

HP Database and Middleware Automation

DB Compliance Solution Pack

for the HP-UX, IBM AIX, Red Hat Enterprise Linux, Solaris, and Windows® operating systems

Software version: 9.10

User Guide



Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2011 Hewlett-Packard Development Company, L.P.

Trademark Notices

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Windows is a U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<http://h20230.www2.hp.com/selfsolve/manuals>

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport user ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

1	Introduction	6
	Audience	6
	About the DB Compliance Solution Pack	6
	How this Solution Pack is Organized	6
	Prerequisites	9
	Supported Platforms	9
	Additional resources	10
2	Quick Start	11
	Install the Solution Pack	11
	Create a Deployable Workflow	12
	Create a Deployment	12
	Run Your Workflow	13
	View the Results	14
	View the Dashboard	14
3	Customizing this Solution	15
	Customizing Either Workflow	15
	Configure Excluded Checks	15
	Find the Names of the Checks to Exclude	16
	Exclude Specific Checks in a Deployment	16
	Configure a Policy to Exclude Specific Checks	17
	Add a New Compliance Check	18
	Customizing the Check Oracle Compliance Workflow	18
	Change the Method of Specifying ORACLE_HOME	18
	Enable the datapal User to Become the Server Superuser	19
	Customizing the Check SQL Server Compliance Workflow	20
	Enable the datapal User to Access the SQL Server	20
	Specify the Virtual Server Name in a SQL Server Cluster	21
4	Troubleshooting	22
	Database Connectivity Issues	22
	Test Ports and Firewalls	22
	Check Target Type	23
	User Permissions and Related Requirements	23
	Agent Discovery in HP Server Automation	23
A	Reference Information	24
B	Using this Solution with HP Server Automation	26

1 Introduction

This document describes the HP Database and Middleware Automation (HP DMA) DB Compliance solution pack, a collection of tools that you can use to automate and simplify the process of bringing your environment into compliance with specific database security standards.

This solution can be used with the following HP products:

- HP Database and Middleware Automation version 1.00 (or later)
- HP Server Automation version 9.02 (or later)

Audience

This solution is designed for database engineers who are responsible for establishing and maintaining database security processes. In most cases, a mandate has been delivered by the security team to bring the environment into compliance with specific standards and benchmarks. It is typically the database engineer's responsibility to ensure that this happens.

To use this solution, you should be familiar with the Center for Internet Security (CIS) benchmarks for Oracle databases and SQL Server environments. You should also be familiar with the terms used in those benchmarks (see [Appendix A, Reference Information](#)).

About the DB Compliance Solution Pack

This solution pack enables you to audit Oracle database instances and SQL Server instances in your enterprise for compliance with the following CIS benchmarks:

- Oracle 9i/10g version 2.01 (April, 2005)
- Oracle Database Server 11g version 1.0.1 (January 2009)
- Microsoft SQL Server 2005 version 1.2.0 (January 2010)

These benchmarks document the settings and procedures required for the secure installation, configuration, and operation of each database environment. By bringing your environment into compliance with these benchmarks, you can better protect it from related threats.

How this Solution Pack is Organized

This solution pack contains two workflow templates: Check Oracle Compliance and Check SQL Server Compliance. These workflows contain a collection of steps that are assembled in a specific operational flow (see [Figure 1](#) and [Figure 2](#)).

Figure 1 Check Oracle Compliance Workflow Template

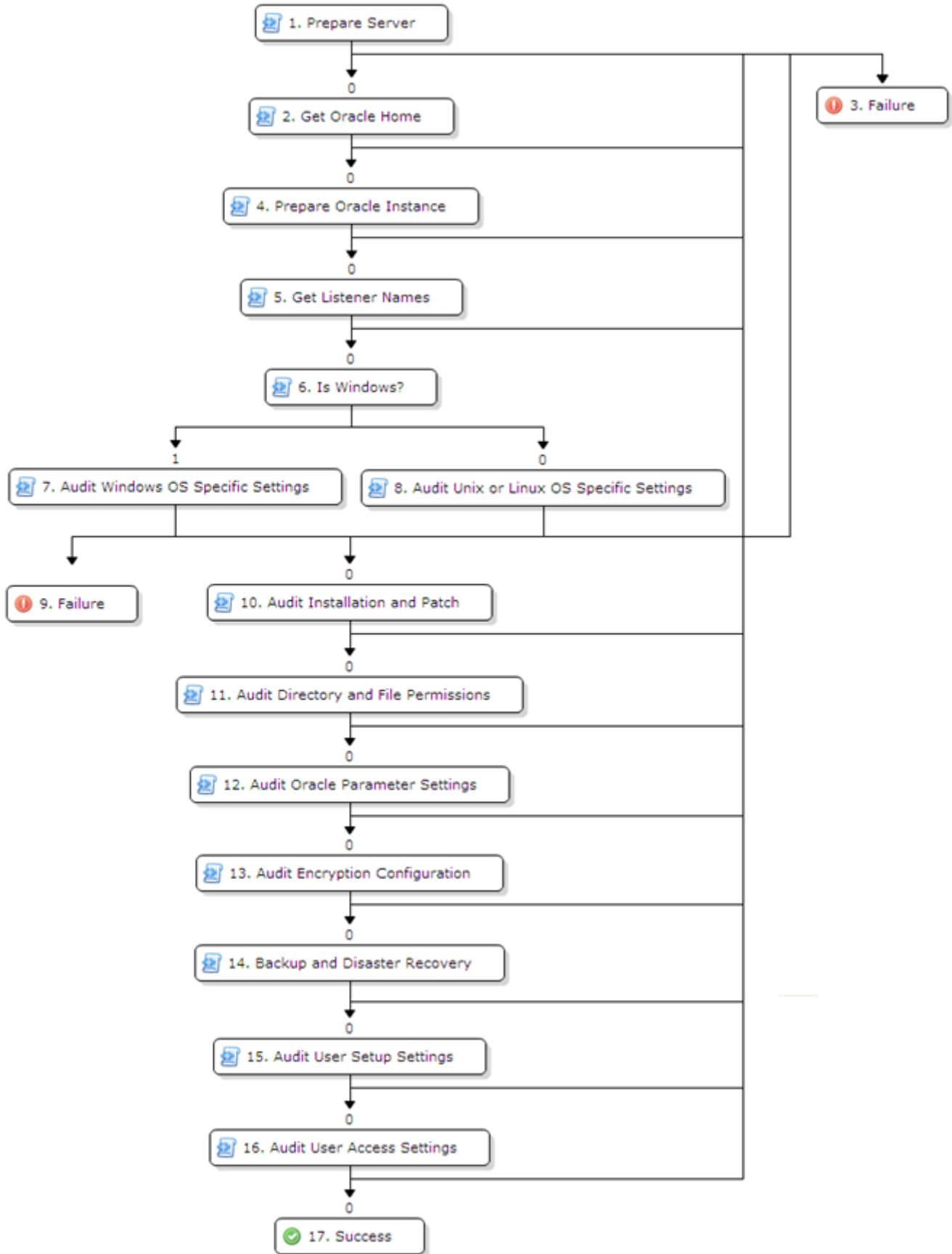
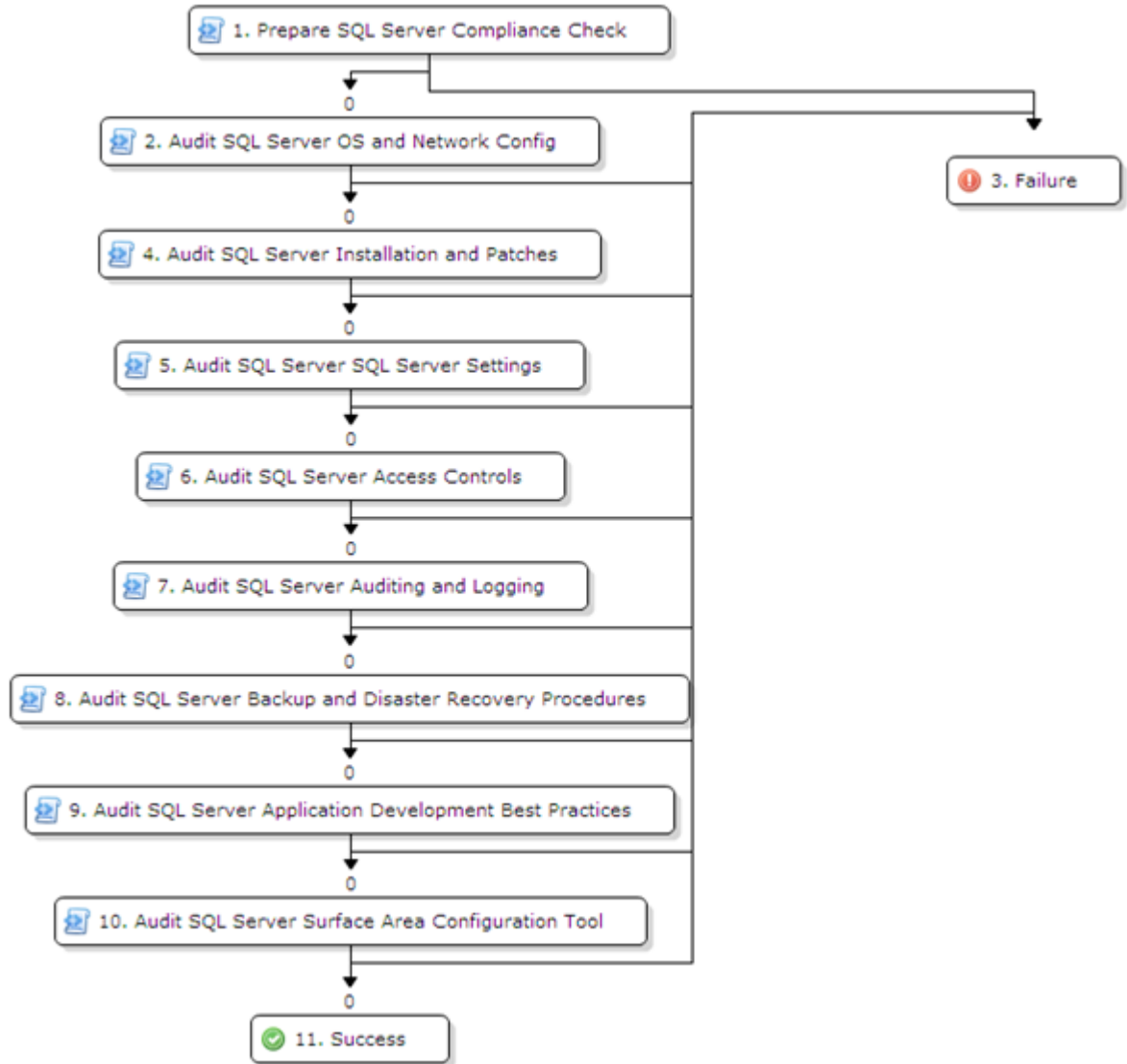


Figure 2 Check SQL Server Compliance Workflow Template



Each step in the workflow performs a unit of work—in this case, gathering information about the Oracle database or SQL Server instance and then performing a group of compliance checks.

Each step is documented in detail. For example, [Figure 3](#) shows the step documentation for the Audit Unix or Linux OS Specific Settings step in the Check Oracle Compliance workflow.

Figure 3 Example of Step Documentation

Documentation

Description:

Audits the UNIX/Linux related scorable recommendations in Section 1, Operating System Specific Settings, of the CIS Security Benchmarks for Oracle 9i/10g and Oracle Database Server 11g.

Dependencies: None

Input Parameters:

- Excluded Checks = Checks to exclude from this portion of the compliance audit
- Oracle Group = The Oracle group used for the ORACLE_HOME installation
- Oracle Home = The fully qualified name of the ORACLE_HOME for this instance
- Oracle User = The OS owner of the ORACLE_HOME
- Oracle Version = The version of SQLPlus from the ORACLE_HOME
- Server Wrapper = String to execute routine as server superuser (by default, sudo su - root /opt/datapalette/jython/jython)

Output Parameters: None

Return Code:

- 0 = Step ran successfully
- 1 = Step failed

▶ Workflow templates and steps are locked in the solution pack. To customize a workflow or a step, you must first create a copy of the workflow template and then modify your copy.

Prerequisites

HP Database and Middleware Automation (or HP Server Automation) must be installed and properly configured before you can use this solution pack.

Supported Platforms

The Check Oracle Compliance workflow can be used to audit instances of Oracle database versions 10g and 11g. Versions 10.2, 11.1, and 11.2 were explicitly tested.

The Check SQL Server Compliance workflow can be used to audit instances of SQL Server 2005, 2008, and 2008 R2. Versions 2005 and 2008 R2 were explicitly tested.

For hardware and operating system requirements, refer to the *HP Database and Middleware Automation Installation Guide*.

If you are using HP DMA in the context of HP Server Automation, refer to the *HP Server Automation Platform Support Matrix*.

Additional resources

For additional information, refer to the following documents:

HP Database and Middleware Automation User Guide

HP Database and Middleware Automation Installation Guide

If you are using HP Server Automation, also refer to these documents:

HP Server Automation Integration Guide

HP Server Automation Application Deployment User Guide

2 Quick Start

This chapter shows you how to install and deploy the HP DMA DB Compliance solution pack and run a database compliance audit in your environment. There are five basic steps:

- [Install the Solution Pack](#)
- [Create a Deployable Workflow](#)
- [Run Your Workflow](#)
- [View the Results](#)
- [View the Dashboard](#)

➤ This chapter presents the simplest method that you can use to run an Oracle database or SQL Server compliance audit. HP DMA provides tools and mechanisms that you can then use to customize this solution for your environment. For more information, see [Customizing this Solution](#) on page 15.

➤ The information presented in this chapter assumes the following:

- HP DMA is installed and operational.
- For the Check Oracle Compliance workflow, at least one target Oracle database instance is available.
- For the Check SQL Server Compliance workflow, at least one target SQL Server instance is available.

For more information, see “Environment” in the *HP Database and Middleware Automation User Guide*.

Install the Solution Pack

The following instructions assume that you have purchased the HP DMA DB Compliance solution pack.

To install the solution pack:

- 1 Using the instructions in your purchase agreement, download the solution pack ISO file, and extract the HP_SA_DB_Comp_SolPk 9.10.zip file.
- 2 On the system where you downloaded the solution pack, open a web browser, and log in to the HP DMA server using an account with administrator privileges.

For instructions, see “Getting Started” in the *HP Database and Middleware Automation User Guide*.

- 3 On the Solutions > Available or Solutions > Installed tab, click the **Browse** button in the lower right corner. The Choose File dialog opens.
- 4 Browse to and select the HP_SA_DB_Comp_SolPk 9.10.zip file, and click **Open**.
- 5 Click **Import solution pack**.

To view the installed solution, go to the Solutions > Installed tab.



Subsequent topics in this chapter assume that you have logged in to the HP DMA server.

Create a Deployable Workflow

The workflow templates provided by HP in your solution pack cannot be deployed. To use them, you must first create your own copies.

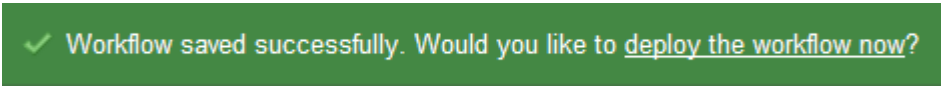
To create a deployable copy of the workflow template:

- 1 In the HP DMA web interface, go to the Automation > Workflows area.
- 2 From the list of workflows, select either the Check Oracle Compliance or the Check SQL Server Compliance workflow template.
- 3 Click the **Copy** button in the lower left corner.
- 4 On the Documentation tab, specify the following:

Name	Name that will appear in the list of available workflows
Tags	Keywords that you can use later to search for this workflow (optional)
Type	Must be Oracle or SQL Server
Target level	Must be Instance

- 5 Click **Save**.

Your new workflow now appears in the list of available workflows, and the following message is displayed:



✓ Workflow saved successfully. Would you like to [deploy the workflow now?](#)

- 6 Click the **deploy the workflow now** link in the green message area.

For more information about creating and working with workflows, refer to “Workflows” in the *HP Database and Middleware Automation User Guide*.

Create a Deployment

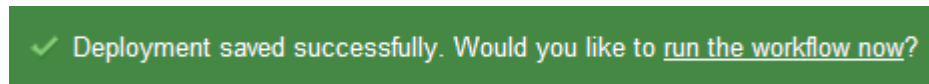
Before you can run your new workflow, you must create a deployment. A deployment associates a workflow with one or more specific targets (in this case, Oracle database or SQL Server instances).

To create a deployment:

- 1 If you do not see the green message bar—for example, if you navigated to another page after you created your copy of the workflow template—follow these steps:
 - a Go to the Automation > Deployments area.
 - b In the lower right corner, click **New deployment**.
- 2 Specify the following:

Name	Name that will appear in the list of available deployments.
Workflow	From the drop-down list, select the workflow that you just created.
Schedule	Frequency with which the workflow will run. If you select None, the workflow will run only once when you explicitly tell it to run.
- 3 From the list of AVAILABLE instances on the left side of the Targets area, add the instances where the workflow will run:
 - To add an individual instance, click the **ADD** link for that instance.
 - To add all the instances on a particular server, click the **ADD ALL** link for that server.Any instances that you add appear in the SELECTED list on the right side.
- 4 Click **Save**.

Your new deployment now appears in the list of available workflows, and the following message is displayed:



- 5 Click the **run the workflow now** link in the green message area.

Run Your Workflow

Now you are ready to run your workflow against all the instances that you selected.

To run the workflow:

- 1 If you do not see the green message bar—for example, if you navigated to another page after you created your deployment—follow these steps:
 - a Go to the Automation > Run area.
 - b In the list of WORKFLOWS on the left side, select the workflow that you created.
 - c In the list of DEPLOYMENTS in the center, double-click the deployment that you just created.
- 2 In the list of targets on the left side, select the check box for each target where you want to run the workflow.
- 3 In the lower right corner of the Run Workflow page, click the **Run workflow** button.

The following message is displayed.

✓ Workflow started successfully. For status, see the [console](#) or [history](#).

To view the progress of your deployment, click the **console** link in the green message area.

View the Results

While your workflow is running, you can watch its progress on the Console page.

To view the progress of the workflow as the deployment proceeds, click the workflow name in the upper box on the Console page.

To view the outcome of a specific step, select that step in the left box in the Output area. Informational messages are displayed in the right box, and the values of any output parameters are listed.

While the workflow is running, its status indicator on the Console says **RUNNING**. After the workflow finishes, its status indicator changes to **SUCCESS**, **FAILURE**, or **COMPLETE**.

You can then view a summary of your deployment on the History page. This page lists all the deployments that have run on this HP DMA server during the time period specified in the Filter box.



While the workflow is running, the History page shows nothing in the status column. A workflow that results in the **COMPLETE** state also shows nothing in the status column on the History page.

To view step-by-step results, select the row in the table that corresponds to your deployment. The tabs below the table show you information about each step in the workflow. This includes the start and end time for each step, the exit code, and the following information:

- Output tab – any informational messages that were produced
- Errors tab – any errors that were reported
- Header tab – values assigned to any output parameters

View the Dashboard

You can also use the Dashboard to view a summary of automation activity over the last 30 days. Click **Database & Middleware Automation** in the title bar to open the Dashboard.

3 Customizing this Solution

This chapter shows you how you can customize the DB Compliance solution for your environment. The topics are grouped as follows:

- [Customizing Either Workflow](#) on page 15
- [Customizing the Check Oracle Compliance Workflow](#) on page 18
- [Customizing the Check SQL Server Compliance Workflow](#) on page 20



The information presented in this chapter assumes the following:

- HP DMA is installed and operational.
- At least one target Oracle database instance or SQL Server instance is available. For more information, see “Environment” in the *HP Database and Middleware Automation User Guide*.
- You are logged in to the HP DMA web interface using an account with Administrator privileges.
- You have successfully run a copy of the Check Oracle Compliance workflow template against at least one target instance in your environment (see [Quick Start](#) on page 11 for instructions).

Customizing Either Workflow

The following topics pertain to both the Check Oracle Compliance workflow and the Check SQL Server Compliance workflow:

- [Configure Excluded Checks](#) on page 15
- [Add a New Compliance Check](#) on page 18

Configure Excluded Checks

It is likely that you will not want to perform the checks included in the Check Oracle Compliance workflow. You can instruct HP DMA to exclude any of these checks. There are two ways to do this:

- Specify the excluded checks in the deployment.
- Configure a policy that specifies the excluded checks, and then associate that policy with your targets.

The first method is simpler, but it requires you to specify the excluded checks each time that you create a new deployment. The second method enables you to specify the excluded checks once and then use this information for all future deployments.

For both methods, you must first find the name of each check that you want to exclude.

Find the Names of the Checks to Exclude

In order to exclude a check, you must know exactly what it is called. After you successfully run a workflow against at least one target, you can view a list of all the checks performed by that workflow.

To list the checks performed:

- 1 Go to the Environments area.
- 2 In the left column, select the environment where your target server resides.
- 3 In the next column, select the server.
- 4 In the next column, double-click the Oracle instance where you ran the workflow.
- 5 Go to the Custom Fields tab. The names of all checks performed by this workflow are shown in the following format: workflow:step:check

For example, here are the checks performed by the Backup and Disaster Recovery step:

```
oracle compliance:  
backup and recovery:  
  archive log files:  
  
oracle compliance:  
backup and recovery:  
  archive log space:  
  
oracle compliance:  
backup and recovery:  
  multiple log files:  
  
oracle compliance:  
backup and recovery:  
multiplex control files:  
  
oracle compliance:  
backup and recovery:  
multiplex online log files:
```

You can copy these names and then paste them into the appropriate fields in the deployment or policy specification. Alternatively, you can copy the check names from the Console page after you run the workflow.

Exclude Specific Checks in a Deployment

The procedure shows you how to specify excluded checks for a particular deployment.

To exclude checks for a deployment:

- 1 In a separate browser window or tab, go to the Automation > Deployments area.
- 2 From the list of deployments, select a deployment that uses your copy of the Check Oracle Compliance workflow.
- 3 Go to the Parameters tab.
- 4 For each check that you want to exclude, follow these steps:

- a Locate the step that contains that check.
- b Paste the step: check portion of the check name (see [Find the Names of the Checks to Exclude](#) on page 16) into the Excluded Checks box.
- c To exclude multiple checks for a single step, separate the check names with commas. For example:

Audit Encryption Configuration

Excluded Checks: Encryption: FIPS 140 Compliance, Encryption: SHA1

The list of checks to be skipped during this compliance check.

- 5 Click the **Save** button in the lower right corner.

When you run the workflow, the Console will show which checks were excluded. For the example shown here, the Console output is:

```
[INFO]: Auditing Oracle Encryption
-----<HEADER START>-----
Instance.Oracle Compliance: Encryption: Client Server Encryption Type = Pass
Instance.Oracle Compliance: Encryption: Client Server Integrity Check = Pass
Instance.Oracle Compliance: Encryption: DBMS Obfuscation Toolkit = Pass
Instance.Oracle Compliance: Encryption: Encryption Client = Pass
Instance.Oracle Compliance: Encryption: Encryption Server = Pass
Instance.Oracle Compliance: Encryption: FIPS 140 Compliance =
Instance.Oracle Compliance: Encryption: SHA1 =
Instance.Oracle Compliance: Encryption: SQLNet Crypto Seed = Pass
Instance.Oracle Compliance: Encryption: SSL Cipher Suite = Pass
Instance.Oracle Compliance: Encryption: SSL Client Authentication = Pass
Instance.Oracle Compliance: Encryption: SSL Server Cert = Pass
Instance.Oracle Compliance: Encryption: SSL Version = Pass
Instance.Oracle Compliance: Encryption: Server Encryption Type = Pass
-----<HEADER STOP>-----
```

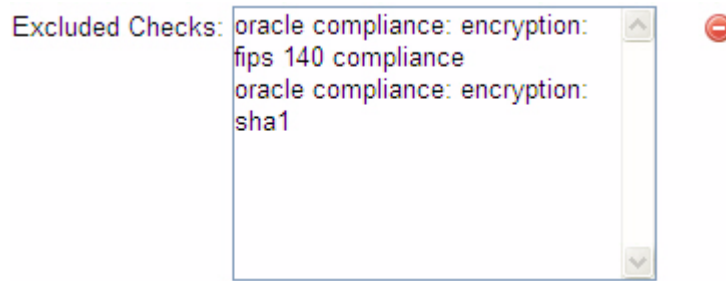
Configure a Policy to Exclude Specific Checks

This procedure shows you how to create and configure a policy to exclude specific checks. Policies are reusable sets of attributes that can be assigned to organizations, servers, instances, or databases. For more information about policies, refer to “Policies” in the *HP Database and Middleware Automation User Guide*.

This approach enables you to specify the excluded checks once and assign them to any or all of your servers.

To create and configure a policy to exclude specific checks:

- 1 In the HP DMA web interface, go to the Automation > Policies area.
- 2 In the lower right corner, click **New policy**.
- 3 Under Properties, enter a Name for your policy.
- 4 Under Attributes, select **List** from the drop-down menu.
- 5 In the text box to the right of the drop-down menu, type Excluded Checks.
- 6 Click **Add**.
- 7 Paste the full name of each check that you want to exclude into the Excluded Checks box (see [Find the Names of the Checks to Exclude](#) on page 16). For example:



- 8 Go to the Usage tab.
- 9 Select **Servers** from the drop-down list.
- 10 Click the **ADD** link for each server to which you want to assign this policy.
- 11 Click the **Save** button in the lower right corner.

Add a New Compliance Check

If you want to add checks that go beyond the scope of the CIS benchmarks, you can write your own steps and functions to do this. Refer to the *HP Database and Middleware Automation Developer Training* for more information.

Customizing the Check Oracle Compliance Workflow

The following topics pertain only to the Check Oracle Compliance workflow:

- [Change the Method of Specifying ORACLE_HOME](#) on page 18
- [Enable the datapal User to Become the Server Superuser](#) on page 19

Change the Method of Specifying ORACLE_HOME

The Check Oracle Compliance workflow template includes a step called Get Oracle Home. This step determines the value of ORACLE_HOME by examining one of the following sources:

- The `/etc/oratab` or `/var/opt/oracle/oratab` file on UNIX targets
- The registry on Windows targets

You may prefer to provide the value of ORACLE_HOME at deployment time or run time—or you may have access to previously discovered metadata that contains this value. You can facilitate this by carefully removing the Get Oracle Home step from your copy of the workflow.



Basic instructions are provided here. For additional information, refer to “Steps” and “Understanding Parameters” in the *HP Database and Middleware Automation User Guide*.



If you have already deployed your copy of the workflow, you will also need to update any existing deployments to reflect these changes.

To remove the Get Oracle Home step from your workflow:

- 1 Go to the Automation > Workflows area.
- 2 From the list of workflows, select your copy of the Check Oracle Compliance workflow.

- 3 Go to the Workflow tab.
Steps 4, 9, and 10 pertain to the table of steps below the workflow diagram.
- 4 In the Next column for the Prepare Server step, add the number of the step after the “Get Oracle Home” step. By default, the new numbers for Prepare Server should be 2, 3, 4.
- 5 Press **Enter**.
Wait until your updated numbers are visible (this operation may take a moment).
- 6 Click the **Save** button in the lower right corner.
- 7 From the list of workflows, select your copy of the Check Oracle Compliance workflow.
- 8 Go to the Workflow tab.
- 9 For the Get Oracle Home step, click the  (Remove) button.
When the removal operation is completed, the Get Oracle Home step will no longer be visible in the workflow diagram or the table of steps. Next, you must specify an alternate source of ORACLE_HOME.
- 10 Click the  (Toggle) button to the left of the Prepare Oracle Instance step. This exposes the input parameters for this step.
 - To specify ORACLE_HOME at deployment time or run time, select **- User Selected -** in the drop-down list for the Oracle Home parameter.
To specify ORACLE_HOME at run time, you must also select **Enter at runtime** when you create the deployment.
 - To retrieve the value of ORACLE_HOME from metadata, select the pertinent metadata field (typically **Instance.oracle home**) from the drop-down list for the Oracle Home parameter.
- 11 Click the **Save** button again.

Enable the datapal User to Become the Server Superuser

By default, the HP DMA agent runs as the “datapal” user on your target servers. Some checks included in this solution, however, must be executed by the server superuser.

Therefore, you must specify a mechanism by which the datapal user can become the server superuser. Here are two such mechanisms:

```
sudo su -root /opt/datapalette/jython/jython
ssh root@localhost /opt/datapalette/jython/jython
```

This mechanism is specified in the Server Wrapper parameter. The value of this parameter is derived during the Prepare Server step based on the values of the following two server level custom fields:

Properties
Custom Fields
Policies
Interfaces

Custom fields
[NEW CUSTOM FIELD](#)

become routine:

become user:

To change the Server Wrapper:

- 1 In the HP DMA web interface, go to the Environment > Dashboard area.
- 2 In the left column, select the organization that you want to work with.
- 3 For each server where you want to change the Server Wrapper, follow these steps:
 - a Double-click the server name.
 - b Go to the Custom Fields tab.
 - c Specify the **become routine** and **become user** values that you want to use. For example:

Custom fields [NEW CUSTOM FIELD](#)

become routine:

become user:

- 4 Click the **Save** button in the lower right corner.



As an alternative, you could run the HP DMA agent as the server superuser. This, however, would require you to log on to each target server and start (or restart) the agent using the `datapal` command.

Customizing the Check SQL Server Compliance Workflow

The following topics pertain only to the Check SQL Server Compliance workflow:

- [Enable the datapal User to Access the SQL Server](#) on page 20
- [Specify the Virtual Server Name in a SQL Server Cluster](#) on page 21

Enable the datapal User to Access the SQL Server

The “datapal” user is the Windows account that starts the HP DMA Agent service on a target server. This user must have the following capabilities on the target server:

- Execute permissions on the following tools:
 - `reg.exe` (the Windows Server command-line registry tool)
 - `wmic.exe` (the Windows Management Instrumentation command-line tool)
 - Windows “net” utilities (included in the base Windows Server installation)
- Windows-authenticated login permissions into the SQL Server instance.
- Upon connecting to the SQL Server instance, the datapal user must have read permissions on the following system tables:
 - `master.dbo.syslogins`
 - `master.dbo.sysusers`
 - `master.sys.linked_logins`
 - `master.sys.servers`

- master.sys.server_principals
- msdb.dbo.backupset
- master.dbo.sysdatabases
- msdb.dbo.backupmediafamily
- master.dbo.sysaltfiles
- master.sys.all_objects
- <database>.sys.objects
- <database>.sys.comments

The datapal user must also have execute permissions on the following system procedures:

- master.dbo.sp_MSforeachdb
- master.dbo.sp_configure



The Windows or domain user who starts the HP DMA Agent service (usually “datapal”) must have the permissions listed here.

Specify the Virtual Server Name in a SQL Server Cluster

In a SQL Server cluster environment, the Check SQL Compliance workflow should determine the host name of any virtual server in a cluster where a SQL Server instance resides. If you suspect that this name is not correct, you can specify it on the Environment page.

To specify the virtual server name in a SQL Server cluster environment:

- 1 Go to the Environments area.
- 2 In the left column, select the environment that includes your SQL Server cluster.
- 3 In the next column, select the pertinent cluster node.
- 4 In the next column, double-click the SQL Server instance where you want to run the workflow.
- 5 Go to the Properties tab.
- 6 In the Host box under Connection, specify the virtual server name where this instance resides.

4 Troubleshooting

The following topics can help you address problems that might occur when you install and run the workflows in this solution pack:

- [Database Connectivity Issues](#) on page 22
- [User Permissions and Related Requirements](#) on page 23
- [Agent Discovery in HP Server Automation](#) on page 23

For additional information, refer to the “Troubleshooting” chapter in the *HP Database and Middleware Automation Installation Guide*.

Database Connectivity Issues

In order to run workflows on targets (servers, instances, or databases), your HP DMA server must be able to connect to and communicate with those targets. If steps in the workflows are failing due to connectivity problems, check the following items:

- [Test Ports and Firewalls](#) on page 22
- [Check Target Type](#) on page 23

Test Ports and Firewalls

Make sure that all pertinent ports are open and any firewalls (hardware or software) in your environment are configured to allow communication between the HP DMA server and the target devices.

To test ports and firewalls:

- 1 On the target machine, log in as the “datapal” user.
- 2 Run the `telnet` command:

```
telnet <IP address> <port>
```

Use the IP Address of the HP DMA server. For example, if the HP DMA server is listening on port 1124, the command would be:

```
telnet 172.68.24.10 1124
```

If you run this command and `telnet` hangs, you will receive a connection error. This error indicates that your firewall is blocking the port.

On UNIX, if `telnet` replies with the escape sequence, then you know you are logged in.

On Windows, `telnet` clears the screen.

If `telnet` cannot connect to the HP DMA server, the agents on the target servers will not be able to connect either.

Check Target Type

In your deployment, make sure that you have specified the correct type of target. The workflow type and the target type must match. A workflow designed to run against an instance target, for example, cannot run against a server target.

User Permissions and Related Requirements

Roles define access (Read or Write) permissions for organizations, workflows, steps, policies, rules, and deployments. Deployments have an extra permission: Execute. Users are assigned to roles and gain access to these items according to the permissions defined for their roles.

Roles can be defined in one of two ways: native or LDAP groups.

- Native roles define groups of HP DMA users in the repository.
- LDAP groups are retrieved from the LDAP server configured in the Setup > Expert Engine area. No user information is stored in the repository for LDAP groups. This allows you to use your corporate directory for defining users and their permissions making security audits easier.

Make sure that the HP DMA users in your environment are assigned roles that grant them the permissions they need to accomplish their tasks. For example:

- To view a workflow, your role must have Read permission for that workflow.
- To view a deployment, your role must have Read permission for that deployment.
- To edit a workflow, your role must have Write permission for that workflow.
- To run a deployment, your role must have Execute permission for that deployment.

Permissions determine what features and functions are available and active in the HP DMA UI. For a detailed breakdown, see the *HP Database and Middleware Automation User Guide*.



Permissions work differently in HP Server Automation. Refer to the *HP Server Automation: Database and Middleware Automation Guide* for more information.

Agent Discovery in HP Server Automation

HP DMA uses a process called “discovery” to find information about the server, network, and database instances on a target machine.

In HP DMA, discovery is automatically activated when an Agent is started on a target machine.

In HP Server Automation, you must explicitly initiate the process of discovery—it is not automatic. Refer to the *HP Server Automation: Database and Middleware Automation Guide* for instructions.

A Reference Information

This solution implements the following Computer Information Security (CIS) benchmarks:

http://www.cisecurity.org/tools2/oracle/CIS_Oracle_Benchmark_v2.01.pdf

http://www.cisecurity.org/tools2/oracle/CIS_Oracle_11g_Benchmark_v1.0.1.pdf

https://www.cisecurity.org/tools2/sqlserver/CIS_SQL2005_Benchmark_v1.2.0.pdf

The following tables show how the workflows included in this solution automate the categories and individual items specified in these benchmarks.

Table 1 Mapping of Check Oracle Compliance Steps to CIS Benchmarks

Steps	Oracle 10g Benchmark	Oracle 11g Benchmark
Prepare Server	These steps prepare the server and gather the information required to perform the audit.	
Get Oracle Home		
Prepare Oracle Instance		
Get Listener Name		
Is Windows?		
Audit Unix or Linux OS Specific Settings	1.19 – 1.20	1.13, 1.14
Audit Windows OS Specific Settings	1.01– 1.04	1.01
Audit Installation and Patch	2.02 – 2.10, 2.12 – 2.13	2.04 – 2.11, 2.13 – 2.14
Audit Directory and File Permissions	3.01 – 3.31	3.01 – 3.26
Audit Oracle Parameter Settings	4.01 – 4.22, 4.25 – 4.28	4.01 – 4.20, 4.23 – 4.43
Audit Encryption Configuration	5.02 – 5.09, 5.16 – 5.19, 5.24	5.02 – 5.06, 5.13 – 5.16, 5.21, 5.24 – 5.26
Backup and Disaster Recovery	7.02, 7.04 – 7.06	7.02, 7.04 – 7.06
Audit User Setup Settings	8.01 – 8.14	8.01 – 8.14
Audit User Access Settings	9.01 – 9.20, 9.22 – 9.24, 9.26 – 9.50, 9.55 – 9.56, 9.58 – 9.59	9.01 – 9.20, 9.22 – 9.24, 9.26 – 9.49, 9.52, 9.54 – 9.56
Success	These steps pertain to the deployment of the workflow. They do not pertain to the audit.	
Failure		

Table 2 Mapping of Check SQL Server Compliance Steps to CIS Benchmarks

Steps	SQL Server 2005 Benchmark
Prepare SQL Server Compliance Check	This step prepares the server and gathers the information required to perform the audit.
Audit SQL Server OS and Network Config	1.5, 1.8.1, 1.8.3, 1.8.4, 1.9, 1.12, 1.19.3
Audit SQL Server Installation and Patches	2.1 – 2.4, 2.6 – 2.7, 2.9 – 2.12
Audit SQL Server SQL Server Settings	3.1, 3.2 (except 3.2.6 and 3.2.7, which are not scorable), 3.3 – 3.10, 3.16 – 3.17
Audit SQL Server Access Controls	4.1, 4.2, 4.4, 4.5, 4.7, 4.9, 4.22, 4.24
Audit SQL Server Auditing and Logging	5.2, 5.3
Audit SQL Server Backup and Disaster Recovery Procedures	6.3, 6.5, 6.6
Audit SQL Server Application Development Best Practices	8.1, 8.3, 8.9, 8.10
Audit SQL Server Surface Area Configuration Tool	9.1 – 9.4, 9.6, 9.8 – 9.10
Success	These steps pertain to the deployment of the workflow. They do not pertain to the audit.
Failure	

B Using this Solution with HP Server Automation

The information contained in this guide pertains to HP Database and Middleware Automation version 1.00, which is compatible with HP Server Automation version 9.02.

For information about running HP DMA workflows from HP Server Automation, refer to the *HP Server Automation Application Deployment User Guide* (version 9.02 and later).

This appendix will be updated when HP Server Automation version 9.10 is available.