Oracle® Advanced Support Gateway

User's Guide

Release 14.x

F24159-03

June 2021

ORACLE

Oracle Advanced Support Gateway User’s Guide, Release 14.x

F24159-03

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface 7

Audience 7
Related Documentation 7
Getting Help 8
Documentation Accessibility 8

About this Release of Oracle Advanced Support Gateway 9

What's New in the Oracle Advanced Support Gateway 14.3.1 Release 9
Platinum Patching 9
What's New in the Oracle Advanced Support Gateway 14.2 Release 10
Platinum Patching 10
Adding ZDLRA System 11
Usability Enhancements 11
What's New in the Oracle Advanced Support Gateway 14.1 Release 12
User Guide Revision History 15

1 About the Oracle Advanced Support Gateway User Interface

Logging onto the Gateway 1-1
About the Gateway User Interface 1-1
About the Navigation Menu 1-2
About the My Services Menu 1-3
Selecting a Service 1-3
Selecting a Service Feature 1-3
About the Dashboard Menu 1-4
Reviewing and Filtering Information 1-5
About the Gateway Menu 1-5
About the Admin Menu 1-6
Viewing Legal and Copyright Information 1-6

2 Using Dashboards

About Dashboards 2-1
Accessing the Dashboard 2-2
About Widgets 2-2
Adding a Dashboard 2-4
Adding a Widget 2-5
Managing Widgets 2-5
Removing a Widget from a Dashboard 2-6
Configuring a Widget 2-6
Reviewing Information about a Widget 2-6

3 Managing the User List

About User Management 3-1
Managing Users 3-1
Viewing Users 3-1
Adding Users 3-2
Activating Users 3-3
Updating Users 3-4
Deleting Users 3-5
Resetting User Passwords 3-5

4 Managing Credentials and Passwords

About Credential Management 4-1
About Oracle Platinum Services Customer Requirements 4-1
Displaying Credentials 4-2
Using Credential Management 4-2
About Credentials 4-2
About Required Credentials 4-2
About Recommended Credentials 4-3
About Additional Credentials 4-4
About Selected Targets and their Associated Credentials 4-4
Viewing Credentials 4-5
Viewing Credentials for Target Children 4-6
Editing Credentials 4-6
Editing Credentials Singly 4-6
Editing Credentials in Bulk 4-7
Creating Credentials 4-8
About Credential Reports 4-9
Viewing Target Credentials 4-9

5 Provisioning Agents

About Provisioning Agents 5-1
About Provisioning Agents for Engineered Systems 5-1
Adding an Oracle Exadata Engineered System 5-4
Adding an Oracle Exalogic Engineered System 5-12
Adding an Oracle SuperCluster Engineered System 5-14
About Provisioning Agents for Single Hosts 5-17
Prerequisites to Installing an OEM Agent 5-18
Adding a Single Host 5-18
Customizing Agent Install Settings 5-23
Customizing Sample Host Files 5-25

6 Managing Systems

About Managing Systems and Hosts 6-1
Adding a New System 6-1
About Adding a New Engineered System 6-2
Viewing Target Configurations 6-4

Viewing Target Details 6-6
Configuring Supported Targets 6-6
Configuring the Monitoring Level on a Supported Target 6-7
Configuring the Lifecycle Associated with a Supported Target 6-8
Viewing Statistics 6-9
Viewing Service Requests 6-10
Viewing the Health Check Report 6-10
Managing Target Performance 6-10
Viewing Recommendations 6-10
Managing System Passwords 6-10
Deactivating Services 6-11

7 Activating Services

About Activating Services 7-1
Selecting a Service for Activation 7-1
Viewing Discovered Databases 7-9
Deactivating Services 7-10

8 Validating Connections

About Gateway Connectivity 8-1
About System Tests 8-2
About Internal System Tests 8-2
About External System Tests 8-2
Viewing System Test Status 8-2
Verifying the External Connection 8-3
Specifying a HTTP Proxy 8-4
Verifying an Internal Connection 8-5
Configuring New System Test Targets 8-8

9 Managing Service Requests

Viewing Service Requests 9-1
Viewing Service Requests Associated with a Managed System 9-2

10 Managing Databases and Database Patches

About Database Management 10-1
Viewing Managed Databases 10-1
Editing Managed Databases 10-4
Editing Managed Databases Using the Edit List 10-4
Editing Managed Databases Using the Actions Icons 10-4
Editing the Monitoring Configuration 10-5
Activating a Service on a Database 10-6
About Patching Requests 10-6
Creating a Patching Request 10-7
Creating an SR for a Patching Request 10-22
Editing the CM for a Patching Request 10-23

Assigning an SR for a Patching Request 10-24
Canceling a Patching Request 10-25
Editing a Patching Request 10-26
Managing Advanced Database Support (ADS) Targets 10-27
Managing Database Patch Compliance 10-28
Setting the Database Patchset Compliance Level 10-28
Viewing the Database Patchset Compliance Widget 10-31
Using Proactive Patch Recommendations for ADS 10-31
About the Proactive DB Advisory 10-32
Viewing Database Details: Proactive Recommendations 10-32
Applying the Patch Set Update 10-34
Creating a Patching Request from the Proactive Advisory Page 10-34
Marking Security Violations as Accepted Risks 10-35

11 Scheduling Database Blackouts

About Database Blackouts 11-1
Creating Database Blackouts 11-1
Managing Database Blackouts 11-3
Viewing Scheduled Blackouts 11-3
Viewing Completed Blackouts 11-3
Editing Blackouts 11-4
Canceling Blackouts 11-5

12 Managing Database Entitlements

About Database Entitlements 12-1
About the High Water Mark 12-1
Viewing Database Entitlements 12-2

13 Managing Health Checks

About Health Checks 13-1
About the ORAchk Report 13-1
About the EXAchk Report 13-1
Installing and Configuring the Health Check Report 13-2
Installing Trace File Analyzer and Scheduling Health Checks 13-2
Rescheduling the Health Check Report 13-7
Canceling a Schedule 13-9
Viewing the Health Check Report 13-9
Running the Health Check Report Immediately 13-10
Viewing Health Check History 13-11

14 Setting the HTTP Proxy Server

About the HTTP Proxy Server 14-1
Specifying the HTTP Proxy Server Setting 14-1
Specifying a HTTP Proxy During Connectivity Tests 14-2

15 Managing Server Certificates

About Server Certificates 15-1
Viewing Server Certificates 15-1
Viewing Certificate Status 15-2
Managing Server Certificates 15-2
Downloading Server Certificates 15-2
Installing Server Certificates 15-3
Generating a Certificate Signing Request 15-4
Replacing the Current Server Certificate 15-5

16 Enabling Remote Access to the Oracle Advanced Support Gateway

About Remote Access 16-1
About the Remote Access Icon 16-1
Enabling Remote Access 16-2
Disabling Remote Access 16-2
Viewing Remote Access History 16-3

Preface

This guide explains how to use Oracle Advanced Support Gateway.

Refer to the following sections:

- Audience
- Related Documentation
- Getting Help
- Documentation Accessibility

Audience

This guide is intended for Oracle Advanced Support Gateway customer users.

Oracle Advanced Support Gateway is a multi-purpose platform designed to facilitate a number of Oracle connected services including Oracle Platinum Services, LifeCycle services, Business Critical Support, Advanced Monitoring and Resolution, and Advanced Database Support.

The Gateway platform is a software appliance, based on the Oracle Linux operating system and hosts a full stack of Oracle software, including Automated Service Request (ASR), Oracle Enterprise Manager, Oracle Configuration Manager (OCM), patch management (such as YUM services), and a suite of Java applications. Together, these applications aggregate and route telemetry messages from the customer environment to the Oracle Support Services infrastructure.

The same Oracle Advanced Support Gateway provides remote access for Oracle engineers to access the customer network (with customer permission) and to carry out approved actions on the customer's monitored systems. In short, the Oracle Advanced Support Gateway allows simplification of the network requirements and a single point of access for the provision and delivery of Oracle connected services.

The Gateway is typically located in the customer data center DMZ behind a firewall, with network access to the infrastructure it is monitoring. It is not directly exposed to the Internet, but it should be continuously accessible from Oracle Cloud Operations infrastructure, using a TLS/VPN tunnel.

Related Documentation

For more information, see the following documents in the Oracle Advanced Support Gateway documentation set:

- *Oracle Advanced Support Gateway Installation Guide*: Describes how to build Oracle Advanced Support Gateway both in the Cloud (using Oracle Cloud Infrastructure, or OCI) and in an on-premises configuration. The document also provides requirements for

installing the Oracle Advanced Support Gateway, installation procedures, and post-installation tasks. Also provides information on activating the Oracle Advanced Support Gateway on which various services are installed and supported.

- *Oracle Advanced Support Gateway Security Guide*: Describes security information and instructions for Oracle Advanced Support Gateway. Includes the requirements for deploying the Oracle Advanced Support Gateway into the customer environment to support the delivery of Oracle Connected Services. The Oracle Advanced Support Gateway is an important part of the Oracle delivery architecture for Oracle Connected Services and its placement must be carefully considered in order for Oracle to deliver Oracle Connected Services. This document outlines network configuration options when integrating the Oracle Advanced Support Gateway device within the customer environment.

Getting Help

If you require assistance using Oracle Advanced Support Gateway, please contact the Oracle Support Services contact with whom you have been engaged for review.

Alternatively, you can use your CSI (Customer Support ID) to access My Oracle Support at:

https://support.oracle.com/.

Thank you for choosing Oracle Advanced Support Gateway.

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 that have purchased support 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.

About this Release of Oracle Advanced Support Gateway

This chapter outlines changes made to **Oracle Advanced Support Gateway** features, functionality, and supported services in the 14.*x* releases, provides information about any known issues, and gives an overview of the ongoing updates to the document.

Refer to the following sections:

- What's New in the Oracle Advanced Support Gateway 14.3.1 Release
- What's New in the Oracle Advanced Support Gateway 14.2 Release
- What's New in the Oracle Advanced Support Gateway 14.1 Release
- User Guide Revision History

What's New in the Oracle Advanced Support Gateway 14.3.1 Release

This release of **Oracle Advanced Support Gateway** introduces a number of enhancements to the Platform used to deliver Oracle Advanced Customer Services (ACS) and Support services.

The following links to these enhancements also list the number of the corresponding Jira epic/story internally maintained by Services Engineering:

- Platinum Patching

Platinum Patching

This section lists features and enhancements to Platinum Patching functionality. Defects addressed in these functional areas are also described.

The following table provide links to these features and enhancements:

Feature/Enhancement
Users Can Now Create and Update Passwords for New ILOM Target Types

Users Can Now Create and Update Passwords for New ILOM Target Types

Customers were unable to create self-service passwords for critical ILOM target types resulting in customer accounts being locked. This issue has been addressed in this release by enabling users to create and update passwords for ILOM systems.

What's New in the Oracle Advanced Support Gateway 14.2 Release

This release of **Oracle Advanced Support Gateway** introduces a number of enhancements to the Platform used to deliver Oracle Advanced Customer Services (ACS) and Support services.

The following links to these enhancements also list the number of the corresponding Jira epic/story internally maintained by Services Engineering:

- Platinum Patching
- Adding ZDLRA System
- Usability Enhancements

Platinum Patching

This section lists features and enhancements to Platinum Patching functionality. Defects addressed in these functional areas are also described.

The following table provide links to these features and enhancements:

Feature/Enhancement
Patching Flow Now Supports OEM 13c Target Types
When Editing a Draft Patch Request for a ZDLRA, Pre-Patch Page Now Enabled
Patch Request Workflow: Patching Options Page Back Button Now Working
Submit Button Disabled Once Pressed

Patching Flow Now Supports OEM 13*c* Target Types

InfiniBand switch Exadata targets are now discovered as Oracle Enterprise Manager (OEM) 13*c* target types.

To provide support for these target types, we have added an enhancement in this release: when scheduling a Patch on the Gateway, the patching workflow now supports InfiniBand switches of Oracle Enterprise Manager (OEM) 13*c* target type.

When Editing a Draft Patch Request for a ZDLRA, Pre-Patch Page Now Enabled

When Editing a draft Patch Request (PR) for a ZDLRA, the Gateway portal does not display the Pre Patch page. As well as a missing prepatch page, users cannot click on the Prepatch page link as it is disabled.

This defect has been addressed in this release.

Patch Request Workflow: Patching Options Page Back Button Now Working

In the previous release, when editing a draft Patch Request (PR), once you reach the **Patch Option** page in the workflow, if you click **Back**, instead of being taken to the **Prepatch** page, you remain on the **Patch Option** page instead.

This defect has been addressed in this release.

Submit Button Disabled Once Pressed

After a user has completed the patching flow by clicking **Submit**, the button is then disabled. This is due to the fact that after submission of the patching plan has been activated (through the **Submit** action), a number of activities, for example, resource allocation, are activated.

On occasion, users clicked **Submit** more than once, and it led to issues. Now, users can click it once only.

Adding ZDLRA System

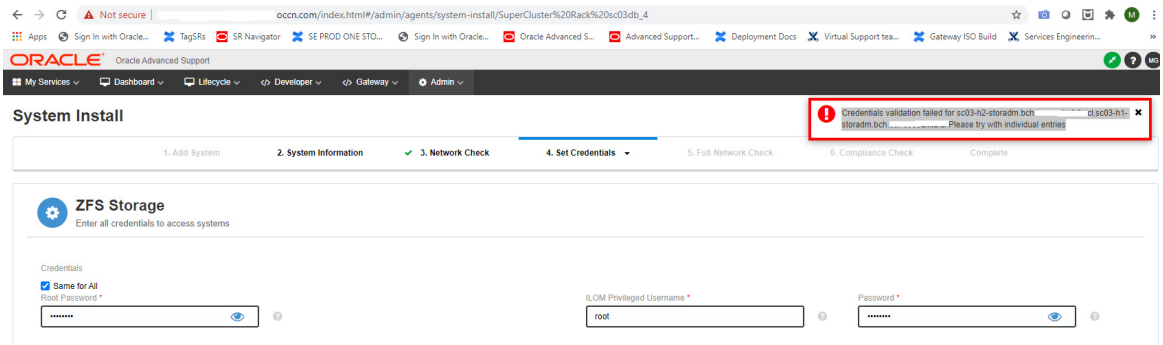
The following table provides a link to a defect related to adding a ZDLRA to the Gateway:

Feature/Enhancement
Adding ZDLRA System to Gateway No Longer Fails Due to Incompatibility

Adding ZDLRA System to Gateway No Longer Fails Due to Incompatibility

When using the **Add System** workflow on the Gateway to create a request for the monitoring of a Zero Data Loss Recovery Appliance (ZDLRA), the checks on the system credentials were failing due to an incompatibility between the ZFS servers for new SuperClusters and the SSH infrastructure used by the Gateway UI for the ZFS components.

This defect - as displayed in the screenshot below - has been addressed in this release.



Usability Enhancements

This section lists features and enhancements to UI/UA functionality. Defects addressed in these functional areas are also described.

The following table provide links to these features and enhancements:

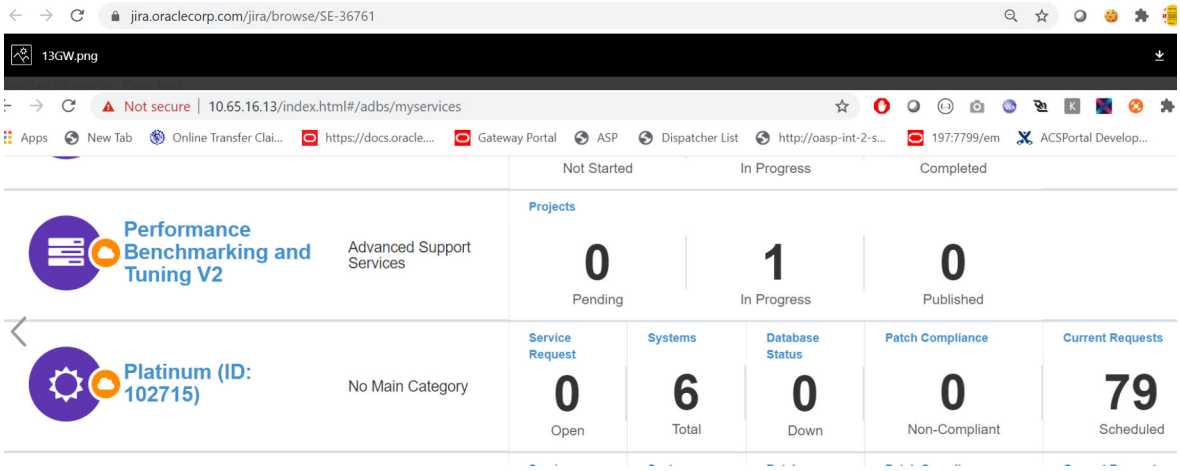
Feature/Enhancement
Gateway UI: My Services Page Alignment Fix

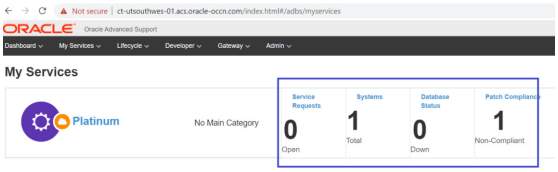
Gateway UI: My Services Page Alignment Fix

As part of the continuous usability improvement, a minor UI alignment issue in the My Services page on the Gateway portal has been fixed in this release.

The issue related to the way that icons and text were not accurately aligned.

Refer to the following screenshots of the current and previous UI representations.





What's New in the Oracle Advanced Support Gateway 14.1 Release

This release of **Oracle Advanced Support Gateway** introduces a number of new features and enhancements to the Platform used to deliver Oracle Advanced Customer Support (ACS) and Support services.

The following tables provide links to the new features and enhancements, and list the Oracle connected services affected:

- **Generic Updates**
- **Service-Specific Updates**

Generic Updates

This section lists generic updates, that is, changes to Oracle Advanced Support Gateway functionality in this release.

Feature or Enhancement
Password Management on the Gateway
Gateway VPN Now Supports Transport Layer Security (TLS) v1.2
Cisco AnyConnect Secure Mobility Client Version Updated

Service-Specific Updates

This section lists service-specific updates, that is, changes to Oracle Advanced Support Gateway functionality in this release that affect a particular service or number of services.

Feature or Enhancement	Affected Service
Patching Automation for Platinum and Cloud at Customer Customers	ADS, Platinum
Database Upgrade Assurance Service Enhancements	Database Upgrade Assurance Service

Password Management on the Gateway

A number of enhancements have been made to password management on the Gateway:

- The **Expiry** date attribute has been removed from the Gateway UI.
- The Password management UI now provides the ability to bulk create and bulk update credentials.

Gateway VPN Now Supports Transport Layer Security (TLS) v1.2

In order to enhance security on Oracle Advanced Support Gateway, the Gateway VPN now supports TLS v1.2 which was requested by customers for secure communications.

For more information about TLS VPN and the Gateway, see here.

Cisco AnyConnect Secure Mobility Client Version Updated

The version of Cisco AnyConnect Secure Mobility Client, that simplifies secure endpoint access and provides the requisite security for users of Oracle Advanced Support Gateway, has been updated from 3.1.x to 4.*x* in this release.

Patching Automation for Platinum and Cloud at Customer Customers

Note: These enhancements apply to Platinum and Cloud at Customer customer users on the Gateway and Oracle Advanced Support Portal.

- A mandatory pre-patch template has been added for Oracle Exadata systems
- A new *Patch Schedule Admin* role is now available to Oracle users. This role enables the user to select any date/time on the Gateway to schedule a patch
- Patching SRs created automatically through the SR framework now include the Gateway name as part of the description
- A reason is now provided for EXAchk failure
- Time of scheduled patch prefixed in SR summary post on creation of an automated patching SR.

Pre-Patch Template Added For Exadata Systems

As part of the patching workflow, users must now complete a mandatory Pre-Patch template - for Exadata systems only - prior to completing the scheduling details.

See "Creating a Patching Request."

There are 5 principal sections to complete:

1. Select an OJVM option.

   Note: Mitigation and OJVM patches can coexist. The mitigation patch can be turned on and off, at will.

Review My Oracle Support (MOS) note 1929745.1 and select one of the options below (applying the OJVM requires approximately one (1) hour of downtime per RAC for both primary and stand-by environments):

- Option 1: Apply OJVM patch (This is the RECOMMENDED option.)
- Option 2: Apply Mitigation patch; this can interfere with other Java applications (RECOMMENDED FOR SHORT TERM ONLY IF OJVM DOWNTIME IS NOT POSSIBLE.)
- Option 3: Apply no patch (This option is NOT RECOMMENDED.)

2. Perform the following tasks:

   a. Provide the Owner and Group details of Grid & Oracle homes to be patched; <Execute the following command as root or sudo user in the first database node of the cluster>:

   ```
   egrep -v "^#|^$|agent" /etc/oratab | cut -d ":" -f2 | sort | uniq |
   while read home;do echo -n "$home==>"; stat -c %U:%G
   $home/inventory; done
   ```

   b. Provide the Agent Details;

   <Execute the following command as root or sudo user in the first database node of the cluster>

   ```
   ps -ef | grep agent | grep java | sed 's/\s\+/ /g' | cut -d " " -f
   1,8 | sed 's/\/jdk.*//'
   ```

3. (Is there an) EBS database/grid/home present in the environment (Y/N):

   If Y, please provide details (for more information about the special instructions that need to be taken in consideration for EBS patching, please review MOS DOC ID 1392527.1)

4. (Is there a) SAP GRID/HOME/DB (Y/N):

   If Y, please provide details of Grid/Oracle_Home path.

5. Normal/High Redundancy (for Rolling events, High Redundancy is recommended).

   Oracle also recommend that you check the following:

   - Oracle Platinum Services - Recommended Best Practices for Patch Events (Doc ID 2147697.1)
   - Exadata Patching Overview and Patch Testing Guidelines (Doc ID 1262380.1)

Patch Schedule Admin Role Added

A new role called *Patch Schedule Admin* has been created as part of the Oracle Advanced Support Portal 20.0 release. An Oracle user with this role can select any date/time on the Oracle Advanced Support Gateway to schedule a patch.

So, in practice, when a customer user logs in to the Gateway, the user can see only those dates and times that are available for the patch duration they have selected. If a different date is required, the user must contact an Oracle Support representative with the Patch Schedule Admin role to select another date which was not displaying as available for selection to the user.

Patching SRs Created Automatically Through SR Framework Include Gateway Name in Description

All patching SRs created automatically through the SR framework now incorporate the Gateway name as part of their description. This enables engineers who work on the SR to more easily find the gateway.

Reason for Prior EXAchk Failure Now Provided

When a user selects the **Gateway Current Requests** page, by hovering above the **Trigger EXAchk** button, the reason for a previous EXAchk failure is displayed. This enables users to troubleshoot and fix issues that prevented EXAchk from running correctly.

Time of Scheduled Patch Prefixed in SR Summary on Creation of Automated Patching SR

The time of the scheduled patch is now prefixed in the SR summary whenever an automated patching SR is created, for example in the highlighted summary below:

01-Nov-2019 10:00 PM ET - AYXAN06 | Anycom Material Supply| ED | August 2019

Database Upgrade Assurance Service Enhancements

The Oracle Database Upgrade Assurance (DUA) service, targeted at customers upgrading to Oracle Database 12*c* R2, provides the following enhancements in this release:

Note: This feature, while driven by Oracle engineers, applies to customer users of the Database Upgrade Assurance (DUA) service on the Gateway.

- The Database Upgrade Assurance service can run against an upgraded database in the OCI environment.
- The Database Upgrade Assurance service can run against a 19*c* upgraded environment (the 11.2.0.4 to 19*c* upgrade has been tested.)

User Guide Revision History

The following table lists the revision history for *Oracle Advanced Support Gateway User's Guide.*

Version	Date	Description
E76461-01	September 2016	Oracle Advanced Support Gateway 6.*x* release
E83211-01	February 2017	Oracle Advanced Support Gateway 7.*x* release
E83212-01	July 2017	Oracle Advanced Support Gateway 8.*x* release
E91025-01	December 2017	Oracle Advanced Support Gateway 9.*x* release
E98167-01	July 2018	Oracle Advanced Support Gateway 10.*x* release
E76461-01	October 2018	Oracle Advanced Support Gateway 11*x* release
F18085-01	May 2019	Oracle Advanced Support Gateway 13.x release **Note**: No user guide was produced for Oracle Advanced Support Gateway 12.*x.*
F24159-01	May 2020	Oracle Advanced Support Gateway 14.x release, first version incorporating the 14.1 release.
F24159-02	November 2020	Oracle Advanced Support Gateway 14.x release, revision incorporating the 14.2.1 release.
F24159-03	June 2021	Oracle Advanced Support Gateway 14.x release, revision incorporating the 14.3.1 release.

1

About the Oracle Advanced Support Gateway User Interface

This chapter offers an introduction to the Oracle Advanced Support Gateway user interface and its principal features.

It includes the following topics:

- Logging onto the Gateway
- About the Gateway User Interface

Logging onto the Gateway

After successfully installing the Oracle Advanced Support Gateway, you can access the Oracle Advanced Support Gateway portal using a Web browser.

Note: In order to access the Gateway, your Web browser must be connected to the Internet to enable Oracle Single Sign-on (SSO) authentication.

To log on to the Gateway:

1. Navigate to the Oracle Advanced Support Gateway portal at *https://<GATEWAY_IP_ADDRESS>*.

   GATEWAY_IP_ADDRESS is the IP address assigned to the physical interface of the Oracle Advanced Support Gateway. Where two interfaces are used, you need to reference the internal interface. This is the IP address which will communicate internally.

2. Log on to the portal.

   Use the customer administrator account configured at installation time or any other user with the customer administrator role.

   The All Services page appears.

About the Gateway User Interface

This section briefly describes the Gateway user interface and provides an overview of the main UI components.

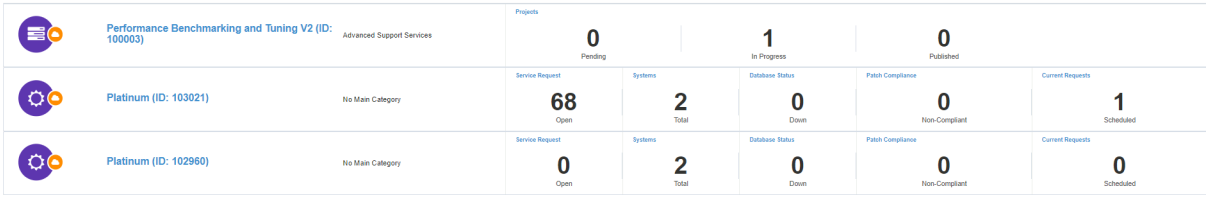
The Gateway user interface is made up of a number of principal elements that enable you to optimally manage your services and to perform tasks, for example:

- Create users and assign passwords
- Activate services
- Provision agents

- Manage systems and hosts
- Review the status of service requests
- Monitor the health of the Gateway

Refer to Figure 1–1 that shows the user interface.

Figure 1–1 Oracle Advanced Support Gateway User Interface



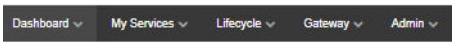
Refer to the following sections that describe the individual elements of the Gateway user interface:

- About the Navigation Menu
- About the My Services Menu
- About the Dashboard Menu
- About the Gateway Menu
- About the Admin Menu
- Viewing Legal and Copyright Information

About the Navigation Menu

The navigation menu is on the page header to the right of the Oracle logo and application name.

Figure 1–2 Viewing the Navigation Menu



The navigation menu comprises:

- Menu items linked to either:
  - A pull down of sub-menu items, for example, **Lifecycle** or **Admin**, *or*
  - An individual screen, for example, **Dashboard**
- Utility links for user information and assistance features:
  - A user support icon displaying links to contact Oracle Support, access the Oracle community forum, and initiate a live chat with an Oracle representative.

    Note: The live chat feature is not enabled in this release.
  - A user settings icon displaying options to:

    Edit your user profile. See "Updating Users."

    Update your user password.

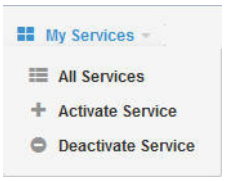
    Log out of the current session.

About the My Services Menu

The My Services menu enables you to:

- Select **All Services** to display all available customer services on the Gateway, as seen on the My Services main page in Figure 1–1
- Select **Activate Service** to activate a service
- Select **Deactivate Service** to deactivate a service

Figure 1–3 Viewing the My Services Menu



Related Information

Selecting a Service

Selecting a Service Feature

Activating Services

Selecting a Service

To select a supported service:

1. Log on to the portal as outlined in "Logging onto the Gateway."
2. From the My Services menu, select **All Services**.

   The My Services page appears. It displays a list of services tailored to the customer contract.
3. From the My Services page, select the required service by clicking it.

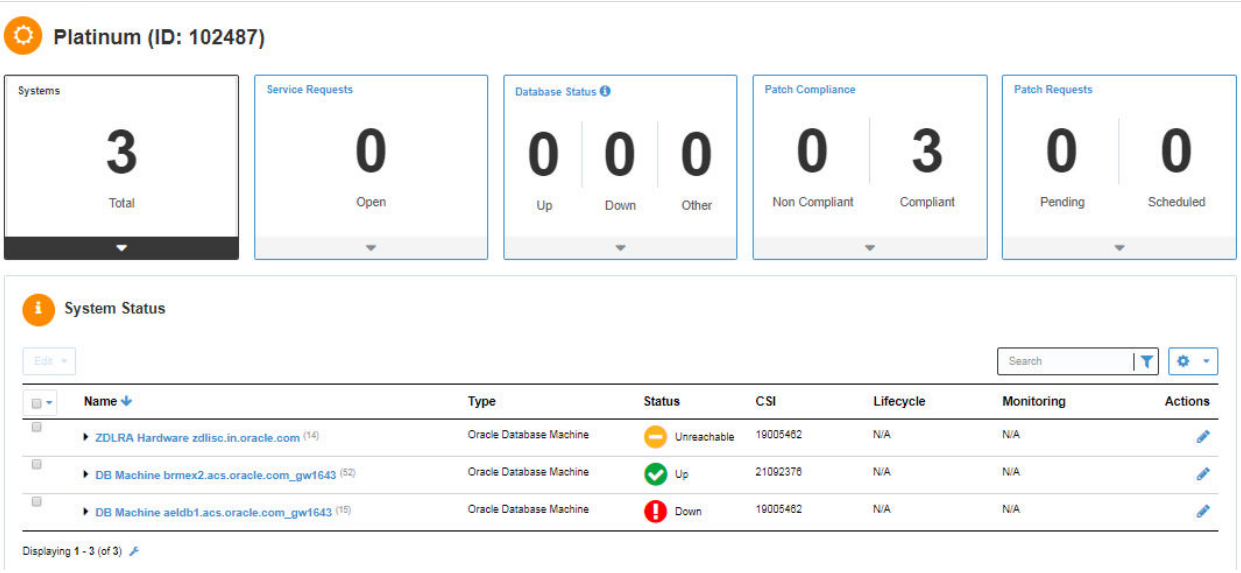
Selecting a Service Feature

To select a supported service feature:

1. Choose the required service as outlined in "Selecting a Service."
2. From the service page, click a tile to select the service feature, for example, click **Systems** as shown in Figure 1–4 to display the system status table.

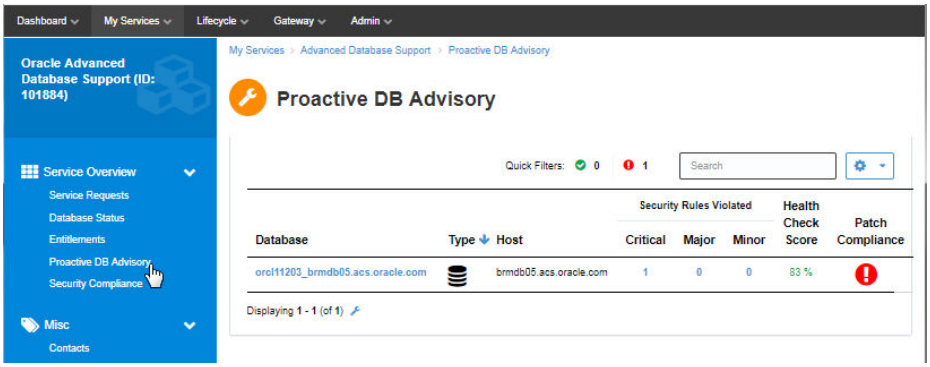
   The selected service feature is displayed.

Figure 1–4 Selecting a Service Feature



3. From the ADS service page shown in Figure 1–4, click a menu item as shown or click one of the tiles that correspond to the menu options to select the service feature.

Figure 1–5 Selecting an ADS Service Feature



About the Dashboard Menu

An Oracle Advanced Support Gateway dashboard is a customizable service dashboard framework that provides an overview of your services and enables you to focus on selected items of interest. The dashboard is made up of a series of data windows called *widgets*. The dashboard provides a layout to display multiple widgets on one page. You can create multiple dashboard pages, with each page made up of multiple widgets. You can use the dashboard to add, remove, or rename pages or widgets.

Figure 1–6 Viewing the Dashboard

Related Information

Using Dashboards

Reviewing and Filtering Information

You can filter, refine, and customize the presentation of results in Gateway tables by performing the following actions:

- **Filter Results** - Click any column name to sort data in that column.

  For example, click **Name** to sort alphabetically by name.

- **Search** - Perform a search for data in the table.

  For example, in the table of Gateway users, In the **Search** field on the menu bar, enter the contact's e-mail address, phone number, type, notification only, user status, applications, or first or last name. You can also use the wildcard symbol. Then click the **Search** icon. The Users page is refreshed, displaying the contact(s) matching the full or partial entry.

- **Re-order** - To reorder a list, use the arrows to alter the display.

- **Customize the page** - In the top right of the page or table, use the menu items under the wheel icon to perform the following actions:

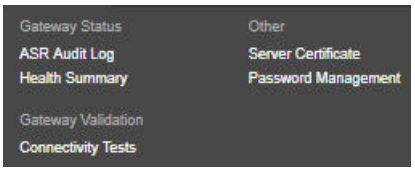
  - Click **Column Visibility** to deselect column names.
  - Click **Print** to print the contents of the page.
  - Click **Excel** to save the contents of the page in Microsoft Excel format.
  - Click **CSV** to save the contents of the page in comma-separated variable format.

About the Gateway Menu

The Gateway menu provides a number of options for configuration and management of the Gateway.

Note: Menu items may vary from those displayed.

Figure 1–7 Viewing the Gateway Menu



Among the tasks that the Gateway menu enables you to perform are:

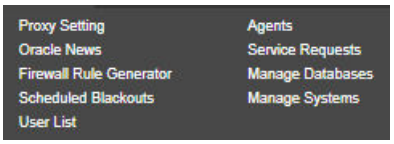
- Managing Health Checks
- Validating Connections
- Managing Server Certificates
- Managing Credentials and Passwords

About the Admin Menu

The Admin menu provides a number of options for administration of the Gateway.

Note: Menu items may vary from those displayed.

Figure 1–8 Viewing the Admin Menu



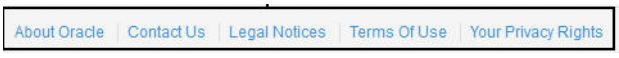
Among the tasks that the Admin menu enables you to perform are:

- Setting the HTTP Proxy Server
- Scheduling Database Blackouts
- Managing the User List
- Provisioning Agents
- Managing Databases and Database Patches
- Managing Systems

Viewing Legal and Copyright Information

The customer information section on the bottom of the screen provides links to Oracle legal notices and policies, as well as displaying a copyright notice.

Figure 1–9 Viewing Customer Information



You can use the customer information section to:

- View details about Oracle
- Contact Oracle
- Review legal notices and policies on privacy rights and terms of use

2

Using Dashboards

This chapter provides information about using Oracle Advanced Support Gateway to configure and use dashboards.

This chapter consists of the following sections:

- About Dashboards
- Accessing the Dashboard
- About Widgets
- Adding a Dashboard
- Adding a Widget
- Managing Widgets

About Dashboards

An Oracle Advanced Support Gateway dashboard is a customizable service dashboard framework that provides an overview of your services and enables you to focus on selected items of interest. The dashboard is made up of a series of data windows called *widgets* as shown in Figure 2–1.

Figure 2–1 The Dashboard

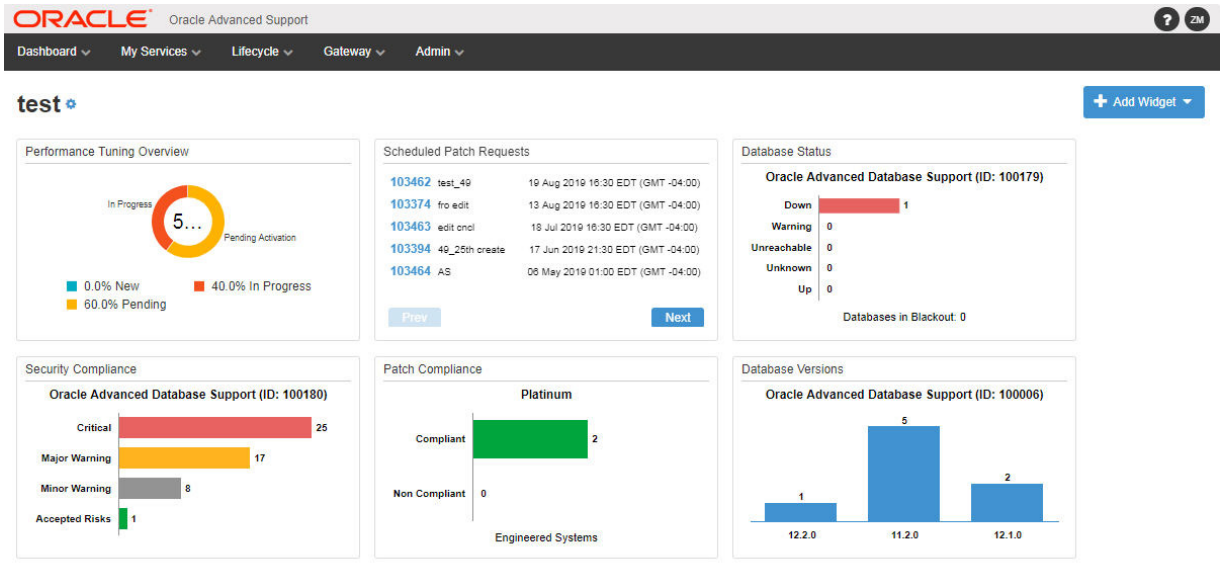


Figure 2–1, "The Dashboard" shows a customer service dashboard that displays the status and statistics relating to their systems, hosts, or databases, as well as information about security compliance and network connectivity. Each widget provides one-click access to additional, detailed information about the data presented in the widget.

The dashboard provides a layout to display multiple widgets on one page. You can create multiple (up to five) dashboard pages, with each page made up of multiple widgets. You can use the dashboard to add, remove, or rename pages or widgets.

Related Information

Accessing the Dashboard

About Widgets

Accessing the Dashboard

To use Oracle Advanced Support Gateway to access the dashboard:

1. Log on to the Oracle Advanced Support Gateway portal.
2. From the top level menu, select **Dashboard**.

You can add widgets (and further dashboards) as required.

Related Information

About Dashboards

Adding a Dashboard

About Widgets

A widget is a data window that provides information about a service, such as database version or status, whether the gateway is connected to the Oracle VPN, whether remote access is enabled on the gateway, and so on.

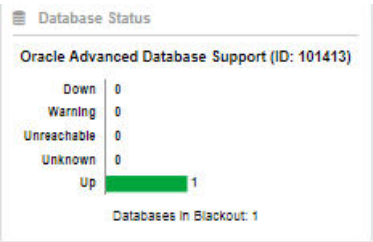
The widgets listed as available are based on the user's role and the services available on the gateway. For example, the Patch Set Update Compliance widget is only available if Platinum Services are installed on the gateway.

You can add and remove widgets from a dashboard, reposition widgets on the screen, and drill down into a widget to view the underlying information.

The Oracle Advanced Support Gateway widgets include:

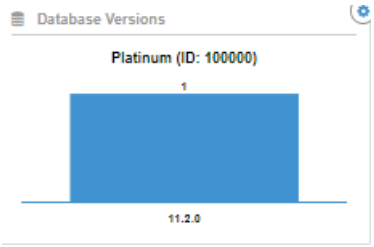
- **Database Status**: Displays the status counts of the databases activated for a specific service.

Figure 2–2 Database Status Widget



- **Database Versions**: Displays the counts of the databases activated for a specific service by their installed database version.

Figure 2–3 Database Versions Widget

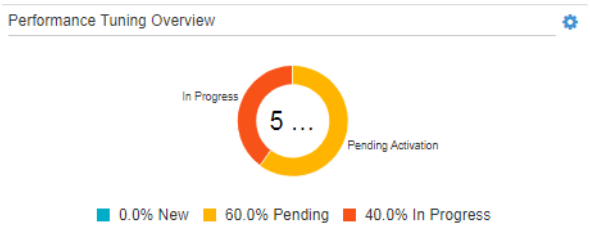


- **Health Check Group**: Displays a summary of the health status of selected hosts. For more information about health checks, see Chapter 13, "Managing Health Checks."
- **Patch Compliance**: Displays the compliance summary for all Oracle Engineered Systems activated under Platinum Services. See Chapter 10, "Managing Databases and Database Patches."

Figure 2–4 Patch Compliance Widget

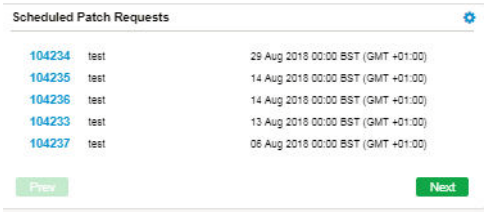
- **Performance Tuning Overview**: Displays an overview of engagement statuses, that is, *new*, *pending*, or *in progress*.

Figure 2–5 Performance Tuning Overview Widget



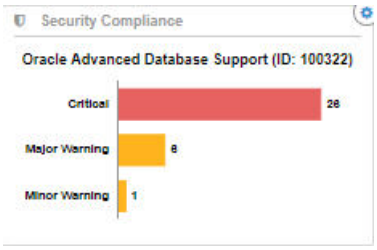
- **Scheduled Patch Requests** Displays scheduled patch requests details. See Chapter 10, "Managing Databases and Database Patches."

Figure 2–6 Scheduled Patch Requests Widget



? **Security Compliance**: Displays the security compliance summary for databases activated on Oracle Advanced Database Support (ADS). See Chapter 10, "Managing Databases and Database Patches."

Figure 2–7 Security Compliance Widget



Related Information

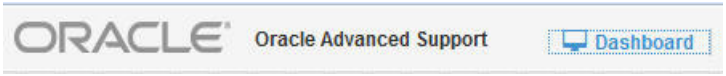
Adding a Widget

Adding a Dashboard

To use Oracle Advanced Support Gateway to add a dashboard:

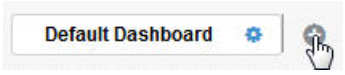
1. Log on to the Oracle Advanced Support Gateway portal.
2. From the top level menu, select **Dashboard,** or its associated icon, as highlighted in Figure 2–8.

Figure 2–8 Accessing the Dashboard



3. Click the + icon to add a dashboard page as shown in Figure 2–9.

Figure 2–9 Adding a Dashboard



4. Provide a meaningful name for the dashboard page, and click **Create**.

   The dashboard page appears.

   You can create up to a total of five dashboards per Gateway instance.

Related Information

Accessing the Dashboard

Adding a Widget

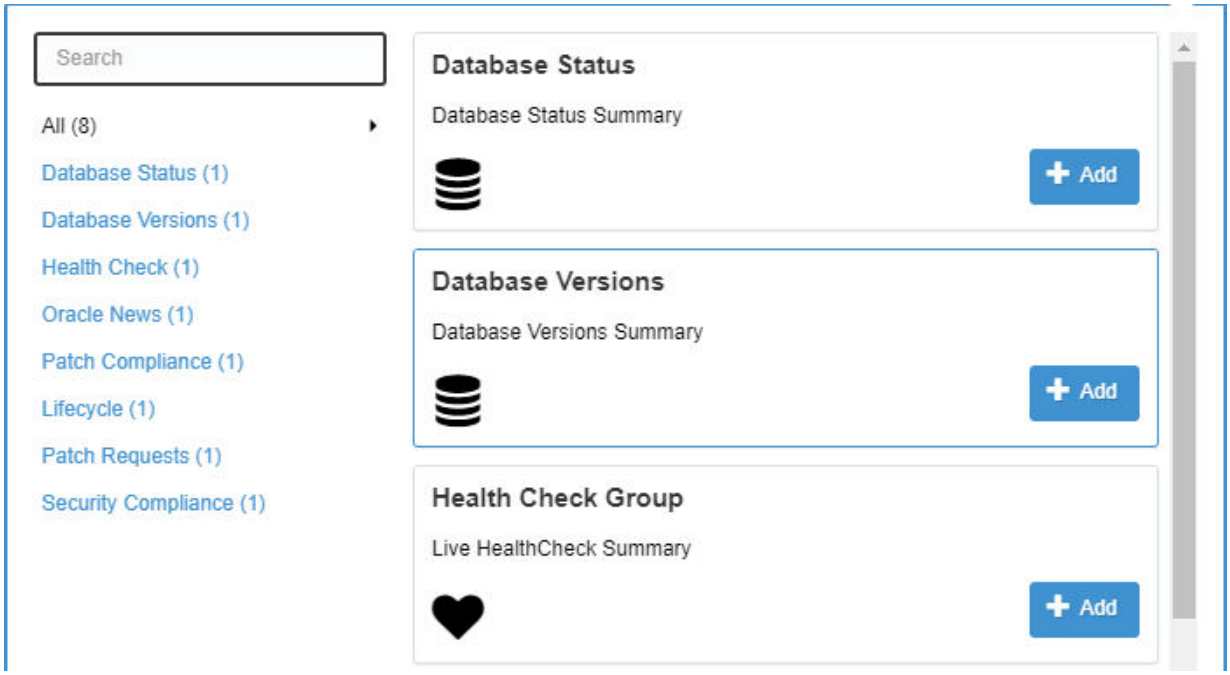
To use Oracle Advanced Support Gateway to add a widget:

1. Click **Add Widget** as shown in Figure 2–10.

Figure 2–10 Adding a Widget

2. From the available widgets, click **Add** to select the required widget. See Figure 2–11.

Figure 2–11 Selecting a Widget



The widget appears on the dashboard page.

3. (Optional) Add further widgets to the dashboard.

   You can add any number of different widgets or multiple instances of the same widget to a dashboard page.

Related Information

Accessing the Dashboard

Managing Widgets

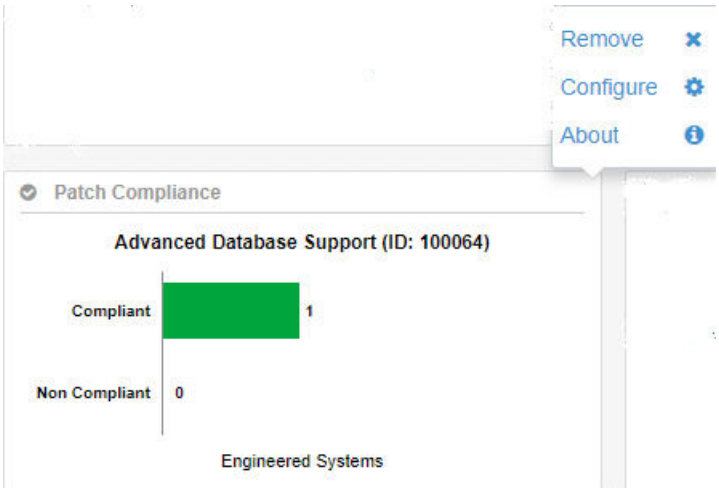
Each widget provides one-click access to additional, detailed information about the data presented in the widget. So, for example, when you click on the Database Status widget, the Fault Management service appears.

You can perform a number of actions on a widget.

To perform an action on a widget:

1. Click the icon associated with a widget as shown in Figure 2–12 to display the actions available on the widget.

Figure 2–12 Viewing the Actions Available on a Widget



2. Select the required action.

Related Information

Removing a Widget from a Dashboard

Configuring a Widget

Reviewing Information about a Widget

Removing a Widget from a Dashboard

To remove a widget from a dashboard:

1. Click the icon shown in Figure 2–12 to display the actions available on the widget.
2. Click **Remove**.

   The widget is removed from the dashboard.

Configuring a Widget

To configure a widget:

1. Click the icon shown in Figure 2–12 to display the actions available on the widget.
2. Click **Configure**.
3. Perform the configuration required on the widget.

   Note: Only certain widgets can be configured in this way.

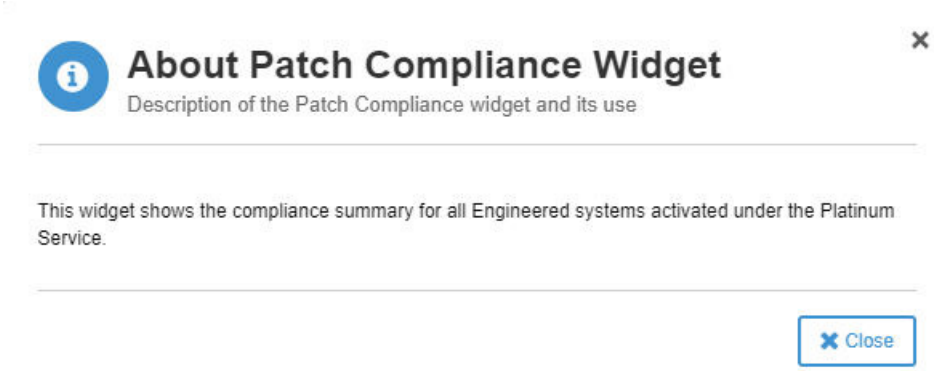
Reviewing Information about a Widget

To review information about a widget:

1. Click the icon shown in Figure 2–12 to display the actions available on the widget.
2. Click **About**.

An information panel appears showing a description of the widget and its use. For example, Figure 2–13 shows the information panel for the Patch Compliance widget.

Figure 2–13 Viewing the Patch Compliance Widget Information Panel



3. Click **Close**.

Related Information

Adding a Widget

3

Managing the User List

This chapter describes how to manage accounts for customer users and customer administrators in Oracle Advanced Support Gateway.

It includes the following topics:

- About User Management
- Managing Users

About User Management

You can use the **User List** option from the **Admin** menu to display the **Users** page. You can use this page to manage Oracle Advanced Support Gateway users.

The **Users** page provides the ability to view, search for, create and edit user information for your organization. All Oracle Advanced Support Gateway users from your organization, and from Oracle, are displayed. The **Users** page enables you to create new customer and provider contacts.

The **Users** page also enables you to customize the way in which fields are displayed, or filter the users displayed by specifying filter criteria. You can also search for users using the Search field. The Search field autocompletes the search criteria entered, returning the first user in the displayed list that matches the criteria.

Managing Users

Oracle Advanced Support Gateway enables customer administrators (CUAs) to add, update, or delete customer users for their organizations. This section contains the following topics:

- Viewing Users
- Adding Users
- Activating Users
- Updating Users
- Deleting Users
- Resetting User Passwords

Viewing Users

The Users page enables you to view and maintain all of your organization's Oracle Advanced Support Gateway users and contacts on one page, where:

Prerequisites

- A **user** has an account in Oracle Advanced Support Gateway, enabling the user to access Oracle Advanced Support Gateway.
- A **contact** is an individual who is involved with Oracle connected services and packages and whose details have been registered in Oracle Advanced Support Gateway. Contacts may or may not have access to Oracle Advanced Support Gateway.

To view users of Oracle Advanced Support Gateway:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Admin** menu, click **User List**.

   The Users page appears, displaying the following information for all entries:

Field	Description
Name	The user name for this Oracle Advanced Support Gateway account.
Status	Indicates whether the user status is: - **Enabled**, where an Oracle Advanced Support Gateway user account has been added and activated. Users with this user status can log in to Oracle Advanced Support Platform. - **Inactive**, where an Oracle Advanced Support Gateway user account has been deactivated due to inactivity. Users with this user status cannot log in to Oracle Advanced Support Platform.
E-mail	The user's e-mail address, as registered in Oracle Advanced Support Platform.
User Type	Indicates whether the user type is: - **Customer**, where an Oracle Advanced Support Gateway user is a customer. - **Oracle**, where an Oracle Advanced Support Gateway user is a provider. Oracle users are notified as certain events relating to the user occur. **Note**: Oracle users are not visible to customer users.
Role	The user's role; for example, Customer or Customer Administrator.
Actions>Invite	Invite an individual to become an Oracle Advanced Support Gateway user.
Actions>Edit	Edit the details of an Oracle Advanced Support Gateway user.
Actions>Remove	Remove the user from the Oracle Advanced Support Gateway.

Adding Users

This section describes how you can add a new user to Oracle Advanced Support Gateway.

Prerequisites

- The individual is not already a contact for this customer organization in Oracle Advanced Support Gateway.
- You are a customer administrator for your organization.

To add a new user of Oracle Advanced Support Gateway:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Admin** menu, click **User List**.

   The Users page appears.

3. Click **Create User**.

The Create New User Profile form appears.

4. Enter the following information for the user:

Field	Description
User ID	The user identifier associated with this user. **Note**: Only letters, numbers, and underscores are allowed. System users are reserved.
First Name	The first name of the user.
Last Name	The last name of the user.
E-mail address	The user's e-mail address. **Note**: Ensure that the email address is valid and that the user can access it to receive an activation email.
Phone	(Optional) The user's telephone number, including country and area codes.
Status	The status of the user, whether *Active* or *Inactive*. An *Inactive* user is one that has been created, but is not yet activated and hence can't log on to the Gateway. To activate a user, see "Activating Users".
Date format	The format to be used when displaying dates for this user.
Time format	The format to be used when displaying times for this user.
User Type	Type of user: - **Customer** - creates a customer user. **Note**: Oracle users may be created on Oracle Advanced Support Platform, but are not visible to customer users.
User Role	Select the type of role (or roles) associated with the user. - **Generic Customer User**: This is a business role. A user with the Customer role can log in to the Gateway. Users with this role can also review connectivity checks (that is, the *Netcheck* functionality.) See Chapter 8, "Validating Connections." - **Generic Customer Admin** This is an administrative role. A user with the Customer Administrator role can manage customer users and perform all customer-facing functions such as password management. **Note**: Selecting the **Generic Customer Admin** role ensures that the new user can create other users.

5. Click **Create** to create the user, or click **Cancel** to quit.

   When you submit the new user data, you will receive confirmation on the Gateway user interface that an activation email has been sent to the email address you entered.

   The Maintain Users page appears, showing information about the new user in the user table.

Activating Users

This section describes how you can activate an Oracle Advanced Support Gateway user.

Prerequisites

- The user is successfully created on the Oracle Advanced Support Gateway.

To activate an Oracle Advanced Support Gateway user:

1. Click the URL in the activation email to direct you to the Oracle Advanced Support Gateway activation page.
2. Enter a password for the new account.

Passwords must be between 6 and 32 characters long and should contain three of the following four items:

- An upper case letter;
- A lower case letter;
- A symbol (for example *?*, *%*, *$*, +);
- A number.

When a valid password is set, the user account is activated.

3. Log in to Oracle Advanced Support Gateway using the user credentials.

Updating Users

This section describes how you can update an Oracle Advanced Support Gateway user.

This function may be required, for example, after creating a new user, where the user cannot log in to the Gateway, and is shown as an *inactive user* on the Maintain Users page (as denoted by a grayed out symbol.) An inactive user is one that is created, but is not yet activated and hence can't log on to the Gateway.

Prerequisites

- The individual is a contact or user for this customer organization in Oracle Advanced Support Gateway.
- You are a customer administrator for this customer organization in Oracle Advanced Support Gateway.

  Customers require the *customer admin* role.

To update an Oracle Advanced Support Gateway user:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Admin** menu, click **User List**.

   The Users page appears.

3. From the list, click the name of the user that you want to update, or select the **Edit** icon associated with the user in the **Actions** column.

   The Users form appears for the individual user.

4. Edit the following information as required:

Field	Description
User ID	The user identifier associated with this user. **Note**: Only letters, numbers, and underscores are allowed. System users are reserved.
First Name	The first name of the user.
Last Name	The last name of the user.
E-mail address	The user's e-mail address. **Note**: Ensure that the email address is valid and that the user can access it to receive an activation email.
Phone	The user's telephone number, including country and area codes.
Date format	The format to be used when displaying dates for this user.
Time format	The format to be used when displaying times for this user.

Field	Description
User Type	Type of user, which is one of the following: ? **Customer** - creates a customer user. ? **Oracle** - creates an Oracle user that is notified as certain events relating to the user occur. **Note**: Oracle users are not visible to customer users.
User Role	Select the type of role (or roles) associated with the user. ? **Generic Customer User**: This is a business role. A user with the **Generic Customer User** role can log in to the Gateway. Users with this role can also review connectivity checks (that is, the *Netcheck* functionality.) See Chapter 8, "Validating Connections." ? **Generic Customer Admin**: This is an administrative role. A user with the **Generic Customer Admin** role can manage customer users and perform all customer-facing functions such as password management. **Note**: Selecting the **Generic Customer Admin** role ensures that the new user can create other users.

5. Click **Save** to update the user (or click **Cancel** to quit without saving.)

   The Users page appears, showing information about the user in the user table.

   In the case of an *inactive user*, after revising the user's data (for example, email address), click **Send Invite** to resend the activation email.

Deleting Users

This section describes how you can delete an Oracle Advanced Support Gateway user.

Prerequisites

? The individual is a contact or user for this customer organization in Oracle Advanced Support Gateway.

? You are a customer administrator for this customer organization in Oracle Advanced Support Gateway.

To delete an Oracle Advanced Support Gateway user:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Admin** menu, click **User List**.

   The Users page appears.

3. Select the **Delete** icon associated with the user in the **Actions** column.

   When prompted, click **Yes** to confirm that you want to delete this user.

   The Users page appears, with a message that the user has been deleted.

Resetting User Passwords

This section describes how you can reset the password of an Oracle Advanced Support Gateway user.

Prerequisites

? The individual is a contact or user for this customer organization in Oracle Advanced Support Gateway.

- You are a customer administrator for this customer organization in Oracle Advanced Support Gateway.

To update the password of an Oracle Advanced Support Gateway user:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Admin** menu, click **User List**.

   The Users page appears.

3. From the list, click the name of the user that you want to update, or select the **Edit** icon associated with the user in the **Actions** column.

   The Users form appears for the individual user.

4. Click **Reset Password** to send the user a form for resetting the password.

5. Click **Yes** to confirm.

4

Managing Credentials and Passwords

This chapter describes how to view and manage customer credentials for hosts or targets associated to at least one service running on the Oracle Advanced Support Gateway production system.

It includes the following topics:

- About Credential Management
- About Credentials
- Viewing Credentials
- Editing Credentials
- Creating Credentials
- About Credential Reports

About Credential Management

The delivery of Oracle connected services using Oracle Advanced Support Gateway requires the safe and secure sharing of passwords between the customer and Oracle. Furthermore, Oracle recommends that you rotate passwords periodically for your production system.

Oracle Advanced Support Gateway provides password or credential management functionality that enables customers to add new accounts, delete existing accounts, and modify stored passwords associated with your databases safely and securely using the customer facing portal running on the Oracle Advanced Support Gateway. All passwords managed via Oracle Advanced Support Gateway are routed securely to Oracle Password Vault, which is an application that ensures only authenticated and authorized users can access the accounts information stored in the database.

The automated ORAchk, EXAchk, and OEM deployment procedures, among others, rely on these credentials, so it is essential that these credentials are stored securely using Oracle Enterprise Manager (OEM.)

This is a write only interface and previously entered passwords cannot be read by customer users.

All users, roles, and privileges are created in the Oracle Advanced Support Platform Refer to the *Managing Users* section of *Oracle Advanced Support Platform User's Guide* on https://docs.oracle.com/cd/E35846_01/.

About Oracle Platinum Services Customer Requirements

For customers availing of Oracle Platinum Services, refer to the Oracle Platinum Services - Fault Monitoring What to Expect document; specifically **Appendix III – Access**

Requirements that describes how Oracle requires a continuous connection to the Certified Platinum Configuration during delivery of Oracle Platinum Services, as described in the Oracle Platinum Services Technical Support Policy. The Appendix provides a table describing the user account access required by Oracle during the implementation and ongoing delivery of Oracle Platinum Services.

Displaying Credentials

Credential sets are displayed by *target type*, where in previous (pre-Oracle Advanced Support Gateway 9.*x*) versions of Oracle Advanced Support Gateway, credentials were displayed by *user* and *account*.

The Password Management page lists the managed accounts used by your Oracle Advanced Support Gateway implementation team for which passwords are currently stored in Oracle Password Vault.

Using Credential Management

To use the credential management features:

1. Log on to the portal.

   See "Logging onto the Gateway."

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Gateway** menu, select **Password Management**.

   The Password Management page appears.

   Credential sets are displayed by target type. You can view and manage target credentials using the target table.

   You can filter the credentials by the target type or name. For example, you can search for Exadata-specific accounts.

   You can use the Password Management page to:

   - Collect and change user credentials;
   - Populate Password Vault (and/or OEM) with passwords;
   - Edit credentials in bulk, that is, update multiple targets at the same time for a given credential or credentials;
   - Review the most up-to-date validation state of credentials.

About Credentials

There are different types of credential defined in Oracle Advanced Support Gateway:

- **Required** credentials. See "About Required Credentials."
- **Recommended** credentials. See "About Recommended Credentials."
- **Additional** credentials. See "About Additional Credentials."

About Required Credentials

Required Credentials are mandatory credentials required for monitoring Gateway targets. Unless these credentials are updated and committed to Password Vault, the target status is displayed as “Failed” as the target cannot be accessed and monitoring of the target cannot proceed. Examples include *orarom* and *dbsnmp*.

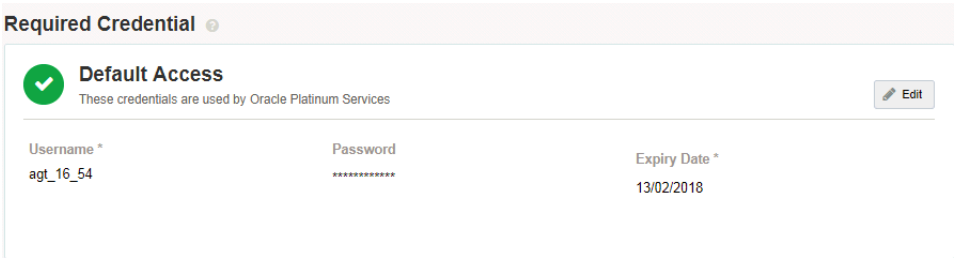
If **Required Credentials** are missing for a particular target, this is flagged using a red warning icon.

In previous releases of Oracle Advanced Support Gateway, **Required Credentials** were shared with Platinum engineers or Oracle engineers to configure in OEM to enable monitoring of targets. But in this release, the customer can directly configure credentials using the Credential Management page. These credentials are then updated in Password Vault as well as in OEM.

These credentials can be viewed and edited singly, or in bulk.

So, for example, in Figure 4–1, for this particular target, required credentials are required for default access by a number of Oracle Support Services.

Figure 4–1 Required Credentials for a Target



Related Information

Activating Services

About Recommended Credentials

About Additional Credentials

About Selected Targets and their Associated Credentials

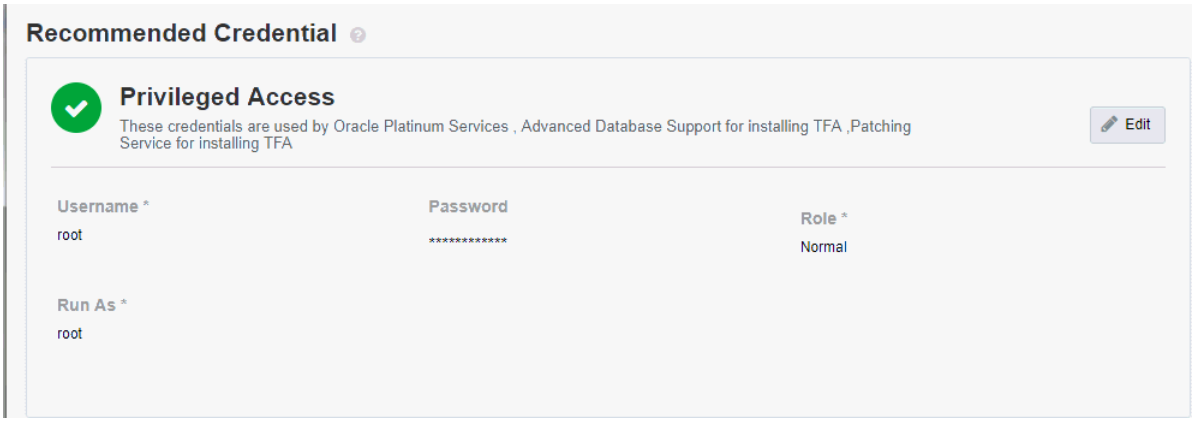
About Recommended Credentials

Recommended Credentials are credentials used to perform particular operations or deliver specific functionality on targets. These operations and functions could include installing Trace File Analyzer (TFA), performing database patching, running EXAchk scripts against an Exadata target, and so on. In other words, these credentials are a temporary requirement; the customer sets these credentials when asked and can later edit or delete them as required. Deleting the credentials does not delete the account from the target, but means that Platinum engineers or other Oracle service engineers can no longer access the targets through OEM or Password Vault. If the customer does not provide these credentials when required, the operation or function - running EXAchk for example - would fail. But not providing Recommended Credentials would not result in an inability to monitor the target.

These credentials can be viewed and edited singly, or in bulk.

So, for example, in Figure 4–2, for this particular target, recommended credentials are used by several services for installing TFA.

Figure 4–2 Recommended Credentials for a Target



Related Information

About Required Credentials

About Additional Credentials

About Selected Targets and their Associated Credentials

About Additional Credentials

Additional Credentials are those credentials - distinct from **Recommended Credentials** and **Required Credentials** - which customers wish to create and store in Password Vault. These credentials are typically used for testing or demonstration purposes.

Related Information

About Recommended Credentials

About Required Credentials

About Selected Targets and their Associated Credentials

About Selected Targets and their Associated Credentials

The following table displays a number of targets and their associated credentials.

Table 4–1 Targets and their Associated Credentials

Target	Required Credentials	Recommended Credentials
Compute/database node	orarom	root
Cell node	celladmin/cellmonitor	root
ILOM	root	Not applicable
Database instance	dbsnmp	Not applicable
PDU	root	Not applicable
ASM instance	asmsnmp	Not applicable
Cisco switch	admin	Not applicable
Infiniband switch	nm2user	root

Viewing Credentials

To view credentials by target type:

1. Log on to the portal.

   See "Logging onto the Gateway."

   The Oracle Advanced Support Gateway home page appears.

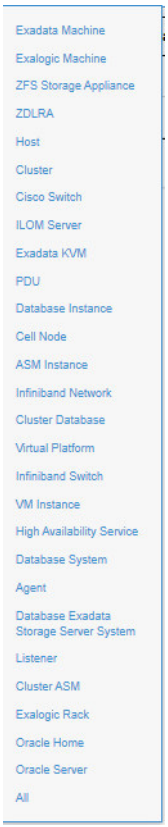
2. From the **Gateway** menu, select **Password Management**.

   The Password Management page appears.

   Credential sets are displayed by target type. You can view and manage target credentials using the target table.

3. To set the target type, select the required value in the filter list on the top right of the Password Management page. See Figure 4–3.

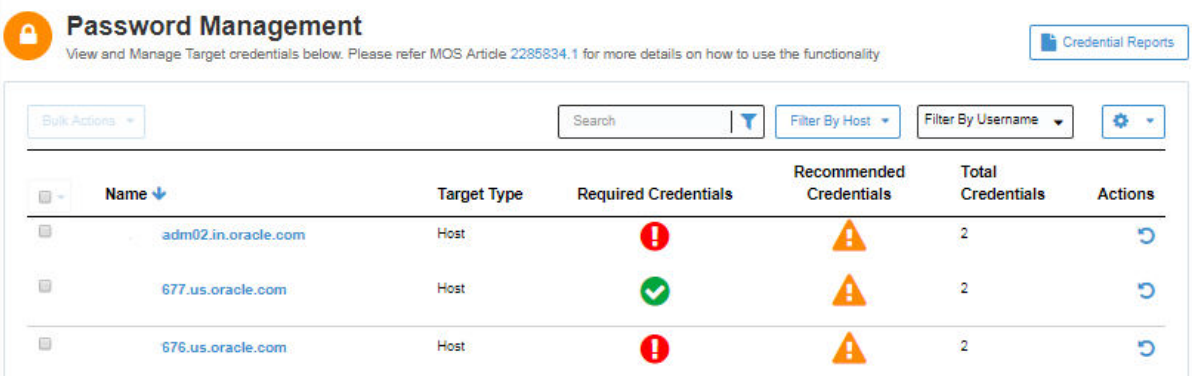
Figure 4–3 Selecting the Target Type



4. All values for the particular target type are displayed.

   See Figure 4–4 that shows the credentials for all host instances on a sample Oracle Advanced Support Gateway system.

Figure 4–4 Displaying Credentials for a Target Type



Related Information

Viewing Credentials for Target Children

Viewing Credentials for Target Children

You can view all credentials for a selected target type, for example, Exadata Machine, as well as its children by expanding the target link.

Editing Credentials

You can edit credentials singly, or in bulk. Refer to the following sections:

- "Editing Credentials Singly."
- "Editing Credentials in Bulk."

Editing Credentials Singly

To edit a credential singly:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Gateway** menu, select **Password Management**.

   The Password Management page appears.

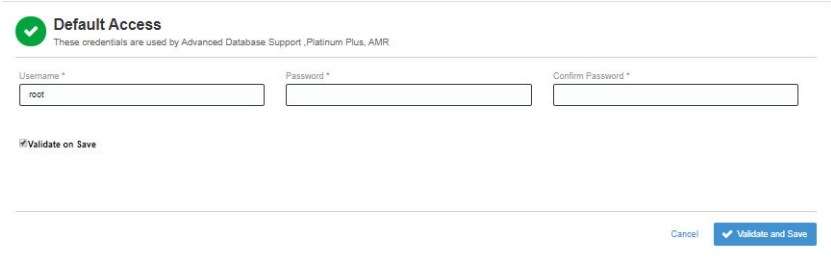
3. Drill down to the level of the target, or child of the target, as required.

   Select the required credential.

   Click **Edit**.

   The credential page appears. See Figure 4–5.

Figure 4–5 Editing Credentials for a Target



4. Edit the following fields as required:
   - **Username**: Enter the username of the target.
   - **Password**: Enter the password associated with the target username.
   - **Confirm Password**: Re-enter the password associated with the target username.
   - (Optional) **Validate on Save**: Select the **Yes** check box to validate the password prior to saving.

     Note: This field is not present for monitoring access, ILOM access, or ASM access.
   - **(Recommended Credentials Only)**

     Role: Select the role associated with the user.

     The options are *Normal* (the default) or *SUDO*.
   - **(Recommended Credentials Only)**

     Run as: Select the user to run as.
5. Click **Save** (or click **Validate and Save**).

Editing Credentials in Bulk

To edit credentials in bulk:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.
2. From the **Gateway** menu, select **Password Management**.

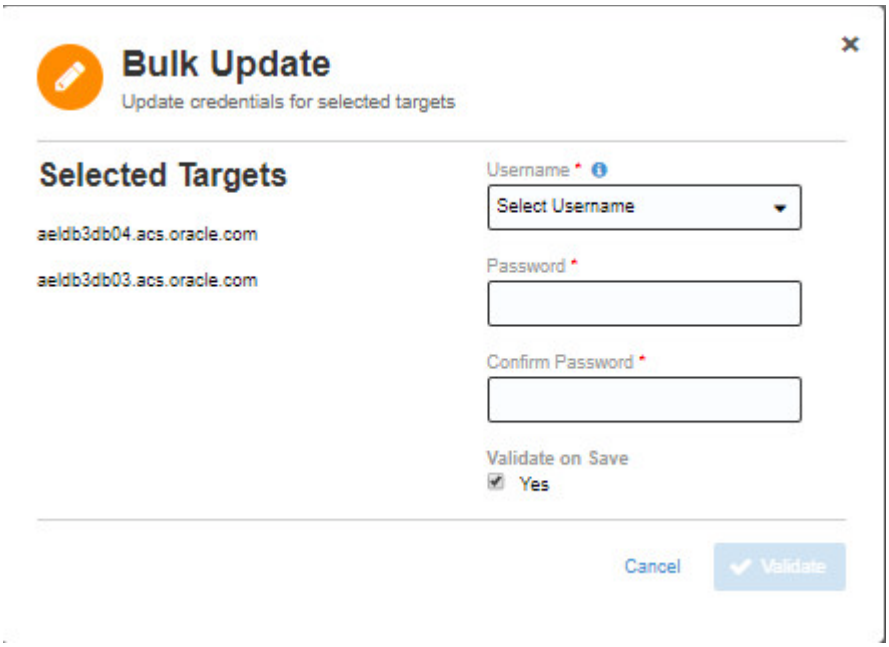
   The Password Management page appears.
3. Drill down to the level of the target, or child of the target, as required.

   Select the required targets, for example, two ILOM servers. You may first need to filter by user.

   When multiple selections are made, the Bulk Actions drop-down list is automatically enabled.
4. From the **Bulk Actions** drop-down list, select **Update**.
5. Select the target for which the bulk edits are required.

   The Bulk Edit> [*Credential Name*] page appears. See Figure 4–6.

Figure 4–6 Performing a Bulk Edit on a Credential



6. Edit the following fields as required:
   - **Username**: Enter the username to associate with the credential.
   - **Password**: Enter the password associated with the credential
   - **Confirm Password**: Re-enter the password associated with the credential.
   - (Optional) **Validate on Save**: Select the **Yes** check box to validate the password prior to saving.

     Note: This field is not present for monitoring access, ILOM access, or ASM access.
7. Click **Save**.

   Confirm the bulk edit.

   Note: The bulk edit overwrites the existing credentials for all selected targets.

Creating Credentials

The **Create New Credential** page enables you to create an additional credential on a target.

To create a credential:

1. Log in to Oracle Advanced Support Gateway.

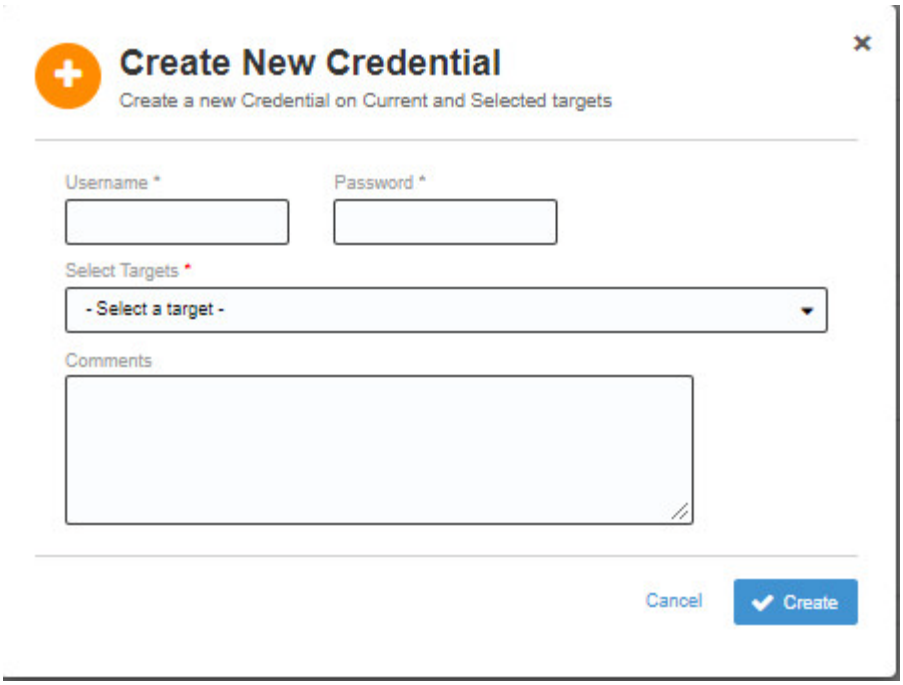
   The Oracle Advanced Support Gateway Home page appears.
2. From the **Gateway** menu, select **Password Management**.

   The Password Management page appears.
3. Drill down to the level of the target, or child of the target, as required.

   In the Additional Credentials section, click **Create New**.

   The Create New Credential page appears. See Figure 4–7.

Figure 4–7 Creating Credentials



4. Complete the following fields as required:
   - **Username**: Enter the username of the target.
   - **Password**: Enter the password associated with the target username.

     Note: The **Expiry Date field,** used to set the date on which the certificate expired, has been removed from this page.
   - **Select Targets**: From the list of available targets, select the Oracle Advanced Support Gateway target associated with the new credential.

     (Optional) Use the Ctrl key to make multiple selections.
   - (Optional) **Comments**: Add any information required, for example, to describe the credential owner or function. Any text entered in this field is appended to the "*These credentials are used by...*" subheading under the username.
5. Click **Create** to create the new credential.

About Credential Reports

You can use the credentials report table to view and manage target credentials.

Viewing Target Credentials

To view target credentials:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.
2. From the **Gateway** menu, select **Password Management**.

   The Password Management page appears.
3. In the top right of the page, click **Credential Reports**.

The credential list appears.

You can search for a particular credential, view a target associated with a credential, print the credential report, or save the report in Microsoft Excel or CSV format.

5

Provisioning Agents

This chapter provides information about using Oracle Advanced Support Gateway to install monitoring agents on standalone systems or to create a request to monitor an Oracle Engineered System.

This chapter consists of the following sections:

- About Provisioning Agents
- About Provisioning Agents for Engineered Systems
- About Provisioning Agents for Single Hosts
- Customizing Agent Install Settings
- Customizing Sample Host Files

About Provisioning Agents

You can use Oracle Advanced Support Gateway to perform automatic agent deployment. The Agent Provisioning feature - which is enabled by the **Add Agent** wizard - provides a framework for automating the end to end flow of Oracle Enterprise Manager (OEM) agent installation on database machines in customer environments.

Alternatively, you can use the Agent Provisioning feature - again enabled by the **Add Agent** wizard - to create a request for the monitoring of an Engineered System. This request is then submitted to an Oracle service engineer to complete the monitoring process.

Refer to the following sections:

- About Provisioning Agents for Engineered Systems
- About Provisioning Agents for Single Hosts

About Provisioning Agents for Engineered Systems

You can use Oracle Advanced Support Gateway to create a request to monitor the following Oracle Engineered Systems:

- Exadata
- Exalogic
- SuperCluster

Note: In order to monitor other Oracle Engineered Systems, such as Zero Data Loss Recovery Appliance, Exalytics In-Memory Machine, and so on, please refer to your Oracle representative for further details.

This section outlines how to collect and validate all required implementation information directly from the customer using the Gateway user interface. There are several stages in creating the monitoring request:

- **Welcome**: Introducing the wizard used to create the monitoring request and confirm the pre-requisite tasks;
- **Add System**: Adding a system, where *system* is understood to mean an Oracle Engineered System, as outlined above;
- **System Information**: Supplying information about the system;
- **Network Check**: Checking system connectivity;
- **Set Credentials**: Performing checks on the system credentials;
- **Full Network Check**: Checking end-to-end system connectivity;
- **Compliance Check**: Verifying system compliance and network connections;
- **Complete**: Submitting the provisioning request to Oracle and receiving confirmation of the request.

To use the Gateway to create a request for the monitoring of an Engineered System:

1. Log on to the Oracle Advanced Support Gateway portal.

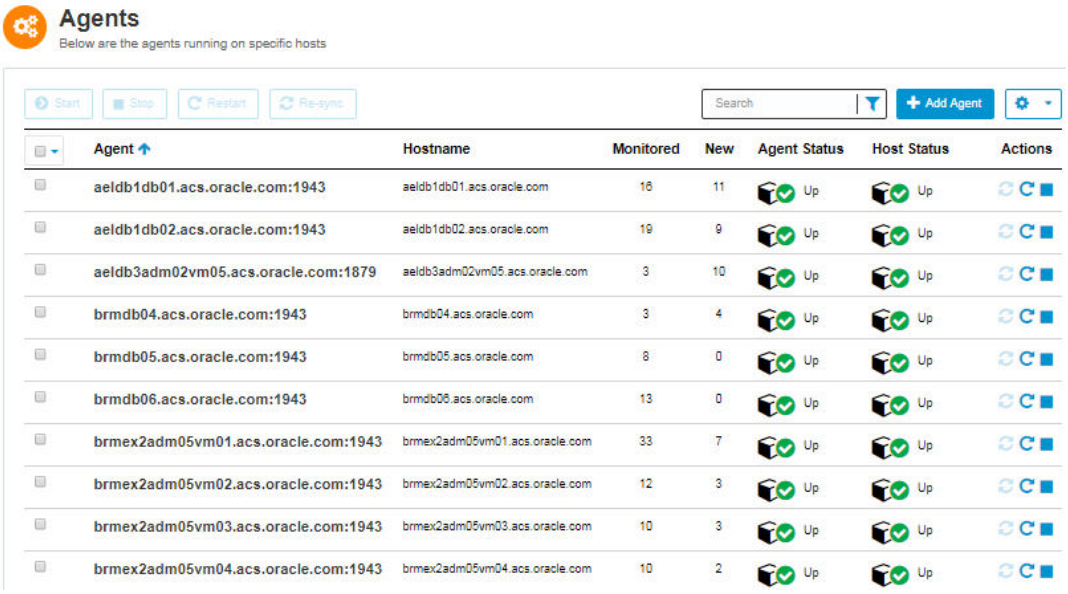
   The Oracle Advanced Support Gateway home page appears.

2. From the top-level **Admin** menu, select **Agents**.

   The Agents page is displayed.

   If there are existing agents running on specific systems, they are displayed on the page.

Figure 5–1 Viewing Agents Running on Specific Systems



3. Click **Add Agent**.

   The Welcome to the System and Host install Wizard page appears.

   This page provides information about tasks to be performed and information you'll need to access before getting started:

This wizard will help you install monitoring agents on standalone systems or create a request for the monitoring of an Engineered System. As part of the wizard workflow you will be requested to provide the following:

- Privileged system credentials;
- For standalone systems: IP addresses and their fully qualified hostnames (FQDN);
- For Engineered Systems: The Engineered System's schematic file, and CSI/MOS ID (and in the case of users of the Platinum Service, the associated Platinum Implementation SR (PISR) number);
- Additional custom install settings.

The wizard will perform the following checks before taking any actions:

- Validate the network connectivity between the Gateway and the hosts;
- Test credentials;
- Check each host meets minimum prerequisites for agent installation.

Before you get started:

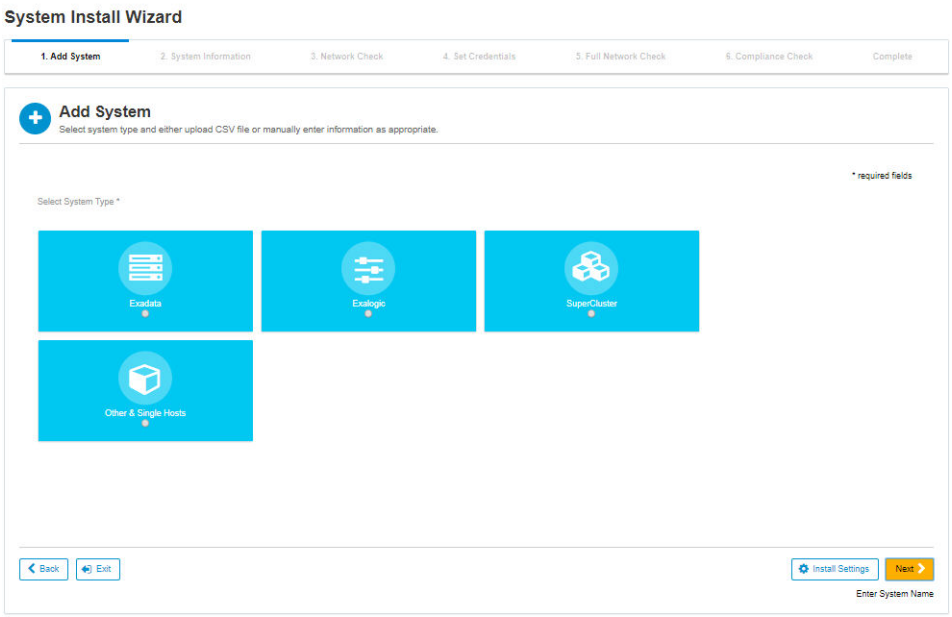
- Please review the Oracle Advanced Support Gateway Security Guide

As part of the wizard workflow, users are requested to provide IP address details and passwords for the required Engineered System. Checks are then performed to validate the network connectivity and passwords before a Service Request (SR) is created and submitted for an Oracle engineer to complete the remaining tasks.

4. (Optional) Select the **Don't show message again** check box so that the Welcome page is never again displayed as part of the Add Agent workflow.
5. Click **Get Started**.

   The Add System page appears.

Figure 5–2 Adding a System for the Agent



In general, you can add systems for agent installation by:

- Importing a schematic file by selecting a comma-separated value (CSV) file from your local computer, *or*
- Manually entering information, for example, system IP address, schematic directory, filename, and SSH credentials, as appropriate

To add a supported Oracle Engineered System, select one of the following options:

- **Exadata**. See "Adding an Oracle Exadata Engineered System."
- **Exalogic**. See "Adding an Oracle Exalogic Engineered System."
- **SuperCluster**. See "Adding an Oracle SuperCluster Engineered System."

Related Information

Adding a Single Host

Adding an Oracle Exadata Engineered System

To add an Exadata system:

1. Follow the initial steps in "About Provisioning Agents for Engineered Systems."
2. From the Select System Type field, select **Exadata.**
3. From the System Information field, select one of the following options:
   - **File Upload**. This option enables you upload a local file.

     Go to step 5.
   - **Remote Upload**. This option enables you to use the file URL from a remote system.

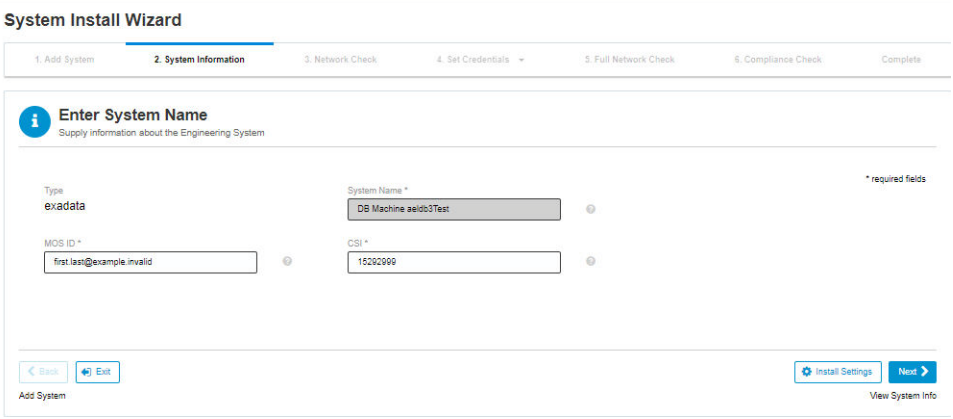
     Go to step 4.
4. (For a remote file upload) Complete the following fields:
   - **Host IP Address**: Enter the IP address of the system on which the file is located.
   - **Schematic Directory**: Enter the directory where the file is located.
   - **Filename**: Enter the full file name.
   - (Optional; if you want to provide SSH credentials) **Username**: Enter the user name associated with the directory.
   - (Optional; if you want to provide SSH credentials) **Password**: Enter the password associated with the user name.

   Continue to step 6.
5. (For a local file upload) In the **Local File** field, click **Browse**, and select a file on your local machine.

   Note: If you don't know how to find the CSV file, refer to instructions in `MOS document 2231081.1`. In particular, you need to raise an SR with My Oracle Support.
6. Click **Next**.

   The Enter System Name page appears. A sample is provided in Figure 5–3.

Figure 5–3 Supplying Engineered System Information



7. Supply the Engineered System information as follows:

   a. The **Type** field is automatically completed with the type of Engineered System. This field cannot be edited.

   b. The **System Name** field is automatically completed with the name of the Engineered System. Edit as required.

   c. In the **MOS ID** field, enter the My Oracle Support (MOS) Single Sign-On (SSO) email address associated with the hardware Customer Support Identifier (CSI) for the Engineered System.

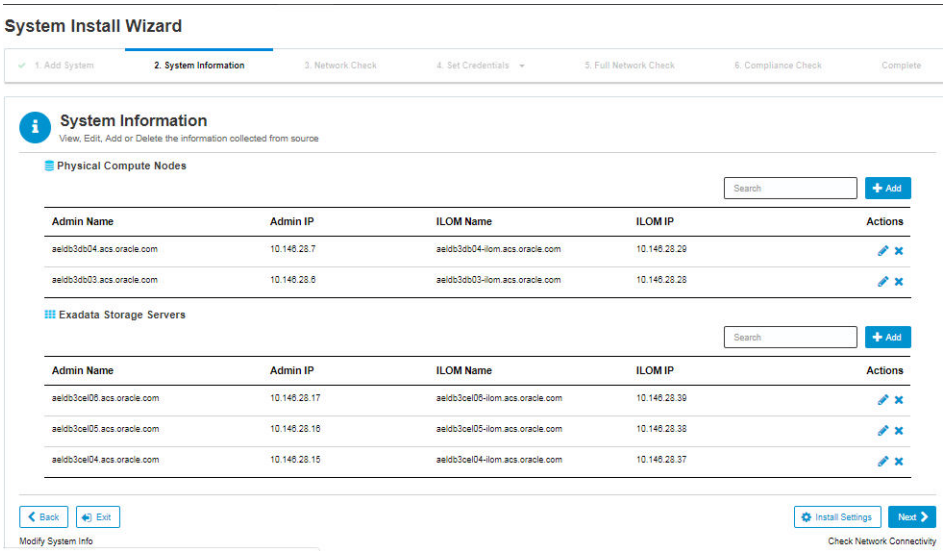
   d. In the **CSI** field, enter the Customer Support Identifier of the Engineered System.

      Note: A Customer Support Identifier (CSI) is a number issued to Oracle Support customers that must be quoted every time a fault for the relevant product or service, for example, Exadata or Platinum Services, is reported to Oracle Support.

8. Click **Next**.

   The View System Information page appears.

Figure 5–4 Viewing System Information



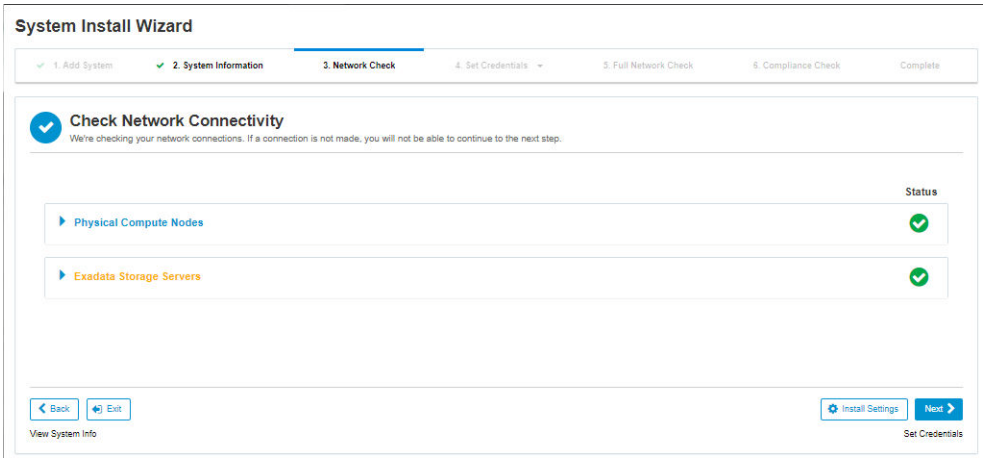
9. Confirm the information collected from the source file.

For example, in the Physical Compute Nodes and Exadata Storage Servers sections, review the systems defined by admin name, admin IP, ILOM name, and ILOM IP.

10. Click **Next**.

    The Check Network Connectivity page appears.

Figure 5–5 Checking Network Connectivity



11. Review the connectivity checks (Netcheck) back to the Gateway for all of the targets uploaded through the schematic file. Expand the type sections, for example, Exadata Storage Servers, to review the details.

    Note: If any mandatory test fails, it is not possible to proceed to the next stage of adding the Engineered System.

    A typical message advises that "The service on the destination must be available and any firewalls between the Gateway and the endpoint must have the required firewall rules (IP address, port, and protocol) that allow for remote connectivity. The ports and protocols are specified in the Network Protocol and Port Matrix of `Oracle Advanced Support Gateway Security Guide`".

    Note: If any non-mandatory test fails, you should review the warning message and take appropriate action before proceeding to the next stage of adding the Engineered System.

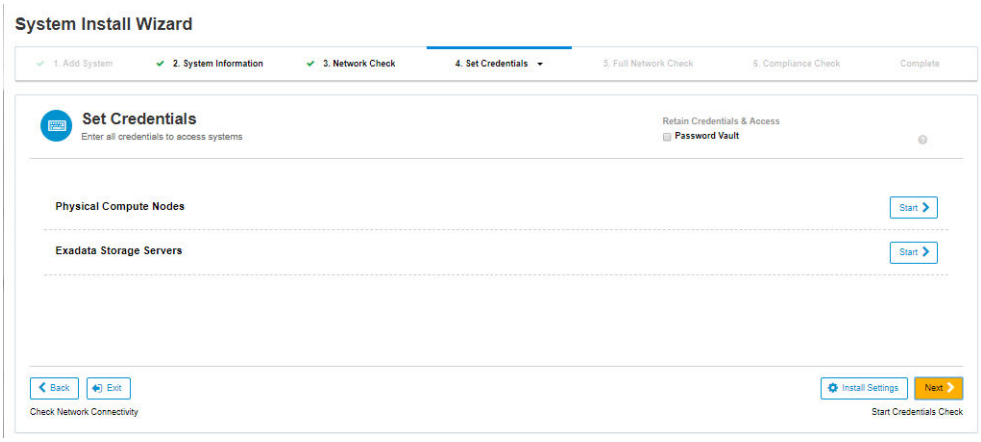
    a. (Optional) Click **Back** to change system details.

    b. (Optional) Click **Retest** to run the connectivity tests again.

    c. Click **Next**.

       The Set Credentials page appears.

Figure 5–6 Setting Engineered System Credentials



12. Supply user credentials for each target to perform validation.

    For database servers and compute nodes:

    a. Click **Start** to begin the validation process for the target group, that is, database servers or compute nodes.

    b. (Optional) In the **Credentials** field, select the **Same for All** check box to apply the credentials to all servers of the same type (database servers).

    c. In the **Host Username** field, enter the name of the system.

    d. In the **Host Password** field, enter the password associated with the system.

       (Optional) Toggle the eye icon to view or hide the details.

    e. In the **Priv Mode** field, select the mode to be used to gain the required root level privilege on the system. The options are **sudo**, **su**, and **pfexec**.

    f. In the **Root Password** field, enter the root password associated with the system.

       (Optional) Toggle the eye icon to view or hide the details.

    g. In the **ILOM Username** field, enter the ILOM username.

    h. In the **ILOM Password** field, enter the password associated with the ILOM.

       (Optional) Toggle the eye icon to view or hide the details.

    In the Monitoring Credentials credentials section, you need to provide details for monitoring that are saved for future usage but which are not validated.

    Complete the following fields to configure monitoring credentials for the Physical Compute Nodes:

    a. In the **Database** field, enter the database name.

    b. In the **DBSNMP Password** field, enter the SNMP password associated with the database.

       (Optional) Toggle the eye icon to view or hide the details.

    c. In the **ASM Cluster Name** field, enter the name of the Automatic Storage Management (ASM) Cluster.

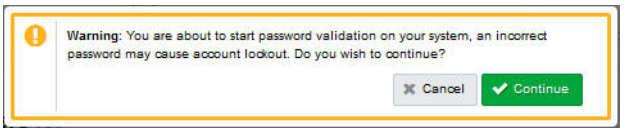
    d. In the **ASMSNMP Password** field, enter the SNMP password associated with the Automatic Storage Management (ASM) Cluster.

       (Optional) Toggle the eye icon to view or hide the details.

e. Click **Next**.

A warning popup appears: supplying incorrect passwords may result in being locked out of your account.

Figure 5–7 Target Validation Warning



For Exadata storage servers:

a. (Optional) In the **Credentials** field, select the **Same for All** check box to apply the credentials to all servers of the same type (Exadata storage servers).

b. The **Host Username** field contains the value, *root*. This field cannot be edited.

c. In the **Host Password** field, enter the root password.

(Optional) Toggle the eye icon to view or hide the details.

d. In the **ILOM Username** field, enter the ILOM username.

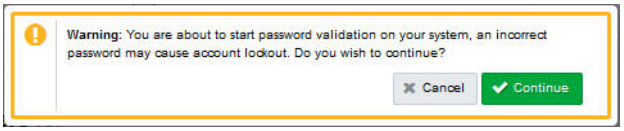
e. In the **ILOM Password** field, enter the password associated with the ILOM.

(Optional) Toggle the eye icon to view or hide the details.

f. Click **Next**.

A warning popup appears: supplying incorrect passwords may result in being locked out of your account.

Figure 5–8 Target Validation Warning



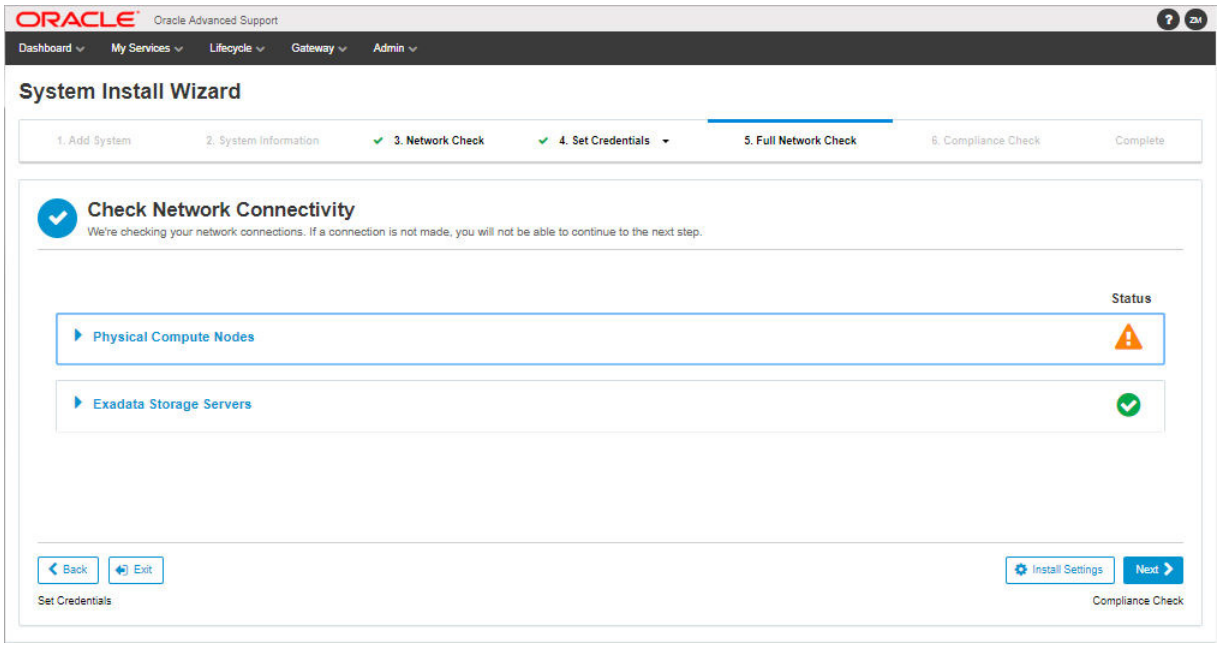
g. Click **Continue**.

The validation check is run and a message appears, stating that the credentials have been validated.

h. Click **Next**.

The Check Network Connectivity page appears.

Figure 5–9 Checking Whole Network Connectivity

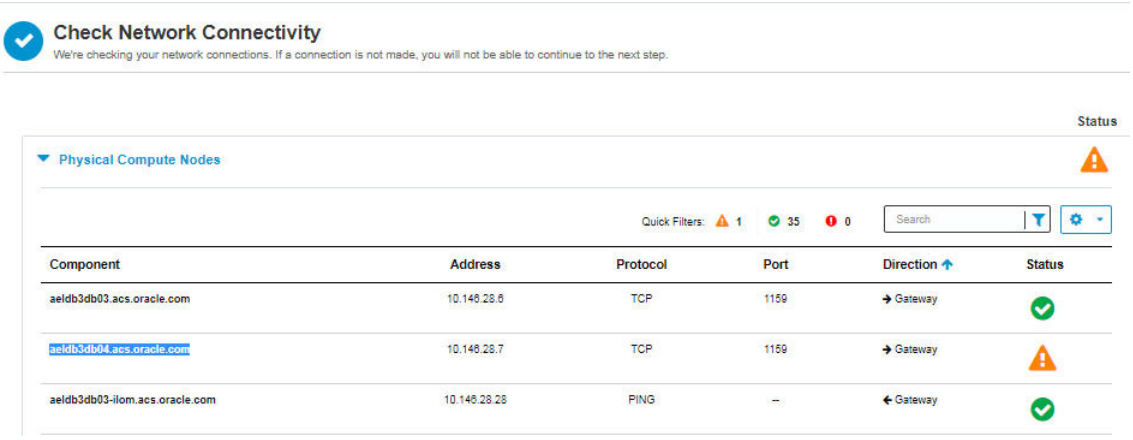


All network connections (that is, to ***or*** from the Gateway to the device) are checked.

If a connection is not made, then a status of *Failed* is displayed as shown for the Physical Compute Nodes in Figure 5–9.

Expand the Physical Compute Nodes to view the node, in this case, *aeldb3db04.acs.oracle.com*, that is failing the connectivity check. See Figure 5–10.

Figure 5–10 Viewing Failing Network Connectivity

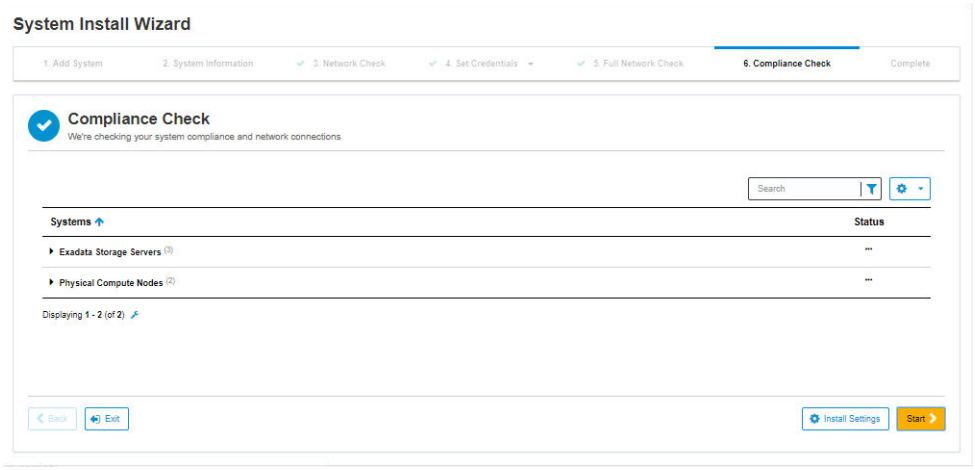


Reconfigure the failing connection and validate it before continuing. When all connectivity passes, continue to the next step.

i. Click **Next**.

The Compliance Check page appears.

Figure 5–11 Checking System Compliance and Network Connections

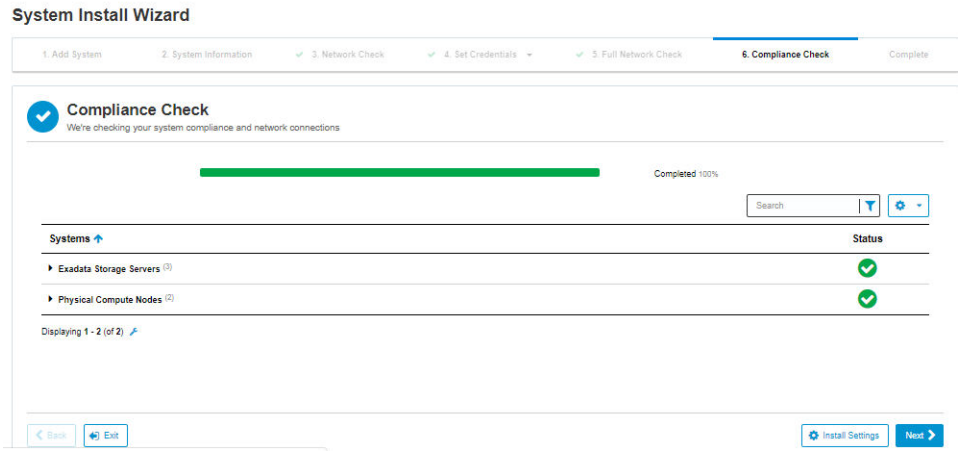


13. To enable Oracle to validate system compliance and network connections:

    a. Click **Start**.

    A progress bar measures the rate of system validation. When it reaches 100%, system status displays as complete and a message appears stating that the compliance check passed successfully.

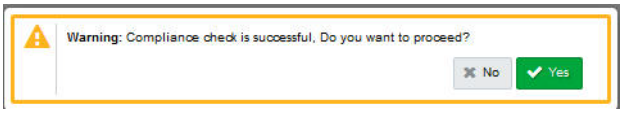
Figure 5–12 System Compliance Validated



    b. Click **Next**.

    A warning message appears stating that the compliance check is successful, and asking whether you would like to proceed.

Figure 5–13 Completing System Installation



    c. Click **Yes**.

    The Submit Provisioning Request to Oracle page appears.

This page states that the system precheck has been completed (that is, all system information has been validated.)

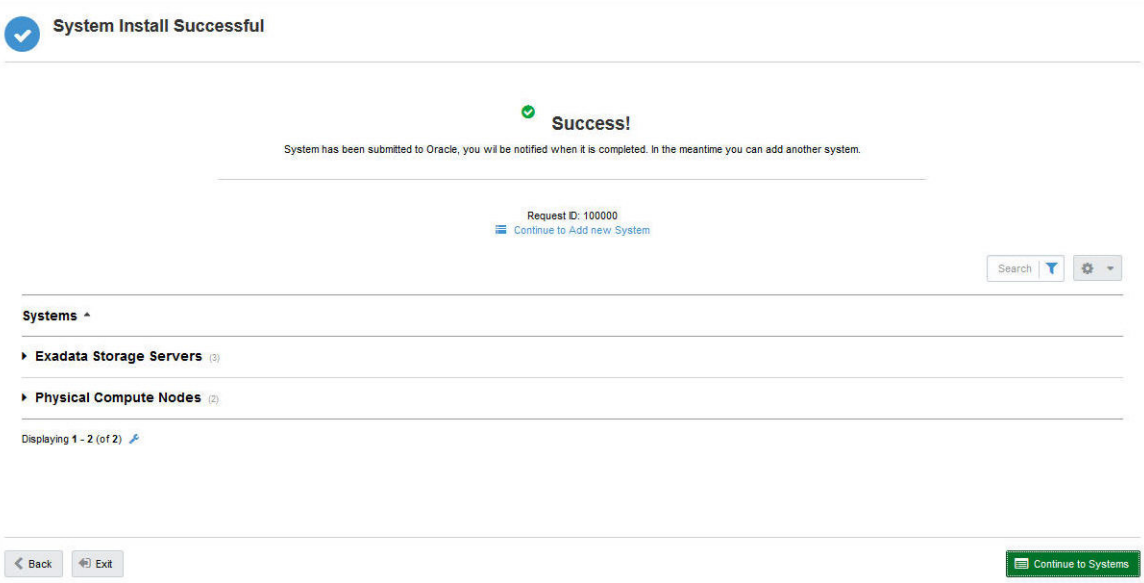
To proceed with system installation, submit the provisioning request for the Engineered System to Oracle.

14. Click **Submit Details to Oracle**.

    A provisioning request is submitted to Oracle. You will be notified when it is completed.

    The System Install Successful page appears.

Figure 5–14 System Installation Successful



15. A service activation request summary is sent to the customer contact by email. It states:

    ```
    Dear Customer,

    We have received your request and will start the planning process for
    <Service Name> Activation on your Exadata sytem <Exa_system_name>.
    Below is a summary of your Service Activation request.
    ```

    See the following table which provides a sample summary response from Oracle.

    Note: Certain values in the table have been obfuscated for security reasons.

Field	Sample value
Request ID	4
System Type	Exadata
System Name	<Exadata_system_name>
HW CSI	*15262999*
Rack Serial Number	<Exa_serial_number>
Gateway	<Gateway_name>
Requested Date DD/MM/YYYY	For example, 11/04/2019
Customer	<Customer_name>

Field	Sample value
Customer Contact	<Customer_contact_name>
Implementation Contact	<Oracle_Implementation_Engineer_contact_name>

16. At this point, you can perform one of the following actions:
    - Select **Continue to Add new System** to install a monitoring agent on a standalone system or to create a request for the monitoring of an Oracle Engineered System.
    - Select **Continue to Systems** to revert to the Systems and Hosts page.

      See Chapter 6, "Managing Systems."
    - Select **Exit** to revert to the Systems and Hosts page.

      See Chapter 6, "Managing Systems."

Adding an Oracle Exalogic Engineered System

To add an Exalogic system:

1. Follow the initial steps in "About Provisioning Agents for Engineered Systems."

   Note: You can review the screengrabs referred to in the following steps in the section on "Adding an Oracle Exadata Engineered System."
2. From the Select System Type field, select **Exalogic.**
3. From the System Information field, select one of the following options:
    - **File Upload**. This option enables you upload a local file.

      Go to step 4.
    - **Remote Upload**. This option enables you to use the file URL from a remote system.

      Go to step 5.
4. (For a remote file upload) Complete the following fields:
    - **Host IP Address**: Enter the IP address of the host on which the file is located.
    - **Schematic Directory**: Enter the directory where the file is located.
    - **Filename**: Enter the full file name.
    - (Optional; if you want to provide SSH credentials) **Username**: Enter the user name associated with the directory.
    - (Optional; if you want to provide SSH credentials) **Password**: Enter the password associated with the user name.

   Continue to step 6.
5. (For a local file upload) In the **Local File** field, click **Browse**, and select a file on your local machine.
6. Click **Next**.

   The Enter System Name page appears.
7. Supply the Engineered System information as follows:
    a. The **Type** field is automatically completed with the type of Engineered System. This field cannot be edited.

b. The **System Name** field is automatically completed with the name of the Engineered System. Edit as required.

c. In the **MOS ID** field, enter the My Oracle Support (MOS) Single Sign-On (SSO) email associated with the hardware Customer Support Identifier (CSI) for the Engineered System.

d. In the **CSI** field, enter the Customer Support Identifier of the Engineered System.

Note: A Customer Support Identifier (CSI) is a number issued to Oracle Support customers that must be quoted every time a fault for the relevant product or service, for example, Exalogic or Platinum Services, is reported to Oracle Support.

8. Click **Next**.

The View System Information page appears.

9. Confirm the information collected from the source file.

10. Click **Next**.

The Check Network Connectivity page appears.

11. Review the connectivity checks (Netcheck) back to the Gateway for all of the targets uploaded through the schematic file.

Note: If any mandatory test fails, it is not possible to proceed to the next stage of adding the Engineered System.

A typical message advises that "The service on the destination must be available and any firewalls between the Gateway and the endpoint must have the required firewall rules (IP address, port, and protocol) that allow for remote connectivity. The ports and protocols are specified in the Network Protocol and Port Matrix of Oracle Advanced Support Gateway Security Guide".

Note: If any non-mandatory test fails, you should review the warning message and take appropriate action before proceeding to the next stage of adding the Engineered System.

a. (Optional) Click **Back** to change system details.

b. (Optional) Click **Retest** to run the connectivity tests again.

c. Click **Next**.

The Set Credentials page appears.

12. Supply user credentials for each target to perform validation.

For database servers:

a. (Optional) In the **Credentials** field, select the **Same for All** check box to apply the credentials to all servers of the same type (database servers).

b. In the **Host Username** field, enter the name of the system.

c. In the **Host Password** field, enter the password associated with the system.

(Optional) Toggle the eye icon to view or hide the details.

d. In the **Priv Mode** field, select the mode to be used to gain the required root level privilege on the system. The options are **sudo**, **su**, and **pfexec**.

e. In the **Root Password** field, enter the root password associated with the system.

(Optional) Toggle the eye icon to view or hide the details.

f. In the **ILOM Username** field, enter the ILOM username.

g. In the **ILOM Password** field, enter the password associated with the ILOM.

(Optional) Toggle the eye icon to view or hide the details.

h. In the Retain Credentials and Access section in the top-right corner of the page, select the **Password Vault** check-box to upload the credentials into Oracle Password Vault once validation is complete.

i. Click **Validate**.

A warning popup appears: supplying incorrect passwords may result in being locked out of your account.

j. Click **Continue**.

The validation check is run and a message appears, stating that the credentials have been validated.

k. Click **Next**.

The Check Network Connectivity page appears.

13. To check end-to-end connectivity:

a. All network connections (that is, *to* or *from* the Gateway to the device) are checked.

If a connection is not made, then a status of *Failed* is displayed.

Reconfigure the failing connection and validate it before continuing. When all connectivity passes, continue to the next step.

b. Click **Next**.

The Compliance Check page appears.

14. To enable Oracle to validate system compliance and network connections:

a. Click **Start**.

A progress bar measures the rate of system validation. When it reaches 100%, system status displays as complete and a message appears stating that the compliance check passed successfully.

b. Click **Next**.

A warning message appears stating that the compliance check is successful, and asking whether you would like to proceed.

c. Click **Yes**.

The Submit Provisioning Request to Oracle page appears.

15. Click **Submit Details to Oracle**.

The System Install Successful page appears.

System prechecks are complete, and a provisioning request is submitted to Oracle.

A service activation request summary is sent to the customer contact by email.

Adding an Oracle SuperCluster Engineered System

To add a SuperCluster system:

1. Follow the initial steps in "About Provisioning Agents for Engineered Systems."

Note: You can review the screengrabs referred to in the following steps in the section on "Adding an Oracle Exadata Engineered System."

2. From the Select System Type field, select **SuperCluster.**

3. From the System Information field, select one of the following options:
   - **File Upload**. This option enables you upload a local file.

     Go to step 5.
   - **Remote Upload**. This option enables you to use the file URL from a remote system.

     Go to step 4.
4. (For a remote file upload) Click **Remote Upload File** and complete the following fields:
   - **Host IP Address**: Enter the IP address of the system on which the file is located.
   - **Schematic Directory**: Enter the directory where the file is located.
   - **Filename**: Enter the full file name.
   - **Username**: Enter the user name associated with the directory.
   - **Password**: Enter the password associated with the user name

   Continue to step 6.
5. (For a local file upload) In the **Local File** field, click **Browse**, and select a file on your local machine.
6. Click **Next**.

   The Enter System Name page appears.
7. Supply the Engineered System information as follows:
   a. The **Type** field is automatically completed with the type of Engineered System. This field cannot be edited.
   b. The **System Name** field is automatically completed with the name of the Engineered System. Edit as required.
   c. In the **MOS ID** field, enter the My Oracle Support (MOS) Single Sign-On (SSO) email associated with the hardware Customer Support Identifier (CSI) for the Engineered System.
   d. In the **CSI** field, enter the Customer Support Identifier of the Engineered System.

      Note: A Customer Support Identifier (CSI) is a number issued to Oracle Support customers that must be quoted every time a fault for the relevant product or service, for example, Exalogic or Platinum Services, is reported to Oracle Support.
8. Click **Next**.

   The View System Information page appears.
9. Confirm the information collected from the source file.
10. Click **Next**.

    The Check Network Connectivity page appears.
11. Review the connectivity checks (Netcheck) back to the Gateway for all of the targets uploaded through the schematic file. Expand the type sections, such as ZFS Storage or Compute Nodes, to review the details.

    Note: If any mandatory test fails, it is not possible to proceed to the next stage of adding the Engineered System.

    A typical message advises that “The service on the destination must be available and any firewalls between the Gateway and the endpoint must have the required firewall rules (IP address, port, and protocol) that allow for remote connectivity. The ports and protocols are

specified in the Network Protocol and Port Matrix of Oracle Advanced Support Gateway Security Guide".

Note: If any non-mandatory test fails, you should review the warning message and take appropriate action before proceeding to the next stage of adding the Engineered System.

a. (Optional) Click **Back** to revise the system details.

b. (Optional) Click **Retest** to run the connectivity tests again.

c. Click **Next**.

   The Set Credentials page appears.

12. Supply user credentials for each target to perform validation.

    For database servers:

    a. (Optional) In the **Credentials** field, select the **Same for All** check box to apply the credentials to all servers of the same type (database servers).

    b. In the **Host Username** field, enter the name of the system.

    c. In the **Host Password** field, enter the password associated with the system.

       (Optional) Toggle the eye icon to view or hide the details.

    d. In the **Priv Mode** field, select the mode to be used to gain the required root level privilege on the system. The options are **sudo**, **su**, and **pfexec**.

    e. In the **Root Password** field, enter the root password associated with the system.

       (Optional) Toggle the eye icon to view or hide the details.

    f. In the **ILOM Username** field, enter the ILOM username.

    g. In the **ILOM Password** field, enter the password associated with the ILOM.

       (Optional) Toggle the eye icon to view or hide the details.

    For Exadata storage servers and ZFS storage arrays:

    a. (Optional) In the **Credentials** field, select the **Same for All** check box to apply the credentials to all servers of the same type (Exadata storage servers).

    b. The **Host Username** field contains the value, *root*. This field cannot be edited.

    c. In the **Host Password** field, enter the root password.

       (Optional) Toggle the eye icon to view or hide the details.

    d. In the **ILOM Username** field, enter the ILOM username.

    e. In the **ILOM Password** field, enter the password associated with the ILOM.

       (Optional) Toggle the eye icon to view or hide the details.

    f. Click **Validate**.

       A warning popup appears: supplying incorrect passwords may result in being locked out of your account.

    g. Click **Continue**.

       The validation check is run and a message appears, stating that the credentials have been validated.

    h. Click **Next**.

       The Check Network Connectivity page appears.

13. To check end-to-end connectivity:
    a. All network connections (that is, *to* or *from* the Gateway to the device) are checked.

       If a connection is not made, then a status of *Failed* is displayed.

       Reconfigure the failing connection and validate it before continuing. When all connectivity passes, continue to the next step.

    b. Click **Next**.

       The Compliance Check page appears.
14. To enable Oracle to validate system compliance and network connections:
    a. Click **Start**.

       A progress bar measures the rate of system validation. When it reaches 100%, system status displays as complete and a message appears stating that the compliance check passed successfully.

    b. Click **Next**.

       A warning message appears stating that the compliance check is successful, and asking whether you would like to proceed.

    c. Click **Yes**.

       The Submit Provisioning Request to Oracle page appears.
15. Click **Submit Details to Oracle**.

    System prechecks have been completed, and a provisioning request is submitted to Oracle.

    The System Install Successful page appears.
16. A service activation request summary is sent to the customer contact by email.
17. At this point, you can perform one of the following actions:
    - Select **Continue to Add new System** to install a monitoring agent on a standalone host or to create a request for the monitoring of an Oracle Engineered System.
    - Select **Continue to Systems** to revert to the Systems and Hosts page.

      See Chapter 6, "Managing Systems."
    - Select **Exit** to revert to the Systems and Hosts page.

      See Chapter 6, "Managing Systems."

About Provisioning Agents for Single Hosts

You can use Oracle Advanced Support Gateway to perform automatic agent deployment. The Agent Provisioning feature provides a framework for automating the end to end flow of OEM agent installation on database machines in customer environments.

As only a single agent may be installed on a host, the Agent Install Wizard (Single Host option) prevents a user from submitting a request to install an agent if it determines that an agent is already present on the target. An error message is displayed if a user attempts to add more than one agent on a host.

Note: Provisioning agents for single hosts is not supported for customers that avail of Oracle Platinum Services.

This automation workflow consists of a number of stages:

- Adding a system

- Performing checks on the system credentials
- Verifying the agent installation prerequisites
- Deploying the agent on target machines

The installation process automatically creates the OS user for the agent and its home directory. It installs the necessary software, performs connectivity checks back to the Gateway, and creates an */etc/hosts* entry for the Gateway on your system.

Prerequisites to Installing an OEM Agent

Prior to deploying an OEM agent using the Oracle Advanced Support Gateway, ensure that your system meets the prerequisite package requirements for Enterprise Manager Cloud Control, specifically the packages required on different platforms (32-bit and 64-bit) for installing an OMS or a Management Agent.

Refer to Package Requirements for Enterprise Manager Cloud Control.

Adding a Single Host

To use the Gateway to add an agent:

1. Log on to the Oracle Advanced Support Gateway portal.

   The dashboard screen appears.

2. From the top-level **Admin** menu, select **Agents**.

   The Agents page appears.

   From the list of agents running on specified hosts, you can search for a particular agent instance, start, stop, or restart an agent, resynchronize an agent, change an agent password, and so on.

   You can also add a new agent.

3. Click **Add Agent**.

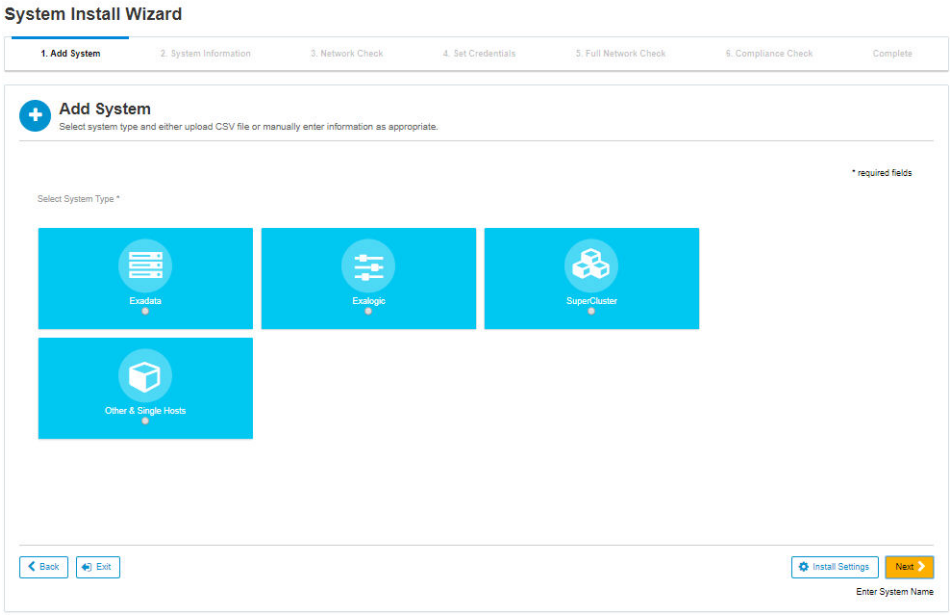
   The Welcome to the System and Host install Wizard page appears.

   This page provides information about tasks to be performed and information you'll need to access before getting started.

4. Click **Get Started**.

   The Add System page appears.

Figure 5–15 Adding a System for the Agent



5. From the Select System Type field, select **Other & Single Hosts**.

   The Agent Install: Add Host page appears.

Figure 5–16 Adding Hosts

6. Supply the system details by clicking **Import** to upload system information in the form of a CSV file from your local computer, or by manually entering them:

   a. In the **Hostname** field, enter the hostname or fully-qualified domain name (FQDN) of the system.

      Note: Oracle Advanced Support Gateway is configured to use Domain Name Service (DNS.)

   b. In the **IP Address** field, enter the IP address of the system.

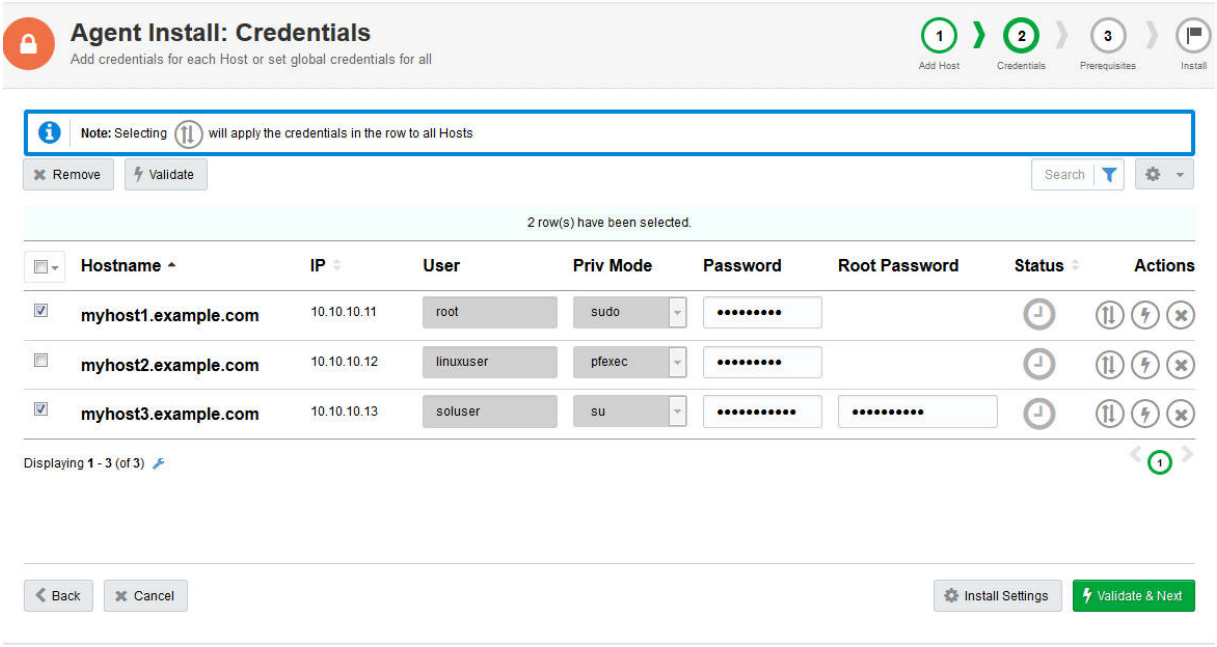
   c. (Optional) Click **Add Host** to add another system.

   d. (Optional) Edit the default agent installation settings. See "Customizing Agent Install Settings."

7. Click **Next**.

   The Agent Install: Credentials page appears.

Figure 5–17 Adding Agent Credentials



8. Supply credentials for each system or set global credentials for all as follows:

   a. In the **User** field, enter the name of the user associated with the system.

      Note: For imported system information, the **User** field is automatically completed, and this field cannot be edited.

   b. In the **Priv Mode** field, select the mode to be used to gain the required root level privilege on the system. The options are **sudo**, **su**, and **pfexec**.

      Note: For imported system information, the **Priv Mode** field is automatically completed, and this field cannot be edited.

   c. In the **Password** field, enter the password associated with the system.

   d. In the **Root Password** field, enter the root password associated with the system.

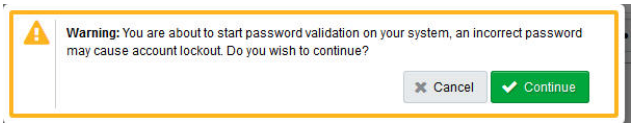
   e. (Optional) Select the check box corresponding to a system and click the arrows icon to apply the credentials in the row to all systems.

   f. (Optional) Select the check box corresponding to a system and click the lightning icon to validate the credentials of a particular system.

   g. Click **Validate and Next**.

      A warning message appears stating that the compliance check is successful, and asking whether you would like to proceed.

Figure 5–18 Completing System Installation



   h. Click **Continue**.

A message appears stating that the system credentials are being validated. Validation progress is shown by the spinning **Status** icon.

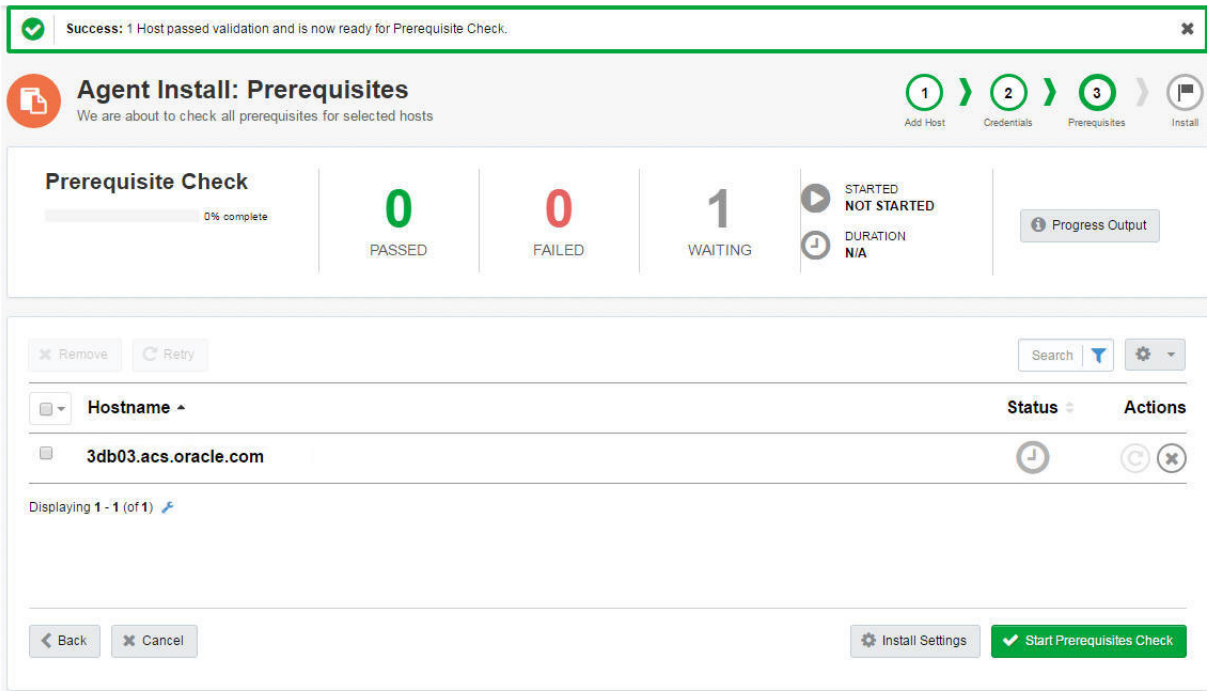
If validation of a system fails, a message appears stating that the system failed credential validation and that the user should review the information and attempt validation again. The **Status** icon changes to a red exclamation mark to denote a failed validation attempt.

If validation of a system succeeds, a message appears stating that the system credential were validated. The **Status** icon changes to a green correct mark to denote a successful validation attempt.

i. Click **Next**.

The Agent Install: Prerequisites page appears.

Figure 5–19 Checking Agent Installation Prerequisites



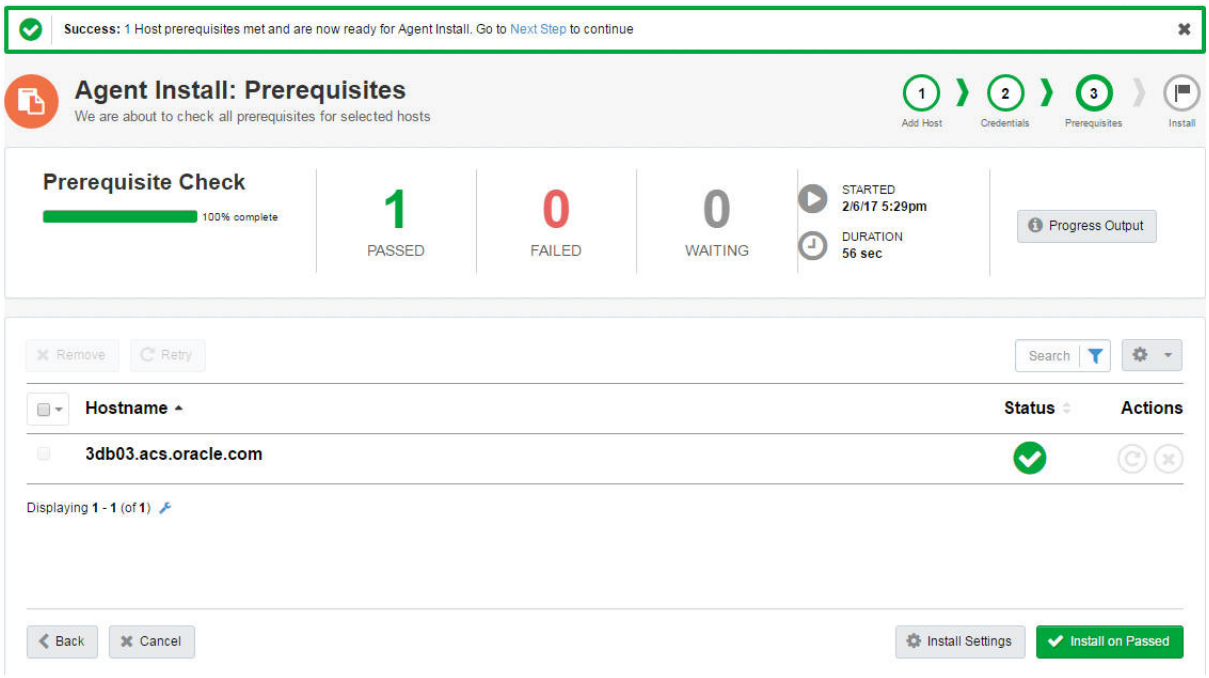
9. Click **Start Prerequisites Check** to ensure that the system meets all prerequisite checks.

Note: If any mandatory test fails, it is not possible to proceed to the next stage of adding the agent.

Note: If any non-mandatory test fails, you should review the warning message and take appropriate action before proceeding to the next stage of adding the agent.

The progress bar displays the results of the check. When the check is complete, a success message appears stating that the system prerequisites are met and that agent installation can now be performed.

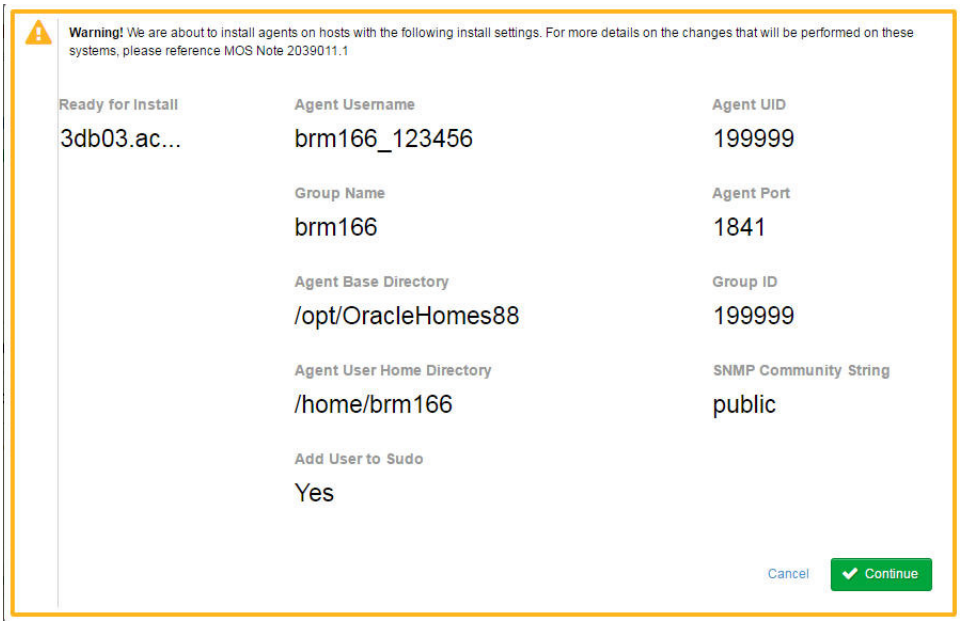
Figure 5–20 Passing Agent Installation Prerequisites



10. Click **Install on Passed** to perform agent installation.

    A warning message appears stating that the agent will be installed on the selected system, and recommends reading a My Oracle Support (MOS) article to ensure users are aware of the scope and nature of the changes:

Figure 5–21 Agent Installation: System Warning



11. Click **Continue**.

Review agent installation progress.

Note: Agent installation may take a number of minutes. The duration depends on the number of systems, and on the number of agents being installed.

a. The **Installed** field displays the number of agents that have successfully installed.

b. The **Failed** field displays the number of agents that did not successfully install.

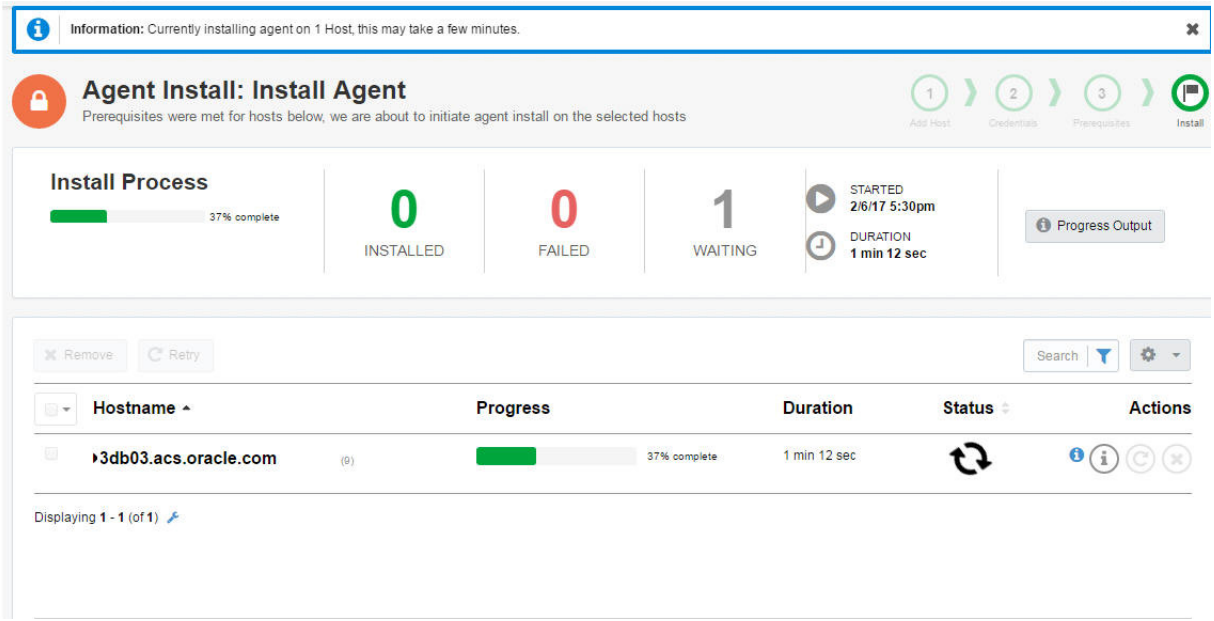
c. The **Waiting** field displays the number of agents pending installation.

d. The **STARTED** field displays the time at which installation commenced.

e. The **DURATION** field displays the time taken for installation.

See Figure 5–22 that shows the installation progress of an agent.

Figure 5–22 Agent Installation: Progress



12. When agent installation is complete, a successful installation message appears.

Related Information

About Provisioning Agents for Engineered Systems

Customizing Agent Install Settings

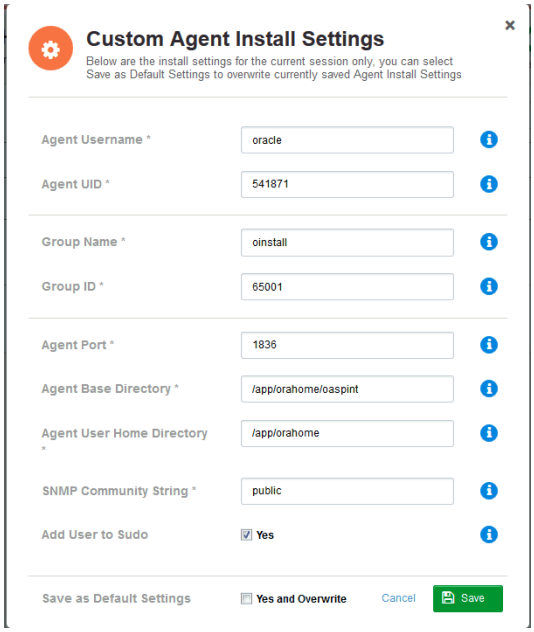
You can edit the installation settings for the current session only, or save the revised settings as the default installation settings.

To apply custom installation settings:

1. On the Agent Install: Add Host page, click **Install Settings**.

The Custom Agent Install Settings page appears. A sample is shown in Figure 5–23.

Figure 5–23 Customizing the Agent Install Settings



2. Accept the install settings for the current session only:
   a. The **Agent Username** field displays a valid agent user name.

      The default is `oracle`.
   b. The **Agent UID** field displays a valid agent user identifier.

      The default is `541871`.
   c. The **Group Name** field displays a valid group name.

      The default is `oinstall`.
   d. The **Group ID** field displays a valid group identifier.

      The default is `65001`.
   e. The **Agent Port** field displays a valid agent port number in the range 1830 to 1849.

      The default is `1836`.
   f. The **Agent Base Directory** field displays a valid agent base directory.

      The default is `/app/orahome/oaspint`.
   g. The **Agent Port** field displays a valid agent port number in the range 1830 to 1849.

      The default is `1836`.
   h. The **Agent User Home Directory** field displays a valid agent user home directory.

      The default is `/app/orahome`.
   i. The **SNMP Community String** field displays a valid SNMP community string.

      The default is `/app/orahome`.
   j. (Optional) Select the **Add User to Sudo** check box to add User to Sudo.

      The default is checked.

3. In the **Save as Default Settings** field, click **Save** to save the installation settings for the current session only.

   (Optional) select the **Yes and Overwrite** check box to save the revised settings as the default installation settings.

Customizing Sample Host Files

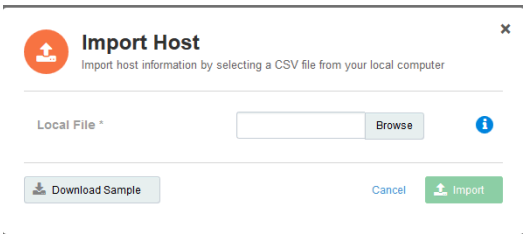
You can import system information by selecting a comma-separated value (CSV) file locally, or by using a sample file provided by Oracle.

To import a system:

1. On the Agent Install: Add Host page, click **Import**.

   The Import Host page appears.

Figure 5–24 Importing a Host



2. Perform one of the following actions:

   a. In the **Local File** field, click **Browse**, and select a CSV system file on your local machine, *or*

   b. Click **Download Sample** to open, or save, a system file called `sample_host_info.csv`.

      See Figure 5–25 for an outline of the file.

Figure 5–25 Sample CSV Host File

Hostname (Fully Qualified)	Primary IP	Installation User	Privilege Mode
myhost1.example.com	10.10.10.11	root	sudo
myhost2.example.com	10.10.10.12	linuxuser	pfexec
myhost3.example.com	10.10.10.13	soluser	su

3. Click **Import** to populate the Agent Install: Add Host page.

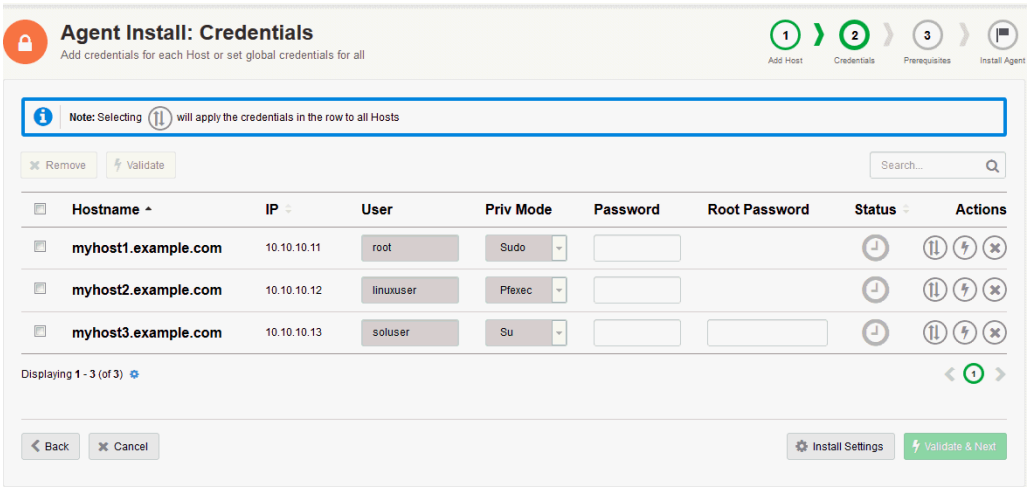
   (Optional) Edit the hostname and IP address settings imported from the sample file.

4. Click **Next**.

   The Agent Install: Credentials page appears.

   Note: This page is populated with values from the sample file.

Figure 5–26 Setting Credentials for the Hosts



6

Managing Systems

This chapter provides information about using Oracle Advanced Support Gateway to manage systems and hosts as well as requesting activations of new systems and the addition of new hosts.

This chapter consists of the following sections:

- About Managing Systems and Hosts
- Adding a New System
- About Adding a New Engineered System
- Viewing Target Configurations
- Managing System Passwords
- Deactivating Services

Related Information

About Patching Requests

Managing Databases and Database Patches

About Managing Systems and Hosts

You can use Oracle Advanced Support Gateway to manage existing systems and hosts as well as requesting the activation of new systems and the addition of new hosts.

Refer to the following sections:

- Adding a New System
- About Adding a New Engineered System

Adding a New System

You can activate new systems that are auto-discovered on the Gateway.

To use Oracle Advanced Support Gateway to activate new systems:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Admin** menu, click **Manage Systems**.

   The Systems and Hosts page appears.

3. Click **Add New**.

The Add System page appears.

You use this page to create a request for the monitoring of an Engineered System. This request is then submitted to an Oracle service engineer to complete the monitoring process.

Refer to the following sections:

- About Adding a New Engineered System
- Adding a Single Host

About Adding a New Engineered System

You can use Oracle Advanced Support Gateway to create a request to monitor the following Oracle Engineered Systems:

- Exadata
- Exalogic
- SuperCluster

Note: In order to monitor other Oracle Engineered Systems, such as Zero Data Loss Recovery Appliance, Exalytics In-Memory Machine, and so on, please refer to your Oracle representative for further details.

This section outlines how to collect and validate all required implementation information directly from the customer using the Gateway user interface. There are several stages in creating the monitoring request:

- **Welcome**: Introducing the wizard used to create the monitoring request and confirm the pre-requisite tasks
- **Add System**: Adding a system, where *system* is understood to mean an Oracle Engineered System, as outlined above
- **System Information**: Supplying information about the system
- **Network Check**: Checking system connectivity
- **Set Credentials**: Performing checks on the system credentials;
- **Full Network Check**: Checking end-to-end system connectivity;
- **Compliance Check**: Verifying system compliance and network connections
- **Complete**: Submitting the provisioning request to Oracle and receiving confirmation of the request

To use the Gateway to create a request for the monitoring of an Engineered System:

1. Log on to the Oracle Advanced Support Gateway portal.

   The Oracle Advanced Support Gateway home page appears.

2. From the top-level **Admin** menu, select **Manage Systems**.

   The Systems and Hosts page appears.

   You use this page to create a request for the monitoring of an Engineered System. This request is then submitted to an Oracle service engineer to complete the monitoring process.

3. Click **Add New**.

   The Welcome to the System and Host install Wizard page appears.

   This page provides information about tasks to be performed and information you'll need to access before getting started:

This wizard will help you install monitoring agents on standalone systems or create a request for the monitoring of an Engineered System. As part of the wizard workflow you will be requested to provide the following:

- Privileged system credentials;
- For standalone systems: IP addresses and their fully qualified hostnames (FQDN);
- For Engineered Systems: The Engineered System's schematic file, and CSI/MOS ID (and in the case of users of the Platinum Service, the associated Platinum Implementation SR (PISR) number);
- Additional custom install settings.

The wizard performs the following checks before taking any actions:

- Validate the network connectivity between the Gateway and the hosts;
- Test credentials; the self-service activation process now enables users to enter credentials for individual nodes (in previous releases of Oracle Advanced Support Gateway, all nodes of a particular host had the same username and password restrictions.)
- Check each system meets minimum prerequisites for agent installation.

  Service activation on multiple targets continues after a single target failure. During service activation, all targets are shown, together with any reason why a target is not eligible for activation.

Before you get started:

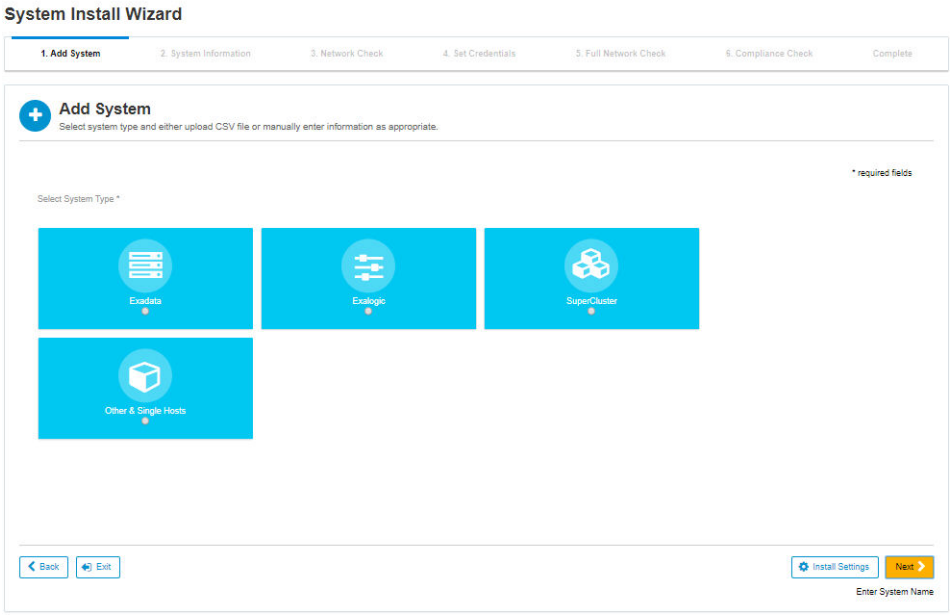
- Please review the Oracle Advanced Support Gateway Security Guide

As part of the wizard workflow, users are requested to provide IP address details and passwords for the required Engineered System. Checks are then performed to validate the network connectivity and passwords before a Service Request (SR) is created and submitted for an Oracle engineer to complete the remaining tasks.

4. (Optional) Select the **Don’t show message again** check box so that the Welcome Message page is not displayed in future as part of the Add Agent workflow.
5. Click **Get Started**.

   The Add System page appears.

Figure 6–1 Adding a System



In general, you can add systems by:

- Importing a schematic file by selecting a comma-separated value (CSV) file from your local computer, *or*
- Manually entering information, for example, host IP address, schematic directory, filename, and SSH credentials, as appropriate

To add a supported Oracle Engineered System, select one of the following options:

- **Exadata**. See "Adding an Oracle Exadata Engineered System."
- **Exalogic**. See "Adding an Oracle Exalogic Engineered System.".
- **SuperCluster**. See "Adding an Oracle SuperCluster Engineered System."

Related Information

Adding a Single Host

Viewing Target Configurations

This section provides information about viewing configuration details about discovered systems and hosts, for example: status, last backup time, lifecycle type, supported services, open SRs, health report details, and so on.

To use Oracle Advanced Support Gateway to manage discovered systems and hosts:

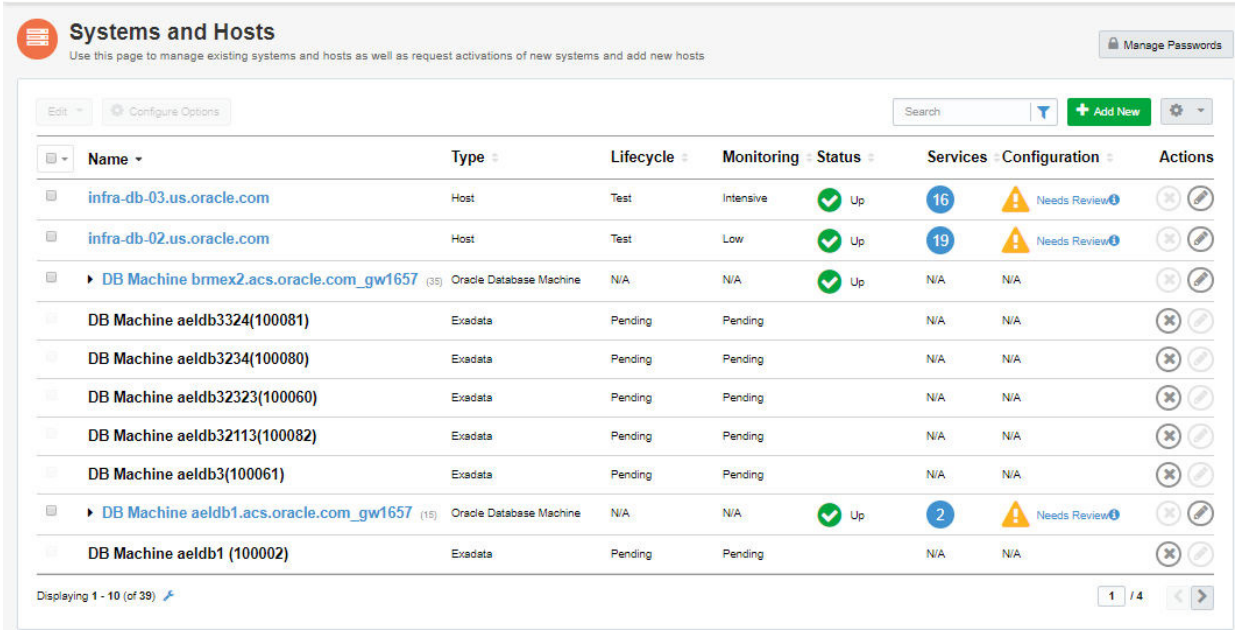
1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Admin** menu, click **Manage Systems**.

   The Systems and Hosts page appears.

Figure 6–2 Viewing Systems and Hosts

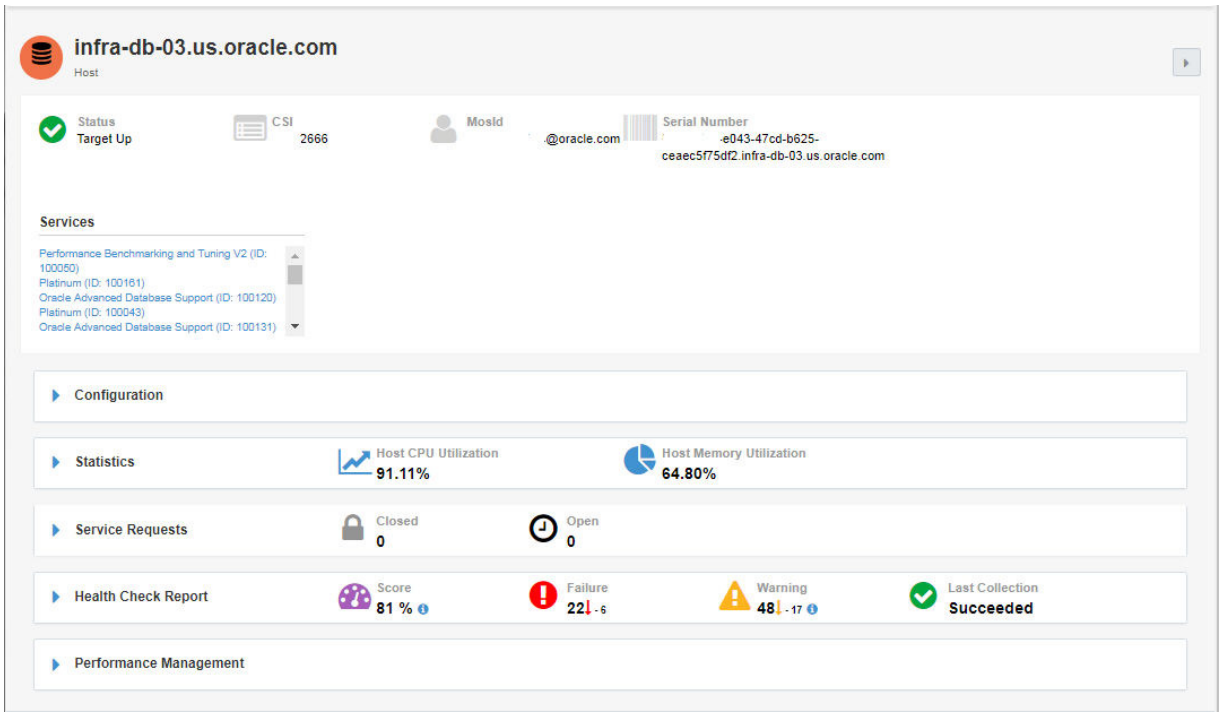


You use this page to manage existing systems and hosts.

3. Click any listed target.

   The target configuration appears.

Figure 6–3 Viewing the Target Configuration



You can use this page to view the target configuration and to manage the target details.

This section contains the following topics:

- Viewing Target Details
- Configuring Supported Targets
- Viewing Statistics
- Viewing Service Requests
- Viewing the Health Check Report
- Managing Target Performance
- Viewing Recommendations

Viewing Target Details

The Target Details landing page offers a consolidated view of target information that is important to the customer. You can review key performance and SR information about the target in a series of intuitive, graphical displays.

Among the details provided are:

- **Status**: Uses icons to indicate that the target is in one of the following states:
  - *Up*: The target is active and reachable
  - *Pending*: The target is not active, and the target details cannot yet be displayed on the Oracle Advanced Support Gateway user interface
  - *Unreachable*: The target was formerly active, but is now unreachable

  The target displayed in Figure 6–3 is up, as denoted by the check mark.
- **Last Backup**: Provides a timestamp of the last database backup.
- **Up Time**: Provides the duration of database machine uptime.
- **Lifecycle**: Provides the lifecycle associated with the database. The options are *Test*, *Production, Development, Stage.*
- **Services**: Provides a list of supported Oracle connected services. Examples might include: Oracle Platinum Services, Business Critical Support, Advanced Monitoring and Resolution, and Advanced Database Support.

  Note: Where more than one instance of a particular service runs on a target, each instance is differentiated by a specific identifier, for example, *Oracle Advanced Database Support (ID: 100080)* and *Oracle Advanced Database Support (ID: 100060).*

Configuring Supported Targets

From the Configuration panel, you can view and set:

- Oracle Advanced Support Gateway monitoring levels for Platinum Services and Advanced Database Support (ADS) fault events; *and*
- Oracle Advanced Support Gateway lifecycle values for Platinum Services and Advanced Database Support (ADS) fault events.

Refer to the following sections:

- Configuring the Monitoring Level on a Supported Target
- Configuring the Lifecycle Associated with a Supported Target

Configuring the Monitoring Level on a Supported Target

You can view and set Oracle Advanced Support Gateway monitoring levels for Platinum Services and Advanced Database Support (ADS) fault events. Monitoring applies to:

- Oracle Platinum Services SR automation for Oracle Exadata OEM fault events;
- Oracle Advanced Database Support (ADS) fault events.

The monitoring level controls automated Service Requests (SRs) for the monitored targets and can be set in the Gateway to one of the following levels: *None*, *Low*, *Regular*, *High*, or *Intensive*.

Note: Selecting a Lifecycle level does not automatically set or change the Monitoring level. Lifecycle levels and Monitoring levels are independent of each other.

Platinum customers are provided a single admin type user who can manage the targets registered with the Gateway. Monitoring levels can be set during OEM Platinum and ADS target activation, after target activation, or left unset.

Both Platinum and ADS services use OEM fault event back-end rules to assign severity to an automated Service Request (SR) based on criteria such as the error type, the monitoring level, target type, and so on.

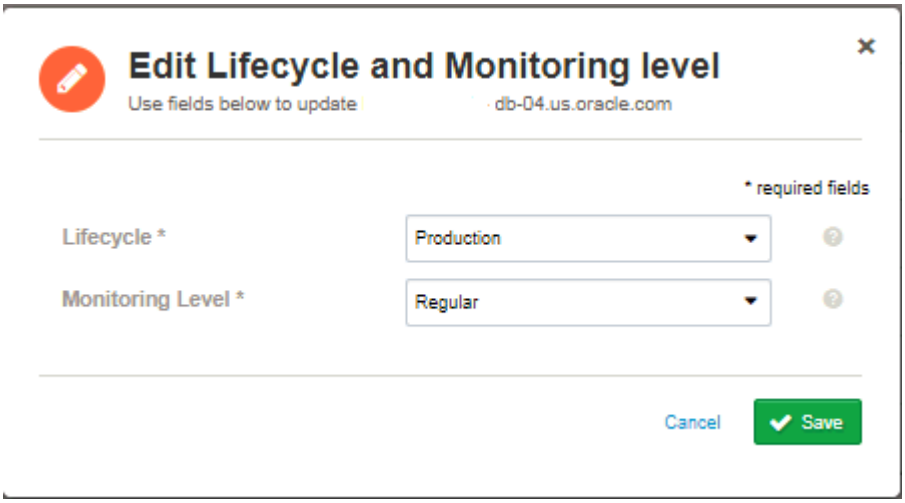
Note: For further information on target monitoring levels delivered via the Oracle Advanced Service Gateway, refer to `MOS Note 2047194.1`.

To configure the monitoring level on a supported target:

1. From the list of supported targets, that is, the systems and hosts listed on the **Systems and Hosts** page, or the databases displayed on the **Manage Databases** page, select the required target.
2. From the **Actions** column or from the **Configuration** panel associated with the target, click **Edit** or click the edit icon.

   The Edit Lifecycle and Monitoring level dialog box appears.

Figure 6–4 Configuring Monitoring Levels on a Supported Target



3. In the **Monitoring Level** field, select the required monitoring level associated with the target from the following list:
   - *Regular*
   - *None*

- *Low*
- *High*
- *Intensive*

4. Click **Save** to complete the monitoring configuration.

Related Information

Configuring the Lifecycle Associated with a Supported Target

Configuring the Lifecycle Associated with a Supported Target

You can view and set the Oracle Advanced Support Gateway lifecycle for Platinum Services and Advanced Database Support (ADS) fault events. “Lifecycle” in the context of Gateway target monitoring is a generic term that defines the level of monitoring for the given target. Setting the lifecycle, for example, enables a customer to disable automatic SR creation for development or staging databases while enabling it for production or test instances.

The Lifecycle can be set in the Gateway to one of the following levels: *Test*, *Production, Development, Stage, or None*.

Note: Selecting a Lifecycle does not automatically set or change the Monitoring level. Lifecycles and Monitoring levels are independent of each other.

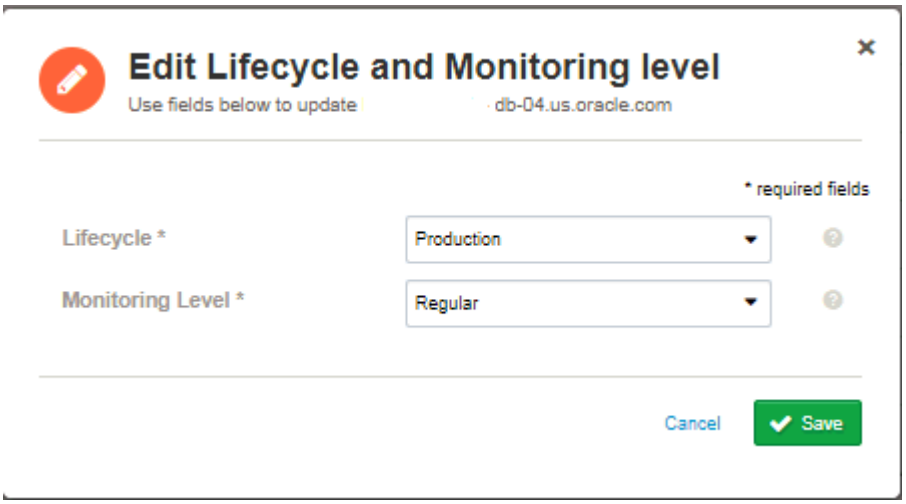
Note: For further information on target lifecycles configured via the Oracle Advanced Service Gateway, refer to `MOS Note 2047194.1`.

To configure the lifecycle on a supported target:

1. From the list of supported targets, that is, the systems and hosts listed on the **Systems and Hosts** page, or the databases displayed on the **Manage Databases** page, select the required target.
2. From the **Actions** column, click the edit icon.

   The Edit Lifecycle and Monitoring level dialog box appears.

Figure 6–5 Configuring Lifecycles on a Supported Target



3. In the **Lifecycle** field, select the required lifecycle associated with the target from the following list:

   - *Production*

- *Test*
- *Development*
- *Stage*
- *None*

4. Click **Save** to complete the lifecycle configuration.

Related Information

Configuring Supported Targets

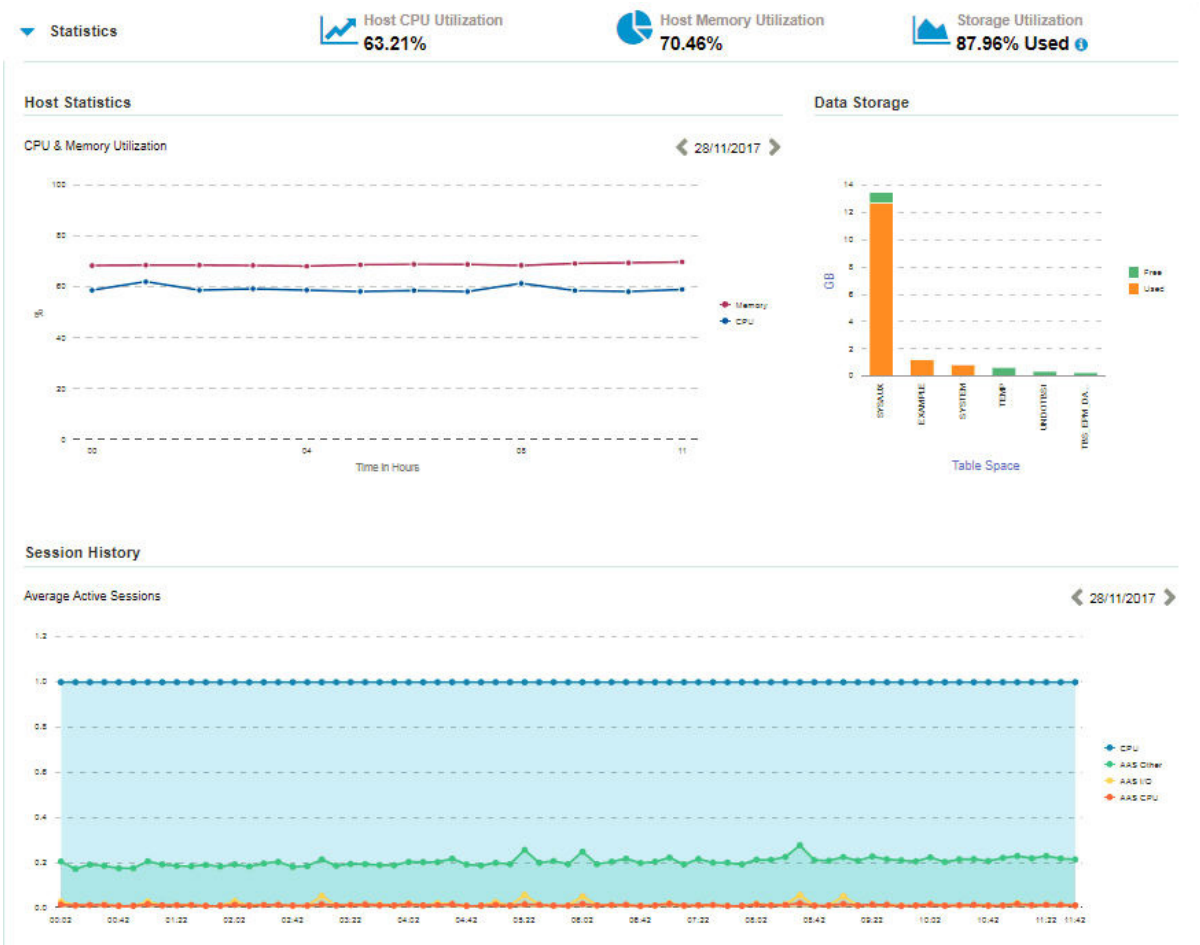
Viewing Statistics

You can expand the Statistics window to review and track CPU, memory, and storage utilization values for the chosen host. See Figure 6–6.

Use the arrows beside the date value to select the required date.

Hover the cursor over the graphs to review further details about the host series CPU group, the host series memory group, and the exact utilization percentages.

Figure 6–6 Viewing the Statistics Details



Viewing Service Requests

See "Viewing Service Requests".

Viewing the Health Check Report

See "Viewing the Health Check Report".

Managing Target Performance

Oracle Advanced Database Support (ADS) service provides performance management offering:

- Reports of summary data on key performance metrics for activated databases;
- Reports of detailed performance trend data for each database on the Database Details page;
- The ability to easily enable or disable the Performance Management feature on a Gateway.

Viewing Recommendations

Recommendations are made following a review by an Oracle engineer of a current customer scenario or engagement.

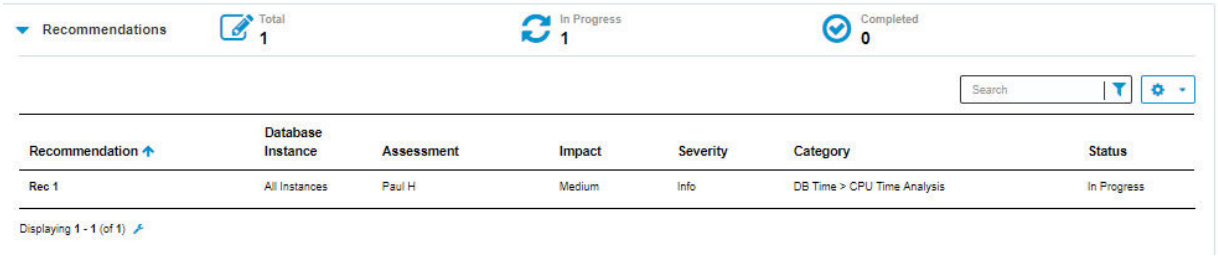
Note: Recommendations apply only to certain, paid, customer engagements, services, and scenarios.

A typical scenario might involve a customer engaging Oracle for a paid performance review, for example, of a number of database instances. The engineer investigates the system and issues a set of results and a series of recommendations.

You can expand the Recommendations window to review:

- *Findings*: The results of the review of the system or host by an Oracle engineer. For example, CPU usage was consistently high and was a bottleneck;
- *Recommendations*: The solution proposed by an Oracle engineer to any issues in the findings; for example, in response to the high CPU usage, the recommendation is to add another CPU.

Figure 6–7 Viewing Recommendations



Managing System Passwords

You can manage the passwords associated with the discovered systems and hosts.

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Admin** menu, click **Manage Systems**.

   The Systems and Hosts page appears.

3. Click **Manage Passwords**.

   The Password Management appears. Periodic rotation of passwords for production systems is recommended. Use this page to update stored passwords in Oracle Password Vault.

   Refer to the following topic:

   - "Managing Credentials and Passwords."

Deactivating Services

You can use Oracle Advanced Support Gateway to deactivate an Engineered System, that is, to stop monitoring of, for example, an Oracle Exadata Database Machine (Exadata), or Oracle Database Machine.

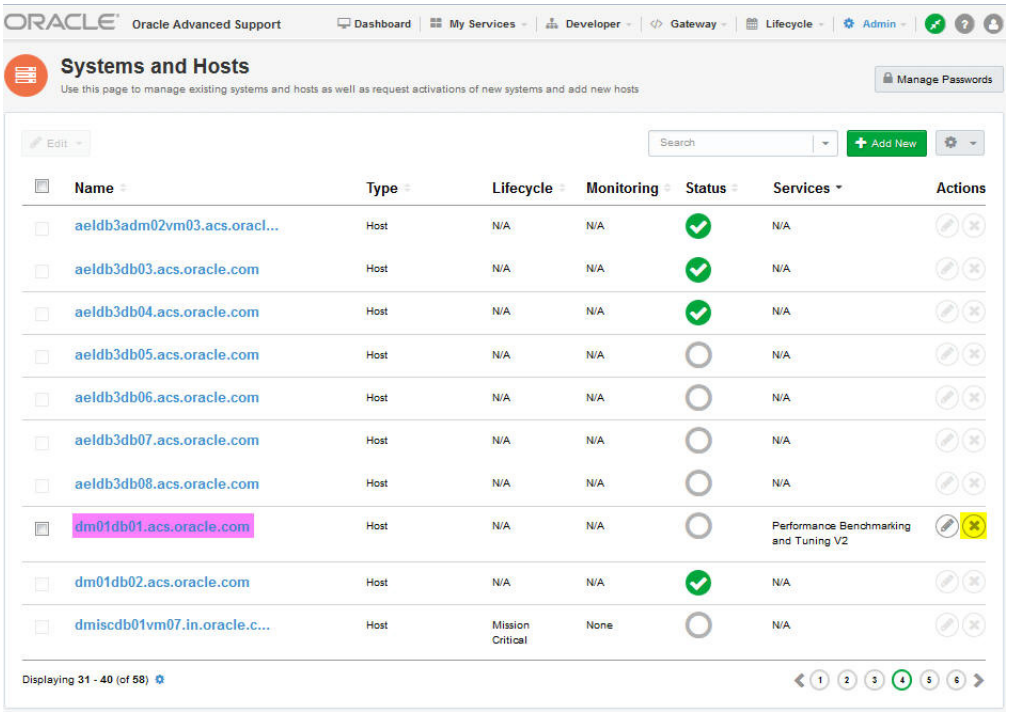
You can only deactivate a service on a target (system or host) on which services are running.

To deactivate an Engineered System:

1. From the Systems and Hosts page, select a target on which a service is running.

   In the example shown in Figure 6–8, the *dm01db01.acs.oracle.com* host is selected for deactivation.

Figure 6–8 Systems and Hosts Page



2. From the **Actions** column, click the **Deactivate (X)** icon, as highlighted.

   A warning dialog asks you to confirm deactivation.

   Click **Yes** to confirm. The host is deactivated.

7

Activating Services

This chapter provides information about using Oracle Advanced Support Gateway to activate services.

This chapter consists of the following sections:

- About Activating Services
- Selecting a Service for Activation
- Viewing Discovered Databases
- Deactivating Services

About Activating Services

In order to activate a service, you first need to select a service for which service activation is to be performed. The list of available services displayed for service activation is based on the contract which you have with Oracle for the services on the gateway.

So, for example, to activate the Oracle Advanced Database Support (ADS) service, you can first select ADS for activation, and then use the Oracle Advanced Support Gateway user interface to select databases from the list of automatically discovered database targets. Databases can be added singly or in groups. After selecting the required databases, you need to enter the database credentials required to enable monitoring prior to service activation. The term *database* can refer to single instances of databases as well as High Availability databases, Clusters, ASM Clusters, and Grids. The activation method, as well as the corresponding wizard steps, varies according to selected targets.

The next activation step for ADS is that Oracle Advanced Support Gateway enables the delivery and validation of all required database implementation information using the Gateway user interface. These collection and validation steps then enable an Oracle engineer to prepare the system and make it ready for activation.

The database activation workflow consists of three principal stages:

- Selecting available databases to activate
- Supplying and testing database credentials
- Activating the databases for your selected service

Selecting a Service for Activation

To use Oracle Advanced Support Gateway to activate a service:

1. Log in to Oracle Advanced Support Gateway.

The Oracle Advanced Support Gateway Home page appears.

2. From the **My Services** menu, click **Activate Service.**

   The Service Activation: Select Service page appears.

   You use this page to select the service you wish to activate.

3. (Optional) You can also activate services from the Manage Databases page that is used to manage all databases and their related cluster and ASM infrastructure.

   To view the Manage Databases page, select **Admin**, then **Manage Databases**, and click **Activate New Service**.

4. Complete the following fields:

   - From the **Select Service** field, select your required service, for example, *Platinum (ID: XXXXXX)* or *Oracle Advanced Database Support (ID: YYYYYY)*.

     The list displayed for service activation is based on the contract which the customer has for supported services on the gateway.

   - From the **Activation** field, select whether to promote the target and activate the service using the wizard, or just promote the target (and activate the service later.)

     a. **Activate**; activate service with promotion, *or*

     b. **Promote**; promote targets without service activation

     If you select (a), continue to step 5.

     If you select (b), continue to step 15.

   - (For Advanced Database Support (ADS) service activation only)

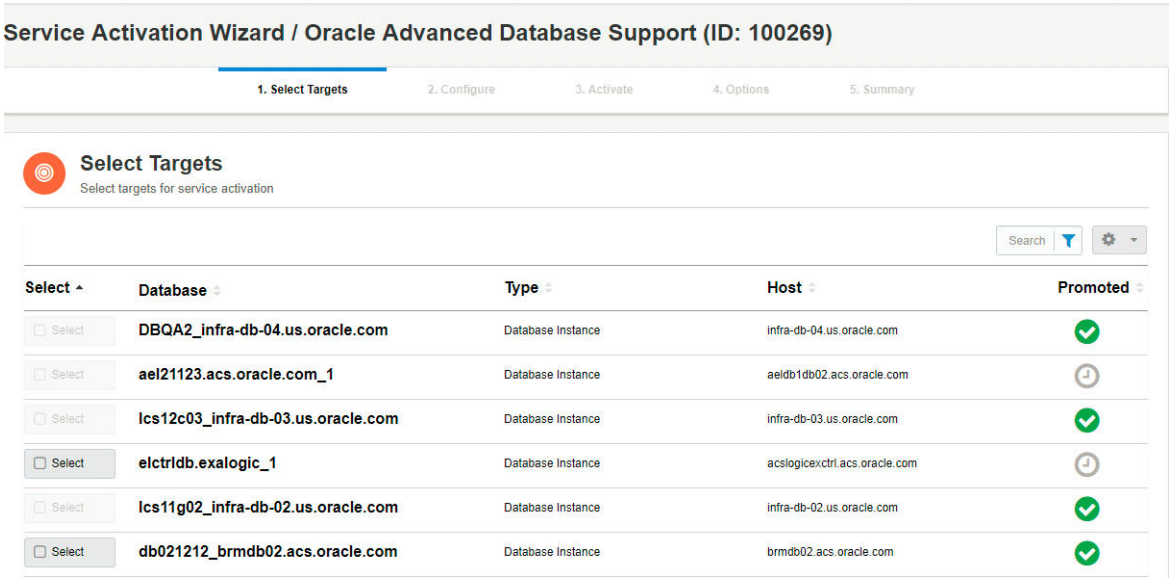
     In the **Compliance Level** field, select one of the values to specify your compliance level: *Latest, Latest-1, Latest-2, Latest-2*.

     The Compliance Level setting indicates whether the installed Patch Set version is within the compliance levels as per your patch policy. You can set the compliance level on a database instance. Changing this setting will affect all of the targets.

     So, for example, if you select the value of the Patch Set Compliance Level setting as *Latest -1*, if the latest Quarterly Full Stack Download Patch (QFSDP) available is Jan 2019 - any engineered system with a QFSDP before Oct 2018 will be considered as “Non-Compliant”.

     The Service Activation: Targets page appears.

Figure 7–1 Selecting Service Activation Targets



5. Add one or more database targets for service activation. Activation of a service on targets which are not eligible for activation is prohibited, and the reason these targets are not eligible is displayed.

   To add a database:

   a. Select the check box associated with the database.

      (To add multiple databases, select all associated check boxes.)

      Note: If the database to be activated is not on the list, contact Oracle to complete the manual installation of the agent and perform a discovery. To request Oracle discoveries, contact My Oracle Support (MOS).

   b. Click **Next**

      The Service Activation: Database/Grid/ASM page appears. The selected databases are displayed.

   c. Click **Validate & Next**.

      Note: In the case of grids, ASM clusters, database clusters, and so on, you are required to validate on multiple pages.

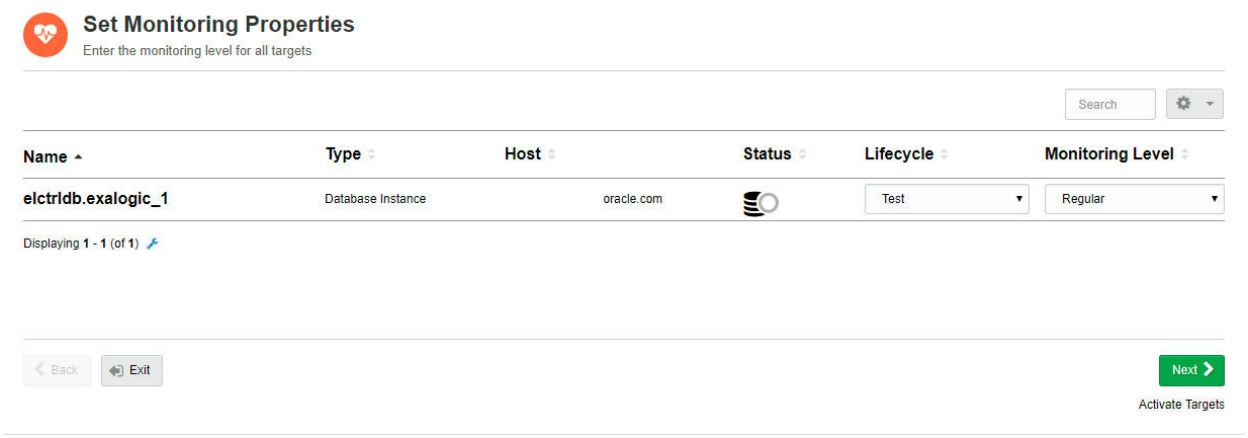
      The Service Activation: Configure page appears. This page enables you to specify service-specific options.

Figure 7–2 Supplying Database Options

6. Click **Next** to set the monitoring properties.

   The Set Monitoring Properties page appears.

Figure 7–3 Setting Monitoring Properties



7. Supply the credentials for each database:

   a. In the **Lifecycle** field, select the lifecycle associated with the database. The options include *Test*, *Production*, *Stage*, or *Development.*

   b. In the **Monitoring Level** field, select the monitoring level associated with the database. Monitoring levels are restricted only to the valid monitoring levels for the target, for example, *None*, *Low*, *Regular, High,* or *Intensive.*

   c. (Optional; depending on the target type) In the **DBSNMP** field, enter the SNMP password associated with the database.

   d. (Optional; depending on the target type) In the **ASMSNMP Password** field, enter the Automatic Storage Management (ASM) SNMP password associated with the database.

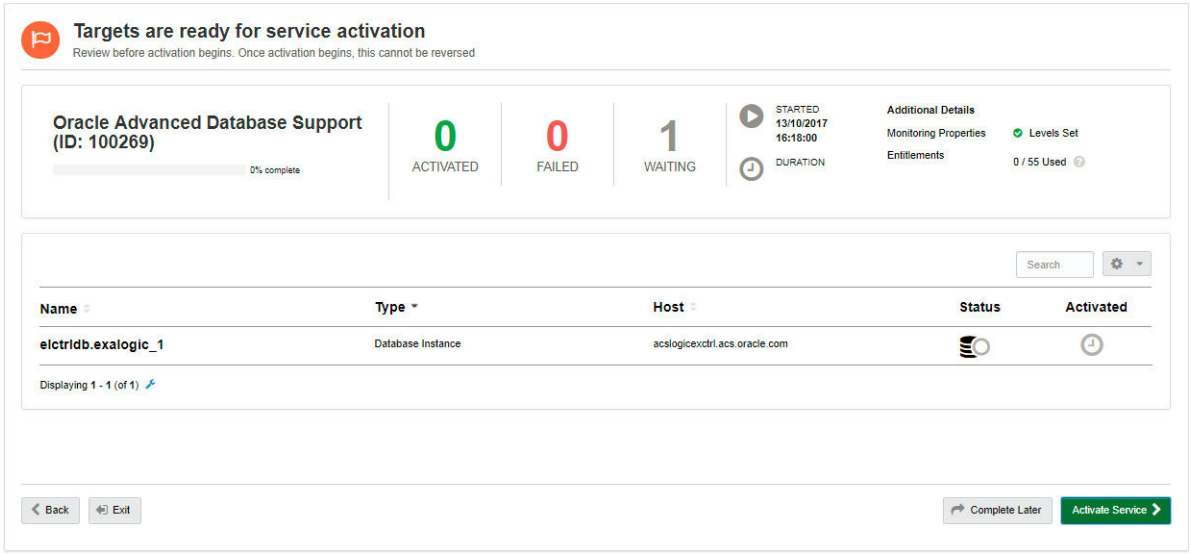
   e. (Optional) You can copy credentials from row to row by clicking the arrows icon in the **Actions** section of the page.

      Note: Users are notified if a credential has already been entered for a particular target.

8. Click **Next**.

   The Service Activation: Review page appears.

Figure 7–4 Reviewing Activation Options



Select whether to use the activation wizard to activate the service now, or postpone completion:

a. **Activate Service**, *or*

b. **Complete Later**

If you select (a), continue to step 9.

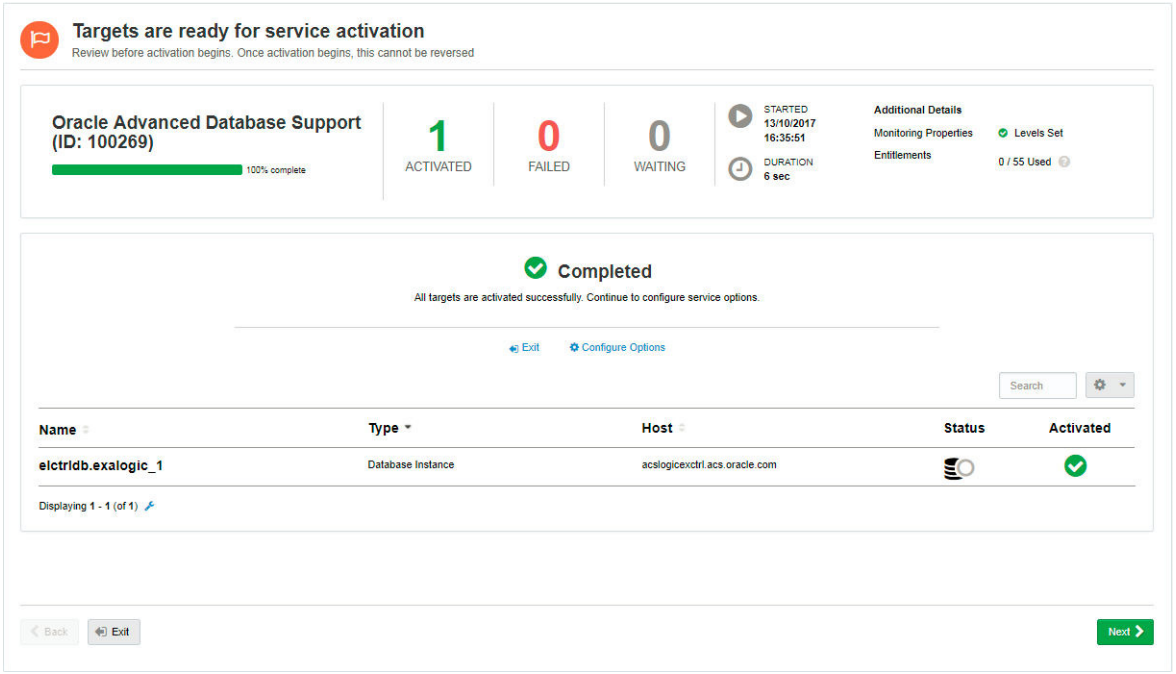
If you select (b), continue to "Viewing Discovered Databases".

9. Click **Activate Service**.

After activating the service, tests are triggered for all untested databases.

Results are displayed at the top of the page. See Figure 7–5.

Figure 7–5 Reviewing Service Activation Options



Review the progress check.

a. The **Activated** field displays the number of databases that were successfully activated.

b. The **Failed** field displays the number of databases that were not successfully activated.

c. The **Waiting** field displays the number of databases pending completion of the activation process.

d. The **Started** field displays the time at which activation commenced.

e. The **Duration** field displays the time taken for activation.

f. The **Additional Details** field displays whether monitoring levels are set, and in the case of databases activated for ADS, displays entitlement usage information.

See Chapter 12, "Managing Database Entitlements" for further information about entitlements.

g. (Optional) If activation is successful, click **Continue to Service** to display the new service.

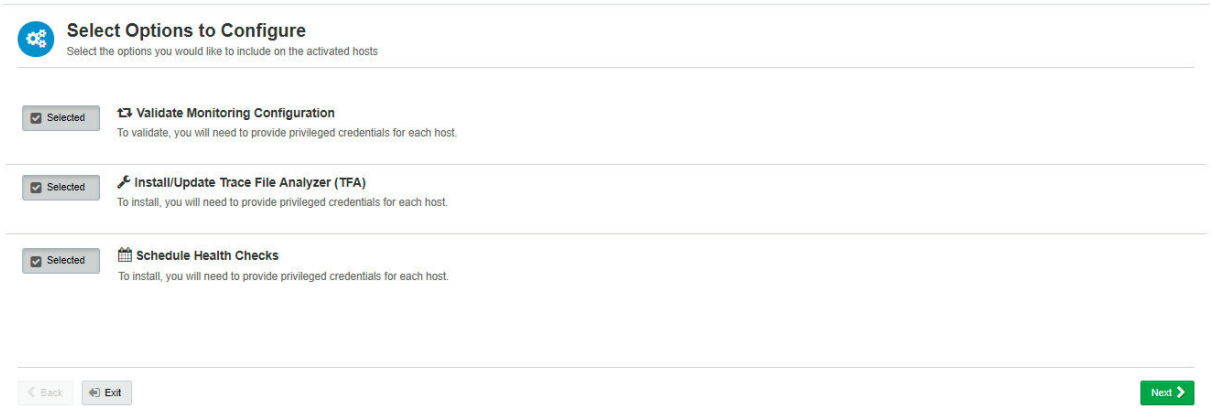
10. Click **Next** to configure options to include on the activated hosts. These options are:

- **Validate Monitoring Configuration**: to validate, you will need to provide privileged credentials for each host;
- **Install/Update Trace File Analyzer (TFA)**: To install, you will need to provide privileged credentials for each host;
- **Schedule Health Checks**: To install, you will need to provide privileged credentials for each host.

Each configuration option follows the same pattern.

The Select Options to Configure page appears.

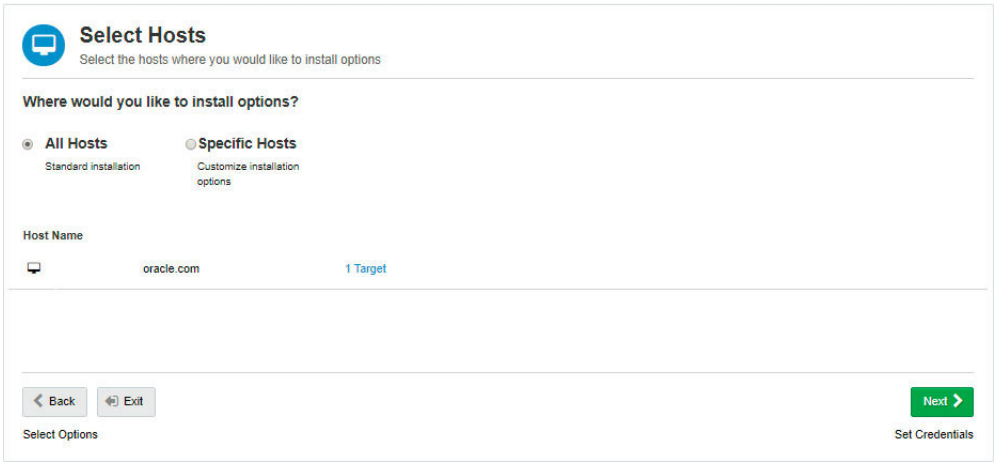
Figure 7–6 Selecting Options to Configure



11. Click **Selected**.

    The Select Hosts page appears.

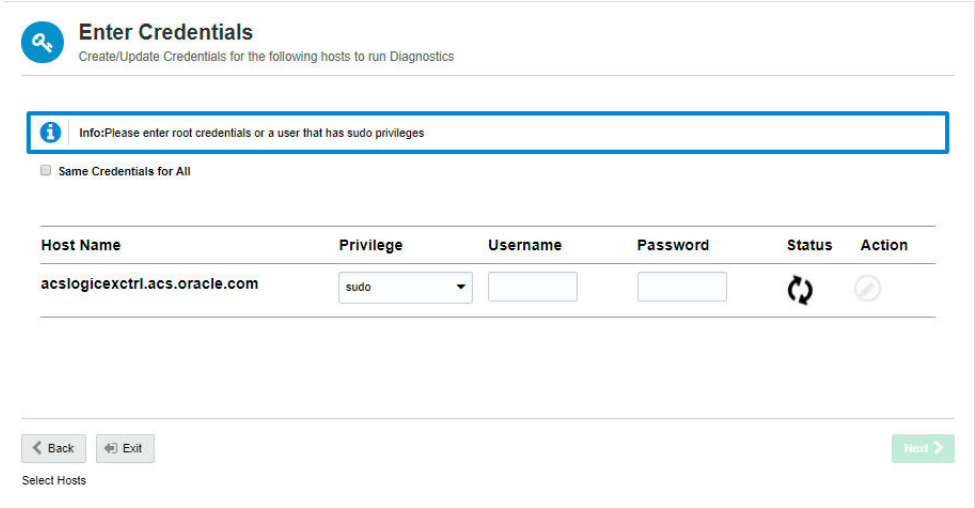
Figure 7–7 Selecting Hosts



12. Select the hosts where you would like to install options by choosing one of the following:
    - **All Hosts,** which is the standard installation option, *or*
    - **Specific Hosts**, which enables you to customize installation options
13. Click **Next**.

    The Enter Credentials page appears.

Figure 7–8 Entering Credentials for the Selected Hosts



Create or update credentials for the following hosts to run diagnostics. Enter root credentials or a user that has sudo privileges:

a. In the **Privilege** field, select the mode to be used to gain the required level privilege on the host. The options are **sudo**, **Normal**, and **None**.

b. In the **Username** field, enter the password associated with the host.

c. In the **Password** field, enter the password associated with the host.

14. Click **Next**.

The Summary page appears. Review the activation details.

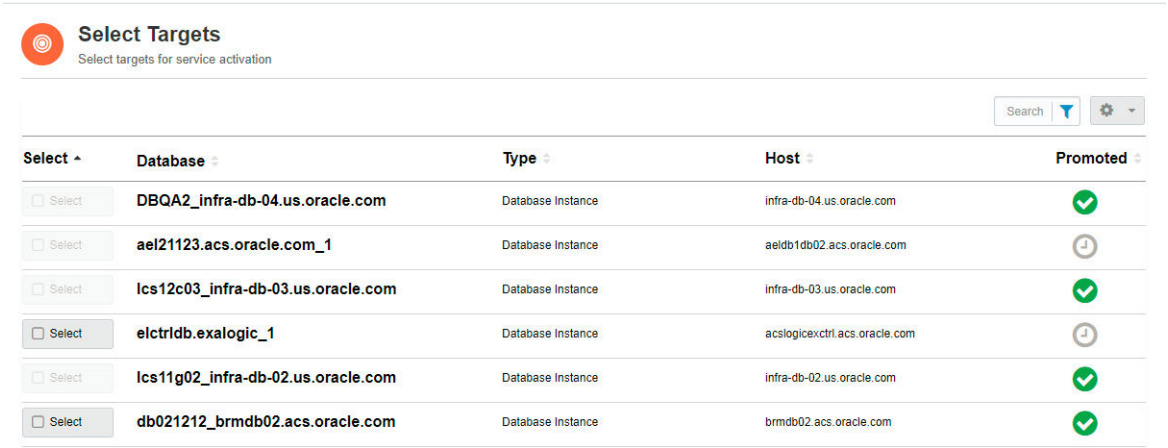
15. (Optional: If you choose to promote targets without service activation)

Select **Promote**; **promote targets without service activation**.

Click **Next**.

The Service Promotion: Targets page appears.

Figure 7–9 Selecting Service Promotion Targets



16. Add one or more database targets for service promotion.

To add a database:

a. Select the check box associated with the database.

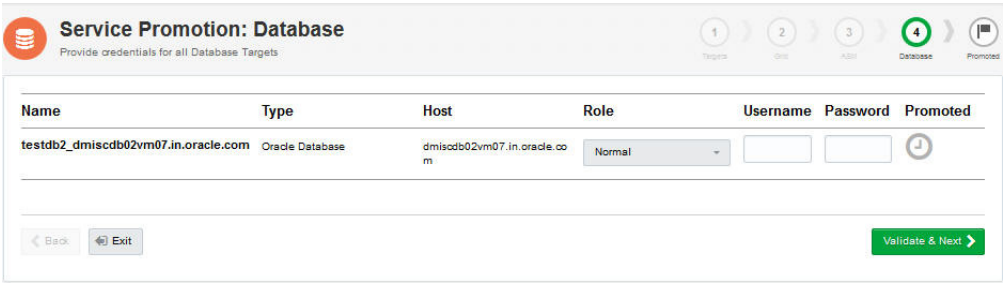
(To add multiple databases, select all associated check boxes.)

Note: If the database you need to activate is not on the list, you need to contact Oracle to complete the manual installation of the agent and perform a discovery. To request Oracle discoveries, contact My Oracle Support (MOS).

b. Click **Next**.

The Service Promotion: Databases page appears.

Figure 7–10 Providing Credentials for Service Promotion Targets



You use this page to provide credentials for all database targets:

In the **Role** field, select the role associated with the database. The options are *Normal* or *SYSDBA*.

In the **Username** field, enter the username associated with the database.

In the **Password** field, enter the password associated with the database.

c. Click **Validate & Next**.

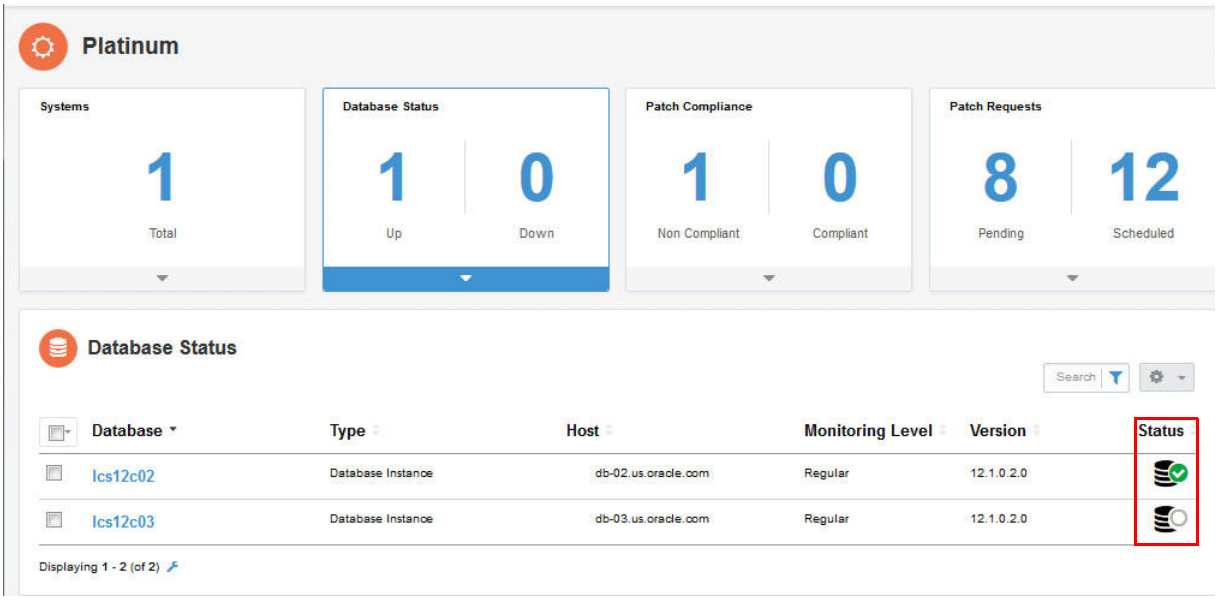
The Service Activation: Promoted page appears. Use this page to specify service-specific options.

Viewing Discovered Databases

This section provides information about viewing discovered databases.

Select the **Database Status** badge to display your discovered databases in the Database Status list.

Figure 7–11 Displaying Discovered Databases



As highlighted in the Status column in the example in Figure 7–11, the database *lcs12c02* is up, denoted by the check mark on its database icon, while *lcs12c03* is unreachable, denoted by the gray circle.

Once the databases are activated, monitoring commences.

Deactivating Services

You can use Oracle Advanced Support Gateway to deactivate a service, that is, to deactivate the targets on which the service is running.

Note: Oracle recommends that Platinum Service customers first refer to their Oracle representative before deactivating a service on an Engineered System.

To deactivate a service:

1. Log on to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **My Services** menu, click **Deactivate Service**.

   The Deactivate Service: Select Service page appears.

   You use this page to select the service you wish to activate.

3. Select the service you want to deactivate (services must be selected singly.)

4. Click **Next**.

   The Select Targets page appears.

5. Select the check box associated with the database.

   (To add multiple databases, select all associated check boxes.)

6. Click **Next**.

   The Service Deactivation page appears.

   You use this page to review targets for service deactivation.

7. Select **Start Deactivation**.

   A warning dialog asks you to confirm deactivation.

   Click **Yes** to confirm. The database is deactivated.

8

Validating Connections

This chapter provides information about using the Connectivity Tests (Netcheck) to validate whether the required firewall ports and connections between Oracle Advanced Support Gateway and the Oracle database, Engineered System, or individual component, such as cell node or Infiniband, are open.

This chapter consists of the following sections:

- About Gateway Connectivity
- About System Tests
- Viewing System Test Status
- Verifying the External Connection
- Verifying an Internal Connection
- Configuring New System Test Targets

About Gateway Connectivity

In order for Oracle to deliver Oracle Connected Services, the following requirements need to be met:

- All monitored devices must be network accessible from the Oracle Advanced Support Gateway.
- Oracle must have the level of access to the monitored devices necessary for Oracle to implement and deliver the service.
- The Oracle Advanced Support Gateway must be continuously accessible from the Oracle Support Platform using the secure protocols.

The Netcheck feature provides a mechanism to test connectivity between the Gateway and the Oracle Support Platform and also between Oracle Advanced Support Gateway and the customer monitored systems.

Connectivity tests are used to validate the ports and connections between Oracle Advanced Support Gateway and the following Oracle Engineered Systems:

- Exadata
- Exalogic
- SuperCluster

These tests help to secure and successfully complete the implementation of services running on Oracle Advanced Support Gateway.

Related Information

Verifying the External Connection

Verifying an Internal Connection

About System Tests

You can use Oracle Advanced Support Gateway to run two separate types of connectivity system test:

- Internal system tests. See "About Internal System Tests."
- External system tests. See "About External System Tests."

About Internal System Tests

An internal system test verifies the connectivity between the Oracle Advanced Support Gateway and the Oracle Engineered System. You can optionally specify a HTTP proxy if the traffic between Oracle Advanced Support Gateway and the Engineered System is routed through a proxy server (depending on the customer's network configuration).

You can also verify the network traffic between Oracle Advanced Support Gateway and the Engineered System in both directions, that is, from Oracle Advanced Support Gateway to the Engineered System, and from the Engineered System to Oracle Advanced Support Gateway. This test typically requires the root password for the system. The connectivity test expects the same root account to work on all of the target systems. After supplying the system details, you select the applicable databasemachine.csv file.

Related Information

Verifying an Internal Connection

About External System Tests

An external system test verifies the connectivity between Oracle Advanced Support Gateway and Oracle (VPN, Monitoring, CCR, and Oracle patch accessibility).

Related Information

Verifying the External Connection

Viewing System Test Status

To use Oracle Advanced Support Gateway to view system test status:

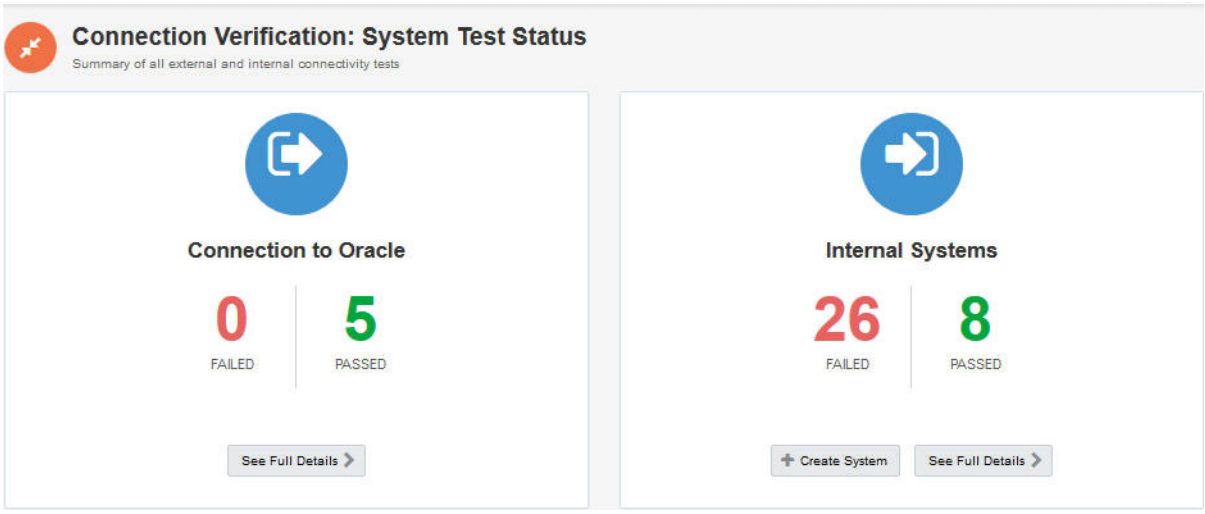
1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Gateway** menu, select **Connectivity Tests**.

   The Connection Verification: System Test Status page appears.

Figure 8–1 Connection Verification: System Test Status



This page provides a summary of all external (that is, connections to Oracle) and internal connectivity tests. From this page, you can perform a number of actions:

- Verify the external connection between Oracle Advanced Support Gateway and Oracle. See "Verifying the External Connection."
- Verify an internal connection between Oracle Advanced Support Gateway and the Engineered System. See "Verifying an Internal Connection."
- View a detailed table of internal connectivity tests. See "Verifying an Internal Connection."

Verifying the External Connection

The external connections between Oracle Advanced Support Gateway and Oracle are established during Oracle Advanced Support Gateway installation. You can continue to monitor connectivity as required.

To use Oracle Advanced Support Gateway to verify connectivity between Oracle Advanced Support Gateway and Oracle:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

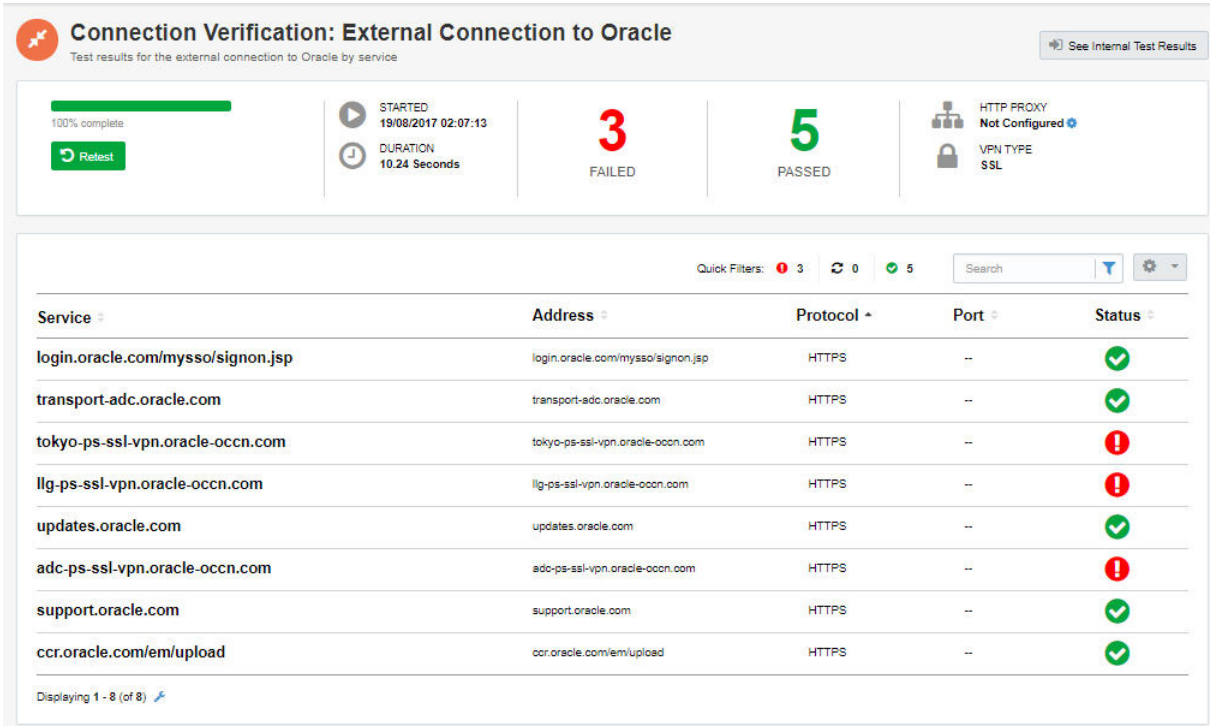
2. From the **Gateway** menu, select **Connectivity Tests**.

   The Connection Verification: System Test Status page appears.

3. From the Connection to Oracle panel, click **See Full Details**.

   The Connection Verification: External Connection to Oracle page appears.

Figure 8–2 Connection Verification: External Connection to Oracle



This page displays test results for the external connection to Oracle by service. As shown in Figure 8–2, five of the supported service connections are up.

4. Click **Retest** to verify the connection to Oracle.

   If the connection is validated, a success message appears.

Specifying a HTTP Proxy

You can optionally specify a HTTP proxy if the traffic between Oracle Advanced Support Gateway and Oracle is routed through a proxy server (depending on the customer's network configuration).

To configure a HTTP proxy:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Gateway** menu, select **Connectivity Tests**.

   The Connection Verification: System Test Status page appears.

3. From the Connection to Oracle panel, click **See Full Details**.

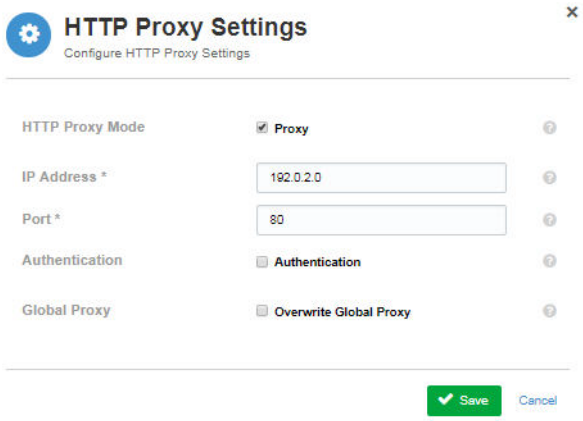
   The Connection Verification: External Connection to Oracle page appears.

4. In the top right of the page, in the HTTP Proxy section, click **Configure**.

   The HTTP Proxy Settings page appears.

   A sample configuration is provided in Figure 8–3.

Figure 8–3 HTTP Proxy Settings



5. Complete the following parameters on the HTTP Proxy server if http-proxy is required for outbound communication.
   a. (Optional) If HTTP Proxy mode is required, select the **Proxy** check-box.
   b. In the **IP Address** field, enter your customer IP address.

      You can use the hostname or fully-qualified domain name (FQDN) as Oracle Advanced Support Gateway is configured to use Domain Name Service (DNS.)
   c. In the **Port** field, enter the port associated with the HTTP proxy server.
   d. (Optional) If authentication is required for the HTTP proxy server, select the **Authentication** check-box, and then enter the proxy username and password.
   e. (Optional) If you want to overwrite the global proxy mode, select the **Overwrite Global Proxy** check-box.
   f. Click **Save** to complete the HTTP proxy configuration.

Verifying an Internal Connection

External connections verify the connectivity between the Oracle Advanced Support Gateway and an Engineered System.

To use Oracle Advanced Support Gateway to verify connectivity between Oracle Advanced Support Gateway and an Engineered System:

1. Log in to Oracle Advanced Support Gateway.

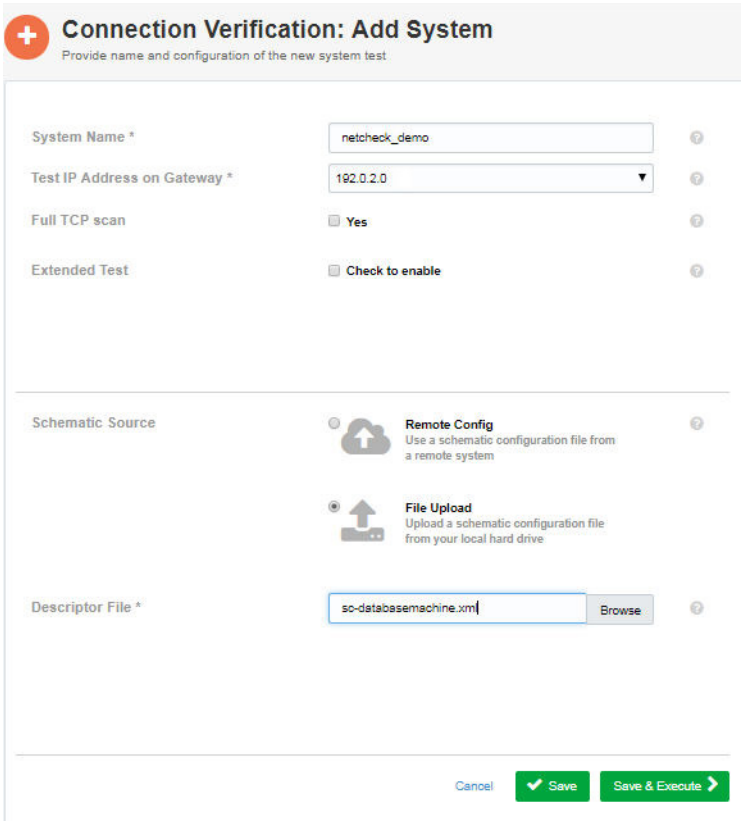
   The Oracle Advanced Support Gateway Home page appears.
2. From the **Gateway** menu, select **Connectivity Tests**.

   The Connection Verification: System Test Status page appears.
3. From the Internal Systems panel, click **Create System**.

   The Connection Verification: Add System page appears.

   A sample configuration is provided in Figure 8–4.

Figure 8–4 Connection Verification: Add System



4. Complete the following parameters to add a system.
   a. In the **System Name** field, enter the name of the Engineered System.
   b. In the **IP Address** field, enter the IP address of the Engineered System.

      You can use the hostname or fully-qualified domain name (FQDN) as Oracle Advanced Support Gateway is configured to use Domain Name Service (DNS.)
   c. (Optional) In the **Full TCP scan** field, if you require a full TCP scan of the target system to discover which TCP ports are open, select the **Yes** check-box.
   d. (Optional) In the **Extended Test** field, if you require a test of the connection from the target system to Oracle Advanced Support Gateway *and* from Oracle Advanced Support Gateway back to the target system, select the **Check to Enable** check-box, and then enter the SSH username and password.
   e. In the **Schematic Source** field, select a schematic source file from either a remote or a local source.

      Select **Remote Config** to choose a schematic source file from a remote source. Continue to step f.

      Select **File Upload** to choose a schematic source file from a local source. Skip to step g.
   f. (**Remote Config** only)

      In the **HOST IP Address** field, enter the IP address of the remote source.

      You can use the hostname or fully-qualified domain name (FQDN) as Oracle Advanced Support Gateway is configured to use Domain Name Service (DNS.)

In the **Schematic Directory** field, enter the path to the schematic directory.

In the **Filename** field, enter the name of the schematic source file.

In the **SSH Credentials for Remote Source File Transfer** section, enter the SSH username and password required for file transfer, or select the **Check to copy extended test SSH credentials** to automatically fill the SSH username and password fields using the input from the **Extended Test** field.

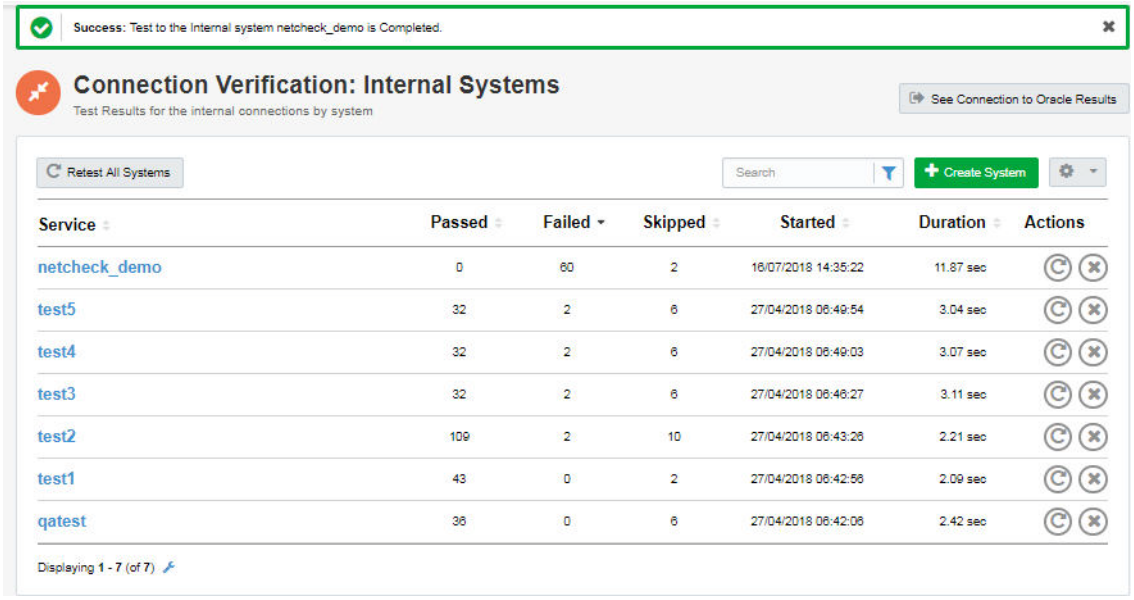
g. (**File Upload** only)

In the **Descriptor File** field, click **Browse** to navigate to the schematic source file on your local machine.

h. Click **Save and Execute** to run the system test or click **Save** to save the test details for execution at a later point.

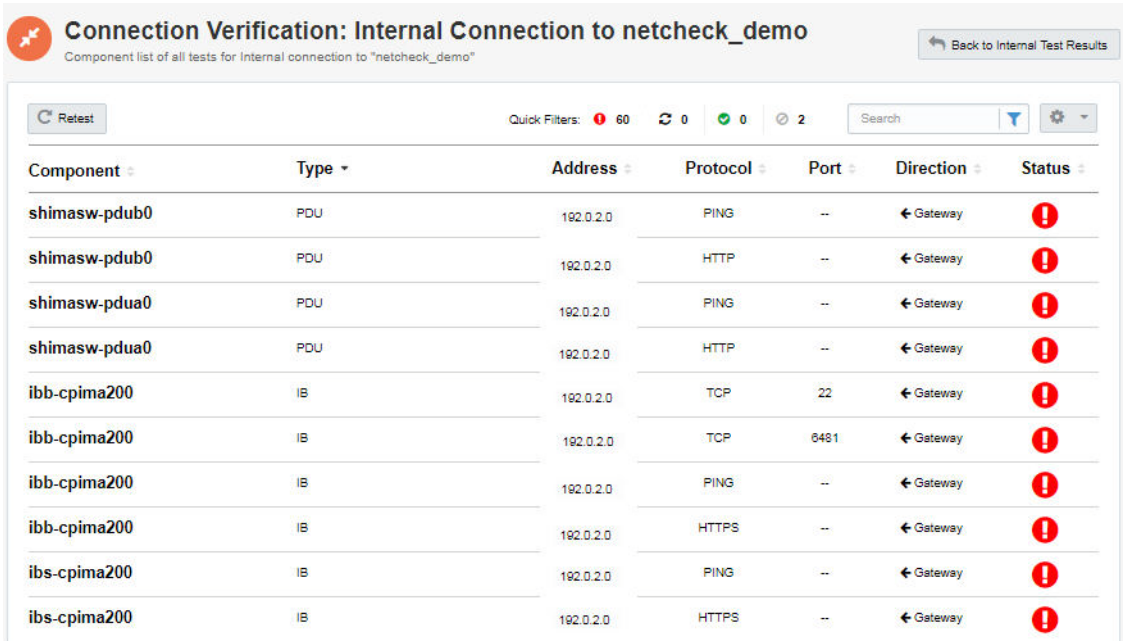
After executing the test, it appears on the Connection Verification: Internal Systems page that shows all test results for the internal connections by system.

Figure 8–5 Connection Verification: Internal Systems



5. Click the test name to list all components of the system test. This might include databases, cell nodes, Infiniband switches, and so on.

Figure 8–6 Connection Verification: Internal Connection



The Status column provides a visual indicator whether an individual component test passed or failed. The filters also provide a snapshot of successful, failed, skipped, or in progress tests.

The Direction column provides a visual indicator whether the connection is *to* or *from* the Gateway.

Oracle recommends that the network administrator should resolve any failed tests.

Click **Retest** to run the system test again.

Click **Back to Internal Test Results** to return to the Connection Verification: Internal Systems page.

Related Information

About Gateway Connectivity

About System Tests

Configuring New System Test Targets

An Oracle engineer can map new targets for connectivity tests by customizing a mapping file.

The file, `netcheck_mappings.properties`, maps target types from the input file to targets in the `connections.tbl` file. The engineer must perform the following actions:

- Add a key value pair per target. The key is the connectivity result value that the customer wants to display in the Connection Verification: Internal Systems page. The value is the new target type, for example: Infiniband Switch, Cell Node, PDU.
- Update the `connections.tbl` file to add the tests required for the new target type.

After the files have been modified and saved, the customer can start the connectivity test, select the new target type, and run tests for the target.

The contents of the `netcheck_mappings.properties` file are as follows:

```
IB=ib,Infiniband Switch,\.*Infiniband\.*Switch\.*,IBSwitch,oracle_ibswitch

DB=db,computenode,\.*DB\.*Node\.*,\.*Compute\.*Node\.*,Exadata OVS Compute
Node,Exadata DB VM,host

CELL_NODE=cel,cellnode,\.*Cell\.*Node\.*,Exadata Cell Node, oracle_exadata

CISCO=cisco,\.*Cisco\.*Switch\.*,oracle_exa_cisco_switch

PDU=pdu,PDU,oracle_exa_pdu

KVM=kvm, oracle_exa_kvm

ZFS=zfs,StorageHead,\.*ZFS\.*Storage\.*

ETHERNET_SWITCH=ethernet_switch

ZFS_ORACLE_ENDPOINTS=zfs_oracle_endpoints[root@ct-testimadsi-59 setup]#
```

9

Managing Service Requests

This chapter provides information about using the Oracle Advanced Support Gateway to monitor and manage Service Requests (SRs).

This chapter consists of the following sections:

- Viewing Service Requests

Viewing Service Requests

After activating databases (see Chapter 7, "Activating Services"), you can view SRs associated with issues occurring on a monitored database instance or a RAC database.

To view service requests:

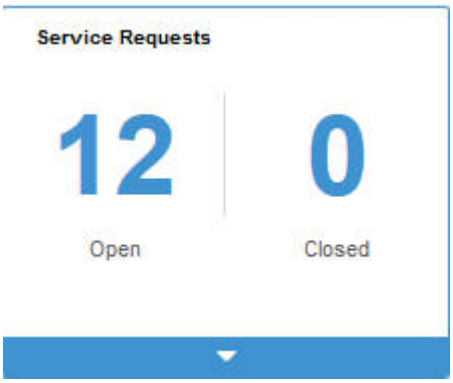
1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **My Services** menu, click the required service.

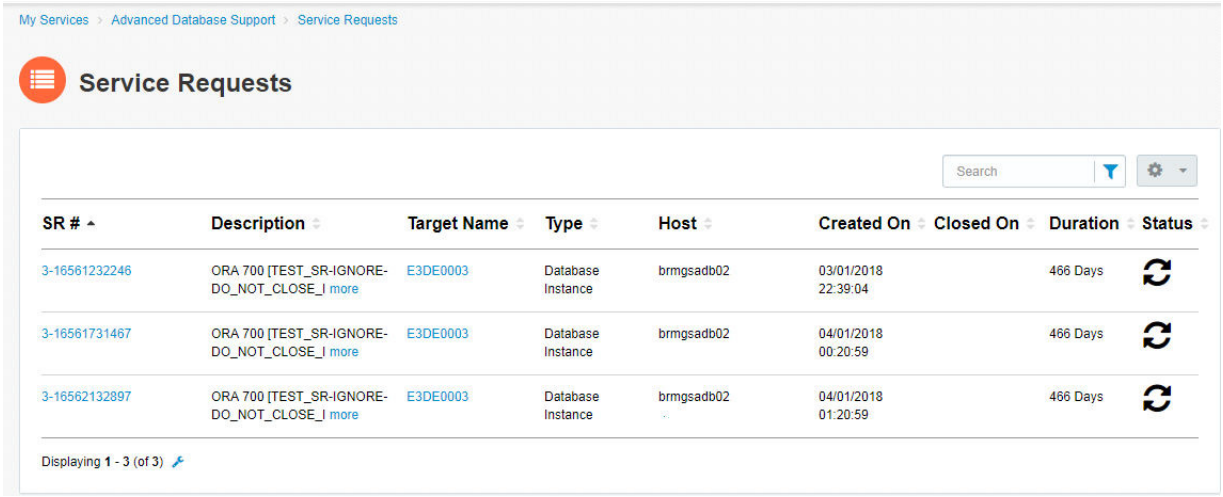
   The service page displays information about the managed databases, including a **Service Requests** badge shown in Figure 9–2.

Figure 9–1 Selecting Service Requests



3. Click the **Service Requests** badge to display a table of SRs as shown in Figure 9–2.

Figure 9–2 Viewing Service Requests



You can view both open and closed SRs.

The example in Figure 9–2 shows open SRs associated with a monitored database. The SR listing provides a link to the SR in MOS, a description of the SR, outlines the target name, type, and host, and lists when the SR was created, when it was closed (not applicable in this case), how long it has been open for, its current status.

You can sort SRs by type, number, or status, for example. You can search for an SR using a keyword in the SR description, or by referencing the host name, for example.

You can use the Quick Filters to quickly assess the number of open and closed SRs associated with a particular target.

You can update an SR by clicking the link to the SR in the table. The SR opens in My Oracle Support.

Viewing Service Requests Associated with a Managed System

To view service requests associated with a particular managed system:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Admin** menu, click **Manage Systems**.

   The Systems and Hosts page appears.

   You use this page to manage existing systems and hosts.

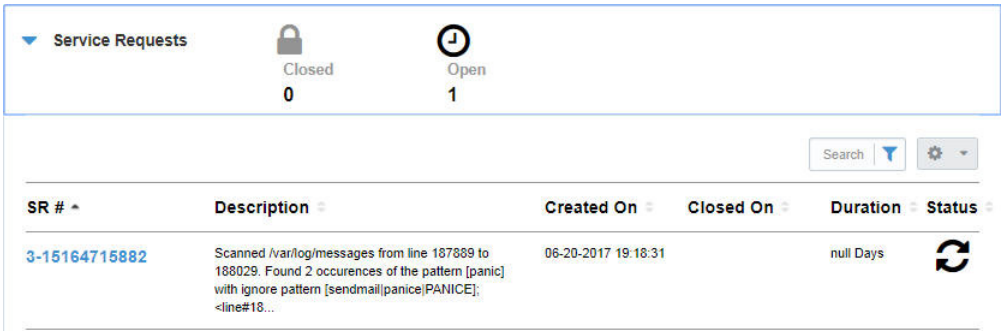
3. Click any listed target.

   The target configuration appears. This section provides information about viewing configuration details about discovered systems and hosts, for example: status, last backup time, lifecycle type, supported services, open SRs, health report details, and so on.

   You can use this page to view the target configuration and to manage the target details.

4. Expand the **Service Requests** window.

Figure 9–3 Selecting Service Requests



The example in Figure 9–3 shows an open SR associated with a managed system. The SR listing provides a link to the SR in MOS, a description of the SR, and lists when the SR was created, how long it has been open for, its current status, and the date on which the SR was closed.

10

Managing Databases and Database Patches

This chapter provides information about using the Oracle Advanced Support Gateway to manage databases and database patches.

This chapter consists of the following sections:

- About Database Management
- Activating a Service on a Database
- About Patching Requests
- Managing Advanced Database Support (ADS) Targets
- Managing Database Patch Compliance
- Using Proactive Patch Recommendations for ADS

About Database Management

You can use Oracle Advanced Support Gateway to manage all supported databases and their related cluster and ASM infrastructure as well as requesting the activation of new services on the databases.

Refer to the following sections:

- Viewing Managed Databases
- Editing Managed Databases

Viewing Managed Databases

You can view all managed databases on Oracle Advanced Support Gateway.

To use Oracle Advanced Support Gateway to view managed databases:

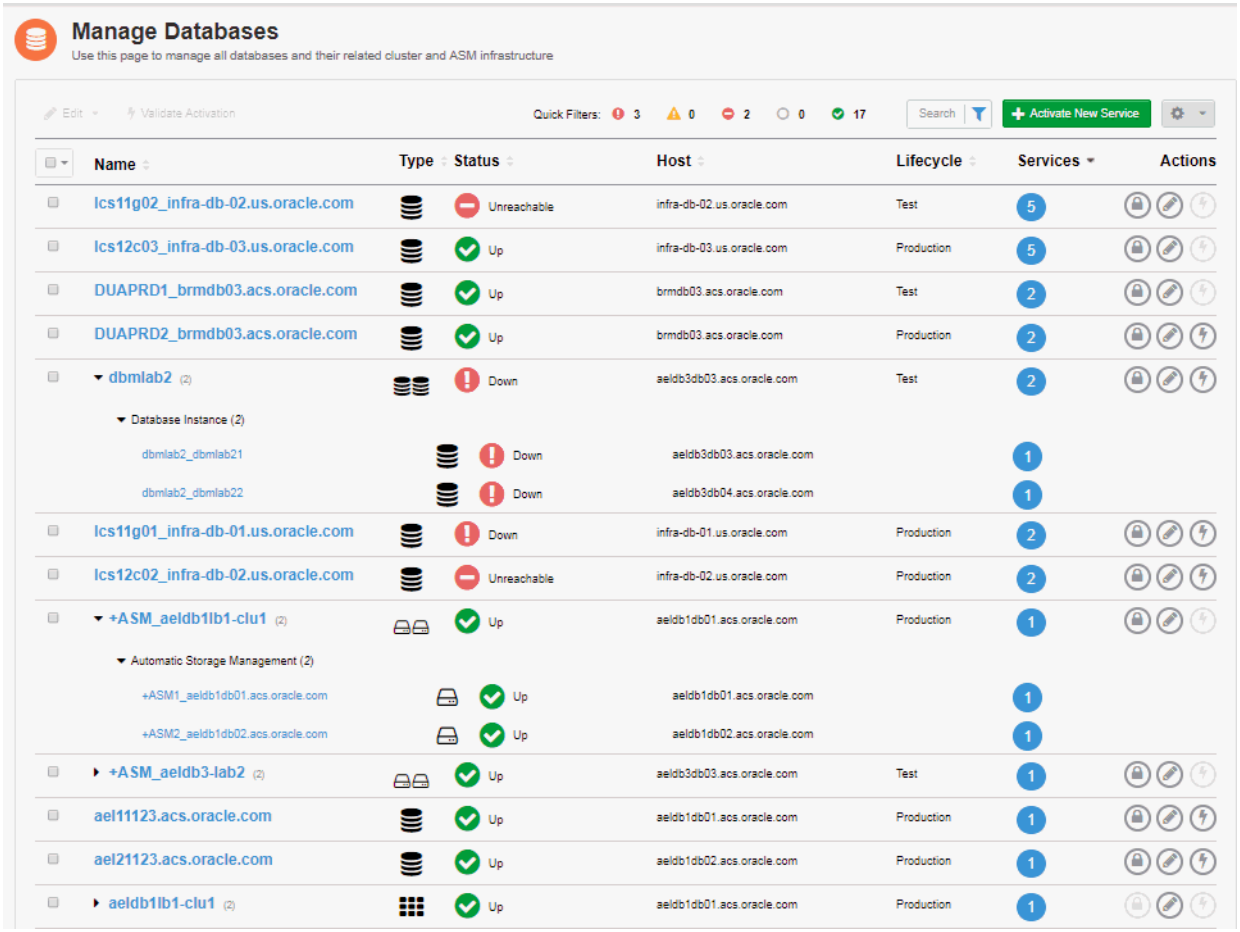
1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Admin** menu, click **Manage Databases**.

   The Manage Databases page appears. So, for example, as shown in Figure 10–1, you can expand a Cluster ASM to view and link to all ASM instances, or expand a database cluster target to view and navigate to its children.

Figure 10–1 Viewing Managed Databases



Databases are defined by:

- **Name**: Displays the database name. You can click any database to display all of its information.

  See Figure 10–2 that provides details of a database instance, including database status, support status, the time of the last backup, the number of days for which the database has been up, the database version, associated MOS and CSI details (both obfuscated in the diagram for security reasons), its associated targets, and the services running on it.

  Furthermore, the Manage Databases page displays other sections that enable users to view and edit database information. For example, these sections include:

  The **Configuration** section that displays database monitoring configuration details such as Oracle Home, the database lifecycle, database monitoring level, service identifier (SID), listener host, and listener port.

  All of these values can be edited in the Configuration section. See "Editing the Monitoring Configuration."

  The **Statistics** section provides information about database CPU, memory, and storage utilization in the form of interactive graphs.

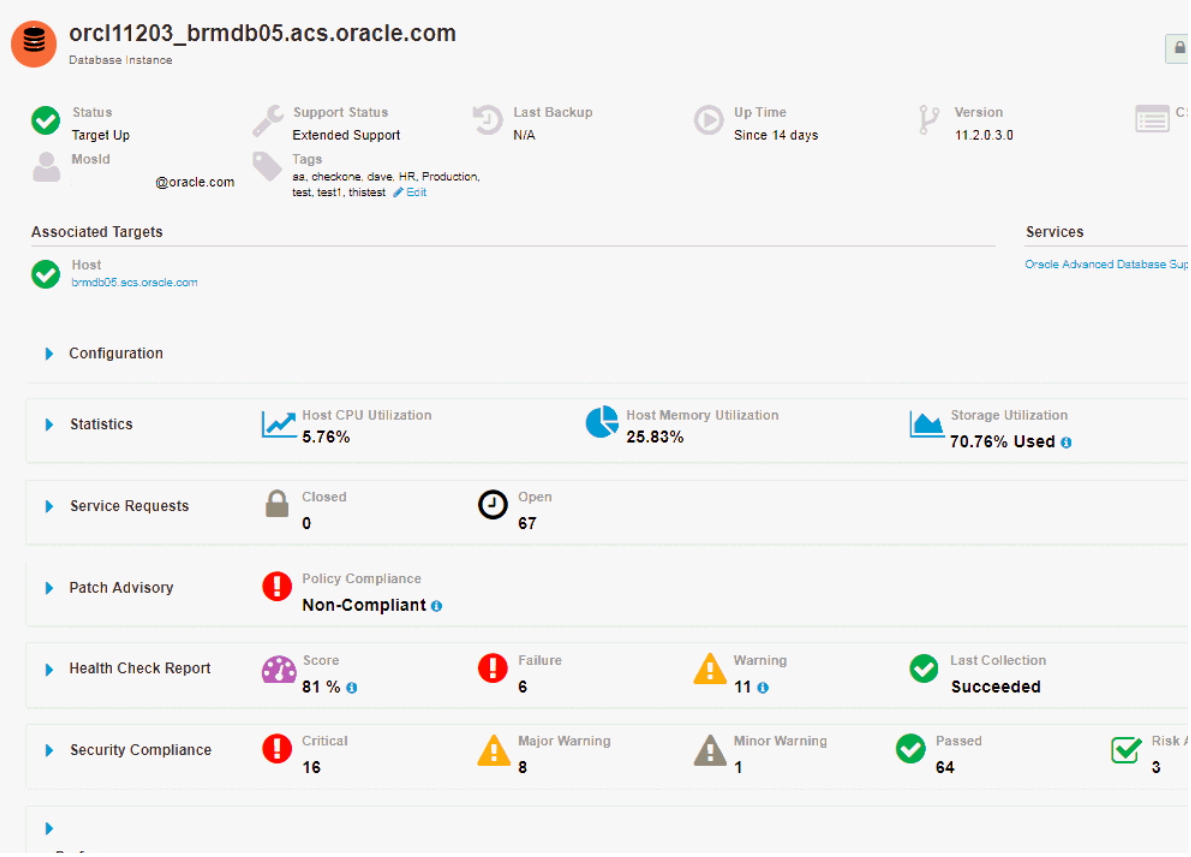
  For some databases, the session history (number of average active sessions) is also displayed in graphical form.

  The **Service Requests** section presents a count of open and closed service requests applicable to the database.

The **Patch Advisory** section displays the patch compliance summary for the database and enables the user to create patching requests.

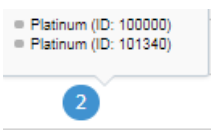
The **Health Check Report** section displays the output from a selection of lightweight Oracle tools - ORAchk, EXAchk, and Diagnostics Logs tools - that are integrated into Oracle Advanced Support Gateway and used to analyze and collect data on the health of database infrastructure.

Figure 10–2 Viewing an Individual Database Configuration



- **Type** - Database Instance, Cluster Database, Cluster ASM, Cluster, Cluster Database Container, and so on - each type denoted by a different icon.
- **Status**: Displays whether the database is currently up, down, or unreachable.
- **Host**: Displays the database host name.
- **Lifecycle**: Displays the lifecycle associated with the database. The values are *Test*, *Production*, *Stage*, or *Development*.
- **Services**: Displays the number of services running on the database. Hover over the number to display a list of individual services. Refer to Figure 10–3 that shows two separate Platinum Services instances running on the database.

Figure 10–3 Displaying the Services Running on a Database



- **Actions**: Displays a number of actions that can be performed on the database.

Related Information

Editing Managed Databases

Editing Managed Databases

You can perform a number of actions on managed databases:

- Use the **Edit** list to edit databases, including bulk edits on multiple databases.

  See "Editing Managed Databases Using the Edit List".

- Use the icons in the **Actions** column for a particular database to set the database lifecycle or fault monitoring level, edit its DBSNMP or ASMSNMP passwords, or validate the ADS or Platinum service running on the target.

  See "Editing Managed Databases Using the Actions Icons".

- Edit monitoring configuration details such as Oracle Home, the database lifecycle, database monitoring level, SID, listener host and listener port.

  See "Editing the Monitoring Configuration".

Editing Managed Databases Using the Edit List

To use Oracle Advanced Support Gateway to edit a database using the Edit list:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Admin** menu, click **Manage Databases**.

   The Manage Databases page appears.

3. Select the checkbox(es) corresponding to one or more databases on the Manage Databases page to enable the **Edit** list on the top left of the page.

   When multiple selections are made, bulk edit functionality is automatically enabled.

   Note: The bulk edit overwrites the existing values for all selected targets.

4. From the **Edit** list, select from the following actions:

   - **Monitoring Level**: Select the fault monitoring level to be applied to the database.

     Monitoring levels are restricted only to the valid monitoring levels for the target, for example, None, Low, Regular, High, or Intensive.

     See "Configuring Supported Targets".

   - **Lifecycle**: Select the lifecycle associated with the database.

     See "Configuring the Lifecycle Associated with a Supported Target".

   - **DBSNMP Password**: Change the DBSNMP password in Password Vault to reflect the database password.

   - **ASMSNMP Password**: Change the ASMSNMP password in Password Vault to reflect the database password.

Editing Managed Databases Using the Actions Icons

To use Oracle Advanced Support Gateway to edit a database using the Actions icons:

1. Log in to Oracle Advanced Support Gateway.

The Oracle Advanced Support Gateway Home page appears.

2. From the **Admin** menu, click **Manage Databases**.

   The Manage Databases page appears.

3. From the **Actions** column on the right of the page, for a chosen database, select one of the icons corresponding to the following options:

   - **Change Password**: Change the DBSNMP password and, optionally, the ASMSNMP password in Password Vault to reflect the database passwords.
   - **Edit**: Select the lifecycle associated with the database and the fault monitoring level to be applied to the database.

     Monitoring levels are restricted only to the valid monitoring levels for the target, for example, None, Low, Regular, High, or Intensive.

     See "Configuring the Lifecycle Associated with a Supported Target" and "Configuring Supported Targets".
   - **Test Readiness**: Select a database which has at least one ADS or Platinum service activated on it. Enter the credentials for the root user on the host, specify the privilege, for example, sudo, and click **Validate** to validate the service running on the database by performing a JDBC connection test.

     Note: Service validation applies only to databases on which at least one ADS or Platinum service is running.

Editing the Monitoring Configuration

To use Oracle Advanced Support Gateway to edit the monitoring configuration on the database:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Admin** menu, click **Manage Databases**.

   The Manage Databases page appears.

3. Select a database.

   On the database instance page, expand the **Configuration** section.

4. Edit the following values:

   - **Oracle Home**: Edit the path to the Oracle Home for the database.
   - **Lifecycle**: Select the lifecycle associated with the database.

     See "Configuring the Lifecycle Associated with a Supported Target".
   - **Monitoring Level**: Select the fault monitoring level to be applied to the database.

     Monitoring levels are restricted only to the valid monitoring levels for the target, for example, None, Low, Regular, High, or Intensive.

     See "Configuring Supported Targets".
   - **SID**: Update the service identifier associated with the database.
   - **Listening Host**: Update the host associated with the database monitoring.
   - **Listening Port**: Update the port associated with the database monitoring.

5. Click **Save** to commit the changes.

Activating a Service on a Database

In order to activate an Oracle service, you first select available databases to activate, then use the Oracle Advanced Support Gateway user interface to supply and test database credentials. Finally, you activate the databases for your selected service.

For further information, see Chapter 7, "Activating Services."

About Patching Requests

Automated patch scheduling is provided through Oracle Advanced Support Gateway and optimizes both time and resources for the patch coordinator and the patching manager. Automation also enables the customer to participate in the scheduling process in a transparent manner, in real time.

Note: In this release, automated patch scheduling is supported for Exadata and database targets for Oracle Advanced Database Support (ADS) and for Oracle Platinum Service. In order to schedule patches for other Oracle Engineered Systems, such as Exalogic or SuperCluster, PR requests must be submitted manually.

Refer to the following sections:

- "Creating a Patching Request"
- "Editing a Patching Request"

From a customer perspective, scheduling a patch event is now a simple, intuitive process that takes the customer through a number of interactive UI steps:

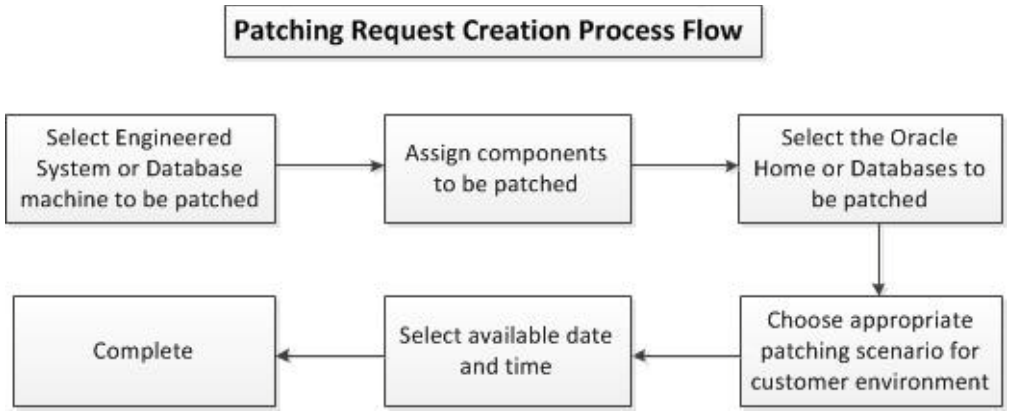
- Review the prerequisites to creating a patching request:
  - Patching requests are supported only on Gateways connected via an SSLVPN network.

    If your Gateway is connected via IPSec, please reach out to your patch coordinator to create the patching request.
  - If your Gateway has the Remote Access Control (Green Button) feature enabled, ensure the VPN is enabled before proceeding to create the patching request.

    See Chapter 16, "Enabling Remote Access to the Oracle Advanced Support Gateway."
- Select the Oracle Engineered System or Database machine to be patched.
- Assign the components (such as Cell Node, Compute Node, and so on) to be patched.
- Select the Oracle Home or Databases to be patched.
- Complete a mandatory Pre-Patch template - for Exadata systems only - prior to completing the scheduling details.
- Choose the patching scenario appropriate for the customer environment.
- Select the available date and time.

See Figure 10–4 that displays the process flow for Patching Request creation.

Figure 10–4 Patching Request Creation Process Flow



Customer requests for patching are then automatically assigned to Oracle Engineers based on their availability, and this information is visible on the Gateway. Requests for patches from patch coordinators for any date, irrespective of availability, are also accepted. In this case, Engineers are not assigned.

Furthermore, the Resource Manager can create Platinum Resource Teams and Members to manage the Engineer time table associated with each day. Assignment hours for Engineers working in Patching Requests can be assigned, deassigned, updated, or reviewed. Additionally, Engineers can be assigned to non-delivery activities such as holidays, training, internal meetings, etc.

Patching automation provides significant features such as:

- Automatic SR creation from the Gateway portal as soon as the patching request is created. This is a hardware SR using the CSI of the Engineered System that has been scheduled for application of the patch.
- Automated running of EXAchk scripts against the Exadata target 4 weeks prior to the Patching event date.
- Following the implementation of the EXAchk scripts, the EXAchk output is automatically attached to the Patching SR to enable customers and Oracle users to view it and take appropriate action.
- The ability to create, update, and test Patching Scenarios on the Oracle Advanced Support Platform portal. As patching scenarios are created or modified, they are transferred to all connected Gateways.

NOTE: SR creation takes place about 10 minutes after the successful creation of a patching request.

However, you can manually create an SR by clicking an action button on the Gateway user interface. In this case, SR creation is instantaneous.

Furthermore, there is also a workaround of manually running EXAchk by clicking an action button on the Gateway user interface.

Creating a Patching Request

To create a patching request:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

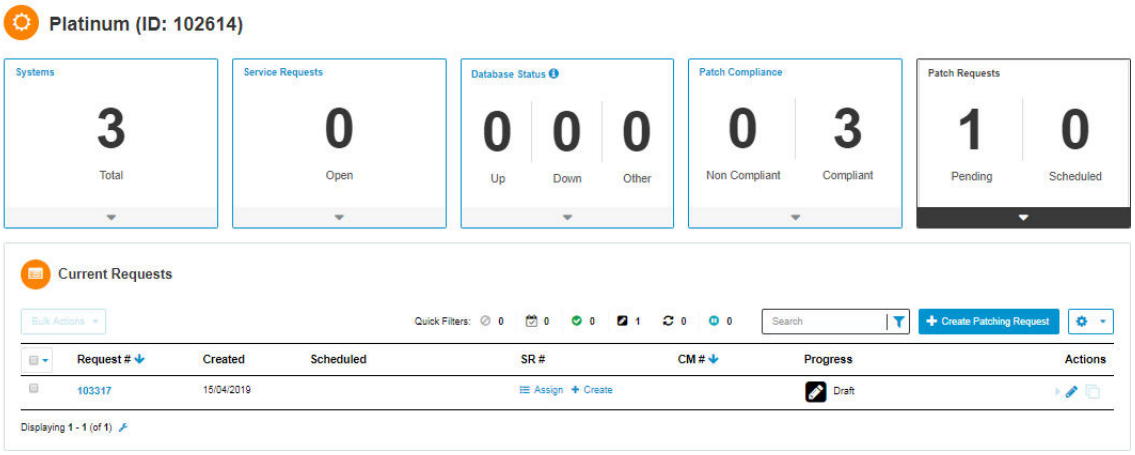
2. From the **My Services** menu, click **All Services**, and then select a service, for example, **Platinum (ID: XXXXXX)**.

   The service page appears.

3. Click **Patch Requests/Patch Compliance**.

   The Current Requests/Patch Compliance page appears.

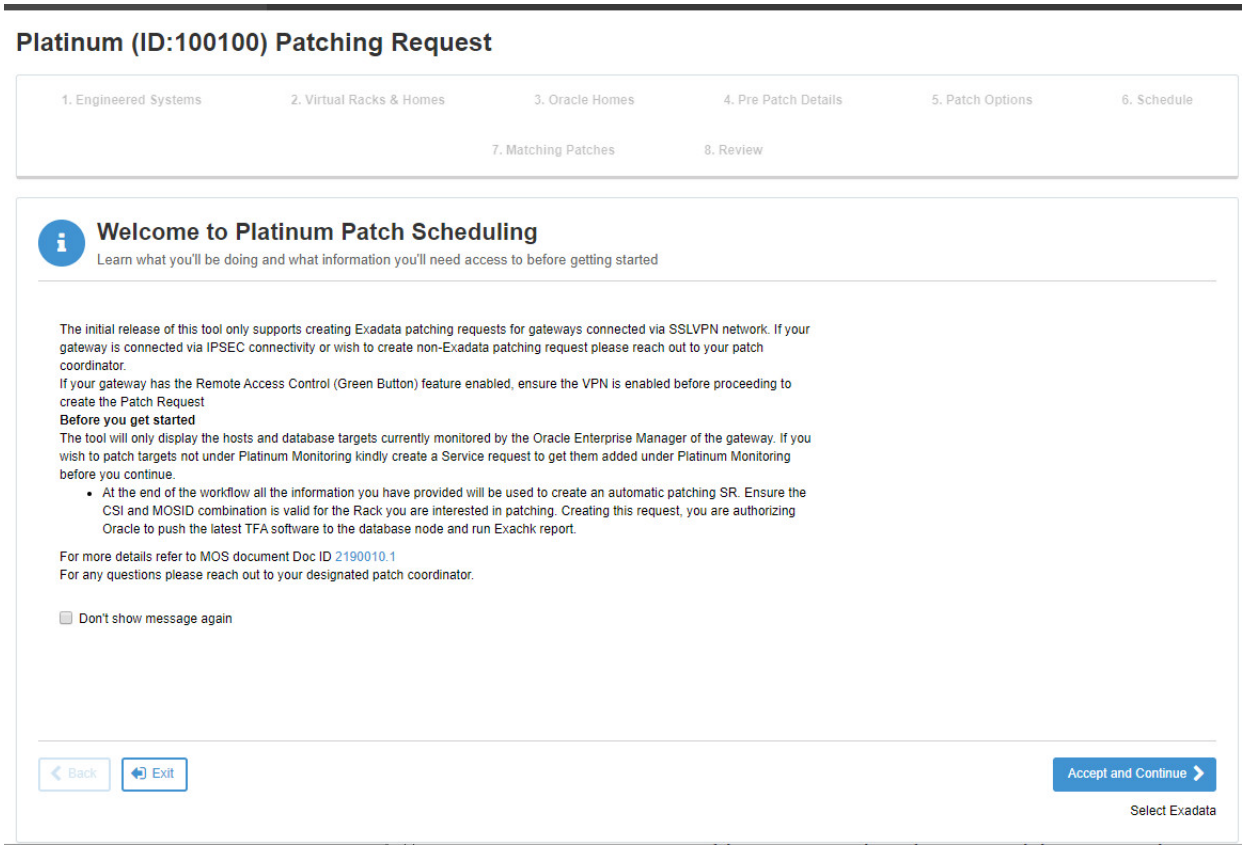
Figure 10–5 Viewing Patch Compliance



4. Click **Create Patching Request**.

   The Welcome to Platinum Patch Scheduling page appears.

Figure 10–6 Learning about the Patching Request Tool



You use this page to review the prerequisites to creating a patching request. So, for Platinum for example:

- The Platinum Patch Scheduling tool supports the creation of Exadata patching requests for Gateways connected using the SSLVPN network.

  If your Gateway is connected using IPSec connectivity, please reach out to your Patch Coordinator to create a patching request.

  If your Gateway has the Remote Access Control (“Green Button”) feature enabled,, ensure the VPN is enabled before proceeding to create the Patch Request.

- By creating this request, you are authorizing Oracle to push the latest Trace File Analyzer (TFA) software to the database node and run the EXAchk report.

  The TFA tools bundle runs on all managed hosts on which you want to run health checks. The TFA contains the ORAchk, EXAchk, and Diagnostics Logs tools.

  ORAchk and EXAchk are lightweight Oracle tools integrated into Oracle Advanced Support Gateway that are used to analyze and collect data on the health of your system infrastructure.

  See Chapter 13, "Managing Health Checks" for further information on the TFA.

Note: For any questions please reach out to your designated patch coordinator.

For more details about fulfilling the prerequisites, refer to `MOS article 2190010.1`.

Note: the content in the informational message may very depending on the service. So, for Advanced Database Support, for example, the welcome message is as follows:

Welcome Message

ADS includes patch deployment performed by Oracle up to four times per year via the Oracle Advanced Support Gateway. This includes analysis, planning, and deploying updates and patches to mitigate risks and complications. This tool is intended to simplify the ADS patching process workflow.

This tool is a one-stop place to request an ADS patching event and get real time confirmation of the event. It includes automatic creation of the Service Request to be used for coordination and collaboration with you in preparation for the patch event and its execution.

Before you get started

The initial release of this tool only supports creating patch requests for gateways connected via the SSLVPN network. If your gateway is connected via IPSEC, please reach out to your patch coordinator for creating the patching request.

If your gateway has the Remote Access Control (Green Button) feature enabled, ensure the VPN is enabled before proceeding to create the Patch Request.

At the end of the workflow all of the information you have provided will be used to create an automatic patching SR. Creating this request, you are authorizing Oracle to push the latest TFA software to the database node and run ORAchk report.

For more details, refer to `MOS article 2190010.1`.

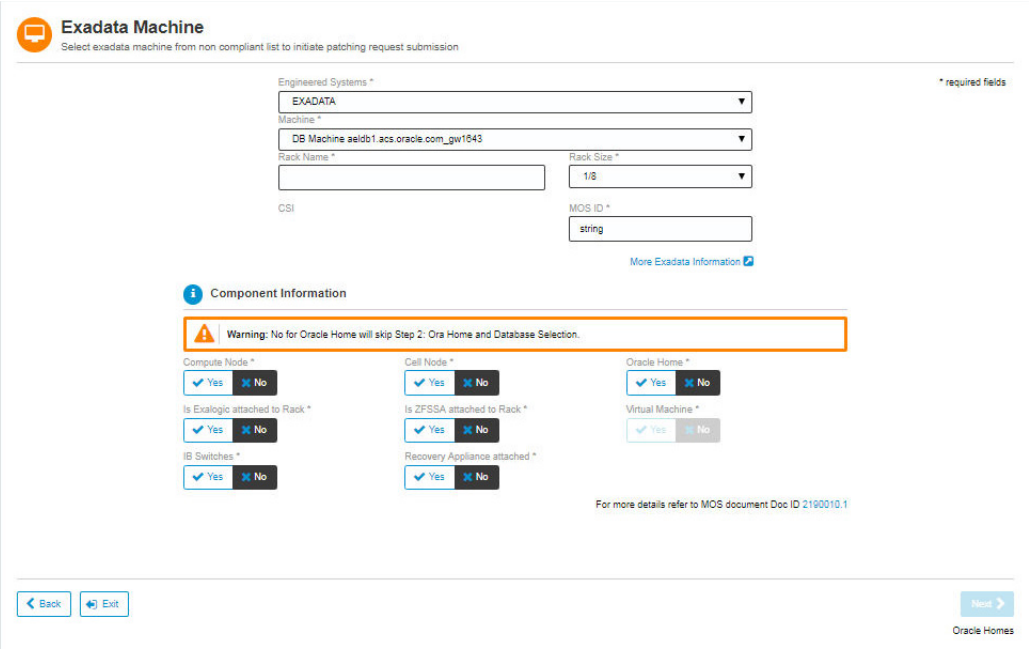
For security reasons, we won't store passwords.

5. Click **Accept and Continue**.

   The Exadata Machine page appears.

   You use this page to select an Exadata machine from the list of non-compliant Exadata machines to initiate a patching request submission.

Figure 10–7 Selecting the Exadata Machine to be Patched



6. Complete the following parameters:

   a. In the **Engineered Systems** field, select *EXADATA* or *ZDLRA*.

b. In the **Machine** field, select the Exadata machine to be patched.

   Note: Ensure that the components to be patched have been added to Platinum monitoring before continuing.

c. In the **Rack Name** field, enter the name of the rack for the selected Exadata machine.

d. In the **Rack Size** field, select the rack size from the options provided: *1/8, 1/4, 1/2,* or *Full*.

e. In the **MOS ID** field, enter the MOS username associated with the CSI that is associated to this system.

   Note: Ensure that the MOS username has the *SR Create* privilege, as this MOS ID and CSI combination is used to create the automatic patching SR in the final step of this wizard.

f. (Optional) Select **More Exadata Information** to display a My Oracle Support (MOS) Knowledge Base article on "Exadata Database Machine and Exadata Storage Server Supported Versions".

g. In the Component Information section, complete the following parameters by selecting **Yes** or **No** for each of the components (the default for each is *No*):

   a. In the **Compute Node** field, select whether compute nodes are required to be patched.

      If you select **Yes**, from the **Compute Node Quantity** field, select the number of compute nodes in the range 1-16.

   b. In the **Cell Node** field, select whether cell nodes are required to be patched.

      If you select **Yes**, from the **Cell Node Quantity** field, select the number of cell nodes in the range 1-24.

   c. In the **Oracle Home** field, select whether Oracle Homes are required to be patched.

      Note: If you select *No*, then the Oracle Homes step in the workflow is skipped.

   d. In the **Is Exalogic attached to Rack** field, select whether the Exalogic is attached to the rack being patched.

   e. In the **Is ZFSSA attached to Rack** field, select whether the ZFSSA is attached to the rack being patched.

   f. (Optional) In the **Virtual Machine** field, select whether the VM is attached to the rack being patched.

   g. In the **IB Switches** field, select whether InfiniBand switches are required to be patched.

      If you select **Yes**, from the **Switches Quantity** field, select the number of Infini-Band switches in the range 1-6. The default is *2*.

   h. In the **Recovery Appliance attached** field, select whether the recovery appliance is required to be patched.

   i. (Optional) Select **For more details refer to MOS document Doc ID 2190010.1** to display the My Oracle Support (MOS) Knowledge Base article on "How to Schedule Exadata Patching Request using Oracle Advanced Support Gateway for Platinum Customers".

7. Click **Next**.

   Select one of the following options:

- If you selected to patch Oracle Homes in the Component Information section above, then the Oracle Homes & Databases page appears.

  Skip to Step 10.

  (Optional) Select **More OJVM Patching Details** to display a MOS Knowledge Base article on "Oracle JavaVM Component Database PSU" (OJVM PSU) Patches".

- If you select to patch Virtual Racks, then the Virtual Racks and Homes page appears and you then skip the Oracle Homes step and continue to patching instead.

  Continue to Step 14.

- If you selected *not* to patch Oracle Homes in the Component Information section above, then the Patch Option page appears.

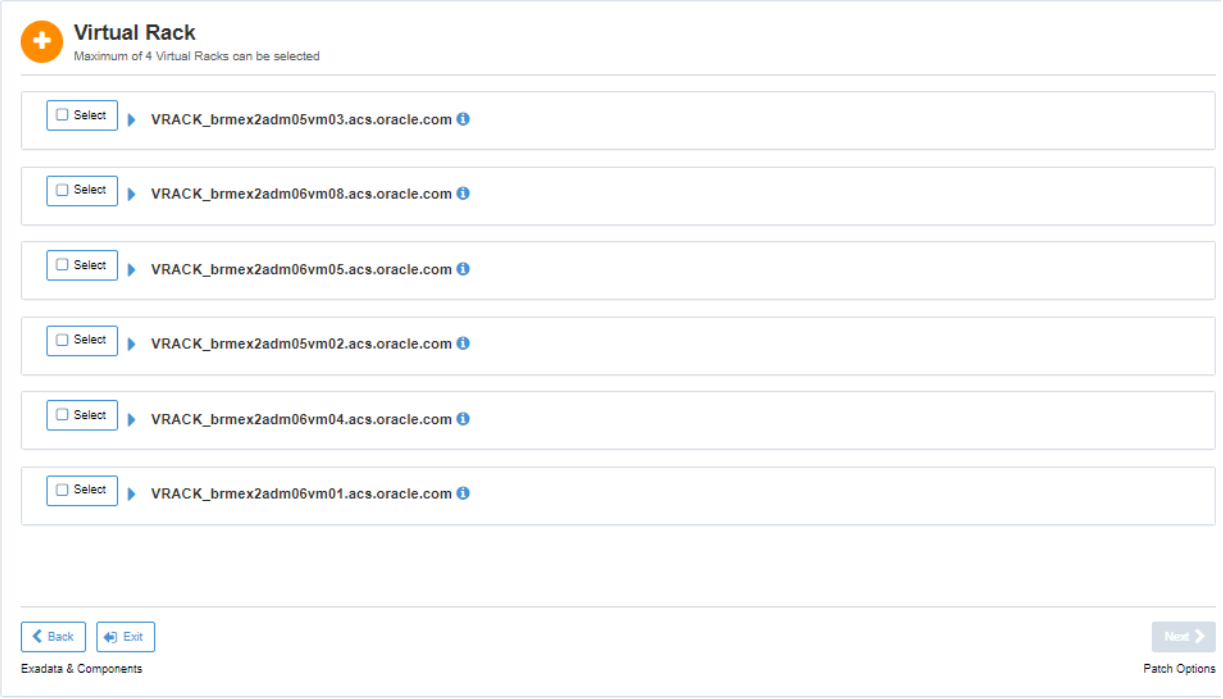
  Skip to Step 14.

  (Optional) Select **More OJVM Patching Details** to display a MOS Knowledge Base article on "Oracle JavaVM Component Database PSU" (OJVM PSU) Patches".

8. Click **Next**.

   The Virtual Racks and Homes page appears.

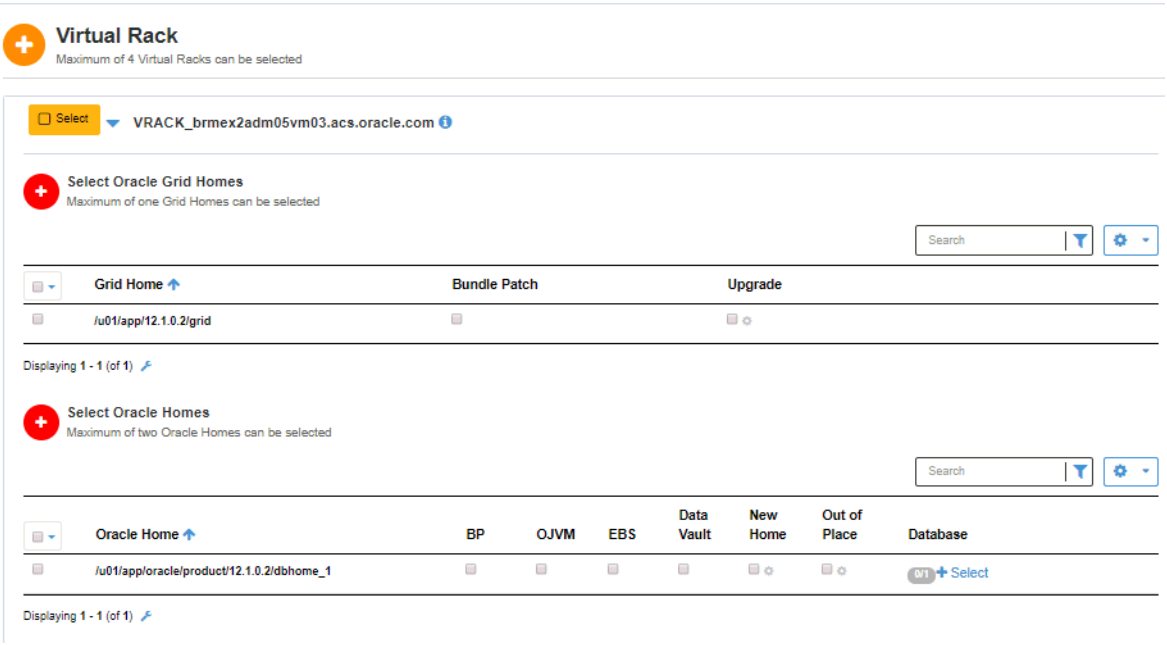
Figure 10–8 Selecting the Virtual Racks to be Patched



9. In the Virtual Rack page, select virtual racks (to a maximum of 4).

   a. Expand the required virtual rack by clicking the appropriate **Select** checkbox:

Figure 10–9 Selecting the Virtual Racks to be Patched



b. (Optional) Select the components on a particular Virtual Rack that require patching:

? In the **Select Oracle Grid Homes** field, select databases (to a maximum number of Grid Homes, depending on the customer contract).

The available Grid Homes are displayed on the Homes page showing Grid Home location, and providing a bundle patch application option and (if applicable) an upgrade option.

For the Grid Home, select whether to apply a bundle patch.

A bundle patch is a cumulative collection of fixes for a specific product or component. A patch of this type is released as needed depending on the product's requirements. You may also know a bundle patch as: maintenance pack, service pack, MLRs, cumulative patch, or update release.

For the Grid Home, select whether to apply an upgrade.

If you select to upgrade, provide a new name for the Grid Home and choose the target grid version.

? In the **Select Oracle Homes** section, select databases (to a maximum number of Oracle Homes, depending on the customer contract).

Select from the following options:

a. Select individual databases by clicking **Select** in the **Oracle Home** column.

b. (Optional) Select the components on a particular Oracle Home that require patching or update the Oracle Home configuration as follows:

Select **BP** to apply a bundle patch.

A bundle patch is a cumulative collection of fixes for a specific product or component. A patch of this type is released as needed depending on the product's requirements. You may also know a bundle patch as: maintenance pack, service pack, MLRs, cumulative patch, or update release.

Select **OJVM** to patch Oracle Java Virtual Machine.

Note: Selecting OJVM may add an additional 90 minutes outage time to Oracle Home, assuming the databases to be patched are configured as a resource in cluster.

For further information, refer to OJVM Patching Details on My Oracle Support.

Select **EBS** to patch Oracle E-Business Suite.

Select **Data Vault** to patch Oracle Database Vault.

Select **New Home** to specify a new Oracle Home. Provide a new name for the target and select a target version, for example, *12.1* or *12.2*.

Select **Out of Place** to specify a new Out of Place (OOP.) Provide the OOP target location.

Note: Out-of-place patching, which is based on cloning, is a patching method where patching is performed by creating a copy of Oracle Home, applying patches to the copied Home, and then switching services to the copied Home. This patching method helps in reducing the downtime of switching of the services from the existing Home to the updated Home.

In the **Database** field, click **+Select** to select constituent databases from the Oracle Home.

From the database list, select the required database and configure it as follows:

Select **Dataguard** to apply Oracle Data Guard. From the **DB Type** field, select *Prime* or *Standby* to specify the database type.

Note: Oracle Data Guard ensures high availability, data protection, and disaster recovery for enterprise data.

Select **Catbundle** to apply the particular scripts that need to run for installation or rollback of each patch in the bundle series.

Select **Upgrade** to apply an upgrade. If you select to upgrade, in the **Standby DB Name** field, provide the location of the standby database, and in the **Standby Node Name**, provide the name of the standby node.

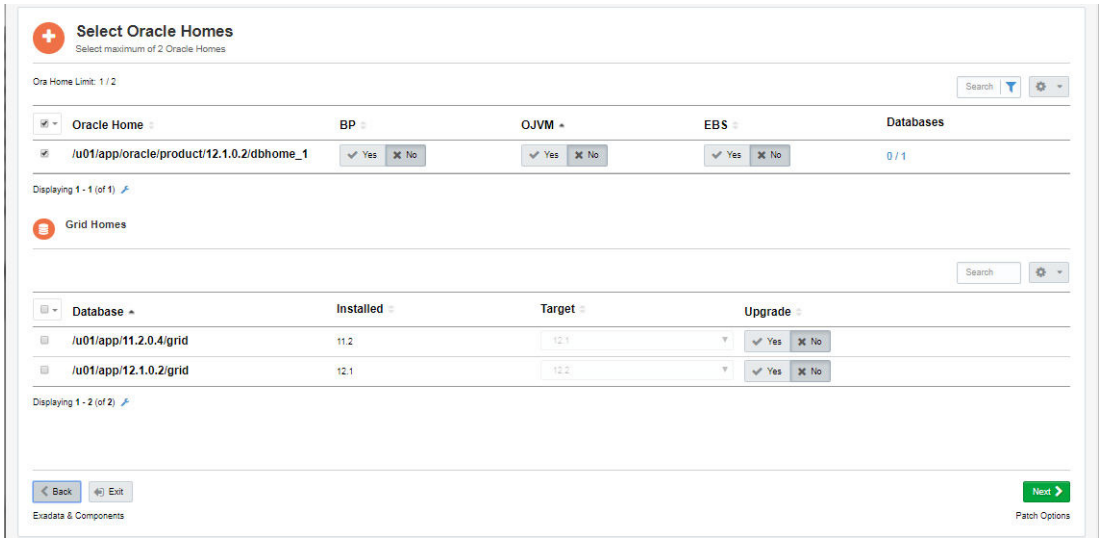
After patching Virtual Racks, you then skip the Oracle Homes step and continue to patching instead.

Continue to Step 14.

10. Click **Next**.

    The Oracle Homes page appears.

Figure 10–10 Selecting the Oracle Homes, Grid Homes, and Databases to be Patched



11. In the Select Oracle Homes section, select databases (to a maximum number of Oracle Homes, depending on the customer contract).

    Select from the following options:

    a. Select individual databases by clicking **Select** in the **Oracle Home** column.

    b. (Optional) Select the components on a particular Oracle Home that require patching:

    - In the **BP** field, click **Yes** to apply a bundle patch.

      A bundle patch is a cumulative collection of fixes for a specific product or component. A patch of this type is released as needed depending on the product's requirements. You may also know a bundle patch as: maintenance pack, service pack, MLRs, cumulative patch, or update release.

    - In the **OJVM** field, click **Yes** to patch Oracle Java Virtual Machine.

      Note: Selecting OJVM may add an additional 90 minutes outage time to Oracle Home, provided the databases to be patched are configured as a resource in cluster.

      For further information, refer to `OJVM Patching Details on My Oracle Support`.

    - In the **EBS** field, click **Yes** to patch Oracle E-Business Suite.

12. (For Oracle Homes) Click **+Select** to select constituent databases from the Oracle Home.

    a. Select individual databases by clicking **Select** in the **Databases** column.

    b. (Optional) Select the components on a particular Oracle Home that require patching:

    - In the **Catbundle** field, click **Yes** to apply the particular scripts that need to run for installation or rollback of each patch in the bundle series.

13. (Optional) In the Grid Homes section, select databases (to a maximum number of Grid Homes, depending on the customer contract. Typically customers have a maximum of 5 Grid Homes.)

    A list of grid homes is displayed on the Homes page - showing grid home location, installed grid version, whether an upgrade is required, and if so, the target grid version.

    You can select to upgrade those required.

Select from the following options:

a. Select individual databases by clicking **Select** in the **Databases** column.

b. (Optional) Select the installed grid versions that require updating:

- In the **Upgrade** field, click **Yes** to enable the **Target** field.
- In the **Target** field, select the required grid version, for example, *12.1* or *12.2*.

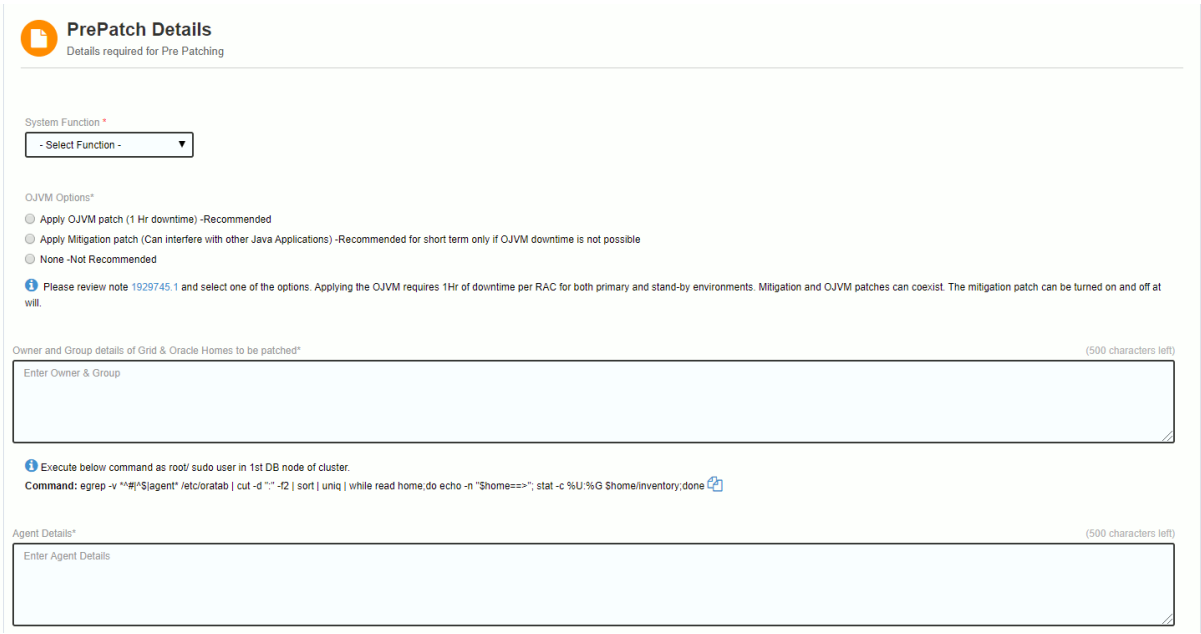
14. Click **Next**.

The Pre-Patch Details page appears.

You use this page to supply information for pre-patching prior to completing the scheduling details.

Note: The Pre-Patch page is mandatory, and for Exadata systems only.

Figure 10–11 Supplying Pre-Patch Information, Part 1



15. Complete the following parameters:

a. In the **System Function** field, select the functional nature of the patch, for example, production, development, test, and so on.

b. In the **OJVM Options** field, select from the following options:

Note: Mitigation and OJVM patches can coexist. The mitigation patch can be turned on and off, at will.

Review My Oracle Support (MOS) note 1929745.1 and select one of the options below (applying the OJVM requires approximately one (1) hour of downtime per RAC for both primary and stand-by environments):

Option 1: Apply the OJVM patch (This is the recommended option.)

Option 2: Apply a Mitigation patch.

This process can interfere with other Java applications and is recommended for short-term patching only if OJVM downtime is not possible.

Option 3: Apply no patch. This option is **not recommended**.

c. In the text box labeled **Owner and Group details of Grid & Oracle Homes to be patched*,** enter the owner and group of Grid & Oracle Home.

d. Execute the following command as the *root*/*sudo* user in the first database node of the cluster:

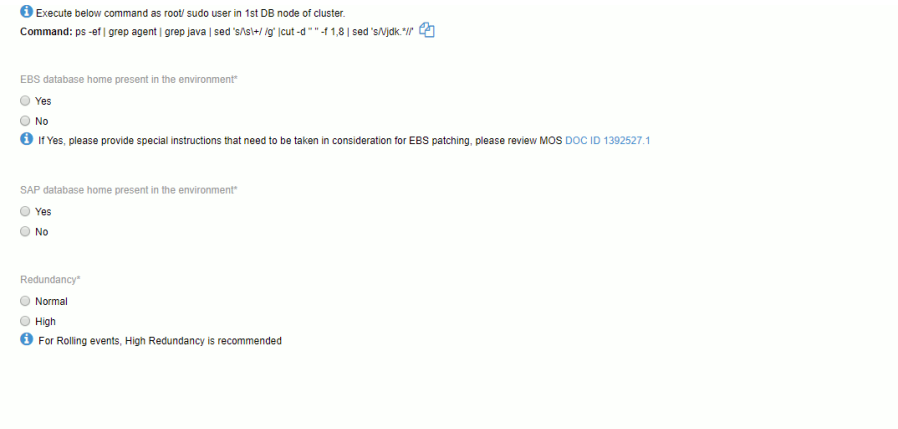
egrep -v *^#|^$|agent* /etc/oratab | cut -d ":" -f2 | sort | uniq | while read home;do echo -n "$home==>"; stat -c %U:%G $home/inventory;done

e. In the text box labeled **Agent Details*,** enter information about the agent.

f. Execute the following command as the *root*/*sudo* user in the first database node of the cluster:

ps -ef | grep agent | grep java | sed 's/\s\+/ /g' |cut -d " " -f 1,8 | sed 's/\/jdk.*//

Figure 10–12 Supplying Pre-Patch Information, Part 2



g. In the **EBS database home present in the environment** field, select **Yes** if an EBS database home is present, or select **No** if this option is not applicable in this instance.

If you select **Yes**, please provide in the text box any special instructions that need to be taken in consideration for EBS patching.

Note: First review the relevant MOS document, ID 1392527.1.

h. In the **SAP database home present in the environment** field, select **Yes** if a SAP database home is present, or select **No** if this is not applicable in this instance.

i. In the **Redundancy*** field, select **Normal** or **High**.

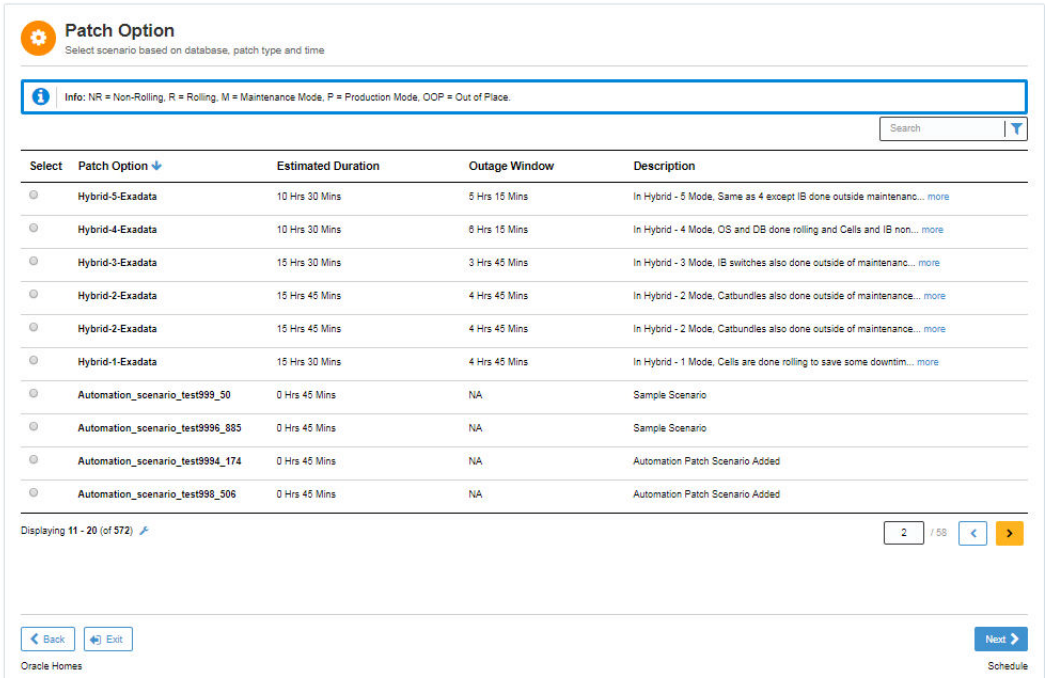
Note: For rolling events, high redundancy is recommended.

16. Click **Next**.

The Patching Request: Patch Option page appears.

You use this page to select a patching scenario based on database, patch type, and time.

Figure 10–13 Selecting the Patch Option



17. Select the applicable patch option using a combination of the following parameters:

    a. The **Patch Option** column displays the patch type; for example: **Hybrid-1-Exadata** or **Hybrid-5-Exadata**.

    b. The **Estimated Duration** column displays the time taken for the patching process.

    c. The **Outage Window** column displays the outage time for the device.

    d. The **Description** column provides a full explanation of the patch types listed in the **Patch Option** column, using the following abbreviations:

       NR = Non-Rolling, **R** = Rolling, **M** = Maintenance Mode, **P** = Production Mode, **OOP** = Out of Place.

       (Optional) Click **More** to display the full details of the patch type.

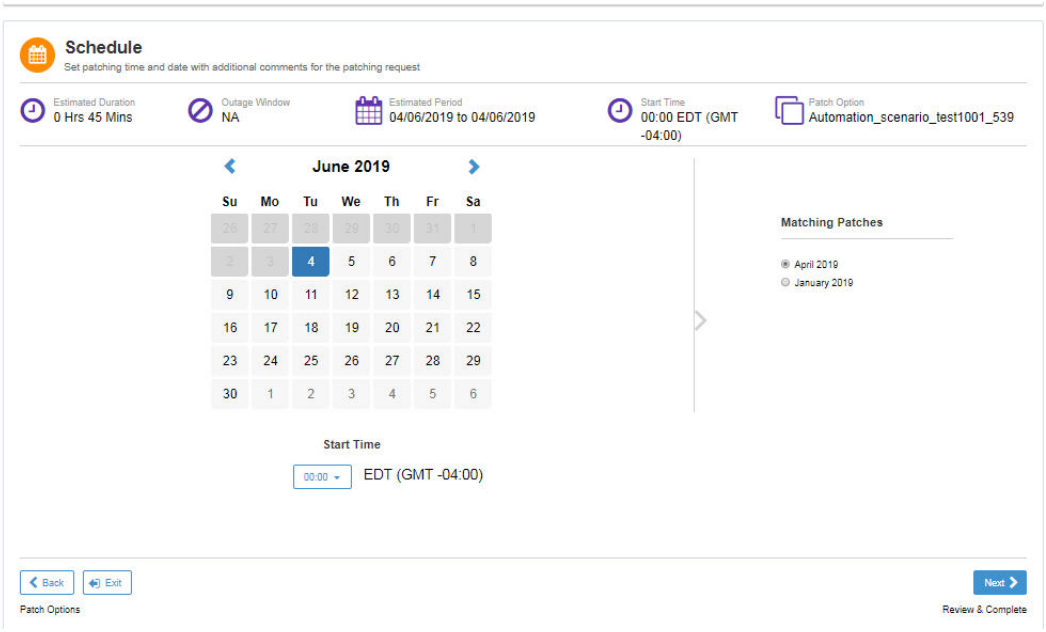
       For example, *In Hybrid - 5 Mode, Same as 4 except IB done outside maintenance window. Compute Nodes = R, Grid Home = R, Database Homes= R, Catbundles = P, Storage Cells = NR, IB Switch = P and OJVM = NR.*

18. Click **Next**.

    The Patching Request: Schedule page appears.

    You use this page to set the patching time and date. All estimates may vary and the final period may change.

Figure 10–14 Selecting the Patch Schedule



19. Select the time and date for the patching request using the following parameters:

- Schedule a patching date a minimum of four (4) weeks from the present date
- Use the calendar to select available dates within an estimated period. So, for example, in the month shown above, the dates in gray are not available.
- You cannot schedule a patch within 90 days of an existing Patch Request on the same database.

  If you attempt to generate a conflicting patch request, an error message appears, requesting you to cancel previous patch request(s), for example *PR 123456*, before scheduling another one.
- Complete all required fields successfully (you cannot submit a patching request in the next step until the configuration is complete)

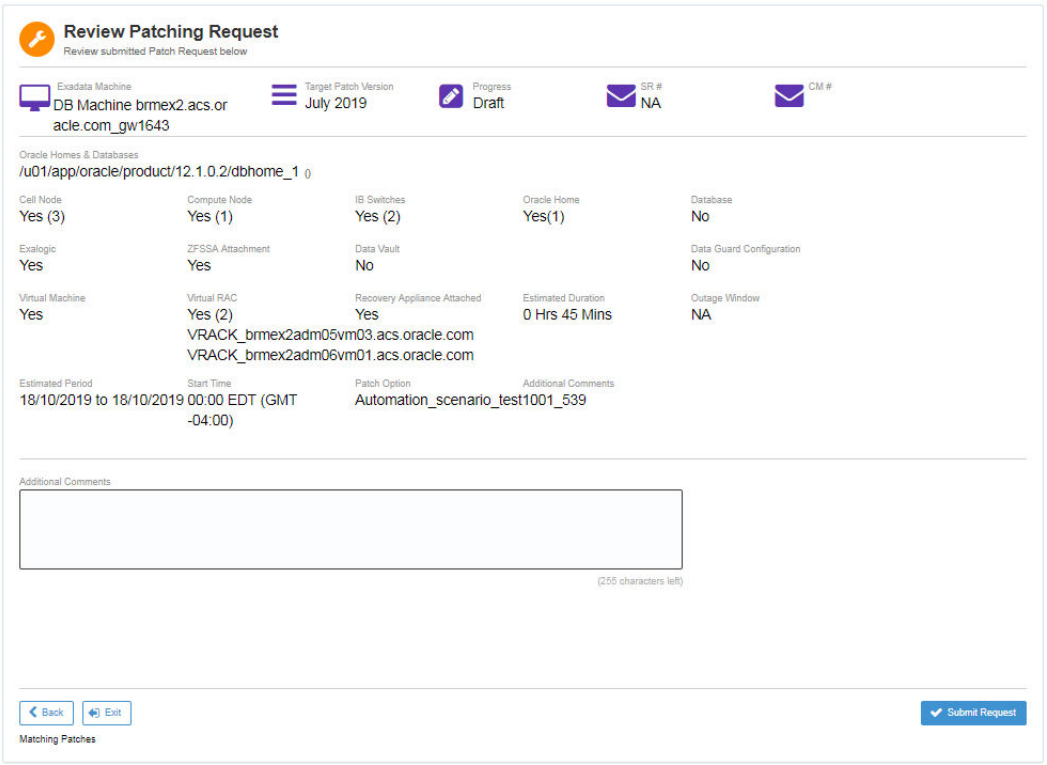
Note: Preferred time and date formats are based on the browser time zone.

Note: If you receive a message stating that a system error has occurred, please contact Oracle Support for help.

20. Click **Next**.

The Review Patching Request page appears.

Figure 10–15 Reviewing the Patch Schedule Request Details



This page requires you to review and confirm the details of the patching request prior to submission.

The page lists the Exadata machine name and patch version. It specifies the components to be patched, such as computer nodes, cell nodes, switches, databases, and so on.

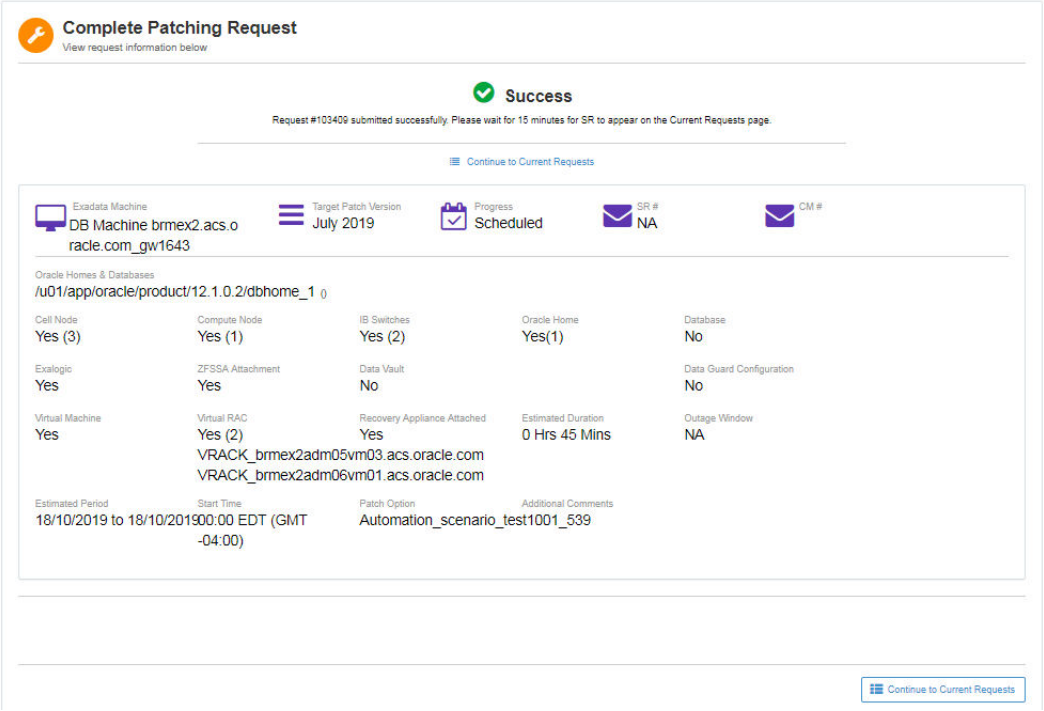
Furthermore, the page specifies the estimated duration and outage window associated with the patching process, the period during which it is likely to take place, the start time, the nature of the patch process, for example, whether rolling or non-rolling, and so on.

Finally, the applicable Oracle Homes, (Grid Homes), and databases are listed.

21. Click **Submit Request**.

    The Complete Patching Request page appears.

Figure 10–16 Confirming the Patch Schedule Request



This page displays a message stating that the patch creation has been successful:

Request #123456 submitted successfully. Please wait for 15 minutes for SR to appear on the Current Requests page.

The Complete Patching Request page also provides details of the patching request as outlined in Step 20.

22. As the patching Request has been created successfully, click **Continue to Current Request**s to review the list of current patching requests.

The Current Requests page appears.

You use this page to:

- Automatically create an SR as soon as you have created the patching request.

  See "Creating an SR for a Patching Request".

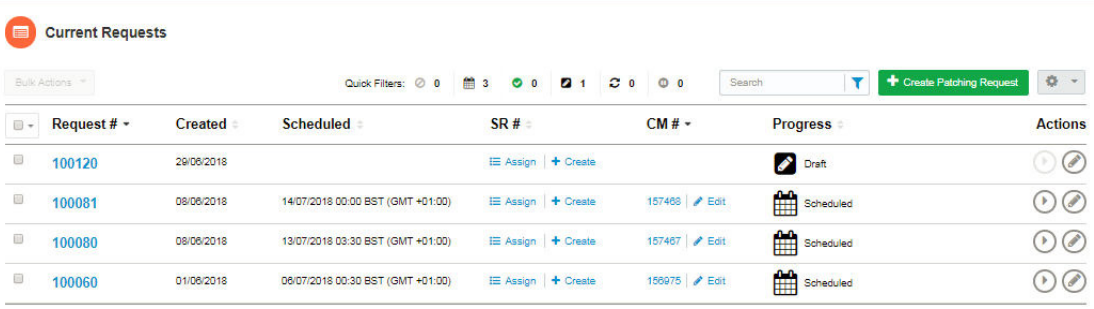
  Note: This is a hardware SR using the CSI of the Engineered System that has been scheduled for application of the patch.

- Edit an existing patching request that is in draft mode.

  See "Editing the CM for a Patching Request".

- Cancel an existing patching request.

Figure 10–17 Viewing Current Patching Requests



Related Information

Creating an SR for a Patching Request

Editing the CM for a Patching Request

Canceling a Patching Request

Creating an SR for a Patching Request

You can automatically create an SR as soon as the patching request is created. This is a hardware SR using the CSI of the Engineered System that has been scheduled for application of the patch.

To create an SR:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

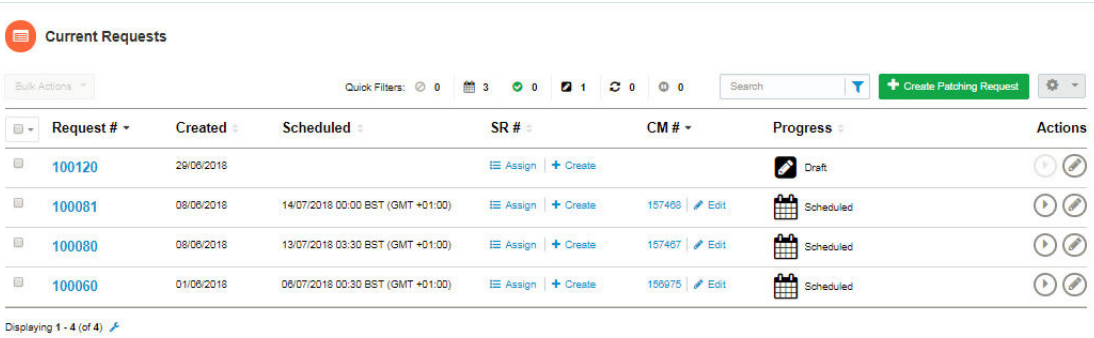
2. From the **My Services** menu, click **All Services**, and then select a service, for example, **Platinum**.

   The Platinum Service page appears.

3. Click **Patch Requests**.

   The Current Requests page appears.

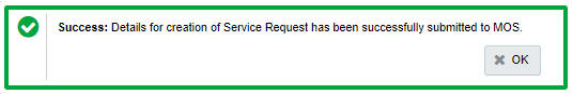
Figure 10–18 Viewing Patching Requests



4. For a request for which an SR has not already been created, for example, the request numbered *10120*, under the SR column, click **Create**.

   A success message appears stating that the details of the SR creation have been submitted to My Oracle Support (MOS):

Figure 10–19 Successfully Creating Patching Request SR



5. Click **OK**.

   An email is sent to the Gateway user associated with the SR creation listing:

   - The SR number (from which you can link to the SR on MOS directly);
   - The hostname;
   - The CSI of the Engineered System that has been scheduled for application of the patch;
   - Links to documentation relating to Oracle Auto Service Request (ASR);
   - Translations of the email in Chinese, Japanese, and Korean.

Figure 10–20 Viewing Oracle ASR: Service Request Creation

Related Information

Editing the CM for a Patching Request

Assigning an SR for a Patching Request

Canceling a Patching Request

Editing the CM for a Patching Request

You can edit an SR associated with a patching request by assigning a new CM number to be associated with the patch.

To edit an SR:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

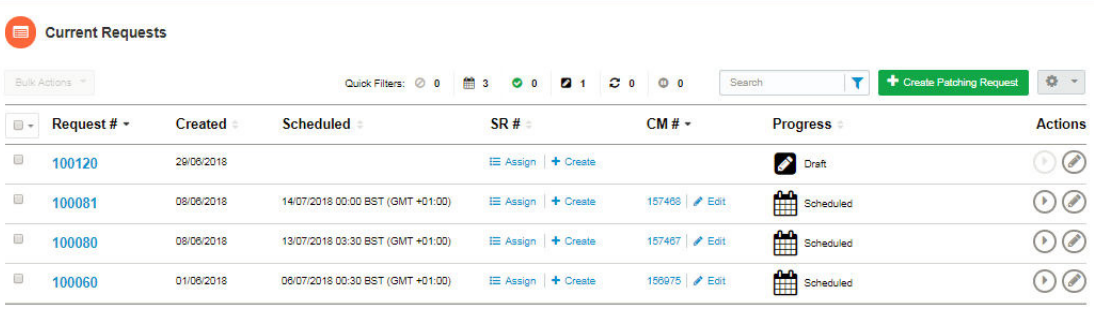
2. From the **My Services** menu, click **All Services**, and then select a service, for example, **Platinum**.

   The Platinum Service page appears.

3. Click **Patch Requests**.

   The Current Requests page appears.

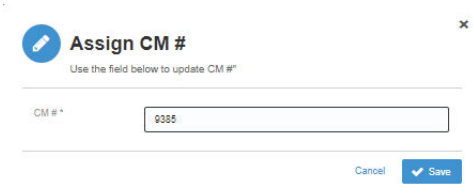
Figure 10–21 Viewing Patching Requests



4. For a request for which an SR has already been created, for example, the request numbered *10081*, under the CM# column, click **Edit**.

   An Assign CM# dialog box appears.

Figure 10–22 Assigning the Patching Request CM Number



5. In the **CM #** field**,** assign a new CM number to be associated with the patch**.**
6. Click **Save**.

Related Information

Creating an SR for a Patching Request

Assigning an SR for a Patching Request

Canceling a Patching Request

Assigning an SR for a Patching Request

You can assign a new SR number to be associated with a patching request.

To assign an SR number to a patch request:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

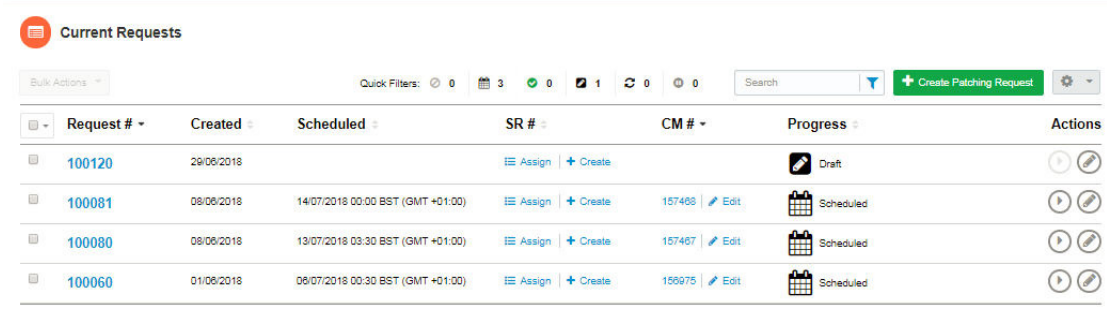
2. From the **My Services** menu, click **All Services**, and then select a service, for example, **Platinum**.

   The Platinum Service page appears.

3. Click **Patch Requests**.

   The Current Requests page appears.

Figure 10–23 Viewing Patching Requests



4. For a patching request, under the SR column, click **Assign**.

   An Assign SR# dialog box appears.

Figure 10–24 Assigning the Patching Request SR Number

5. In the **SR #** field**,** assign a new SR number to be associated with the patch**.**
6. Click **Save**.

   An email is sent to the Gateway user associated with the SR creation specifying:

   - The new SR number (from which you can link to the SR on MOS directly);
   - The hostname;
   - The CSI of the Engineered System that has been scheduled for application of the patch;
   - Links to documentation relating to Oracle Auto Service Request (ASR);
   - Translations of the email in Chinese, Japanese, and Korean.

Related Information

Creating an SR for a Patching Request

Canceling a Patching Request

Canceling a Patching Request

To cancel a patching request:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

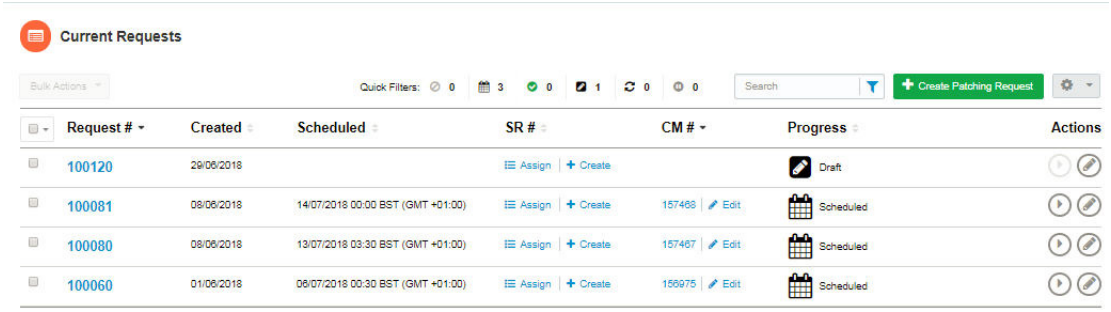
2. From the **My Services** menu, click **All Services**, and then select a service, for example, **Platinum**.

   The Platinum Service page appears.

3. Click **Patch Requests**.

   The Current Requests page appears.

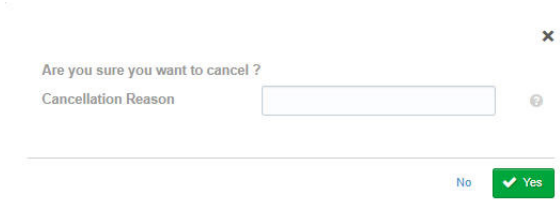
Figure 10–25 Viewing Patching Requests



4. For a request for which an SR has already been created, for example, the request numbered *10080*, under the Actions column, click the icon signifying **Cancel**.

   A cancellation request dialog box appears.

Figure 10–26 Confirming the Cancellation of a Patching Request



5. In the **Cancellation Reason** field**,** enter a justification for canceling the patching request.
6. Click **Yes**.

   The Current Requests table is refreshed and the patching request status changes to Canceled in the Progress column.

Related Information

Creating an SR for a Patching Request

Editing the CM for a Patching Request

Editing a Patching Request

To edit a patching request:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **My Services** menu, click **All Services**, and then select, a service, for example, **Platinum**.

   The Platinum Service page appears.

3. Click **Patch Requests**.

   The Current Requests page appears.

4. In the Actions column, click the icon signifying **Edit**.

   The Prerequisites to Create a Patching Request informational message appears.

5. Follow the steps listed in "Creating a Patching Request" and edit the details as required.

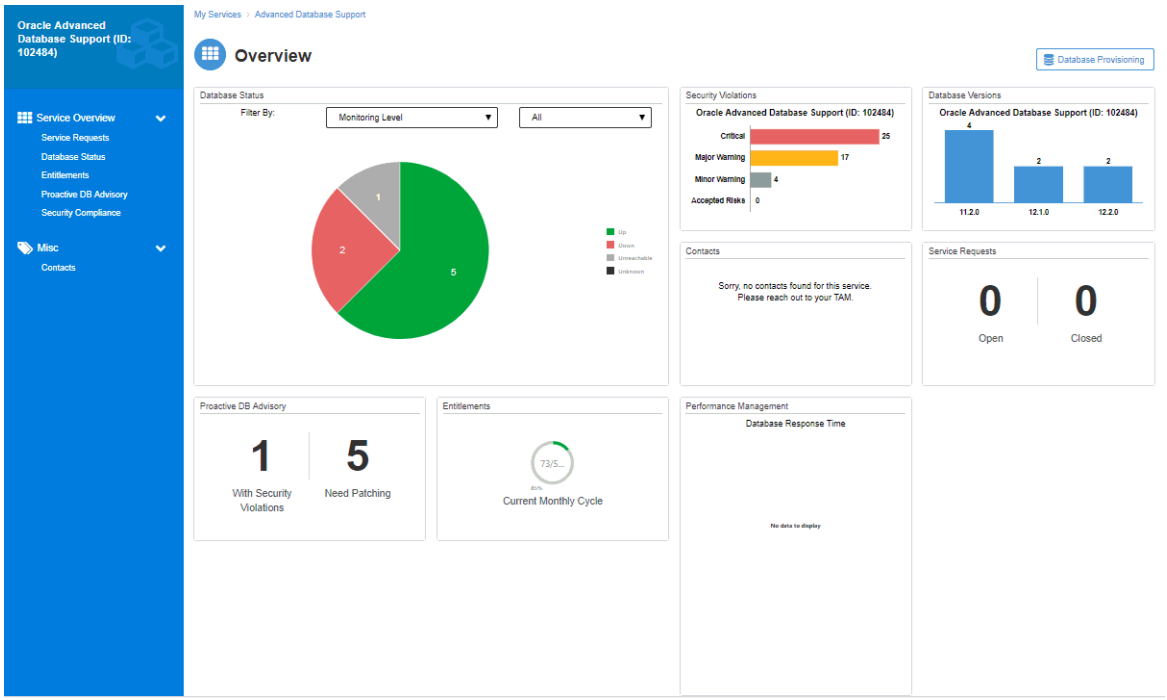
Related Information

Creating a Patching Request

Managing Advanced Database Support (ADS) Targets

This section outlines the unique Advanced Database Support (ADS) service user interface as shown in Figure 10–27, "Viewing the Oracle Advanced Database Support (ADS) User Interface"and provides information on how to manage targets on the ADS service.

Figure 10–27 Viewing the Oracle Advanced Database Support (ADS) User Interface



The Service Overview menu provides a number of database configuration options:

- **Service Requests**: See Chapter 9, "Managing Service Requests."
- **Database Status**: Displays all discovered databases for this service instance. Among the actions you can perform are: activating a new service (see Chapter 7, "Activating Services,"), creating a database blackout (see Chapter 11, "Scheduling Database Blackouts,"), or configuring the monitoring options (see "Editing the Monitoring Configuration.")
- **Entitlements**: See Chapter 12, "Managing Database Entitlements."
- **Proactive DB Advisory**: See "About the Proactive DB Advisory."
- **Security Compliance**: See "Marking Security Violations as Accepted Risks."

Managing Database Patch Compliance

Customers can view the compliance summary for Oracle Engineered Systems activated under Oracle Platinum Service. Compliance is determined by comparing the installed patchset version with the value of the Oracle Advanced Support Gateway setting: *Patch Set Compliance Level*.

Refer to the following sections:

- "Setting the Database Patchset Compliance Level"
- "Viewing the Database Patchset Compliance Widget"

Setting the Database Patchset Compliance Level

You can set the patch set compliance level for your service, for example, for supported Oracle Engineered Systems activated under Oracle Platinum Service.

The Compliance Level setting indicates whether the installed Patch Set version is within the compliance levels as per your patch policy. You can set the compliance level on a database instance. Changing this setting will affect all the targets.

So, for example, if you select the value of the Patch Set Compliance Level setting as *Latest -1*, if the latest Quarterly Full Stack Download Patch (QFSDP) available is Jan 2018 - any engineered system with a QFSDP before Oct 2017 will be considered as “Non-Compliant”.

For Oracle Advanced Database Support (ADS), you set the compliance level when activating the service. See "Activating Services."

To set the database patchset compliance level:

1. Log in to Oracle Advanced Support Gateway.

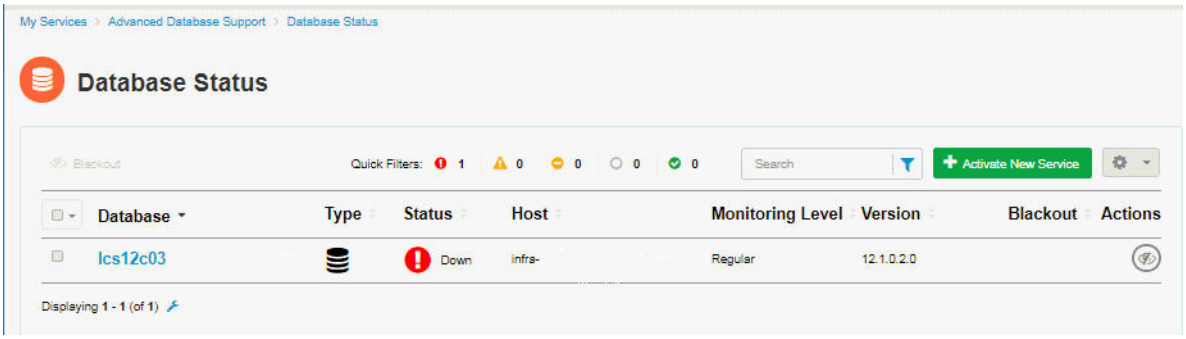
   The Oracle Advanced Support Gateway Home page appears.

2. From the **My Services** page, select the required service.

   The service home page appears, displaying various database tabs.

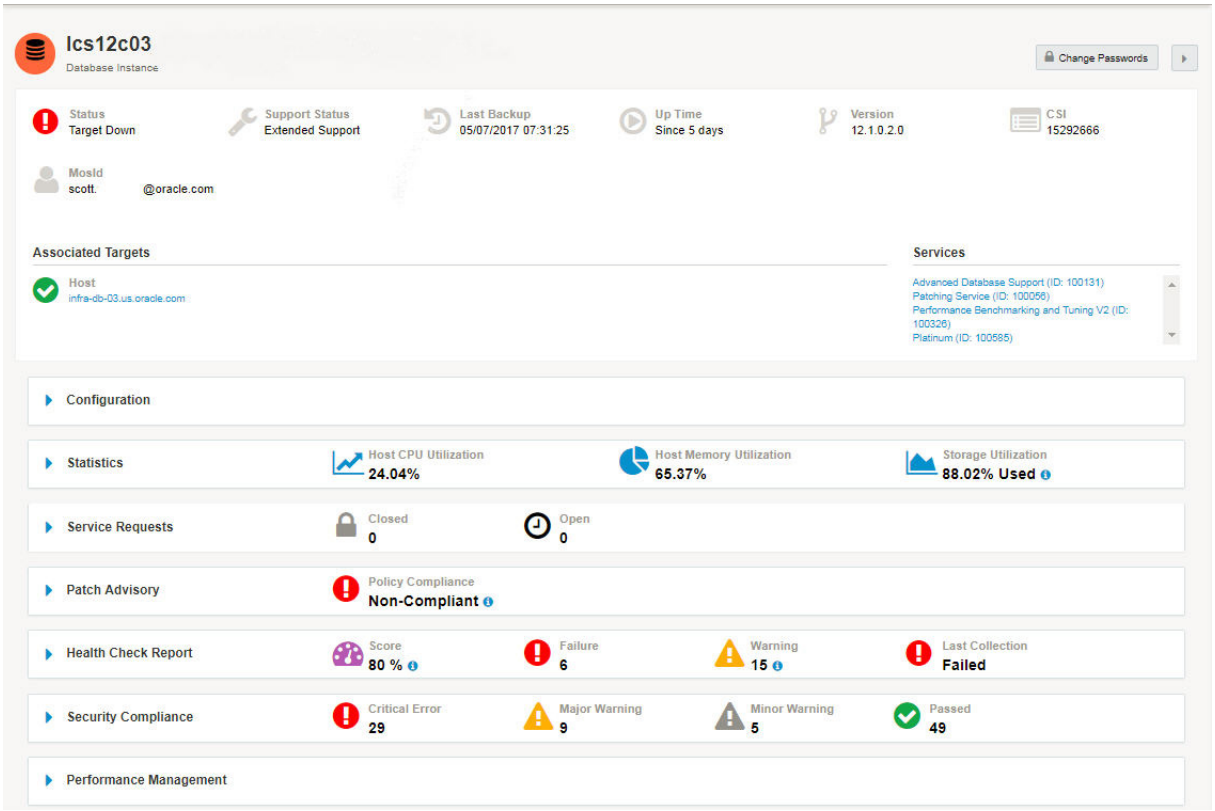
3. Select the **Database Status** badge to display your discovered databases in the Database Status table.

Figure 10–28 Viewing Database Status



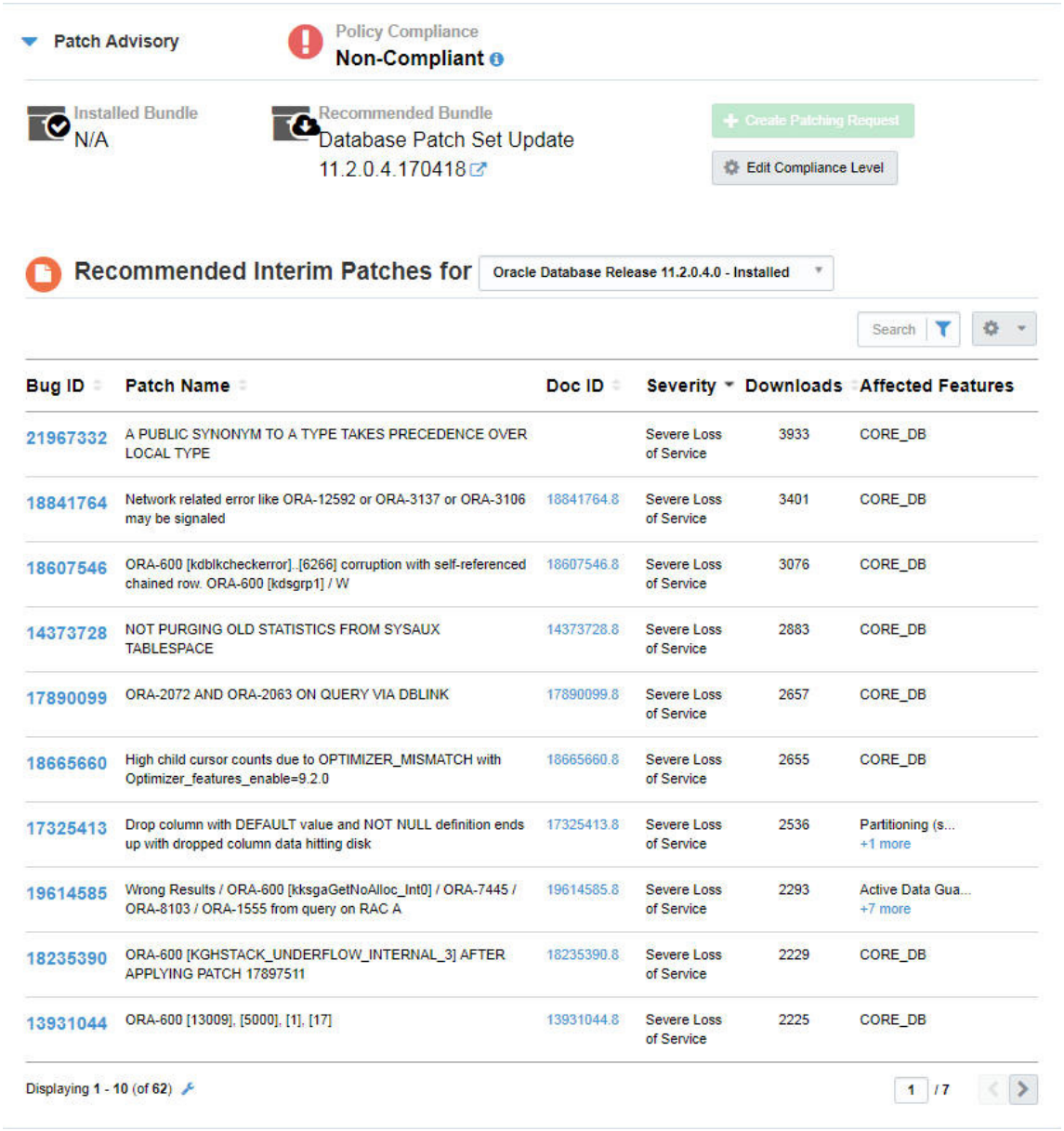
4. Select a database instance to display the database configuration.

Figure 10–29 Displaying the Database Configuration



5. Expand the **Patch Advisory** section.

Figure 10–30 Viewing the Patch Advisory Details



6. Click **Edit Compliance Level.**

   The Patch Policy Settings dialog box appears. The Compliance Level setting indicates whether the installed Patch Set version is within the compliance levels as per your patch policy.

   Select the required compliance level to set across the targets. Changing this setting will affect all the targets. The options are:

   - *Latest*
   - *Latest - 1*
   - *Latest - 2*
   - *Latest - 3*

   The default is *Latest-2* and is part of the initial reference schema of the Gateway.

7. Click **Save** to confirm.

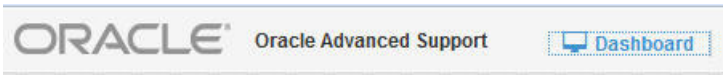
Viewing the Database Patchset Compliance Widget

On the Oracle Advanced Support Gateway service dashboard, there is a data window called a widget that displays the database patchset compliance summary for Oracle Engineered Systems activated under the Platinum Service.

To use Oracle Advanced Support Gateway to view the Patch Compliance widget:

1. Log on to the Oracle Advanced Support Gateway portal.
2. From the top level menu, select **Dashboard,** or its associated icon, as highlighted in Figure 10–31.

Figure 10–31 Accessing the Dashboard



A dashboard comprised of widgets appears.

3. Select the Patch Compliance widget, as shown in Figure 10–32.

Figure 10–32 Patch Compliance Widget

The compliance takes the form of a bar chart showing the counts of systems that are compliant and non-compliant.

Related Information

Setting the Database Patchset Compliance Level

Using Proactive Patch Recommendations for ADS

Oracle Advanced Database Support (ADS) customers are offered a patch advisory on supported databases that displays patch policy compliance, installed patch bundles, and recommended patches, among other database patch information.

On Oracle Advanced Support Platform, the patch inventory enables Oracle Support engineers to view bundle patches, as well as add interim patches. All patch updates are synchronized from Oracle Advanced Support Platform to the Gateway.

The proactive patch recommendation are typically bundled patches like Database Patch Set Updates (DBPSU) and interim patches that are personalized for each database. The list of patch recommendations for each database is generated by Oracle Enterprise Manager (OEM) through its integration with Oracle Support.

For each customer that avails of the proactive patch recommendation feature, the patch inventory maintained on the Oracle Advanced Support Portal is synchronized to the Oracle

Advanced Support Gateway on a regular basis. Each patch recommendation is curated based on Oracle Support knowledge and best practice and is based on:

- The database version as well as the currently installed PSUs and interim patches
- The database features used by the customer

Note: Integration of OEM and Oracle Support requires customers to log on to Oracle Advanced Support Gateway using their My Oracle Support (MOS) credentials. Ensure that you use your MOS login to avail of the proactive patch recommendation feature.

Customers can also create a patching request using the **Proactive Advisory** page.

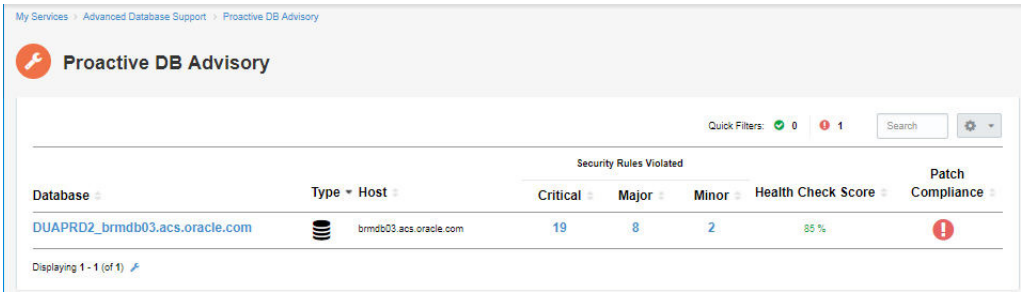
Refer to the following:

- About the Proactive DB Advisory
- Viewing Database Details: Proactive Recommendations
- Creating a Patching Request from the Proactive Advisory Page
- Marking Security Violations as Accepted Risks

About the Proactive DB Advisory

After activating databases (see Chapter 10, "Managing Databases and Database Patches"), you can select the **Proactive DB Advisory** badge to display a table of patches required for a monitored database instance or a RAC database. See Figure 10–33.

Figure 10–33 Proactive Database Advisory



Patch compliance is determined by whether the installed bundle patch is within the range defined by the “Desired Compliance Level” setting on the Gateway. See "Managing Database Patch Compliance."

In Figure 10–33, the database displays the non-complaint patch indicator in the **Patch Compliance** column. This signifies that the database has patch bundles installed that are not compliant.

If you drill down on the database, you can view the proactive patch recommendations for that database.

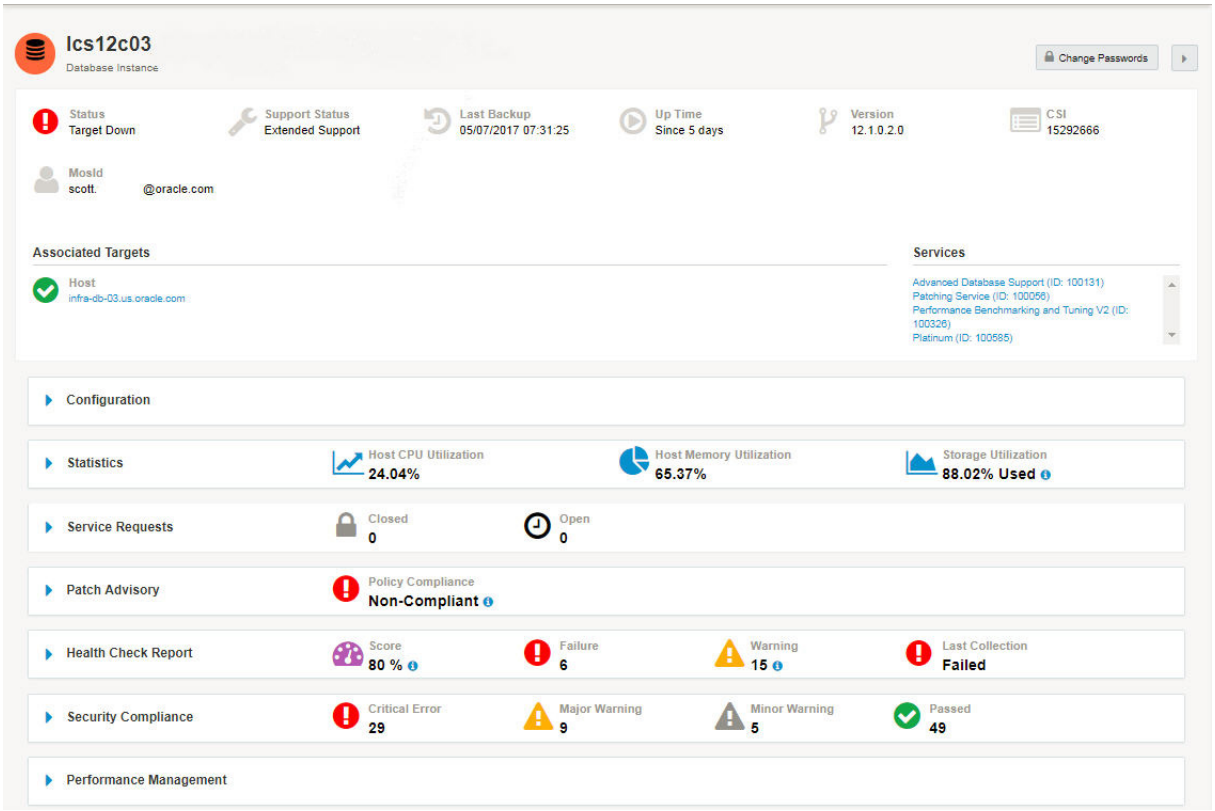
Viewing Database Details: Proactive Recommendations

To view the proactive patch recommendations for a non-compliant database:

1. From the **Proactive Advisory** page, select the required database.

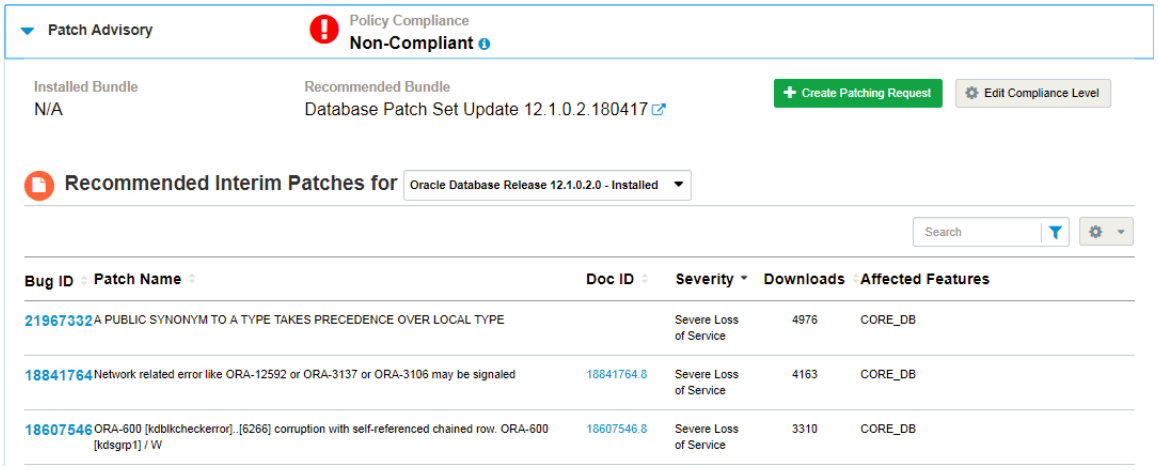
   The database instance page appears, displaying a series of panels showing database information such as service requests, patches applied, and utilization data for the target.

Figure 10–34 Database Instance Displaying Proactive Patch Recommendations



2. Expand the **Patch Advisory** panel.

Figure 10–35 Patch Advisory Panel Showing Patch Recommendations



3. Review the contents of the **Patch Advisory** panel.

   The panel displays the currently installed bundle (if applicable) as well as the Policy Compliance indicator.

   Patch recommendations are displayed in a separate section. The recommended bundle patch is defined by:

   - **Bug ID**: The marker bug for the applicable Database Patch Set Update (PSU)

- **Patch Name**: Name of the PSU, for example: Database Patch Set Update 11.2.0.4.0
- **Doc ID**: Consists of a link to the MOS marker bug document for the patch. This document provides an outline of the patch contents, a link to download the PSU from MOS, as well as general information about Patch Set Updates, known issues, and so on.
- **Severity**: Indicates how the patch installation affects the service, for example, *Severe Loss of Service* or *Complete Loss of Service*.
- Number of downloads: Shows the number of times the patch has been downloaded.
- Affected Features: Shows the features impacted by the patch, for example, CORE_ DB, OJVM (system), OJVM (user.)

Applying the Patch Set Update

To apply the patch set update for the non-compliant database:

1. Drill down to the **Recommended Patches** section of the Patch Advisory panel of the database instance page as outlined in "Viewing Database Details: Proactive Recommendations."
2. Click the link displayed in the **Doc ID** column to display the relevant Knowledge Base article on My Oracle Support (MOS).
3. In the Description section of the article, click the link to download the relevant patch.

   A Patch Details page appears under the Patches & Updates tab.
4. On the right side of the page, select your platform, click **Download**, and follow the instructions to complete database patching.

Creating a Patching Request from the Proactive Advisory Page

You can also create a patching request from the Proactive DB Advisory page:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.
2. From the **My Services** menu, click **All Services**, and then select **ADS**.

   The ADS page appears.
3. Click the **Proactive DB Advisory** badge.

   The **Proactive Advisory** page appears. See Figure 10–33.
4. Click **Create Patching Request**.
5. Complete the parameters outlined in "Creating a Patching Request":
6. When the configuration is completed, click **Confirm Request**.

   The Patching Request: Submitted page appears.

   This page confirms the successful submission of the patching request and provides the Patching Request number.

   The page lists the database or target machine name and patch number. It specifies the components to be patched.

   Furthermore, the page specifies the estimated duration and outage window associated with the patching process, the period during which it is likely to take place, the start time, the nature of the patch process, whether rolling or non-rolling, whether the patch applies to a Production environment, and so on.

Finally, the applicable Oracle Homes, Grid Homes (if applicable), and databases are listed.

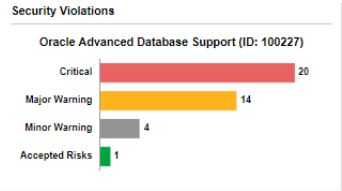
7. As the patching request has been created successfully, click **Continue to Current Request**s to review the list of current patching requests.

Marking Security Violations as Accepted Risks

Note: This feature applies only to Oracle Advanced Database Support (ADS.)

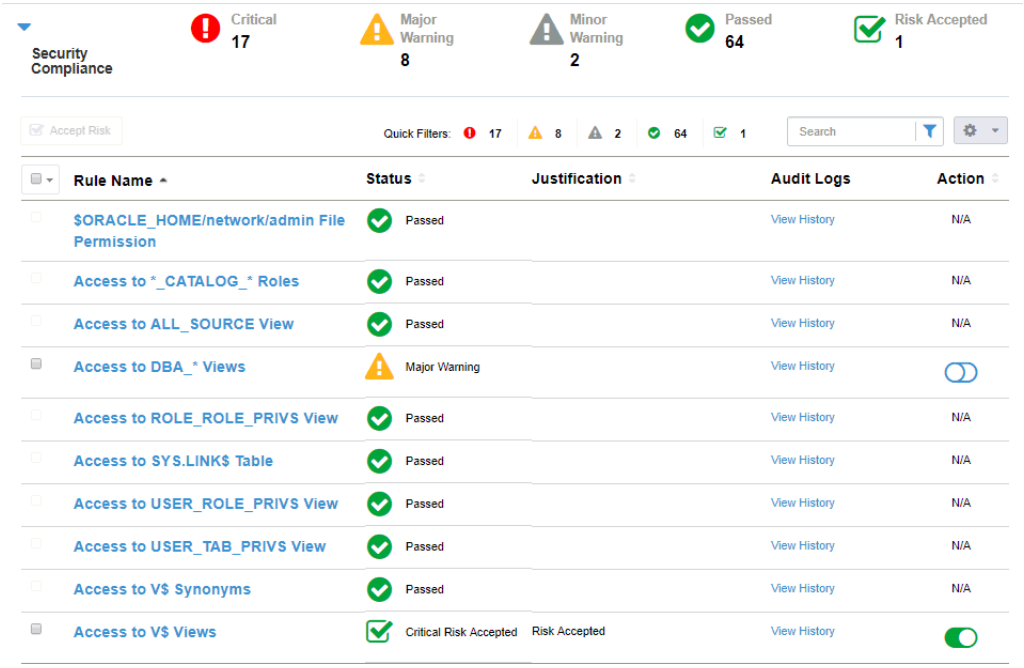
On the ADS service home page, the Security Violations widget lists critical, major, and minor security violations, and also includes the accepted risks explicitly added by the ADS service customer user. See:

Figure 10–36 Viewing the Security Violations Widget



On the database details page a toggle is provided for each database so that users can select one or more rules that the current database is violating and mark it as an accepted risk. On marking rules as an accepted risk, users can add a justification for the decision. See the following database Security Compliance panel:

Figure 10–37 Viewing the Database Security Compliance Panel



The *Access to DBA_* Views* rule above displays a Major Warning status. To accept the risk:

1. In the Action column, select the toggle.

   The Accept Risk for Security Rule dialog box appears.

2. (Optional) Enter a justification for risk acceptance as shown:

Figure 10–38 Accepting a Risk for a Security Rule

3. Click **Accept Risk**.

   The Status changes to Risk Accepted (see the Access to V$ Views rule status, for example), and the Security Compliance panel is updated with the correct count for accepted risks. In addition, the widget that displays security compliance on the ADS home page incorporates this count.

11

Scheduling Database Blackouts

This chapter provides information about using Oracle Advanced Support Gateway to manage database blackouts.

Note: Database blackouts can be scheduled only on databases running on the Oracle Advanced Database Support (ADS) service.

It includes the following topics:

- About Database Blackouts
- Creating Database Blackouts
- Managing Database Blackouts

About Database Blackouts

Blackouts allow Oracle Advanced Support Gateway users and administrators to suspend monitoring of databases for a specified time. If a fault is detected for the database under blackout during this scheduled period, no SR is generated.

A blackout can be defined for an individual database, a group of multiple databases that reside on different hosts (as in a RAC configuration, for example), or for all targets on a host. The blackout can be scheduled to run immediately or in the future, and to run indefinitely or stop after a specific duration. Blackouts can be created on an as-needed basis, or scheduled to run at regular intervals. If, during the maintenance period, the Oracle Advanced Support Gateway administrator discovers that he needs more (or less) time to complete his maintenance tasks, he can easily extend (or stop) the blackout that is currently in effect.

Creating Database Blackouts

You can use Oracle Advanced Support Gateway to create blackouts both for single database instances and for a clustered database. You can set either single or recurring blackouts.

To create a blackout using the Admin screen:

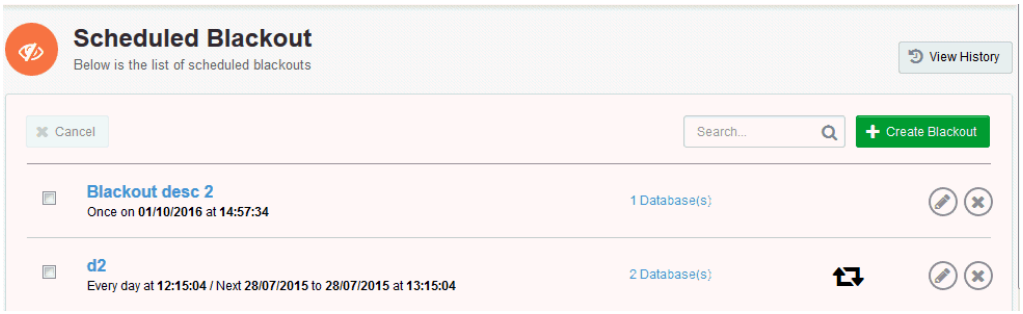
1. Log on to the Oracle Advanced Support Gateway portal.

   The Oracle Advanced Support Gateway screen appears.

2. Under Admin, select **Scheduled Blackouts**.

   The Scheduled Blackouts screen appears.

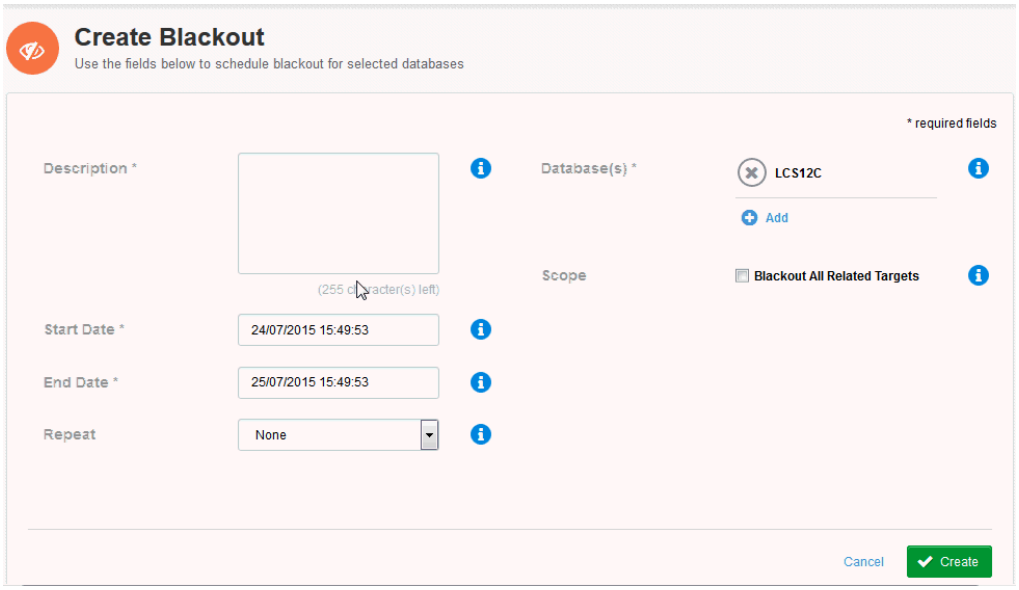
Figure 11–1 Scheduled Blackouts Page



3. Click **Create Blackout**.

   The Create Blackout screen appears.

Figure 11–2 Create Blackout Screen



   a. In the **Description** field, enter a name and a description.

   b. In the **Start Date** field, specify a date and time for the start of the blackout period.

   c. In the **End Date** field, specify a date and time for the end of the blackout period.

   d. (Optional) From the **Repeat** list, select an interval for the blackout to execute. The recurrence values are **Daily**, **Weekly**, **Monthly**. The default is **None**.

   e. In the **Databases** field, select database targets to add to the blackout list.

      (Optional) Click **Add** to choose other targets from the **Select Databases** page.

   f. (Optional) In the **Scope** field, select the **Blackout All Related Targets** check box to enable all related targets for blackout.

   g. Click **Create**.

      After creating the blackout, you can manage it by, for example, editing the recurrence interval, changing the end date, or by adding further databases to be used in the blackout schedule.

See "Managing Database Blackouts" for more information about editing scheduled blackouts.

Managing Database Blackouts

You can use Oracle Advanced Support Gateway to view a list of scheduled and completed database blackouts. You can edit existing blackouts, create or extend an existing blackout, or cancel a scheduled blackout.

This section consists of the following topics:

- Viewing Scheduled Blackouts
- Viewing Completed Blackouts
- Editing Blackouts
- Canceling Blackouts

Viewing Scheduled Blackouts

You can use Oracle Advanced Support Gateway to view your scheduled database blackouts.

To use Oracle Advanced Support Gateway to view a blackout:

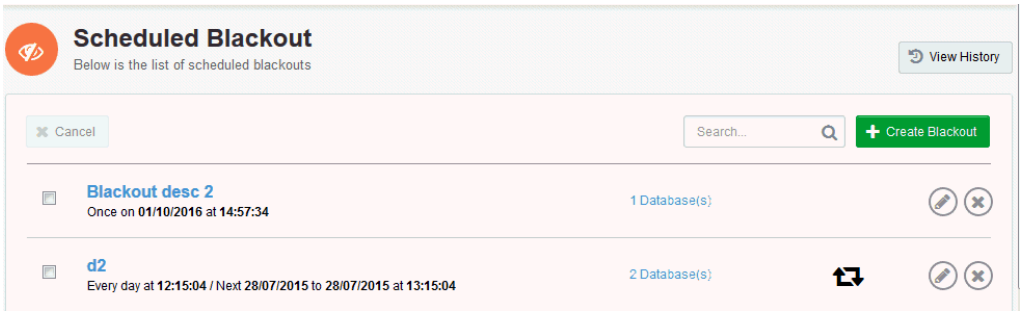
1. Log on to the Oracle Advanced Support Gateway portal.

   The dashboard screen appears.

2. From the top-level **Admin** menu, select **Scheduled Blackouts**.

   The Scheduled Blackout page appears.

Figure 11–3 Scheduled Blackout Page



From the list of blackouts, you can search for a particular blackout instance, create a new blackout, edit or cancel an existing blackout, and so on.

Viewing Completed Blackouts

You can use Oracle Advanced Support Gateway to view your database blackout history.

To use Oracle Advanced Support Gateway to view a completed blackout:

1. Log on to the Oracle Advanced Support Gateway portal.

   The dashboard screen appears.

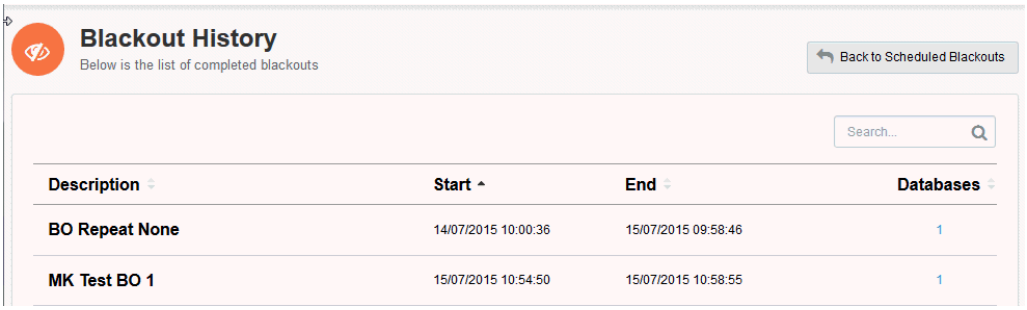
2. From the top-level **Admin** menu, select **Scheduled Blackouts**.

   The Scheduled Blackouts page appears.

3. Click **View History**.

   The Completed Blackouts page appears.

Figure 11–4 Completed Blackouts Page



From the list of completed blackouts, you can search for a particular blackout instance, review the dates between which a blackout occurred, and view the affected databases.

Editing Blackouts

You can use Oracle Advanced Support Gateway to edit an existing database blackout.

To use Oracle Advanced Support Gateway to edit a blackout:

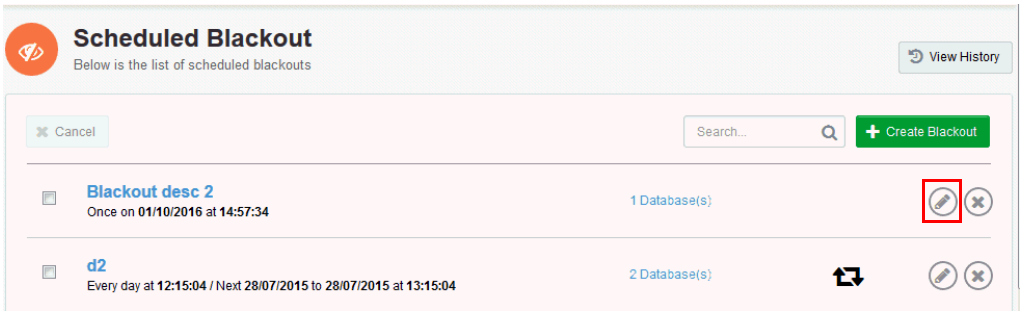
1. Log on to the Oracle Advanced Support Gateway portal.

   The dashboard screen appears.

2. From the top-level **Admin** menu, select **Scheduled Blackouts**.

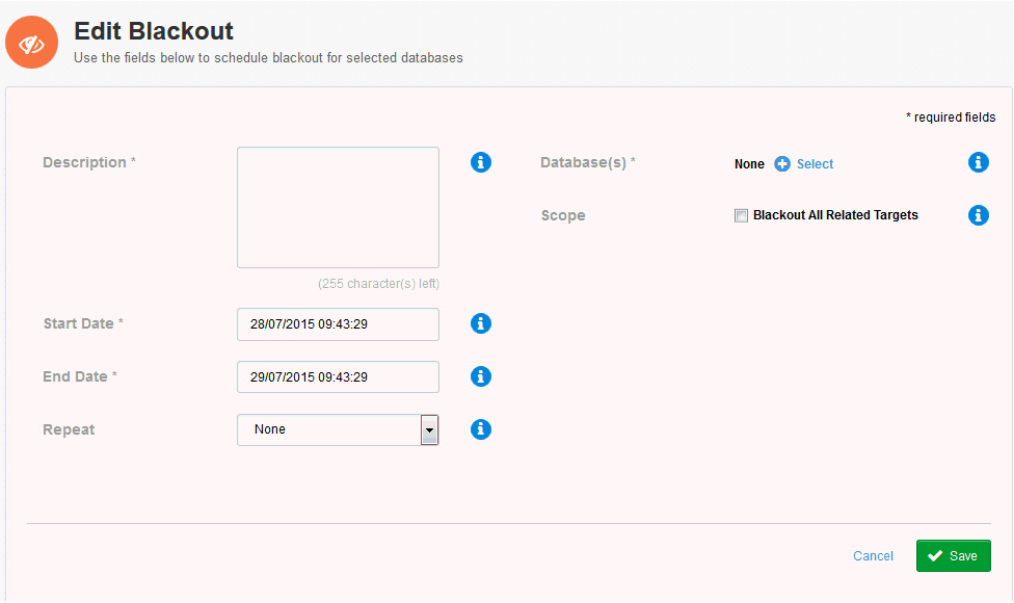
3. For the selected database, click the **Edit** icon as highlighted in Figure 11–5.

Figure 11–5 Editing a Blackout



The Edit Blackout screen appears.

Figure 11–6 Edit Blackout Screen



a. In the **Description** field, enter a name and a description.

b. In the **Start Date** field, specify a date and time for the start of the blackout period.

c. In the **End Date** field, specify a date and time for the end of the blackout period.

d. (Optional) From the **Repeat** list, select an interval for the blackout to execute. The recurrence values are **Daily**, **Weekly**, **Monthly**. The default is **None**.

e. (Optional) Click **Select** to choose other targets from the **Select Databases** page.

f. (Optional) In the **Scope** field, select the **Blackout All Related Targets** check box to enable all related targets for blackout.

g. Click **Save**.

Canceling Blackouts

To cancel a blackout:

1. Log on to the Oracle Advanced Support Gateway portal.

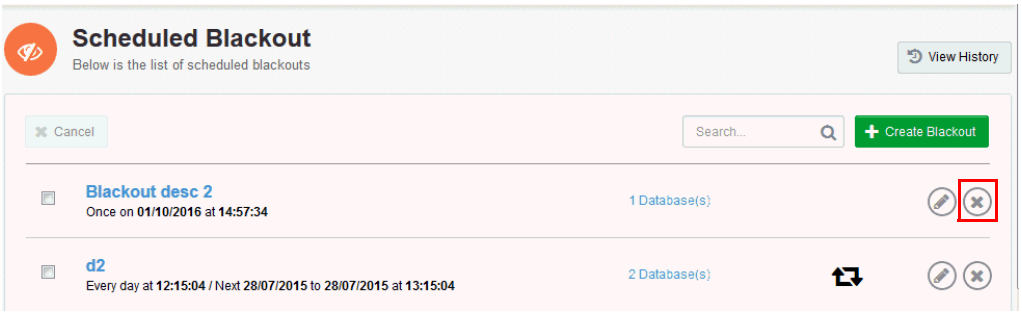
   The dashboard screen appears.

2. From the top-level **Admin** menu, select **Scheduled Blackouts**.

   The Scheduled Blackouts page appears.

3. For the selected database, click the **Cancel** icon as highlighted in Figure 11–7.

Figure 11–7 Canceling a Blackout



A warning message appears asking you to confirm that you wish to cancel the blackout.

4. Click **Yes** to confirm.

12

Managing Database Entitlements

This chapter provides information about managing the Oracle Advanced Support Gateway database entitlements.

Note: This chapter applies only to the Advanced Database Support service (ADS) and to the Patching Service.

This chapter consists of the following sections:

- About Database Entitlements
- About the High Water Mark
- Viewing Database Entitlements

About Database Entitlements

Users and administrators can choose to enable Oracle Advanced Support Gateway on databases at their customer facilities once they ensure they are within the entitled usage limit (measured in database cores per month). Any usage beyond the entitlement limit for the month is then charged separately.

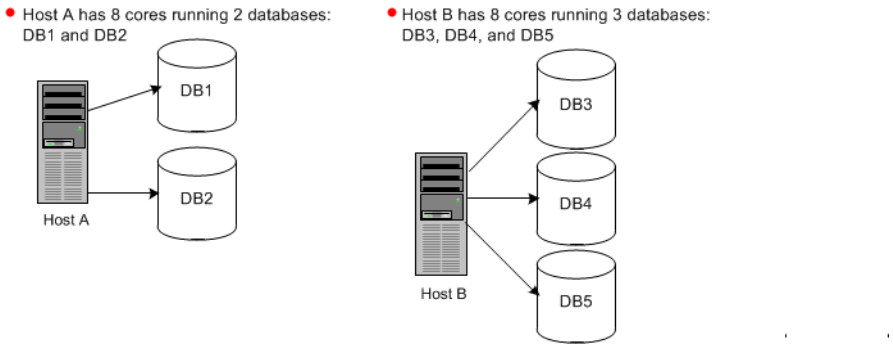
The rules for fair entitlement usage for Oracle Advanced Support Gateway are as follows:

- Entitlement usage is based on the number of hardware cores on which databases are running, and is billed on a monthly basis, for example, 60 cores per month.
- Entitlement is based on a “use it or lose it” model, that is, there is no carry forward of entitlement from month to month.
- Entitlement usage is governed by the High Water Mark. See "About the High Water Mark".
- Entitlement usage metrics are sent to Oracle Advanced Support Platform at regular intervals for consolidated entitlement reporting.
- Oracle Advanced Support Portal synchronizes usage across multiple Gateways in accordance with the customer contract.
- There is no limit on the number of databases running on a single piece of hardware.

About the High Water Mark

Monthly fair entitlement usage is governed by the “High Water Mark”. To better understand the concept of the high water mark and how it applies to entitlement usage, consider the following example for a customer user with an entitlement of 60 cores, as displayed in Figure 12–1.

Figure 12–1 High Water Mark Example



The customer user network is configured as follows:

- Host A has 8 cores running two databases: *DB1* and *DB2*
- Host B has 8 cores running three databases: *DB3*, *DB4*, and *DB5*

The customer user's usage pattern for August is as follows:

1. On August 1, the user activates *DB1*, *DB3*, and *DB5*. The usage is then calculated on a per-core basis across both hosts as follows:

   8 (*DB1*) + 8 (*DB3*, *DB5*) = 16

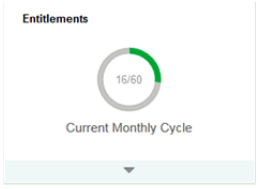
2. On August 5, *DB2* is activated. As a database (*DB1*) on Host A is already activated, no further usage is added.

   Usage remains at 16 (cores).

3. On August 12, *DB3* and *DB5* are deactivated. As both databases are on Host B, and no other database on this host is active, the usage for the day is reduced by 8.

   The usage for the day is now 8 (from Host A). However, as the usage for the month to date has already reached 16 (the current high water mark), the entitlement continues to be displayed as 16/60. See Figure 12–2.

Figure 12–2 Entitlements Example

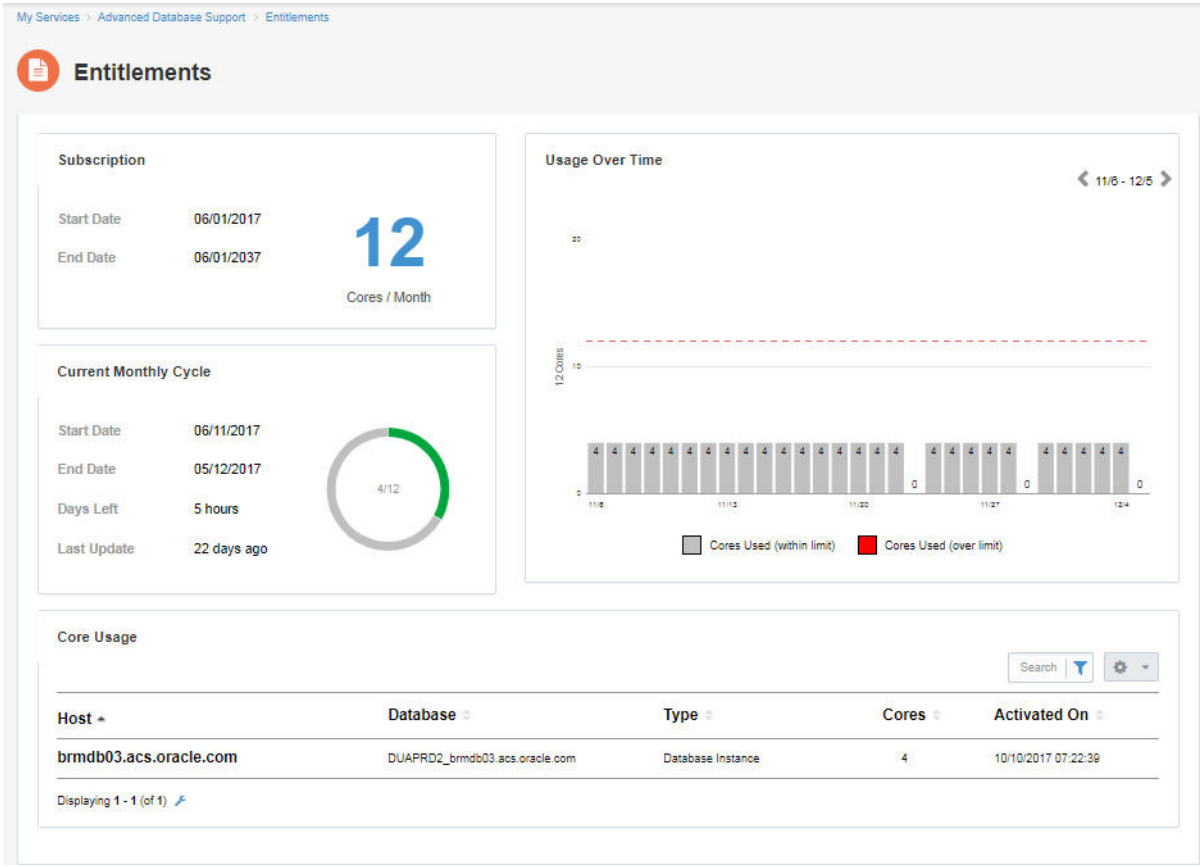


4. Over the remainder of August, the customer user can add further hardware to reach the maximum core usage of 60. However, even if core usage never exceeds the current high water mark of 16, billing is for 60 cores per month.
5. When the August cycle ends, the current usage on the first day of September becomes the initial high water mark for September.

Viewing Database Entitlements

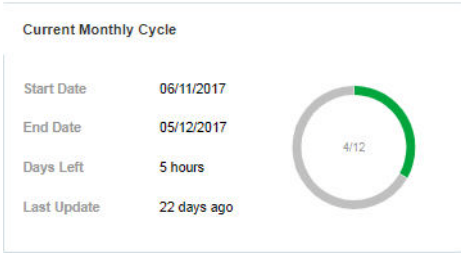
Select the **Entitlements** badge to display your database entitlement contract, based on the core limit for the host database. You can view the current monthly contract cycle in terms of cores used, shown in gray, cores available, shown in green.

Figure 12–3 Viewing Database Entitlements



The sample customer entitlement contract shown is for 12 purchased cores over a one-month duration.

Figure 12–4 Selecting Database Entitlements



You can also view the entitlement usage over time, so that you can determine, for example, the time of month when the demand for cores is highest.

Cores used over the limit are displayed in red.

13

Managing Health Checks

This chapter provides information about managing the Oracle Advanced Support Gateway Health Checks.

This chapter consists of the following sections:

- About Health Checks
- Installing and Configuring the Health Check Report
- Rescheduling the Health Check Report
- Viewing the Health Check Report
- Running the Health Check Report Immediately
- Viewing Health Check History

About Health Checks

You must install the Trace File Analyzer (TFA) tools bundle on all managed hosts on which that you want to run health checks. The TFA tools bundle contains the ORAchk, EXAchk, and Diagnostics Logs tools. ORAchk and EXAchk are lightweight Oracle tools integrated into Oracle Advanced Support Gateway that are used to analyze and collect data on the health of your system infrastructure.

Health Check execution is scheduled to run on the customer system on a weekly basis, although on-demand execution is also possible. The specific health check that is run depends on the type of target: EXAchk is run if an Oracle Engineered System is detected; otherwise ORAchk is used. See:

- About the ORAchk Report
- About the EXAchk Report
- Installing Trace File Analyzer and Scheduling Health Checks

About the ORAchk Report

ORAchk proactively scans for the most impactful customer problems and presents a dashboard of known issues. You can drill down into specific problems on the ORAchk report to understand their resolutions.

About the EXAchk Report

EXAchk is used to perform health checks for Oracle Engineered Systems, for example, the Exadata infrastructure, that is, the compute nodes, switches, storage appliance, and, additionally, the Exadata Control stack in the case of a machine in a virtual configuration.

Installing and Configuring the Health Check Report

In previous releases of Oracle Advanced Support Gateway, Oracle Support field engineers were generally required to perform the manual installation steps required to enable ORAchk, EXAchk, or Diagnostic Logs Collection on the Gateway. Alternatively, Oracle Support field engineers provided guidance to customers who wished to enable health checks.

In this release, you can use a self-service wizard on the Gateway user interface to perform installation of TFA and/or Health Check scheduling, but if you require assistance, please contact the Oracle Support Services contact with whom you have been engaged for review.

Installing Trace File Analyzer and Scheduling Health Checks

Installation of Trace File Analyzer (TFA) and/or Health Check scheduling is part of the overall process of activating services on a host and can be configured on the **Systems and Hosts** page, which you use to manage existing systems and hosts as well as requesting activations of new systems and adding new hosts.

To install the TFA tools bundle and schedule health checks on a host:

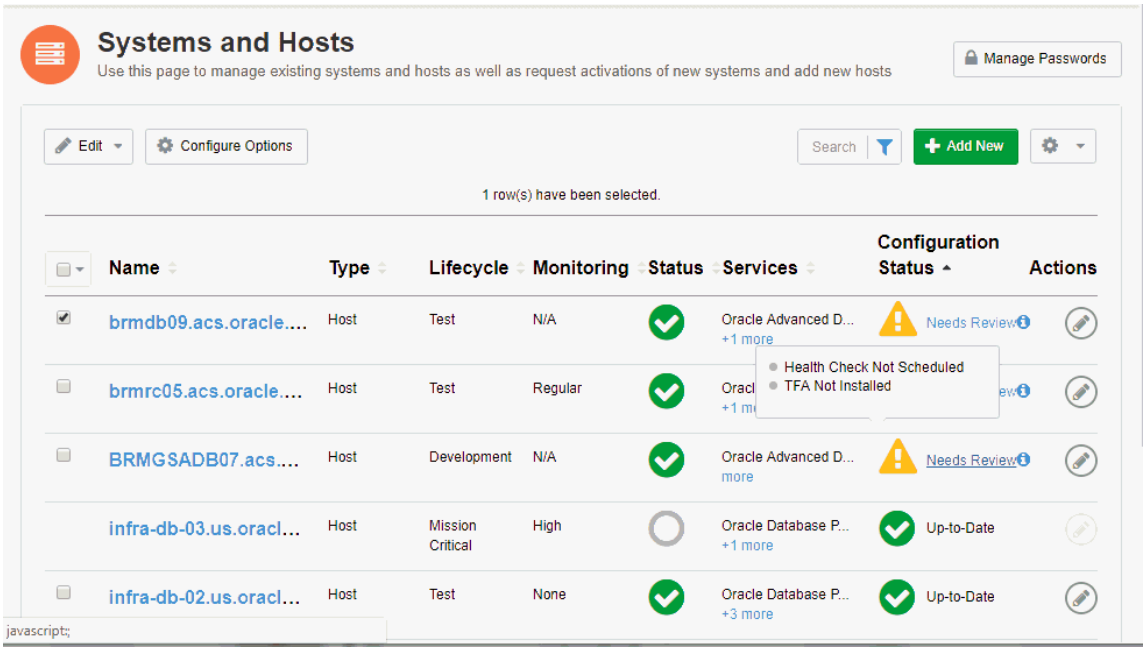
1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Admin** menu, click **Manage Systems**.

   The Systems and Hosts page appears.

Figure 13–1 Viewing the Systems and Hosts Page



3. Select the required target.

   The selected target in Figure 13–1 has a clickable configuration status of *Needs Review*, which means, as shown in the hovertext message, that the host still requires the following configuration steps to be performed:

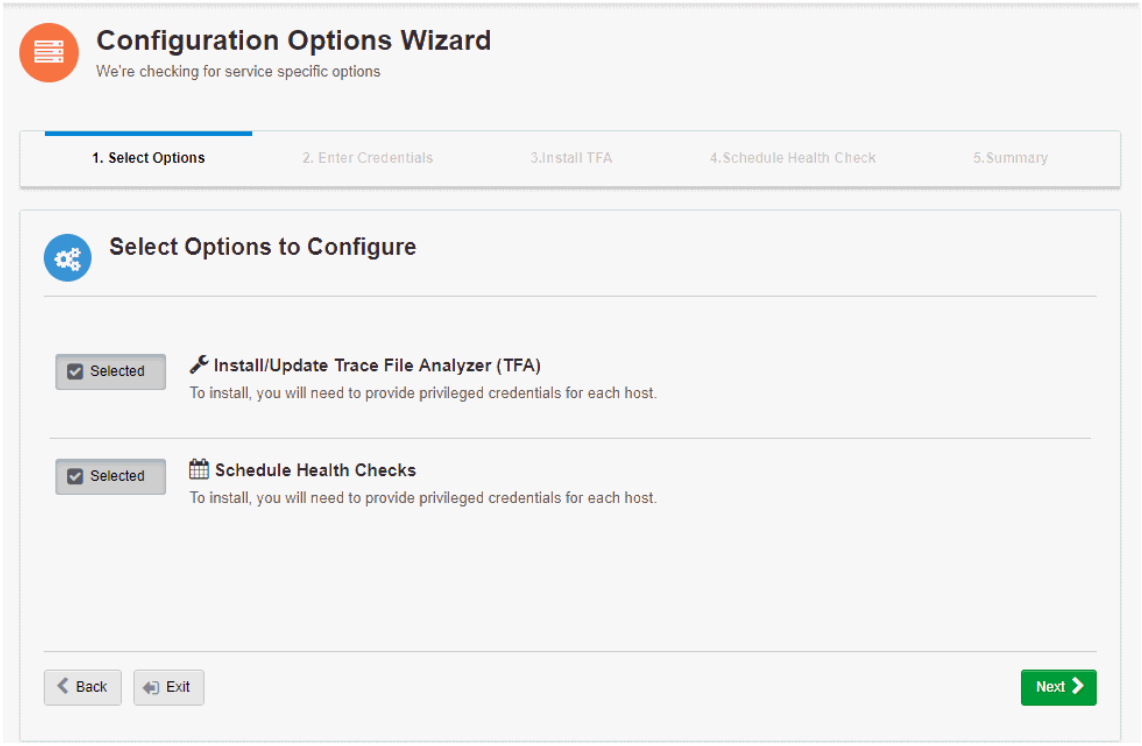
   - Health Check Not Scheduled
   - TFA Not Installed

Note: If a host is in pending or unreachable status, then no configuration of the host is possible, and the *Needs Review* configuration status message cannot be clicked.

4. Click **Needs Review** (or the informational icon beside it).

   The Configuration Options Wizard screen appears.

Figure 13–2 Selecting the Host Configuration Option



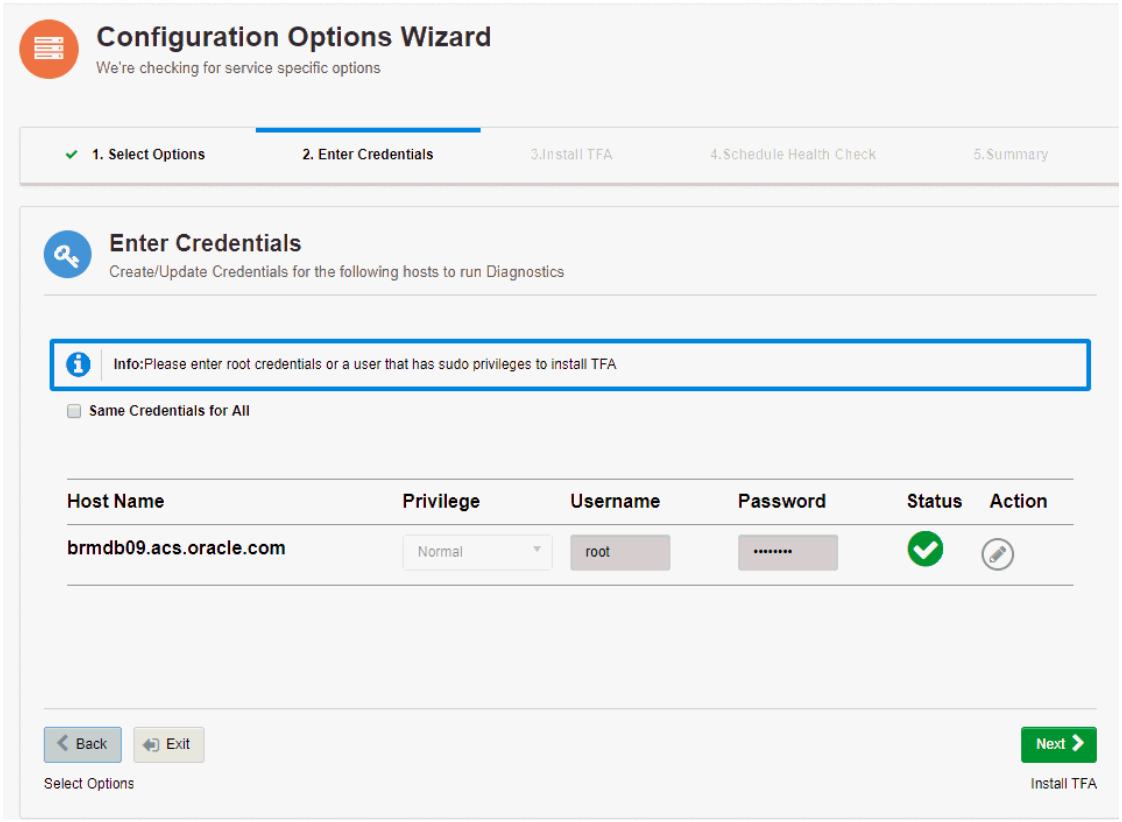
Both configuration options are selected by default:

- Install/Update Trace File Analyzer (TFA)
- Schedule Health Checks

5. Click **Next**.

   The Enter Credentials screen appears.

Figure 13–3 Entering Host Credentials



You use this screen to create or update host credentials enabling them to run diagnostics.

Note: If valid credentials already exist for a host, its status will be shown as green.

6. Complete the following parameters:

   a. (Optional) Select the **Same Credentials for All** check box to apply the same credentials to all selected hosts.

   b. In the **Privilege** field, select the role associated with the user. The options are *Sudo* (the default), *Normal* or *None*.

   c. In the **Username** field, select the name of the user associated with the host.

   d. In the **Password** field, select the password associated with the user.

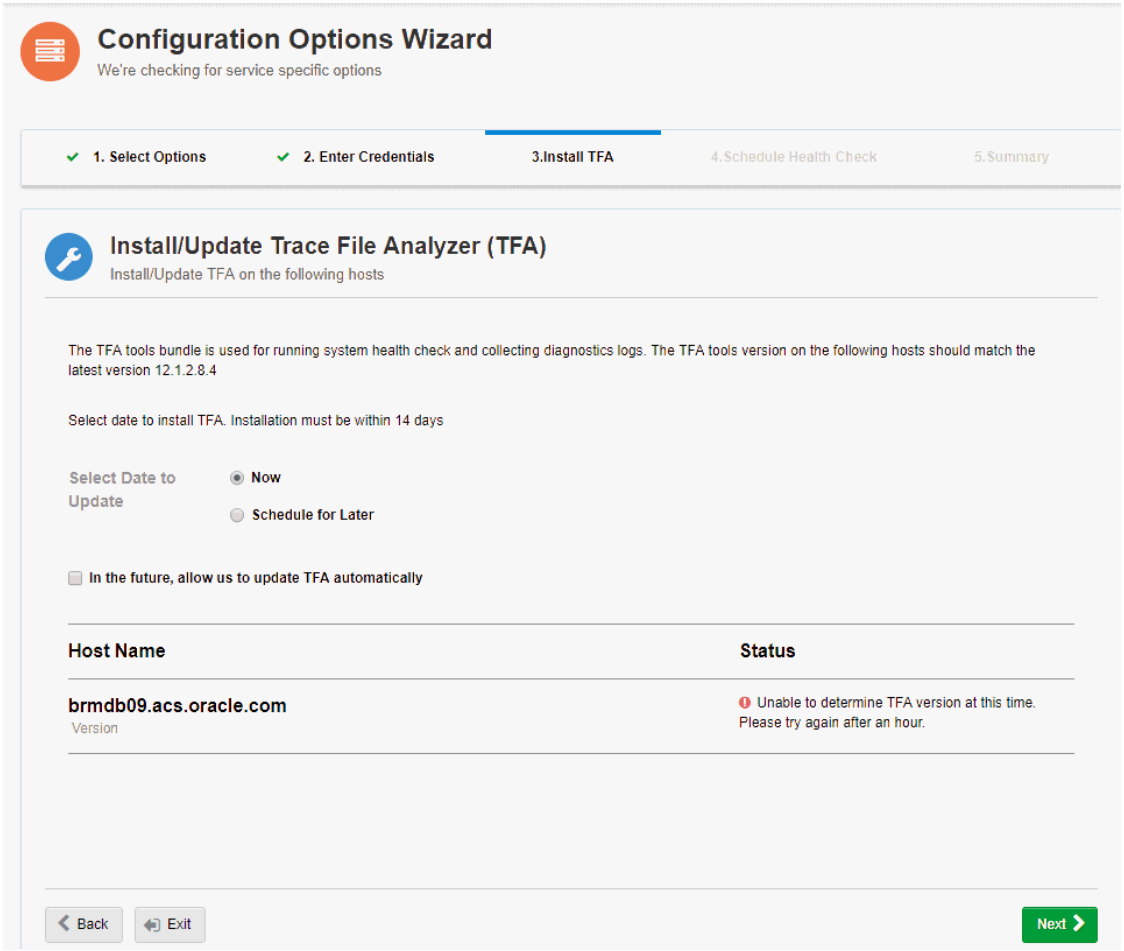
7. Click **Next**.

   The Install TFA screen appears.

   You use this screen to install the TFA tools bundle for running system health checks and collecting diagnostics logs. The TFA tools version on the following hosts should match the latest specified version.

   You can install TFA immediately or schedule the installation within the next two weeks.

Figure 13–4 Installing TFA



8. Complete the following parameters:

   a. In the **Select Date to Update** field, select when to install. The options are *Now* (the default) or *Schedule for Later*.

      Note: If you select **Schedule for Later**, you must select a date within the next 14 days.

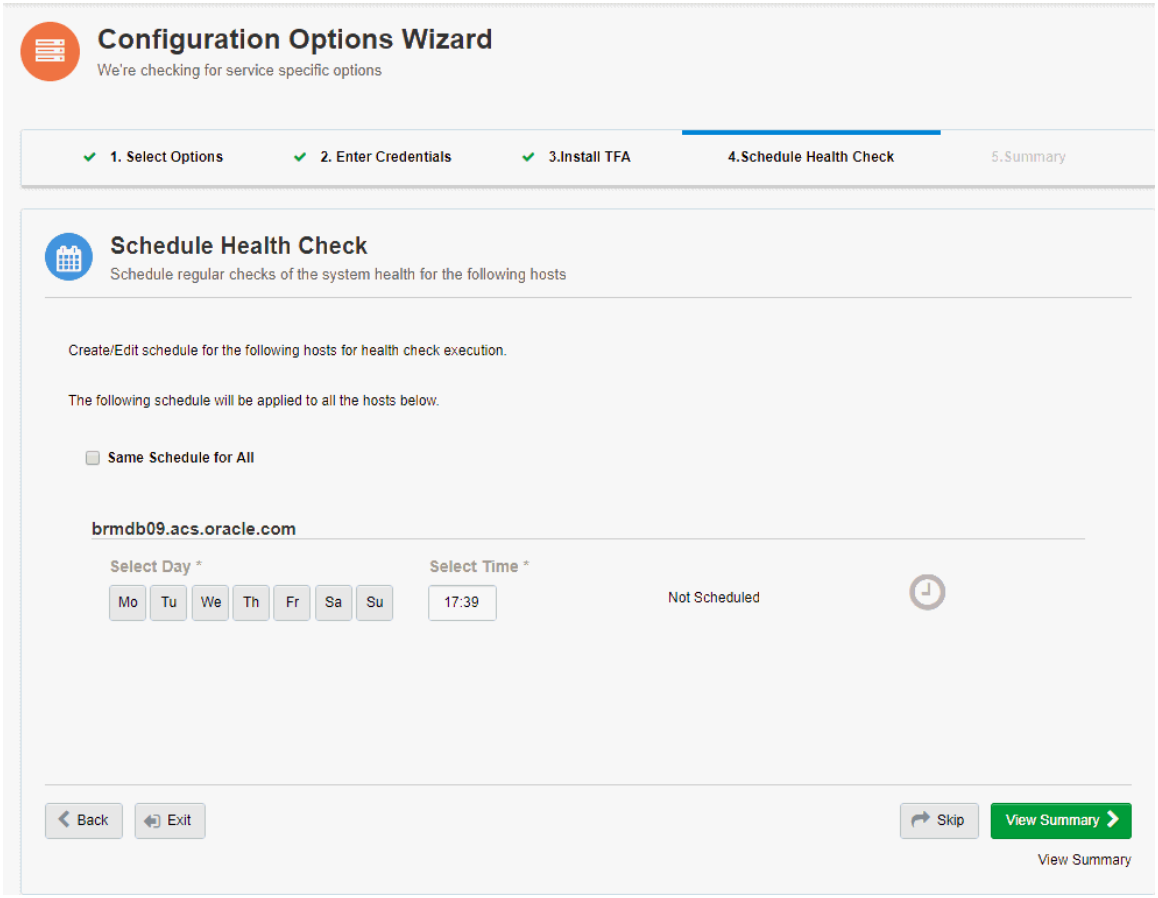
   b. (Optional) Select the **In the future, allow us to update TFA automatically** check box to enable Oracle to update TFA automatically in future (that is, after this TFA configuration is performed.)

9. Click **Next**.

   The Schedule Health Check screen appears.

   You use this screen to set a weekly schedule for the selected hosts for health check execution.

Figure 13–5 Scheduling the Health Check



10. Complete the following parameters:

    a. (Optional) Select the **Same Schedule for All** check box to apply the same schedule to all selected hosts.

    b. In the **Select Day** field, select the day of the week on which the schedule runs.

    c. In the **Select Time** field, select the time of day at which the schedule runs.

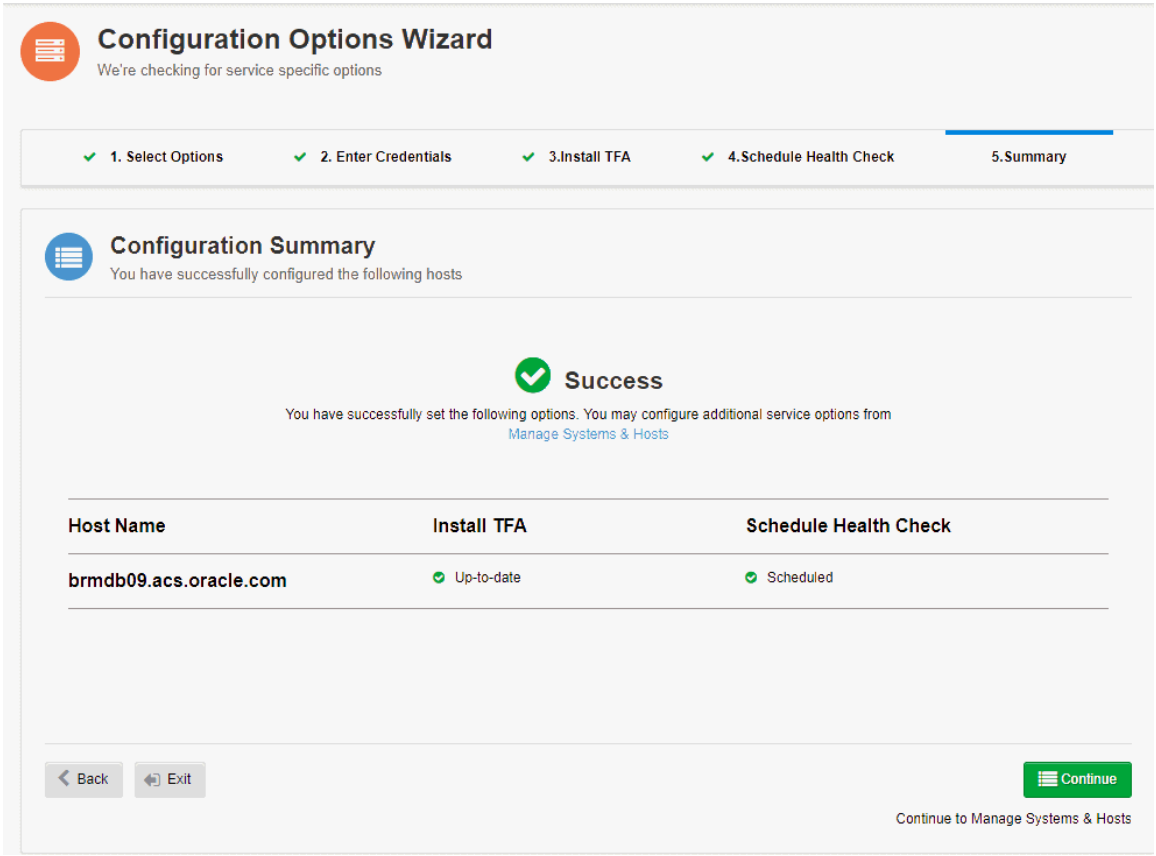
    d. (Optional) Click **Skip** to bypass the Schedule Health Check screen.

11. Click **View Summary**.

    The Configuration Summary screen appears.

    You use this screen to review the details of the TFA installation and health check schedule for each host.

Figure 13–6 Viewing the Schedule Summary



Related Information

Running the Health Check Report Immediately

Rescheduling the Health Check Report

Rescheduling the Health Check Report

You can schedule a health check report for supported targets, or you can opt to run the report immediately. Health checks run on a weekly basis. Execution takes place 30 to 50 minutes after it is scheduled to run.

To schedule the health check report:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

   Choose one of the following options:

   - From the **Admin** menu, click **Manage Databases**.

     The Manage Databases page appears.

     Select the required database.

     The database instance page appears, displaying a series of panels showing database information such as service requests, patches applied, utilization data for the target, and health check reports.

   - From the **Admin** menu, click **Manage Systems**.

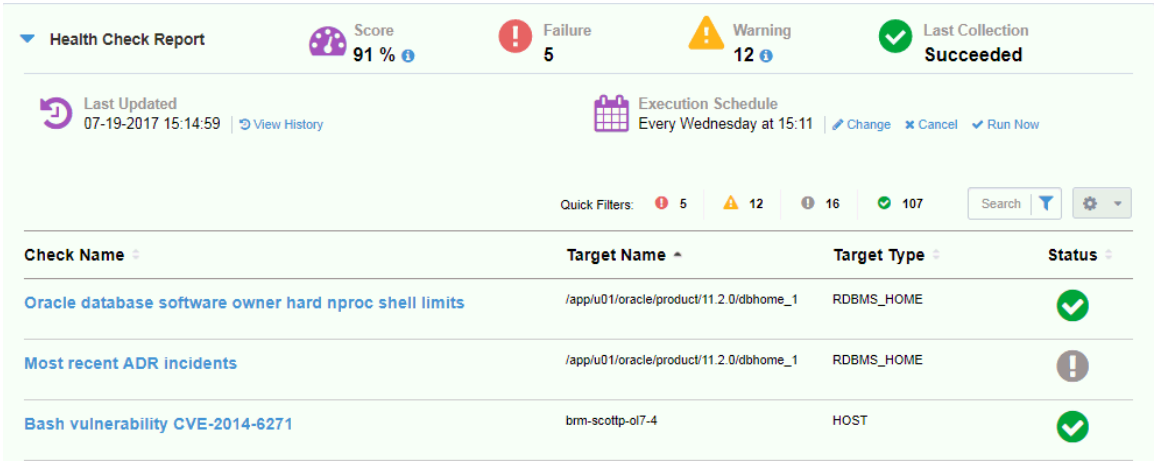
The Systems and Hosts page appears.

Select the required target.

2. The target or database instance page appears, displaying a series of panels showing information such as service requests, patches applied, and utilization data for the target.
3. Expand the Health Check Report section**.**

   The Health Check Report page appears.

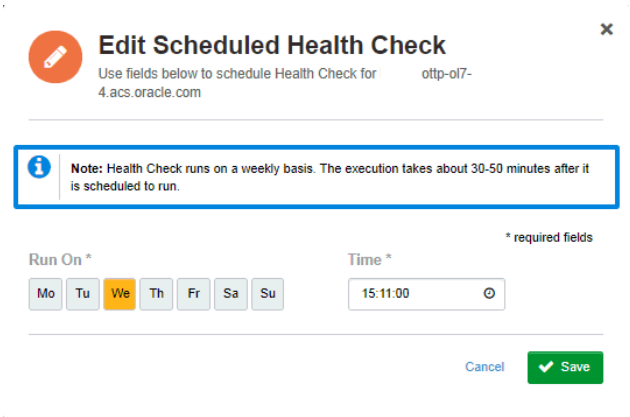
Figure 13–7 Running the Health Check Manually



4. From the list of actions under **Execution Schedule**, click **Change**.

   The Edit Scheduled Health Check page appears.

Figure 13–8 Scheduling the Health Check



5. Complete the following parameters:
   a. Select a day on which the schedule runs.
   b. Select a time at which the schedule runs.
6. Click **Save** to create the schedule.

   A message appears to confirm the creation of the schedule:

   Health Check run scheduled every Wednesday at 15:10. Next run will occur on 07-26-2017 15:10.

Related Information

Running the Health Check Report Immediately

Viewing the Health Check Report

Viewing Health Check History

Canceling a Schedule

To delete the health check report:

1. Follow the instructions in "Rescheduling the Health Check Report" to display the Health Check Report page.
2. From the list of actions under **Execution Schedule**, click **Cancel**.
3. Click **Yes**, **Cancel** to **c**onfirm the cancellation of the schedule.

   The status of the Execution Schedule changes to *Not Scheduled*.

Viewing the Health Check Report

There are a number of different ways to access health check reports for supported databases or hosts.

To view the health check report:

1. Follow the instructions in "Rescheduling the Health Check Report." to display the Health Check Report page.
2. The target or database instance page appears, displaying a series of panels showing information such as service requests, patches applied, and utilization data for the target.
3. Expand the **Health Check Report** panel.
4. Review the contents of the panel**.**

   The panel displays a dashboard of check results:

   - **Score**: The health check status expressed as a percentage of passed checks. This is the overall host score for the host and all of its database components.
   - **Failure**: Number of failing checks.
   - **Warning**: Number of warning checks. Also shows the delta (difference in number, for example, *+3* or *-7*) between the most recent health check and the previous one.

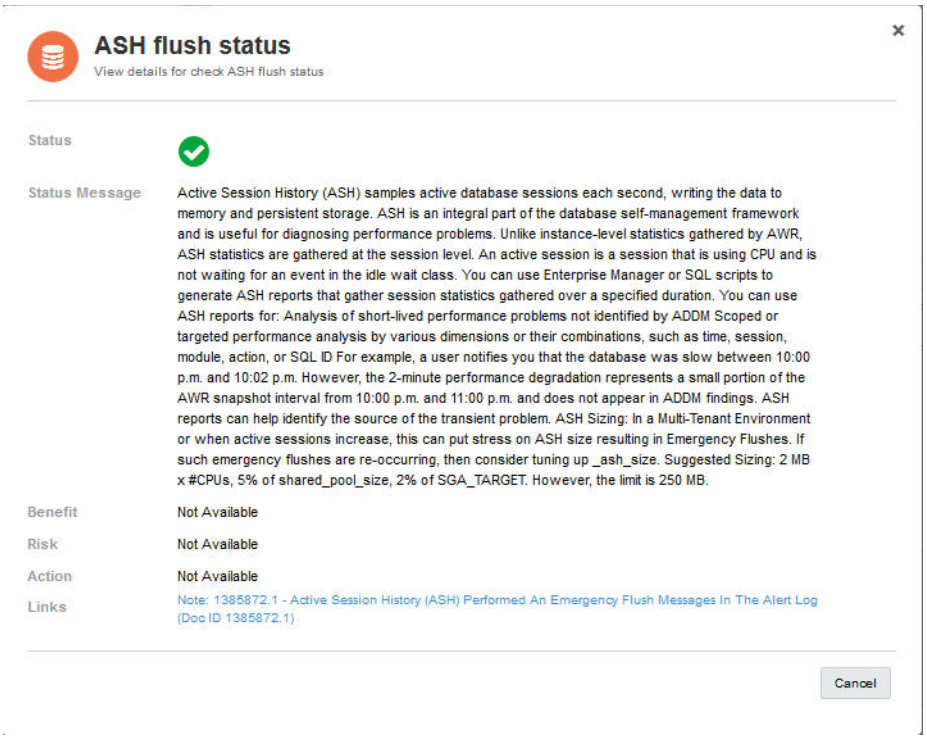
     If no delta is displayed, there has been no change from the previous results.
   - **Last Collection**: Shows whether the last collection succeeded or failed.
   - **Last Updated**: Shows when the health check was last performed.

     (Optional) Click **View History** to review the health check history.
   - **Execution Schedule**: Date and time of the health check run.
   - **Info**: Number of informational checks.
   - **Passed**: Number of successful checks.

   The panel also displays a table of individual checks, defined by check name, type, and status.

   Click a check to display more information. For example, the ASH flush status check is displayed in Figure 13–9.

Figure 13–9 Health Check Example



Related Information

Rescheduling the Health Check Report

Running the Health Check Report Immediately

Viewing Health Check History

Running the Health Check Report Immediately

You can schedule a health check report for supported targets, or you can opt to run the report immediately by triggering it manually.

To run the health report immediately:

1. Follow the instructions in "Rescheduling the Health Check Report" to display the Health Check Report page.
2. From the list of actions under **Execution Schedule**, click **Run Now**.

   A message appears to confirm the health check run:

   Running Health Check now. It will take 30-50 minutes to finish running.

   After the health check completes, you can review the status of the checks.

Related Information

Rescheduling the Health Check Report

Viewing the Health Check Report

Viewing Health Check History

Viewing Health Check History

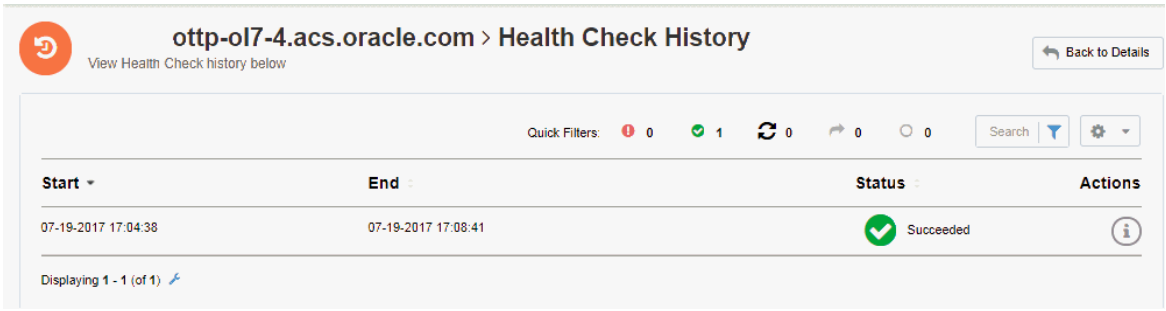
You can review when health checks were carried out, the status of the health check, and the collection details.

To view the health check history:

1. Follow the instructions in "Rescheduling the Health Check Report" to display the Health Check Report page.
2. From under the **Last Updated** section of the Health Check report, click **View History**.

   The Health Check History page for the selected target appears.

Figure 13–10 Viewing the Health Check History

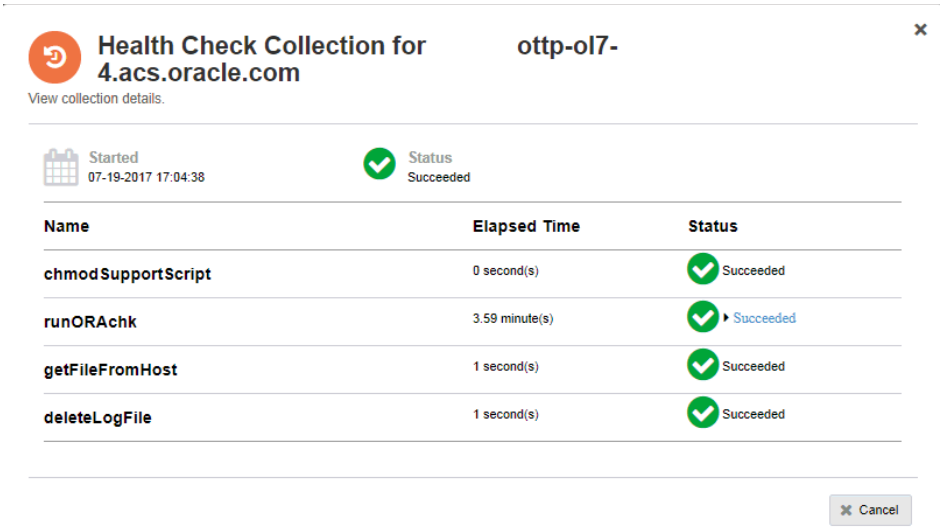


For each health check run, the start and end times and the overall status of the health check run are shown. The filters display the health check runs by status: failed, succeeded,

- Failed
- Succeeded
- Processing
- Suspended
- Unknown

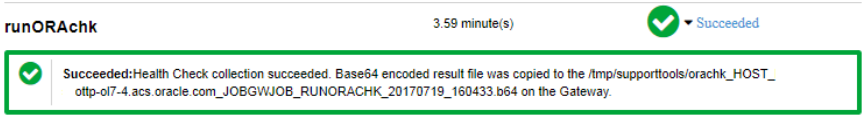
Click the information icon under **Actions** to view details of the actual health checks themselves. Each health check in the collection is defined by name, time taken to run the check, and status.

Figure 13–11 Viewing the Health Check Collection



In the status column, there is a link beside the ORAchk or EXAchk listing that points to the location of the actual encoded result file. Click **Succeeded** to view details of the file location.

Figure 13–12 Viewing the Health Check Collection File Location



Related Information

Rescheduling the Health Check Report

Viewing the Health Check Report

14

Setting the HTTP Proxy Server

This chapter provides information about optionally configuring the HTTP Proxy server if http-proxy is required for outbound communication from the Oracle Advanced Support Gateway. Details of the server IP address and port number can be provided by the customer's network administrator.

It includes the following topics:

- About the HTTP Proxy Server
- Specifying the HTTP Proxy Server Setting

About the HTTP Proxy Server

Configuration of the HTTP Proxy server is an optional step, but may be required for certain Oracle Advanced Support Gateway customer configurations.

HTTP Proxy server settings can also be configured during Gateway installation. Refer to *Oracle Advanced Support Gateway Installation Guide* for more information.

Specifying the HTTP Proxy Server Setting

To specify the HTTP Proxy server setting:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Admin** menu, click **Proxy Setting**.

   The Configure HTTP Proxy Settings page appears.

3. (Optional) Complete the following parameters on the HTTP Proxy server if http-proxy is required for outbound communication.

   a. (Optional) If HTTP Proxy mode is required, select the **Enable** check-box.

   b. In the **IP Address** field, enter your customer IP address.

      You can use the hostname or fully-qualified domain name (FQDN) as Oracle Advanced Support Gateway is configured to use Domain Name Service (DNS.)

   c. In the **Port** field, enter the port associated with the HTTP proxy server.

   d. (Optional) If authentication is required for the HTTP proxy server, select the **Check if required** check-box.

   e. In the **Proxy Username** field, enter a valid email address.

   f. In the **Proxy Password** field, enter the password associated with the user.

4. Complete the configuration as follows:
   a. Click **Create** to complete the configuration of the HTTP Proxy server.
   b. (Optional) Click **Cancel** to exit the Configure HTTP Proxy Settings page.

Specifying a HTTP Proxy During Connectivity Tests

Connectivity Tests (the *Netcheck* feature) are used to validate the required firewall ports and connections between Oracle Advanced Support Gateway and Oracle, which were established during Gateway installation. You can continue to monitor connectivity using Netcheck as required.

In order for Oracle to deliver Oracle Connected Services, the following requirements need to be met:

- All monitored devices must be network accessible from the Oracle Advanced Support Gateway.
- Oracle must have the level of access to the monitored devices necessary for Oracle to implement and deliver the service.
- The Oracle Advanced Support Gateway must be continuously accessible from the Oracle Support Platform using the secure protocols.

The Netcheck feature provides a mechanism to test connectivity between the Gateway and the Oracle Support Platform - external connections, in other words, and also between Oracle Advanced Support Gateway and the customer monitored systems, that is, internal connections.

These tests help to secure and successfully complete the implementation of services running on Oracle Advanced Support Gateway.

You can optionally specify a HTTP proxy if the traffic between the Gateway and the Engineered System is routed through a proxy server (depending on the customer's network configuration).

See "Specifying a HTTP Proxy."

15

Managing Server Certificates

This chapter describes how to manage and generate server certificates for Oracle Advanced Support Gateway.

It includes the following topics:

- About Server Certificates
- Viewing Server Certificates
- Managing Server Certificates

About Server Certificates

The Oracle Advanced Support Gateway server certificate is a public key certificate. This is a digitally signed statement that binds the value of a public key to the identity of the person, device, or service that holds the corresponding private key. One of the main benefits of certificates is that hosts no longer have to maintain a set of passwords for individual subjects who need to be authenticated as a prerequisite to access. Instead, the host merely establishes trust in a certificate issuer.

The server certificate is valid only for the period of time specified within it; every certificate contains **Valid From** and **Valid To** dates, which set the boundaries of the validity period. Once a certificate's validity period has passed, a new certificate must be requested by the subject of the now-expired certificate.

You can use Oracle Advanced Support Gateway to generate new server certificates when required.

Viewing Server Certificates

The **Server Certificate** page enables you to manage and generate your server certificate.

To view your server certificate information:

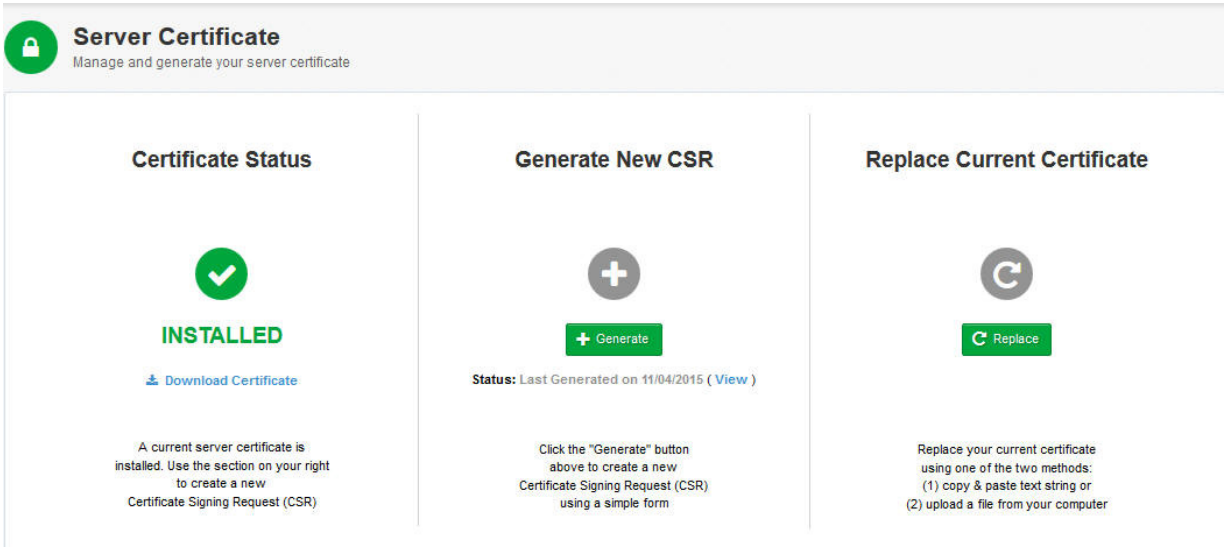
1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Gateway** menu, click **Server Certificate**.

   The Server Certificate page appears.

Figure 15–1 Server Certificate Page



Viewing Certificate Status

The Server Status section of the **Server Certificate** page enables you to view whether you have a server certificate installed on Oracle Advanced Support Gateway. You can also use the Server Status section to download and review your server certificate.

To view your server certificate status:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Gateway** menu, click **Server Certificate**.

   The Server Certificate page appears.

   If a server certificate is installed, an Installed message and corresponding check mark are displayed as shown in Figure 15–1.

   If a server certificate is not installed, and you want to install a certificate, see "Installing Server Certificates".

Managing Server Certificates

There are a number of actions that you can perform on server certificates using Oracle Advanced Support Gateway:

- Downloading server certificates. See "Downloading Server Certificates".
- Installing server certificates. See "Installing Server Certificates".
- Generating a certificate signing request. See "Generating a Certificate Signing Request".
- Replacing the current server certificate. See "Replacing the Current Server Certificate".

Downloading Server Certificates

You can use the Server Status section of the **Server Certificate** page to download and review your server certificate.

To download your server certificate:

1. Log in to Oracle Advanced Support Gateway.

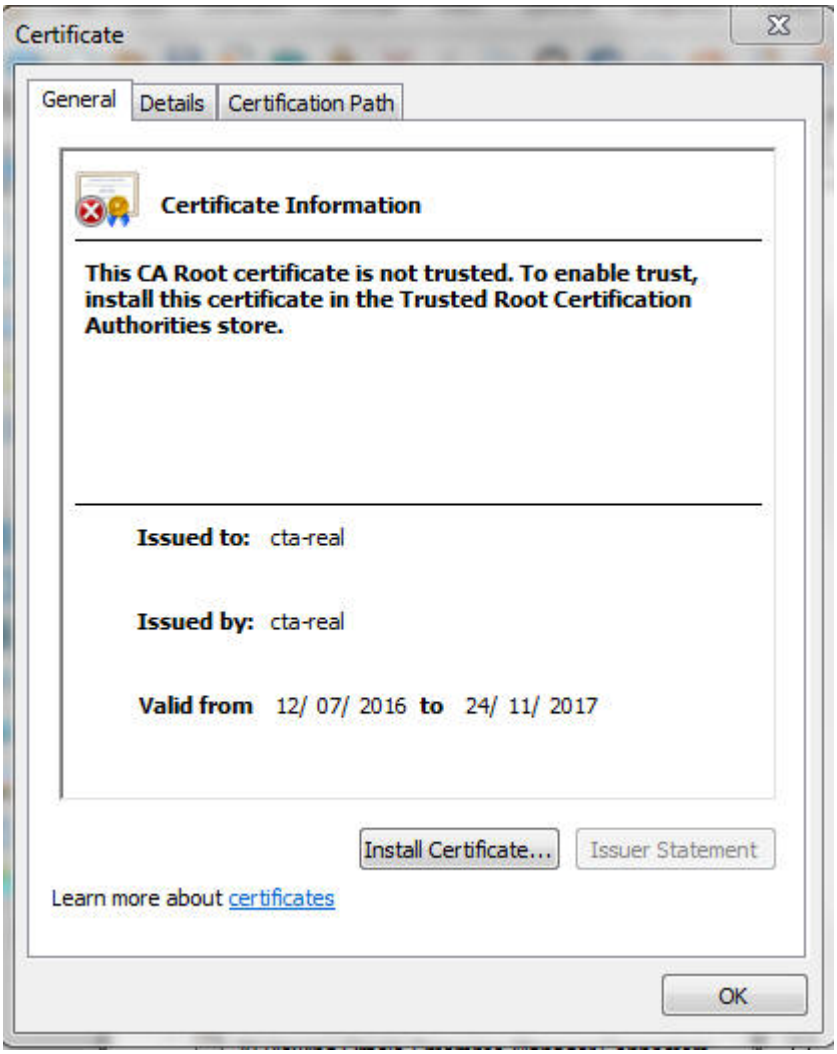
   The Oracle Advanced Support Gateway Home page appears.

2. From the **Gateway** menu, click **Server Certificate**.

   The Server Certificate page appears.

3. If a server certificate is installed, click **Download Certificate** and open the file to display the certificate shown in Figure 15–2.

Figure 15–2 Server Certificate



Installing Server Certificates

After downloading the server certificate, you can choose to import it to a certificate store. The wizard helps you to copy certificates, certificate trusts lists, and certificate revocation lists from your disk to a certificate store, which is the system area where certificates are kept.

To install your server certificate:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Gateway** menu, click **Server Certificate**.

   The Server Certificate page appears.

3. If a server certificate is installed, click **Download Certificate** and open the file.

4. On the certificate, click **Install**.

   The certificate import wizard Welcome page appears.

5. Click **Next.**

   The Certificate Store page appears.

   Use this page to allow Windows to automatically select the location for the certificate store, or to enable you to specify another location.

6. Select one of the following options:

   a. **Automatically select the certificate store based on the type of certificate**, *or*

   b. **Place all certificates in the following stor**e

   If you select(a), continue to step 7.

   If you select(b), continue to step 8.

7. (*For automatic selection of the certificate store*)

   Click **Next**.

   The Select Certificate Store page appears.

   The certificate store is automatically selected.

   Continue to step 9.

8. (*For self-selection of the certificate store*)

   Click **Browse**.

   The Select Certificate Store page appears.

   Select the required certificate store.

   Click **OK**, and then click **Next**.

9. Click **Finish** to complete the installation of the server certificate.

Generating a Certificate Signing Request

You can use Oracle Advanced Support Gateway to generate a Certificate Signing request (CSR).

A CSR is a block of encrypted text that is generated on the Oracle Advanced Support Gateway server that the certificate will be used on. It contains information that will be included in your certificate such as your organization name, common name (domain name), locality, and country.

To generate a new CSR:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.

2. From the **Gateway** menu, click **Server Certificate**.

   The Server Certificate page appears.

3. In the middle pane, Generate New CSR, click **Generate**.

The Server Certificate: Generate CSR page appears.

4. Complete the following parameters to generate a new CSR.
   a. In the **Server Name** field, enter the fully qualified domain name for your web server.
   b. In the **Org Unit** field, enter the organization unit.
   c. In the **Organization** field, enter the exact legal name of your organization. Do not use abbreviated forms of the organization name.
   d. In the **City** field, enter the name of the city where your organization is legally located.
   e. In the **State** field, enter the name of the state, county, or region where your organization is legally located. Do not use abbreviated forms of the name.
   f. In the **Country** field, select the country in which your organization is legally located.
5. Click **Generate** to complete the creation of the CSR.

Replacing the Current Server Certificate

After the end of the validity period for the server certificate, the certificate is no longer considered an acceptable or usable credential. You can use the Certificate Renewal Wizard on Oracle Advanced Support Gateway to replace or renew a certificate issued from a Windows enterprise certification authority (CA) before or after the end of its validity period.

You can replace your current certificate using one of two methods:

- Copying and pasting a text string, *or*
- Uploading a file from your computer

To replace the current server certificate:

1. Log in to Oracle Advanced Support Gateway.

   The Oracle Advanced Support Gateway Home page appears.
2. From the **Gateway** menu, click **Server Certificate**.

   The Server Certificate page appears.
3. In the right pane, Replace Current Certificate, click **Replace**.

   The Server Certificate: Apply Certificate page appears.
4. In the **Certificate Source** field select one of the methods below.
   a. **Copy & Paste; paste the text of the certificate**, *or*
   b. **File Upload; upload certificate as a file**

   If you select(a), continue to step 5.

   If you select(b), continue to step 6.
5. (*To copy and paste the text of the server certificate*)

   Paste the text of the certificate into the Certificate String field.

   Continue to step 7.
6. (*To upload a local certificate*)

   Click **Browse**.

   Select the required certificate from your local server.

   Click **Open**.

7. Click **Apply Certificate** to complete the replacement of the certificate.

16

Enabling Remote Access to the Oracle Advanced Support Gateway

This chapter provides information about enabling remote VPN access to the Oracle Advanced Support Gateway.

It includes the following topics:

- About the Remote Access Icon
- Enabling Remote Access
- Disabling Remote Access
- Viewing Remote Access History

About Remote Access

Oracle security policies require a VPN between Oracle and the customer so that Oracle can access the customer systems.

For more information about Oracle security policy and requirements, see *Oracle Advanced Support Gateway Security Guide*.

However, in certain limited cases, Oracle Advanced Support Gateway also enables the customer to control remote access by providing the capability to enable and disable VPN connectivity with Oracle.

Note: Remote VPN Access - also referred to as “Green Button” functionality - is not enabled by default and customers that wish to avail of it must first open a Service Request. Please refer to your Oracle representative for further details.

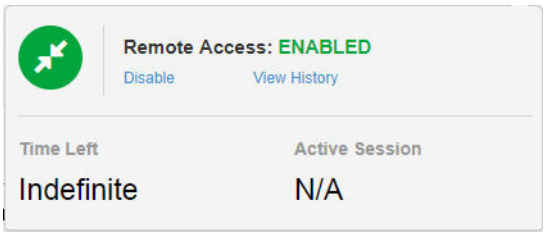
For example, Oracle recommends keeping remote access enabled for smooth delivery of Platinum Services. Not keeping remote access enabled may negatively impact your SLA.

Furthermore, remote VPN Access is not available for all Oracle connected services on Oracle Advanced Support Gateway.

About the Remote Access Icon

The Remote Access icon, also referred to as the *Green Button*, is displayed in the utility section of the navigation menu on the top-right of the Oracle Advanced Support Gateway user interface. See Figure 16–1.

Figure 16–1 Remote Access Icon



The icon is a toggle button that controls VPN connectivity and enables a customer to check VPN connectivity status.

When you click the Remote Access icon, you can enable or disable the remote access session, or view a history of remote access control sessions.

Enabling Remote Access

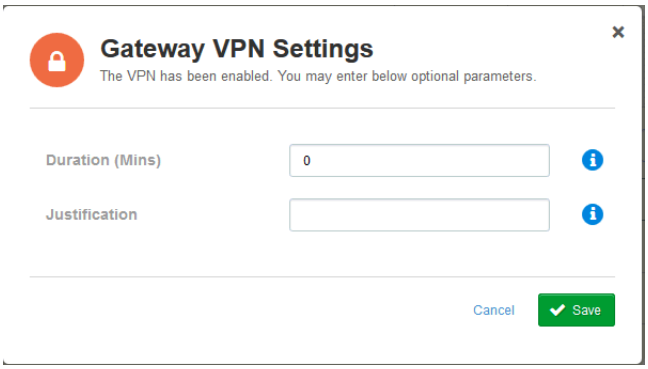
You can use the Remote Access icon to enable a Remote Access session.

To enable a Remote Access session:

1. Click the Remote Access disabled icon in the utility menu.
2. Select the **Enable** option.

   The Gateway VPN Settings page appears. See Figure 16–2.

Figure 16–2 Gateway VPN Settings Page



3. (Optional) Complete the following parameters to specify the VPN duration, and provide a justification for enabling the VPN.
   a. In the **Duration** field, enter the VPN duration in minutes.
   b. In the **Justification** field, enter a reason for enabling the VPN.
   c. Click **Save** to complete the configuration of the VPN.

   Note: On subsequent sessions, when you click **Enable**, the saved VPN settings are used by default, and the Gateway VPN Settings page is not displayed.

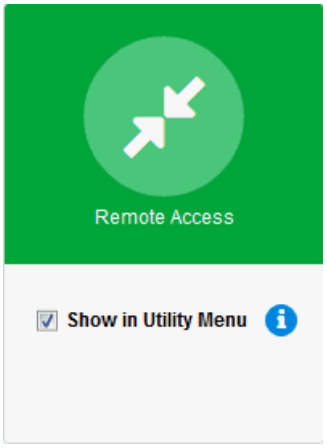
Disabling Remote Access

You can use the Remote Access icon to disable a Remote Access session.

To disable a Remote Access session:

1. Click the Remote Access icon in the utility menu.
2. Select the **Disable** option as shown in Figure 16–3.

Figure 16–3 Disabling the Remote Access Feature



The session is disabled after a short period.

Viewing Remote Access History

You can use the Remote Access icon to view a history of remote access control sessions.

To view remote access history:

1. Click the Remote Access icon in the utility menu.
2. Select the **View History** option.

   The Remote Access session history table appears, showing the enablement or disablement action, the time at which it was performed, the user that performed the action, as well a justification for the action. See Figure 16–4.

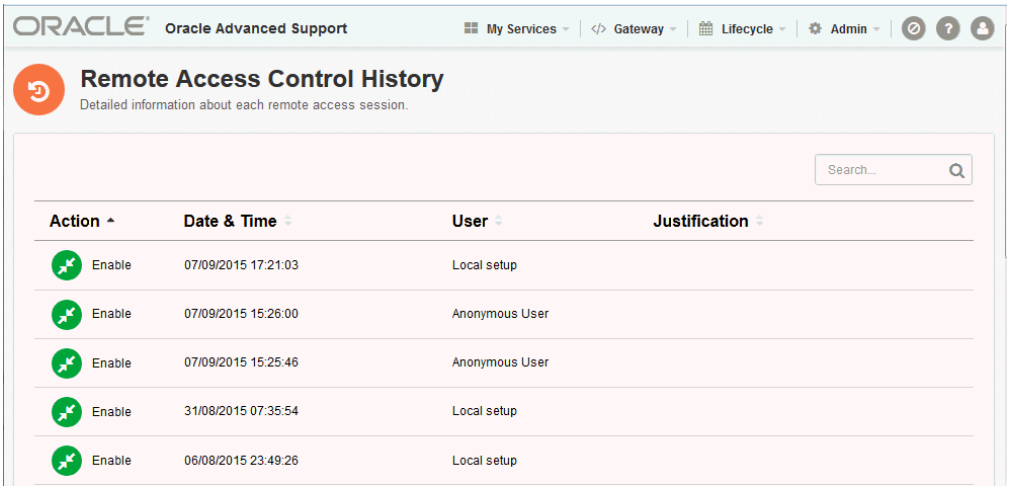



Figure 16–4 Remote Access Session History