1

```
common=oracle_common/patch
dir=oud/patch
oam=iamsuite/patch/oam
ohs=webtier/patch
ohswg=webgate/patch
oim=iamsuite/patch/oim
soa=soa/patch
wls=smart_update/weblogic
```

The patchtop-contents.properties file includes a default directory structure for all product patches. If you do not want to use the default directory structure to organize your patches, edit the file to declare the correct relative paths for your patch top, so that the Patch Manager can correctly detect all patches provided. If any of the parameters are commented out or removed from the file, the Patch Manager does not attempt to search for patches of those products within the patch top.

The IAM_LCM_TOP directory also contains the following properties files:

- common.properties
- patch.properties

4.1.3 Verifying common.properties File

The common.properties file is located in *IAM_LCM_TOP*/common/config/. It contains the environment variables JAVA_HOME, IAM_TOP, and LCM_CONFIG, required for patching Oracle Identity and Access Management.

Ensure that you set the environment variables listed in Table 4–2 before running the Oracle Identity and Access Management Patch Manager and Oracle Identity and Access Management Patcher.

Table 4–2 Variables Listed in common.properties File

Variable	Description
JAVA_HOME	The path pointing to the JDK location.
IAM_TOP	The absolute path of the IAM_TOP where Oracle Identity and Access Management products are installed.
LCM_CONFIG	Absolute path where the configuration of the Lifecycle Tools is stored.

4.1.4 Verifying patch.properties File

The patch.properties file is located in *IAM_LCM_TOP*/patch/config/. It contains preferences about low-level patching details, that you can modify. You need not edit this file as the default values that are available in the file are sufficient for most environments.

Ensure that you set the environment variables listed in Table 4–3 before running the Oracle Identity and Access Management Patch Manager and Oracle Identity and Access Management Patcher tools.

Table 4–3 Variables Listed in patch.properties File

Variable	Description
RETURN_MESSAGE_BUFFER_SIZE	The size of return message that is stored for each command executed. This buffer size includes standard output and error messages stored in log files. This variable affects the size of output printed to console and logs. Following are the available units: - B (byte) - KB (kilobyte) - MB (megabyte) - GB (gigabyte) Default value of the variable is 8KB.
COMMAND_TIMEOUT	The value consists of a timeout value followed by the unit. If the command execution takes longer, then the execution is terminated. Following are the permissible units for this variable: - ms (milliseconds) - s (seconds) - m (minutes) - h (hours) - d (days) Default value of the variable is 3600s (1 hour).

Note:

The `common.properties` file and `patch.properties` are populated during the deployment. However, if you are administering multiple `IAM_TOP` using a single Oracle Identity and Access Management deployment and patching tools install, then you should delete the values of `IAM_TOP` and `LCM_CONFIG` variables from the files and set the correct values.

You also have the option of setting the environment variables through the command-line interface, using the commands listed. However, ensure that you delete any existing values from the files before setting them in the environment.

For example, if you are using a `POSIX-compliant` shell, use the following command:

```
export JAVA_HOME=jdk_absolute_path
```

4.2 Creating a Patch Plan

Before running the Patcher, generate a patch plan on the hosts that you want to patch. The patch plan creates a list of comprehensive steps to patch a deployment.

Using various commands and options, you can use the `iampatchmgr` utility to generate a patch plan, rollback a patch session, abort or end a patch session, or monitor the progress of a session. See Section 2.3.

Note:

- Run the Patch Manager against an `IAM_TOP` environment.
- A new patch session cannot be created until the existing session is completed or aborted.

This section describes how to create a patch plan.

It contains the following topics:

- Preparing a Patch Top
- Procedure for Creating a Patch Plan
- Understanding Other Functions of Patch Manager

4.2.1 Preparing a Patch Top

The Lifecycle Tools work with patches organized within a patch top directory. This directory contains patches that have been unzipped and then categorized by product. The Patch Manager scans the patch top directory to find patches, validates their contents, and prepares them for execution as part of the patch session.

To apply patches downloaded from My Oracle Support, you need to organize them into a patch top so that the Patch Manager can find, validate, and execute them. To do this, perform the following steps before invoking the Manager:

- Create the root directory for the patch top. Any random name can be used. Oracle recommends that you provide a name that denotes the contents that this patch top will hold. For example, `1404-idm-r2ps2-bp`
- Create a set of subdirectories, one for each product for which you have patches. You need not create directories for all the products supported.

  Note: Open the `patchtop-contents.properties` file (see Section 4.1.2), and verify that the directories created match one of the relative paths declared for each product, whether those were set by default, or if you have added or changed the paths for the deployment.

- Unzip all patches, and copy the unzipped directory and its contents for each patch to the correct patch top directory for that product. For example, if the downloaded patch is for OAM and is named `12345.zip`, the unzipped `12345` directory should be copied to the location *`PATCH_TOP`*`/iamsuite/patch/oam/12345`. The zipped copies must not be placed in the patch top.

4.2.2 Procedure for Creating a Patch Plan

A patch plan contains instructions for applying patches to an Oracle Identity and Access Management environment. See Section 2.3.2.

The plan that is generated by running the Patch Manager can be executed by running the Oracle Identity and Access Management Patcher.

To create a patch plan, run the Oracle Identity and Access Management Patch Manager utility (`iampatchmgr`) with the `apply` command:

Note: Run the Oracle Identity and Access Management Patch Manager on the primordial host.

For UNIX

```
IAM_LCM_TOP/patch/bin/iampatchmgr.sh apply -patchtop patch_top_location
```

For Windows

```
IAM_LCM_TOP\patch\bin\iampatchmgr.bat apply -patchtop patch_top_location
```

The `apply` command performs the following tasks:

- It validates the given patch top location and the existence of the patch session with `ACTIVE` or `FAILED` status. If one exists, instead of beginning a new session, the output of the current session is displayed.
- If no patch session exists, the patch top is scanned for patches as directed by the `patchtop-contents.properties`. The resulting set of patches is copied into the `LCM_CONFIG` directory for use by the patch session.
- Using the information in the staged patches and the topology store, a plan containing instructions for applying that set of patches to the deployment is generated.

  A human-readable version of the plan is created in HTML and plain text formats, and saved to the following location:

  ```
  LCM_CONFIG/patch/status/session_ID/manager/log/PatchInstructions.html

  LCM_CONFIG/patch/status/session_ID/manager/log/PatchInstructions.text
  ```

- The patch plan begins with an overview of the Oracle Identity and Access Management deployment. See Section A.1.

  The plan also provides information such as steps to be executed, total number of steps, steps that require downtime, and so on. See Section A.2, Section A.3, and Section A.4.

  The Patch Manager writes log messages to the following locations:

  While outside of a patch session

  ```
  LCM_CONFIG/patch/status/log/iampatchmgr.log
  ```

  While within a patch session

  ```
  LCM_CONFIG/patch/status/session_ID/manager/log/iampatchmgr-session.log
  ```

4.2.3 Understanding Other Functions of Patch Manager

Run the `iampatchmgr` utility using the following syntax:

For UNIX

```
IAM_LCM_TOP/patch/bin/iampatchmgr.sh command [-option]
```

For Example:

```
iampatchmgr.sh abort
IAM_LCM_TOP/patch/bin/iampatchmgr.sh progress -all
```

For Windows

```
IAM_LCM_TOP\patch\bin\iampatchmgr.bat command [-options]
```

For Example:

```
IAM_LCM_TOP\patch\bin\iampatchmgr.sh abort
IAM_LCM_TOP\patch\bin\iampatchmgr.sh progress -all
```

See Table 4–4 for a description of the commands that you can use with the `iampatchmgr` utility.

Table 4–4 Oracle Identity and Access Management Patch Manager Commands

Command	Description
`apply`	Starts a patch session where selected patches will be deployed. You must provide the location of the patch top with this command. For example: **For UNIX** *IAM_LCM_TOP*/patch/bin/iampatchmgr.sh apply -patchtop *patchtop_location* **For Windows** *IAM_LCM_TOP*\patch\bin\iampatchmgr.sh apply -patchtop *patchtop_location* For more information, see Section 4.2.2.
`rollback`	Starts a patch session where selected patches will be removed. You must provide the location of the patch top with this command. For example: **For UNIX** *IAM_LCM_TOP*/patch/bin/iampatchmgr.sh rollback -patchtop *patchtop_location* **For Windows** *IAM_LCM_TOP*\patch\bin\iampatchmgr.sh rollback -patchtop *patchtop_location* For more information, see Section 4.6.5.
`abort`	Stops executing a patch session without completing all planned steps. Changes the status of the patch session to `INCOMPLETE`, preventing the Patcher from further execution. For more information, see Section 4.6.3.
`end`	Ends and removes the entire patch session entirely. See Section 4.6.4.
`progress`	Displays the status for an ongoing patch session. For more information, see Section 4.6.1.

Note: To view additional information about any `iampatchmgr` command, use the following syntax:

For UNIX

IAM_LCM_TOP/patch/bin/iampatchmgr.sh *command* -help

For Windows

IAM_LCM_TOP\patch\bin\iampatchmgr.bat *command* -help

Table 4–5 describes the status that you see when you run the `progress` command during a patch session.

Table 4–5 Status of Patch Session

Status	Description
ACTIVE	Session in progress.
FAILED	Session halted due to failure in execution of a step.
ABORTING	Session halted as a result of step aborted by the administrator.
COMPLETE	Session complete.
INCOMPLETE	Failure in step execution or otherwise.

Note: The status `COMPLETE` and `INCOMPLETE` are the terminal states; whereas, `FAILED` and `ABORTING` are recoverable states.

4.3 Applying Patches

The Oracle Identity and Access Management Patcher is a utility that completes the steps for applying patches. It applies product patches to the hosts in a patch session, as listed in the patch plan.

Run the Patcher by executing the following command in the command-line utility:

Note: In ongoing patching, the administrator runs the Patcher to apply patches to an existing deployment. These may be one-off patches related to certain bugs, or security issues, or staged patches for Oracle Identity and Access Management products.

For UNIX

IAM_LCM_TOP/patch/bin/iampatch.sh run

For Windows

IAM_LCM_TOP\patch\bin\iampatch.bat run

The Oracle Identity and Access Management Patcher `run` command performs the following tasks:

- The command validates the existence of a patch session and the availability of one or more steps with the status `PLANNED`, for the host where the tool is running. If such steps exist, then the Patcher proceeds to execute each step as follows:

  - The session status is updated to show that this step is in the status RUNNING.
  - The Patcher determines the command for the step, and invokes it.
  - If invocation is successful, the status for that step changes to COMPLETE and the session is updated.
- Step execution continues until the next step is to be executed on a different host, or execution of a step fails, or until there are no more steps in the plan.
- The next time you run the Patch Manager progress command, its output reflects the outcome of the steps executed.

You can also use the prereq option with this syntax to execute only steps related to prerequisite validation. This does not stop or start services, or apply or rollback patches.

The Patcher writes log messages to the following locations:

While outside of a patch session

LCM_CONFIG/patch/status/log/iampatch.log

While within a patch session

LCM_CONFIG/patch/status/*session_ID*/manager/log/iampatch-session.log

4.4 Applying Artifact Changes

The Oracle Identity and Access Management Lifecycle Tools support the application of post-patch artifact changes, such as adding an entry within a configuration file, invoking a product's MBean, and so on. Most patches do not require such changes. To determine if a particular patch requires changes, see the corresponding README.txt file for that patch.

For patches that require changes, the Patcher automatically executes the changes after you run all the binary patch applications for a single product.

Prerequisites for Applying Artifact Changes

The post-patch artifact changes require additional Perl libraries to perform certain tasks such as connecting to the database and executing sql queries.

Note:

- Ensure that Perl 5 version 5.8.8 or later is present on the system PATH.
- Ensure that the DB.pm module is present within a directory on the list Perl searches when loading modules, obtainable using the array @INC.

  For example, the contents of @INC for a given host can be obtained using the following command:

  ```
  perl -le 'print foreach @INC'
  ```

Artifact Log File

The output of the artifact installation is saved to the following log file:

LCM_CONFIG/patch/status/*session_ID*/hosts/*host_name*/log/*patch_id*-artifactlog

4.5 Alternative Patching Scenarios

The Oracle Identity and Access Management Lifecycle Tools additionally support the following scenarios for applying patches:

- Patching During Deployment
- Patching Disconnected Hosts

4.5.1 Patching During Deployment

Any product patches present within the deployment repository are automatically applied by the Oracle Identity and Access Management Deployment Tool, as the corresponding product is installed and configured.

> **Note:** The deployment repository must not be used for ongoing patching. A separate patchtop directory containing the downloaded patches that need to be applied must be assembled.

The Oracle Identity and Access Management deployment tool invokes the Patcher for installing the post-installation patches, using additional options. These are applicable only to patching during the deployment process. For example, patches are applied before any server instance is configured so that the Deployment Tool can bypass the steps to start or stop servers.

In this release, such options are not supported for ongoing patching.

4.5.2 Patching Disconnected Hosts

You can deploy the Web and Directory tier hosts in network segments different from the network segments containing the primordial host. For example, commonly, the Web tier is deployed to a network DMZ. In this deployment configuration, the shared `LCM_CONFIG` directory that contains information about a patch session might not be available from such hosts. In this case, complete the following steps to run the Oracle Identity and Access Management Patcher on such disconnected hosts:

Generate a patch plan using the Oracle Identity and Access Management Patch Manager `apply` command.

Run the Patcher on non-disconnected hosts using the `run` command.

When the next host on which the plan needs to be executed is disconnected, perform the following steps:

On the primordial host

1. Run the Patch Manager `createhostbundle` command to generate a host bundle containing the latest session information required for executing the Patcher on that specific disconnected host:

   ```
   ./iampatchmgr.sh createhostbundle
   ```

2. On running the progress command, a host bundle is generated in the location *`LCM_CONFIG`*`/patch/status/`*`session_id`*`/hosts/`*`disconnected_host_name`*`/hostbundle-`*`disconnected_host_name`*`.zip`.

The `hostbundle-disconnected_host_name.zip` file contains information about executing the Patcher on the disconnected host.

3. Copy the bundle `hostbundle-disconnected_host_name.zip` to the disconnected host.

On the disconnected host

1. Read the host bundle using the Patcher `readhostbundle` command:

   ```
   ./iampatch.sh readhostbundle -file path_to_the_host_bundle
   ```

2. Run the Patcher using `run` command.
3. After running the Patcher, use the Patcher `createhoststatus` command to generate a host status file that contains the status information resulting from Patcher execution:

   ```
   ./iampatch.sh createhoststatus
   ```

4. The host status is generated in the location *LCM_CONFIG*`/patch/status/`*session_id*`/hosts/`*disconnected_host_name*`/hoststatus-`*disconnected_host_name*`.zip`.
5. Copy the generated status from the disconnected host to the primordial host.

On the primordial host

Read the status using the Patch Manager `readhoststatus` command:

```
./iampatchmgr.sh readhoststatus -file path_to_the_host_status
```

Proceed to execute the Patcher on non-disconnected hosts using the `run` command. If the Patcher prompts you that the next host from which to execute the Patcher is disconnected, repeat the steps listed in this section.

4.6 Monitoring Patch Sessions and Troubleshooting Issues

This section describes how to monitor patch sessions and troubleshoot issues that you might encounter while patching Oracle Identity and Access Management using the Patcher.

It contains the following topics:

- Tracking the Progress of a Patch Session
- Restarting a Failed Step
- Aborting a Patch Session
- Ending a Patch Session
- Rolling Back Patches

4.6.1 Tracking the Progress of a Patch Session

Use the `progress` command to track the state of a patch session. The command displays a configurable report about the patch session.

You can use the option `-all` with the `progress` command to view the complete list of hosts and their status in the patch session.

Run the following command:

On UNIX

```
IAM_LCM_TOP/patch/bin/iampatchmgr.sh progress -all
```

On Windows

```
IAM_LCM_TOP\patch\bin\iampatchmgr.bat progress -all
```

Section A.5 shows a sample report that is displayed when you run the `progress` command.

The `progress` command displays the status of the patch session. Table 4–6 describes the status of the patch steps, and Table 4–7 describes the status of the patch session that you will see when you run the `progress` command.

Options that you can use

Use the verbose option with the `progress` command to get a detailed list of each individual step within the current phase of the patch session. Each step contains the step number so that it can be correlated with the detailed information on each step within the Patch Plan.

Use the `all` option with the `progress` command to get a detailed list of every step within the patch session.

Table 4–6 Status of a Patch Step When the progress Command is Executed

Status	Description
`PLANNED`	Step has not been executed by the Oracle Identity and Access Management Patcher.
`RUNNING`	Step is in the process of being executed by the Patcher.
`COMPLETED`	Step execution successful.
`FAILED`	Step execution failed. See "Restarting a Failed Step".

Table 4–7 Status of a Patch Session When the progress Command is Executed.

Status	Description
`ACTIVE`	Patching in progress.
`FAILED`	Patching halted due to failure of patch step.
`ABORTING`	Patching halted due to abortion of patch step.
`COMPLETE`	Terminal state showing that all steps were executed.
`INCOMPLETE`	Terminal state due to an aborted session either in response to a step execution failure or otherwise.

4.6.2 Restarting a Failed Step

If the patch session shows the status `FAILED` due to a failed execution step, you can attempt to resume session execution from that failed step by using the `retry` command as shown below.

On UNIX

```
IAM_LCM_TOP/patch/bin/iampatch.sh retry
```

On Windows

```
IAM_LCM_TOP\patch/bin\iampatch.bat retry
```

The `retry` command performs the following functions:

- Validates the existence of the patch session with the status FAILED or RUNNING, identifies the step with the status FAILED.

  It also ensures that the failed step needs to be executed from the current host.

- The status of the session is updated to show that this step is in RUNNING status. The overall session status is changed from FAILED to ACTIVE.
- The step that are retried and successful are executed as documented in "Applying Patches".

Use the prereq option with the retry command to run only the prerequisites. This does not stop or start services, or apply and rollback patches.

Run the following command with the prereq option:

On UNIX

```
IAM_LCM_TOP/patch/bin/iampatch.sh retry -prereq
```

On Windows

```
IAM_LCM_TOP\patch\bin\iampatch.bat retry -prereq
```

4.6.3 Aborting a Patch Session

The abort command changes the status of the patch session to INCOMPLETE, preventing the Patcher from further execution.

If the progress command is executed after a session is aborted, details of the session and steps continue to be displayed. If the session that is aborted was in FAILED status, and if it is required to restore some or all products to the status that existed before patching was attempted, the details of the session and steps can be used to assemble the correct patch top directory to be provided to the Patch Manager rollback command.

To abort a patch session, run the following commands:

On UNIX

```
IAM_LCM_TOP/patch/bin/iampatchmgr.sh abort
```

On Windows

```
IAM_LCM_TOP\patch\bin\iampatchmgr.bat abort
```

4.6.4 Ending a Patch Session

You can end a patch session by running the end command. This command removes the patch session entirely.

If the progress command is executed after a session is ended, no report is produced as no session exists. All log files produced during the session are retained, and can be examined to obtain information about the session, if required. To end the session without concern to the current status of session execution, the administrator can use the end command.

To end a patch session, run the following commands:

On UNIX

```
IAM_LCM_TOP/patch/bin/iampatchmgr.sh end
```

On Windows

```
IAM_LCM_TOP\patch\bin\iampatchmgr.bat end
```

4.6.5 Rolling Back Patches

You can create a session to roll back patches that you have applied to the tiers. To roll back patches in the current tier or for tiers to which you have already applied a patch, initiate a new rollback session.

To roll back patches, do the following:

1. Create a patch plan by running the `rollback` command:

   On UNIX

   ```
   IAM_LCM_TOP/patch/bin/iampatchmgr.sh rollback -patchtop patchtop_location
   ```

   On Windows

   ```
   IAM_LCM_TOP\patch\bin\iampatchmgr.bat rollback -patchtop patchtop_location
   ```

2. Run the Patcher as described in Section 4.3.

The `rollback` command performs the following tasks:

- It validates the given patch top location and the existence of the patch session with `ACTIVE` or `FAILED` status. If a session exists, instead of beginning a new session, the output of the current session is displayed.
- If a patch session does not exist, the patch scanner is internally invoked to validate and generate patches from the patch top location provided. This staged patch is internally used to generate the patch plan.
- A patch plan is generated with instructions for rolling back patches, using the topology store information and staged patches.
- The `rollback` command generates an HTML and text format of the patch plan in the following location:

  ```
  LCM_CONFIG/patch/status/session_ID/manager/log/PatchInstructions.html
  LCM_CONFIG/patch/status/session_ID/manager/log/PatchInstructions.text
  ```

- After generating the patch plan, the Patch Manager starts a new patch session with the status `ACTIVE`. It then adds the status `PLANNED` to the step that is being executed on each host, as a subordinate to the patch session. The Patch Manager saves details of the patch session to the log files.
- The `rollback` command generates log files for reference.

A

Automated Patching Screens

This appendix contains screenshots and descriptions of the screens that you see when you run the Oracle Identity and Access Management Lifecycle Tools.

The following screenshots are described:

A.1 Patch Plan: Hosts Listed in the Environment

This figure shows an example of the hosts displayed in the patch plan that is generated when you run the Oracle Identity and Access Management Patch Manager. The plan lists the hosts in the order in which they will be patched, and the components on each host that will be patched.

A.2 Patch Plan: Patch Apply Prerequisite Phase

This figure shows an example of the steps listed in the Patch Apply Prerequisite Phase of a patch plan. It displays the list of steps planned for the hosts in the first phase of patching.

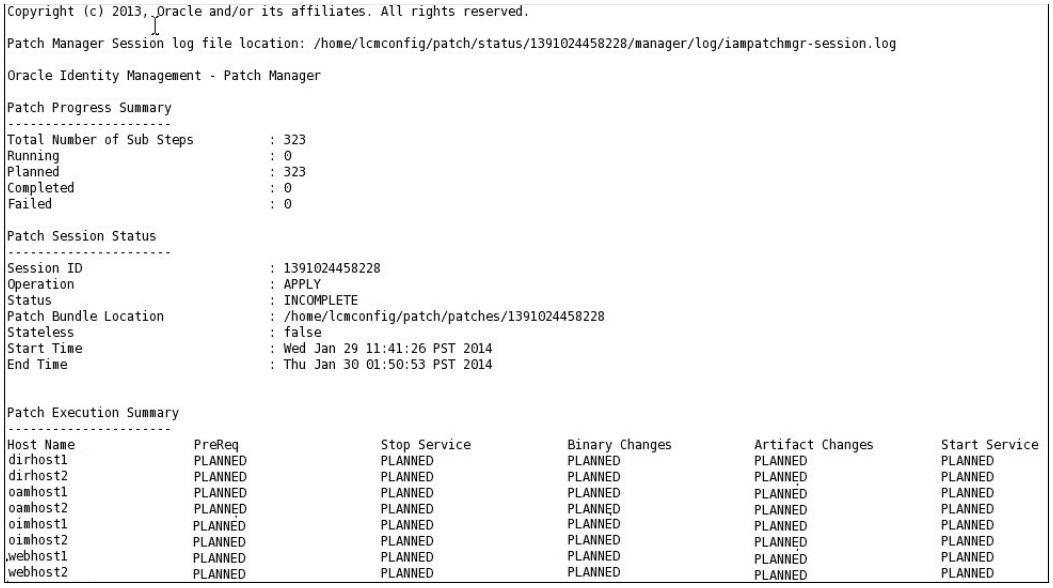
A.3 Patch Plan: Patch Pre-Apply Phase

This figure shows an example of the steps listed in the Patch Pre-Apply Phase of a patch plan. It displays the list of steps planned for the hosts in the second phase of patching.

A.4 Patch Plan: Patch Apply Phase

This figure shows an example of the steps listed in the Patch Apply Phase of a patch plan. It displays the list of steps planned for the hosts in the third phase of patching.

A.5 Sample Report of progress Command



```
Copyright (c) 2013, Oracle and/or its affiliates. All rights reserved.

Patch Manager Session log file location: /home/lcmconfig/patch/status/1391024458228/manager/log/iampatchmgr-session.log

Oracle Identity Management - Patch Manager

Patch Progress Summary
----------------------
Total Number of Sub Steps          : 323
Running                            : 0
Planned                            : 323
Completed                          : 0
Failed                             : 0

Patch Session Status
----------------------
Session ID                         : 1391024458228
Operation                          : APPLY
Status                             : INCOMPLETE
Patch Bundle Location              : /home/lcmconfig/patch/patches/1391024458228
Stateless                          : false
Start Time                         : Wed Jan 29 11:41:26 PST 2014
End Time                           : Thu Jan 30 01:50:53 PST 2014


Patch Execution Summary
----------------------
Host Name               PreReq                  Stop Service            Binary Changes          Artifact Changes        Start Service
dirhost1                PLANNED                 PLANNED                 PLANNED                 PLANNED                 PLANNED
dirhost2                PLANNED                 PLANNED                 PLANNED                 PLANNED                 PLANNED
oamhost1                PLANNED                 PLANNED                 PLANNED                 PLANNED                 PLANNED
oamhost2                PLANNED                 PLANNED                 PLANNED                 PLANNED                 PLANNED
oimhost1                PLANNED                 PLANNED                 PLANNED                 PLANNED                 PLANNED
oimhost2                PLANNED                 PLANNED                 PLANNED                 PLANNED                 PLANNED
webhost1                PLANNED                 PLANNED                 PLANNED                 PLANNED                 PLANNED
webhost2                PLANNED                 PLANNED                 PLANNED                 PLANNED                 PLANNED
```

This figure shows a sample report that is displayed when you run the `progress` command with the `-all` option.