Oracle® Real User Experience Insight

Installation Guide

11*g* Release 1 for Linux x86-64

E22308-03

April 2011

ORACLE®

Oracle Real User Experience Insight Installation Guide, 11*g* Release 1 for Linux x86-64

E22308-03

Primary Author: Paul Coghlan

Contributing Author: Eddy Vervest

Contents

Preface

Oracle Real User Experience Insight (RUEI) provides you with powerful analysis of your network and business infrastructure. You can monitor the real-user experience, define Key Performance Indicators (KPIs) and Service Level Agreements (SLAs), and trigger alert notifications for incidents that violate them.

Audience

This document is intended for the following people:

- System administrators responsible for the installation of RUEI. This assumes a sound understanding of the Linux operating system.
- The person within your organization designated as RUEI Super Administrator (that is, the `admin` used). They are responsible for post-installation configuration, and system maintenance.

Some familiarity with network and Web technology is assumed. In particular, you should have a sound understanding of network topology, and a good operational knowledge of your organization's network and application environment.

This guide is organized as follows:

- Chapter 1, "Getting Started" introduces RUEI. In particular, how it monitors data traffic, the role of the Reporter and Collector modules, and the supported configurations.
- Chapter 2, "Installing the RUEI Software" describes the procedure for preparing the server system(s) for RUEI, and installing the RUEI software.
- Chapter 3, "Upgrading to RUEI 11.1" describes the procedure for upgrading an existing RUEI 6.*x* installation to release 11.1.
- Chapter 4, "Configuring RUEI" describes the procedure for initially configuring RUEI. This procedure is performed by the person within the organization who has been assigned the role of RUEI Super Administrator.
- Chapter 5, "Installing and Configuring SSO Authentication Integration" describes the procedure for installing and configuring the Oracle HTTP server. This is an optional part of the RUEI installation process, and is only required if you intend to use the Oracle Single Sign-Off (SSO) service to authenticate RUEI users.
- Chapter 6, "Configuring the Oracle Access Manager (OAM)" describes the procedure for configuring OAM. This is an optional part of the RUEI installation process, and is only required if you intend to identify users within OAM-based network traffic.

- Chapter 7, "Configuring a Failover Reporter System" describes the procedure for configuring a failover Reporter system that will immediately take over processing of RUEI traffic in the event that the primary Reporter system becomes unavailable.
- Chapter 8, "Configuring a Failover Collector System" describes the procedure for configuring a faolover Collector system that will immediately take over monitoring network traffic in the event that the primary Collector system becomes unavailable.
- Appendix A, "Generic Database Instance Setup" describes how you can setup an Oracle database instance for use by the RUEI Reporter that is running on a platform other than Oracle Linux 5.x or RedHat Enterprise Linux 5.x. RUEI supports Oracle database version 11gR1 and 11gR2.
- Appendix C, "The ruei-check.sh Script" provides a detailed explanation of the `ruei-check.sh` script. It is strongly that you use this script to verify successful installation, and to troubleshoot any issues that occur during the installation process.
- Appendix D, "Verifying Monitored Network Traffic" describes how you can use the TCP diagnostic facility to verify that RUEI "sees" all required network traffic. It is *strongly* recommended that a network engineer within your organization validates collected network traffic after installation and configuration of RUEI.
- Appendix E, "Troubleshooting" highlights the most common issues encountered when installing RUEI, and offers solutions to quickly locate and correct them. It should be reviewed before contacting Customer Service.
- Appendix F, "Installation Checklist" provides a checklist of actions that should be completed, and the information gathered, before starting to install the RUEI software.
- Appendix G, "Third-Party Licenses" contains licensing information about certain third-party products included with RUEI.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at `http://www.oracle.com/accessibility/`.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at http://www.fcc.gov/cgb/consumerfacts/trs.html, and a list of phone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html.

Related Documents

For more information, see the following documents in the Oracle Real User Experience Insight (RUEI) documentation set:

- *Oracle Real User Experience Insight User's Guide.*

The latest version of this and other RUEI books can be found at the following location:

http://www.oracle.com/technetwork/documentation/realuserei-091455.html

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 Getting Started

This chapter introduces the role of Oracle Real User Experience Insight (or RUEI for short), its architecture, attachment, and deployment options.

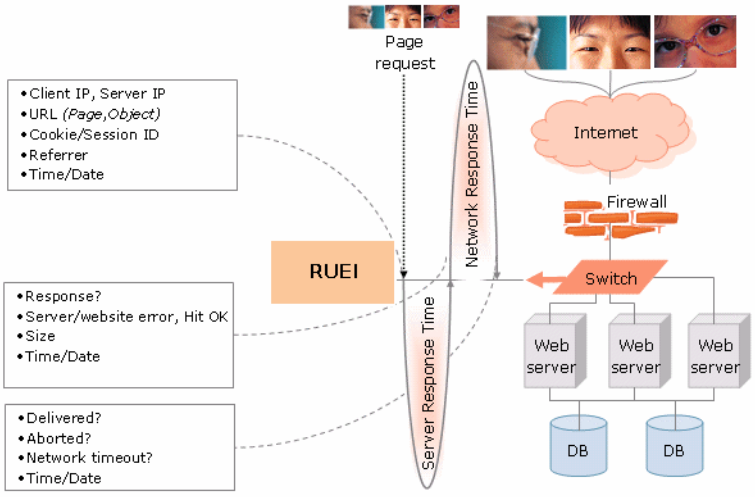
1.1 What is RUEI?

The usage of Web applications and services continues to grow. This includes not only the use of the Internet as a marketing channel, but also Extranet-based supply chain and back-office integration, and Intranet deployment of internal applications. Increasingly, it also includes the utilization of Web services which implement clearly defined business functions. RUEI is designed for measuring, analyzing, and improving the availability and performance of all of these deployment scenarios.

1.1.1 Data Collection

Typically, RUEI is installed before the Web servers, behind a firewall in the DMZ (as shown in Figure 1–1). The data collection method is based on Network Protocol Analysis (NPA) technology. This method is 100% non-intrusive. Hence, it does not place any load on a Web server, or require installing software agents that will impact performance. In addition, it does not require any change to the current application or infrastructure. When a new application release is deployed, or when an additional Web server is added, there is no or very little change required to RUEI's monitoring environment.

Figure 1–1 How RUEI Collects Data



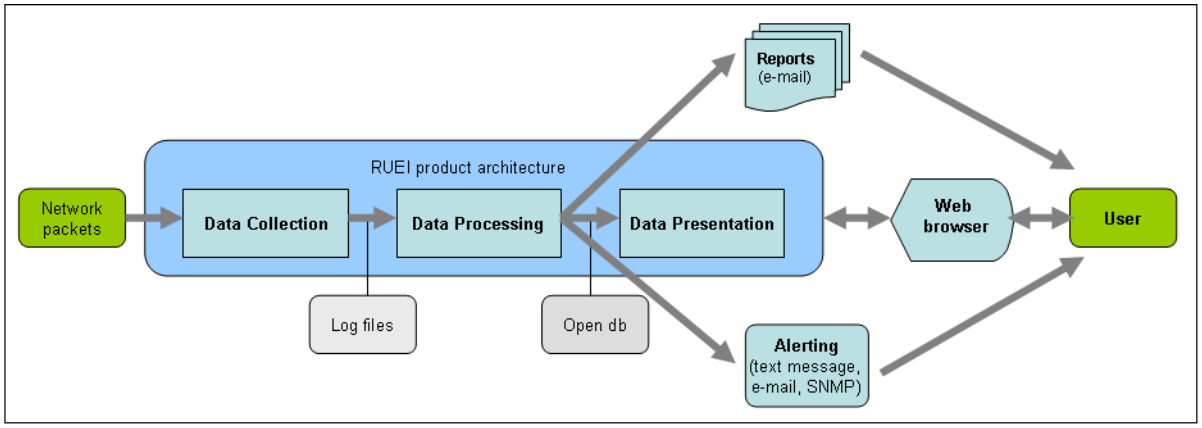
When an object is requested by a visitor, RUEI sees the request and measures the time the Web server requires to present the visitor with the requested object. At this point, RUEI knows who requested the page (the client IP), which object was requested, and from which server the object was requested (server IP).

When the Web server responds and sends the requested object to the visitor, RUEI sees that response. At this point, RUEI can see whether there is a response from the server, whether this response is correct, how much time the Web server required to generate the requested object, and the size of the object. In addition, RUEI can also see whether the object was completely received by the visitor, or if the visitor aborted the download (that is, proof of delivery). Hence, RUEI can determine the time taken for the object to traverse the Internet to the visitor, and calculate the Internet throughput between the visitor and the server (that is, the connection speed of the visitor).

1.1.2 Product Architecture

RUEI is based on a three layer product architecture, as shown in Figure 1–2.

Figure 1–2 RUEI Product Architecture



The monitored data packets are processed by the following layers:

- **Data collection**

  This layer is responsible for acquiring raw data and delivering it to the Data processor. This data can be collected from multiple sources. The available attachment options are described later in this section.

- **Data processing**

  This layer converts the raw data into OLAP data sets. These comprise the multidimensional data structure that is viewable within the data browser.

- **Data presentation (reporter)**

  This layer is RUEI's analysis and reporting environment. This is a Web-based information portal that can be accessed from any selected browser. The interface between the data processing and data presentation layer is based on open db calls.

1.2 Security

To read HTTP(S) data streams, a proprietary software module reassembles TCP/IP packet streams. Because the data collectors do not have an assigned IP number, and

the software using these data collectors does not have a functional IP stack, RUEI is not able to respond to incoming traffic received on the data collectors. This makes RUEI "invisible" to the monitored networks, and completely secure.

> **Note:** Because of the non-intrusive way in which RUEI collects data, it is not possible for it to request retransmission in the event of an error on the measurement port.

Data collection can be configured to log encrypted data. To facilitate this, a copy of the Web server's private SSL keys needs to be set up in the data collector. In addition, RUEI can be configured to omit logging of sensitive data in the arguments of POST requests of forms or content; so called *data masking* (or blinding).

1.3 Connection Options

RUEI supports the use of both copy ports[1] and TAPs[2] for monitoring network traffic (10/100 Mbps and 1/10 Gbps Ethernet connections are supported). Copy ports and TAPs are available for copper or fibre-based network infrastructures. While both devices allow non-intrusive monitoring of network traffic, there are differences between these two connection options. These are highlighted in the rest of this section.

Monitoring SSL and Forms Traffic

Be aware that SSL and Oracle Forms traffic are particularly sensitive to disruptions in the TCP packet stream. This is because they require state information to be maintained for the duration of the connection, and any lost packets can cause that information to be lost, preventing RUEI from accurately monitoring and reporting the connection.

Therefore, you should ensure that each Collector is connected to a reliable network device, such as a TAP. In addition, it is *strongly* recommended that you regular review the information available through the Collector Statistics window (select **System**, then **Status**, and then **Collector status**) to verify the integrity of the TCP packet stream. Particular attention should be paid to the reported TCP and SSL connection errors.

1.3.1 Copy Ports

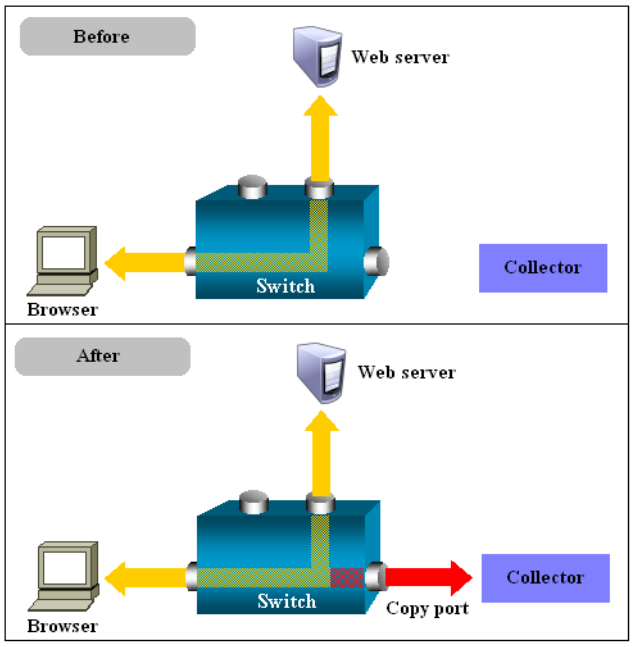
A copy port is a switch that starts to build up a Layer 2 forwarding table on the basis of the source MAC address of the different packets that the switch receives. After this forwarding table is built, the switch forward traffic that is destined for a MAC address directly to the corresponding port.

For example, after the Web server MAC in Figure 1–3 is learned, unicast traffic from the browser to the Web server is only forwarded to the Web server port. Therefore, the Collector does not see this traffic.

[1] Copy ports are also known as Switched Port Analyzer (SPAN) ports which is a feature of Cisco switches.

[2] Test Access Port (TAP) devices are provided by specialist vendors, such as NetOptics Inc.

Figure 1–3 Network Connection Using a Copy Port



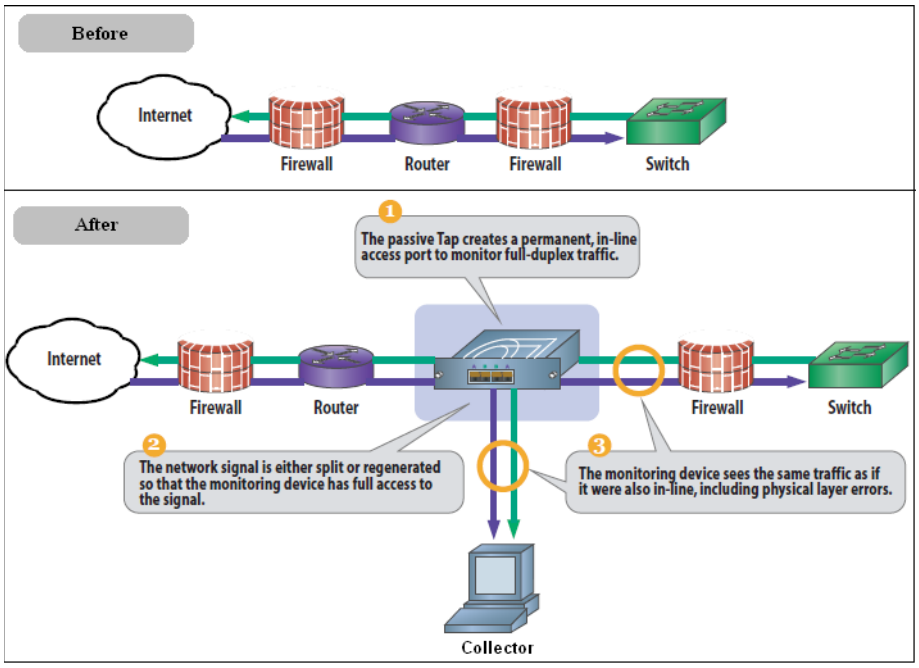
In the configuration shown in the lower part of Figure 1–3, the Collector is attached to a port that is configured to receive a copy of every packet that the browser sends and receives. This port is called a copy port. Copy ports can copy traffic from any or all data ports to a single unused port and prevents bi-directional traffic on the port to protect against backflow or traffic into the network.

Be aware that activating a copy port on a switch can have a performance impact. Typically, copy ports support a wide range of configuration options, and for further information about these options you should consult your switch documentation or contact the vendor.

1.3.2 TAPs

TAPs can be placed between any two network devices (such as routers and firewalls). Any monitoring device connected to a TAP receives the same traffic as if it were in-line, including all errors. This is achieved through the TAP duplicating all traffic on the link, and forwarding it to the monitoring port(s). The example shown in Figure 1–4 illustrates a typical TAP deployment for one Collector.

Figure 1–4 Network Monitoring Using a TAP



Important

Unlike copy ports, in the event of power failure, TAPs continue to allow data to flow between network devices. In addition, copy ports are prone to packet loss when under load. TAP devices are available for copper or fibre-based infrastructures. Moreover, they can be easily deployed when and where required, but without reconfiguration of switches or engineers needing to re-cable a network link. For these reasons, the use of TAPs is *strongly* recommended over that of copy ports.

Broadly speaking, there are three types of TAPs: network, regeneration, and aggregation TAPs. RUEI supports the use of network and regeneration TAPs. The use of aggregation TAPs is *not* recommended because they can lose data, and do not provide an acceptable level of accuracy. However, the deployment of multiple Collectors, or the connection of multiple links directly to one Collector, is available for the aggregation of data from multiple streams. In addition, be aware that when capturing data with a network-TAP device, the use of cascaded TAP configurations is not supported.

1.4 Installation and Deployment Options

A RUEI system can be configured in two different ways: as a Reporter, or as a Collector. Each installation option is reviewed in the following sections.

Reporter

Here, the Reporter provides a browser-based interface to the collected data. After processing, this data is stored in an Oracle database. This database can reside locally (that is, on the Reporter system), or on a remote database server.

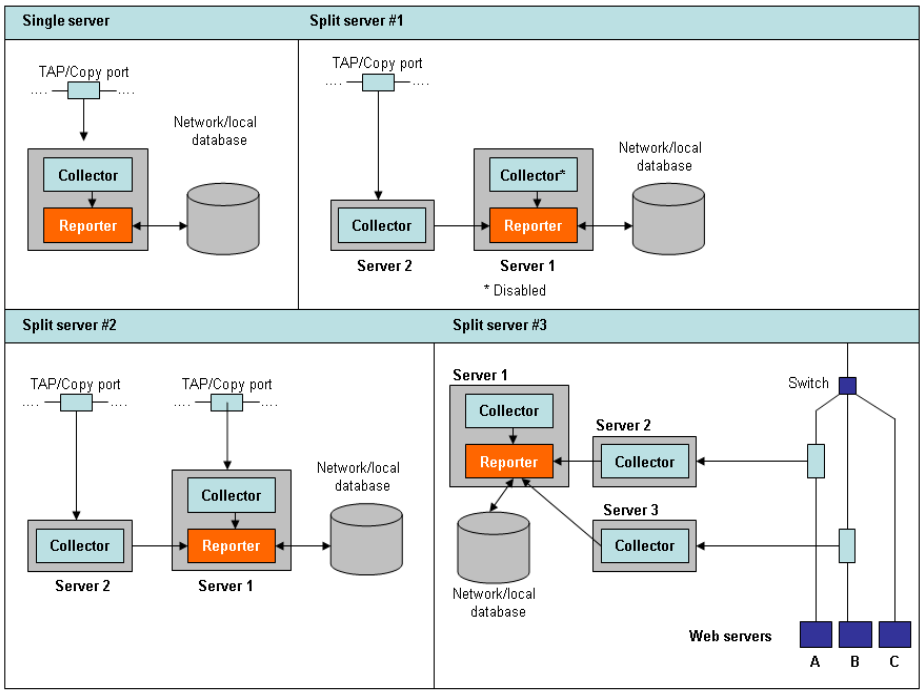
Note that each Reporter installation also contains a local Collector instance. The Reporter can either be configured to just process information gathered by this local Collector (this is a single-server configuration similar to the one shown in Figure 1–5), or can (optionally) be configured to receive information from additional Collector

installations. Note the local Collector instance on the Reporter system can also be disabled if not required.

Collector

If a RUEI system is installed as a Collector, it submits the data it gathers to a Reporter system. Multiple Collectors can be attached to the same Reporter. Split server #1 in Figure 1–5 is an example of a single Collector split-server configuration, while split server #2 is an example of a split-server configuration using two Collectors. Note that a direct network connection is required between the Collector(s) systems and the Reporter system.

Figure 1–5 Configuration Options



1.4.1 Local and Remote Database Installations

As mentioned earlier, the data available via the Reporter system is stored in an Oracle database. This database can reside locally on the Reporter system, or on a remote database server (such as a database cluster).

The use of a remote database server provides a number of potential advantages over a locally installed database. In particular, it offers easier integration with existing security and back-up policies, as well as improved performance through the use of dedicated servers.

Currently, RUEI 11.1 supports the Oracle 11g database. While the procedure for 11gR1 is described, 11gR2 is also supported. Note the Oracle 10g (or older) database is not supported.

1.4.2 Scalability Options

The use of multiple Collectors may be considered when there is a need to monitor very high levels of data traffic. In addition, this deployment also provides the possibility of

enhanced security. For example, by placing the Collector(s) outside the office network, while placing the Reporter system within the network.

Split-server configuration #1 in Figure 1–5 shows an example of a typical DMZ installation. The Collector is located in the DMZ, and the Reporter is within the server network environment. Note that the local Collector instance is disabled. Split-server configuration #2 shows an example of a deployment consisting of two Collectors. This could, for example, be used between two data centers (both monitoring the DMZ), where one data center acts as a failover for the other.

Split-server configuration #3 shows an example of a deployment in which both data lines are monitored in the same reporting environment. It also features the use of offloading to a database on a separate server. Note this deployment assumes that the traffic on each line is mutually exclusive. It also shows an example of a deployment used for security reasons. While the traffic from Web servers A and B are monitored and reported, the traffic from Web server C is not. This is also the reason why the Collectors are not placed above the switch.

For security reasons, it is recommended that access to the Reporter system is restricted to trusted IP ranges. Similarly, you may want to locate the Reporter system inside the internal network to maximize its security. The Collector's data gathering ports should be in the DMZ.

1.5 Hardware Requirements

The required minimum system specifications for the selected configuration (as explained in Section 1.4, "Installation and Deployment Options") are described in the following sections.

Network Cards

It is recommended that you carefully consider the selection of network cards for your infrastructure. Depending on the connection option you selected in Section 1.3, "Connection Options", both copper and fibre-based network cards may be required. If necessary, consult both your network and systems management teams.

Note: For more information about required and recommended system specifications, please contact Customer Support.

1.5.1 Single-Server Requirements

Table 1–1 Single-Server System Minimum Requirements

Element	Requirements
CPU	64-bit Intel or AMD dual-CPU, dual-core processor (> 2 G Hz) or equivalent.
Memory	16 GB.
Disk space	Minimum 400 GB HDD free space.[1,2]
Network interfaces	When using a network-TAP device[3], a minimum of three network interfaces is required: ■ Two interfaces for network traffic capturing. ■ One interface for network services.

Table 1–1 (Cont.) Single-Server System Minimum Requirements

Element	Requirements
GSM modem (optional)	Optional support for a GSM modem to send text messages messages. The modem needs to be either GSM07.05 or GSM07.07 compatible. It can be connected through a serial or USB port. If USB is used, RUEI uses the first available port (ttyUSB0). Alternative methods of sending text messages are available (http/e-mail).

1 To ensure acceptable performance of the RUEI installation, it is recommended to use high performance disk systems, with a minimum supported I/O rate of 70 MB/s. When monitoring high volumes of traffic, more powerful disk systems may be required. (Hardware) RAID-5, RAID-10, or equivalent storage configurations are strongly recommended.

2 This may need to be increased if Enriched data exchange is enabled.

3 When capturing data with a network-TAP device, the use of cascaded TAP configurations is not supported.

1.5.2 Reporter Requirements

Table 1–2 Reporter System Minimum Requirements

Element	Requirements
CPU	64-bit Intel or AMD dual-CPU, dual-core processor (> 2 G Hz) or equivalent.
Memory	16 GB.
Disk space	Minimum 400 GB HDD free space[1,2].
Network interfaces	A minimum of 1 network interface is required.
GSM modem (optional)	Optional support for a GSM modem to send text messages. The modem needs to be either GSM07.05 or GSM07.07 compatible. It can be connected through a serial or USB port. If USB is used, RUEI uses the first available port (ttyUSB0). Alternative methods of sending text messages are available (http/e-mail).

1 To ensure acceptable performance of the RUEI installation, it is recommended to use high performance disk systems, with a minimum supported I/O rate of 70 MB/s. When monitoring high volumes of traffic, more powerful disk systems may be required. (Hardware) RAID-5, RAID-10, or equivalent storage configurations are strongly recommended.

2 This may need to be increased if Enriched data exchange is enabled.

1.5.3 Collector Requirements

The requirements for Collector systems are shown in Table 1–3.

Table 1–3 Collector System Minimum Requirements

Element	Requirement
CPU	64-bit Intel or AMD dual-core processor or equivalent.
Memory	8 GB.
Disk space	Minimum 200 GB HDD free space.

Table 1–3 (Cont.) Collector System Minimum Requirements

Element	Requirement
Network interfaces	When using a network-TAP[1] device, a minimum of three network interfaces are required: ■ Two interfaces for network traffic capturing[2]. ■ One interface for communication with the Reporter system. When using a network-copy port, a minimum of two network interfaces are required: ■ One interface for network traffic capturing. ■ One interface for communication with the Reporter system.

[1] Capturing data with a network-TAP device prevents the use of a cascaded TAPs configuration.

[2] For up and down stream traffic. Note that the use of TAPs that integrate up and down stream traffic on one line is not recommended.

Important: Please note that an Intel (or compatible) 64-bit platform is a *strict* requirement for both the hardware and the operating system in all deployment scenarios.

1.5.4 Deployment Best Practices

This section presents a best practices framework within which to optimize your RUEI deployment. It is recommended that you carefully review the following information.

Planning Your Deployment

It is important that the nature of the monitored network environment is clearly understood before deciding upon your RUEI deployment strategy. This includes not only the basic network connectivity, ports, addressing, and physical device requirements, but also a sound understanding of the monitored applications.

Moreover, before deploying RUEI, the basic traffic flows within the network must have been identified. This should include information about average and peak volumes of traffic. Any physical deployment requirements (such as space limitations, distances, power planning, rack space and layout, or cabling) should also have been identified.

You can use the checklist presented in Appendix F, "Installation Checklist" to capture much of this information.

Forms-Based Traffic

If you are planning to monitor Forms-based traffic, be aware that the memory requirements may be higher than those outlined in Section 1.5, "Hardware Requirements". This is especially the case in deployments with heavy levels of Forms traffic. In this case, you should consider a split-server deployment.

Full Session Replay

If you are planning to make use of the Full Session Replay facility, you may need to configure additional storage capacity. This is explained in Section 1.5.6, "Full Session Replay Storage Requirements".

Encrypted Traffic

If a significant level of the monitored traffic is encrypted, this can increase the CPU overhead. In this case, it is recommended that you consider configuring additional CPUs or, alternatively, a split-server deployment.

Very High Levels of Traffic

When very high levels of traffic are being monitored (that is, more than 10 million page views per day), you should consider a split-server deployment. Alternatively, consider the use of a remote database. The latter has the effect of significantly reducing (by up to 30%) the CPU overhead on the Reporter system. Monitored environments with more than 20 million page views per day should consider the use of both a split-server deployment and a remote database.

1.5.5 Data Retention Policies

As explained in the *Oracle Real User Experience Insight User's Guide*, the availability of specific data within the Data Browser, as well as reports based on that data, depends on the Reporter data retention policies defined for your RUEI installation. By default, RUEI retains information on daily, monthly, and yearly levels for 32 days, 13 months, and 5 years, respectively. In addition, information about failed pages, URLs, and services is retained for 15 days. The maximum amount of database storage required to maintain the default data retention policies is shown in Table 1–4.

Table 1–4 Default Required Database Storage

Type of data retained	Default retention policy	DB space required per period (GB)	Total DB space required (GB)
Failed pages/URLs/services	15	1.5	22.5
Daily[1]	32	1	32
Monthly	13	1	13
Yearly	5	1	5
Suites[2]	15	0.5[3]	7.5
Additional overhead			10
Total required DB space			90

[1] This includes the All pages, All sessions, All functions, All transactions, Key pages, and URL diagnostics groups.

[2] Suites use the Daily retention policy setting.

[3] 0.5 GB is required per day for each configured suite type.

Be aware that, in addition to the database storage required for each retained type of data, appropriately 10 GB of database storage is also required for other purposes. This includes KPIs, SLAs, and processing requirements. In Table 1–4, it is assumed that one suite type is configured.

If you modify the default Reporter data retention policies, it is recommended that you use the **Calculate** facility to see the effect your new retention policy would have on required database storage. Note that the projected database utilization is based on previous database utilization, rather than maximum database usage.

The default amount of database storage available to the Reporter is 200 GB, and for most deployments, this will meet your operational requirements.

Example - Increasing the Number of Groups

Consider the following situation. You have decided to retain information on daily, monthly, and yearly levels for 90 days, 24 months, and 5 years, respectively, and failed pages, URLs, and services information should be retained for 90 days. For the purposes of this example, it is assumed that only one suite type is configured. The maximum amount of database storage required to maintain this data is shown in Figure 1–5.

Table 1–5 Required Database storage

Type of data retained	Default retention policy	DB space required per period (GB)	Total DB space required (GB)
Failed pages/URLs/services	90	1.5	135
Daily	90	1	90
Monthly	24	1	24
Yearly	5	1	5
Suites	90	0.5	45
Additional overhead			10
Total required DB space			264

Maximum Data Browser Group Sizes

In addition to modifying the data retention policy settings, you can also modify the maximum size to which Data Browser groups are allowed to grow before data is condensed. This is fully explained in Appendix C, "Setting the Maximum Data Group Size".

1.5.6 Full Session Replay Storage Requirements

If you are planning to make use of the Full Session Replay facility, you may need to configure additional storage capacity available to the Collector system. This should be a separate device (not a partition of the Collector server's existing hard drive), and made accessible to the RUEI file system. The procedure to do this, together with guidance on storage requirements, is described in the rest of this section. Note that this procedure must be repeated for each Collector for which full session replay information is required.

Configuring Additional Storage for Full Session Replay

To configure the additional required storage, do the following:

1. Mount the device. For example, under `/mnt/external_storage`.
2. Temporarily stop the Collector by issuing the following command:

```
appsensor stop wg
```

3. Move the `$APPSENSOR_HOME/wg/REPLAY` directory to the new device. In the above example, this is `/mnt/external_storage`, and the result is that the replay files are now located in the `/mnt/external_storage/REPLAY` directory.
4. Create a symbolic link from `/mnt/external_storage/REPLAY` to `$APPSENSOR_HOME/wg/REPLAY`.
5. Restart the Collector by issuing the following command:

   ```
   appsensor start wg
   ```

6. Calculate the required storage capacity. To do so, multiple the average number of daily page views by the average page size. Then, multiple this number by the number of days you wish full session replay data to be retained. Use Table 1–6 as guidance.

Table 1–6 Full Session Replay Storage Estimates

	Low page weight (~10 Kb)		**Medium page weight (~50 Kb)**		**High page weight (~100 Kb)**	
Page views per day (millions)	Size per day (GB)	Disk I/O (MB/sec)	Size per day (GB)	Disk I/O (MB/sec)	Size per day (GB)	Disk I/O (MB/sec)
0.5	5	0.1	25	0.3	50	0.6
2	20	0.2	100	1.2	200	2.3
5	50	0.6	250	2.9	500	5.8
10	100	1.2	500	5.8	1000	11.6
20	200	2.3	1000	11.6	2000	23.1
50	500	5.8	2500	28.9	5000	57.9

Important: Table 1–6 is intended for guidance only. It is *strongly* recommended that you regularly review average page sizes and daily page views, and adjust the required storage size as necessary.

Note: Be aware that FSR functionality uses a significant number of non-sequential read operations. Please consult your hardware vendor for information on how to optimize your I/O performance.

7. Select **Configuration**, then **General**, then **Advanced settings**, and then **Collector data retention policy**. Click the **Full session replay storage size (GB)** setting. Specify (in gigabytes) the required storage size. Note that the maximum that can be specified is 100 TB. When ready, click **Save**.

1.5.7 Memory Requirements

When calculating the amount of RAM required by your RUEI installation, it is recommended that you consider the following:

- For the Reporter system, each million visitor sessions per day requires 256 MB. Hence, 3 million visitor sessions per day would require 768 MB. In addition, each million page views requires 100 MB - 256 MB. Note that exact amount depends the length of monitored URLs, average session duration, and the number of events (such as custom dimensions).

- For each Collector system, each 10,000 hits requires 200 MB, and each 1000 SSL connections require 1 MB. In addition, up to 600 MB of network traffic can be buffered before individual TCP sessions start to be dropped. Up to 600 MB should also be assumed for content checks (such as XPath queries and error strings). Note that if you define a large number of content checks, or specify that they contain NLS character sets, the memory required may increase.

1.6 Software Requirements

The following GNU/Linux distributions are supported:

- Oracle Linux 5.*x*.
- RedHat Enterprise Linux 5.*x*.

Encrypting Sensitive Data

If sensitive data needs to be encrypted, you have the opportunity to encrypt your entire disk configuration during the disk partitioning phase of the Linux installation procedure. For more information, see Section 2.4, "Set up Disk Partitioning".

1.7 Network Requirements

- All server system clocks should be synchronized via NTP using UDP port 123.
- Support DNS information requests over TCP and UDP port 53.
- Support reports and e-mail alerts using TCP port 25.
- Support SNMP traps on request from an SNMP Manager using UDP port 161/162.
- The RUEI user interface is accessible over HTTPS port 443.
- In the case of a remote database setup, access to TCP port 1521 is required between the Reporter and remote database server.
- Each remote Collector system should be accessible by the Reporter system over TCP port 22. It is recommended all other ports be blocked.
- If you are configuring a failover Reporter system (described in Chapter 7, "Configuring a Failover Reporter System"), the primary and secondary Reporter systems need to be able to contact each other using ICMP.
- If you are configuring a failover Collector system (described in Chapter 8, "Configuring a Failover Collector System"), the primary and secondary Collector systems need to be able to contact each other using ICMP.

Collector-Reporter Bandwidth

The amount data transferred between a remote Collector and the Reporter system largely depends on the type and level of network application traffic monitored by RUEI. In addition, the configuration of RUEI (such as defined functional errors, content checks, and page naming schemes) also influences the size of Collector files that need to be transferred to the Reporter system.

At peak times, the amount of data that needs to be transferred will be higher than during low traffic periods. Note that the exact amount of the data transmission from a remote Collector to the Reporter system can only be determined after the actual RUEI deployment.

For an initial deployment, the following simple rule can be used: each 5 million daily page views will result in a peak transfer of approximately 125 MB at peak time, and

approximately 1 GB per day. Hence, typically only a few percent of the actual monitored traffic will be stored by a Collector and transferred to the Reporter. When you want or need to minimize this data transfer, it is recommended that you minimize the amount of monitored HTTP traffic which is not required by RUEI. For example, by using a subnet or VLAN-filtered network.

Firewall Requirements

Table 1–7 shows the firewall requirements for your RUEI deployment.

Table 1–7 RUEI Firewall Rules

From	To	Port(s)	Socket type	Required	Description
Reporter	Collector	22 (SSH)	TCP	Y	Each remote Collector system must be accessible by the Reporter system over TCP port 22.
Reporter	NTP server	123 (NTP)	UDP	Y	All server system clocks must be synchronized via NTP.
Collector	NTP server	123 (NTP)	UDP	Y	All server system clocks must be synchronized via NTP.
Remote DB server	NTP server	123 (NTP)	UDP	Y	All server system clocks must be synchronized via NTP.
Reporter	DNS server	53 (DNS)	TCP/UDP	N[1]	Support DNS information requests.
Collector	DNS server	53 (DNS)	TCP/UDP	N[1]	Support DNS information requests.
Remote DB server	DNS server	53 (DNS)	TCP/UDP	N[1]	Support DNS information requests.
Reporter	Mail server	25 (SMTP)	TCP	N	Support reports and E-mail requests.
Reporter	SNMP Manager server	161, 162 (SNMP)	UDP	N	Support SNMP traps on request from an SNMP Manager.
Client browsers	Reporter	443 (HTTPS)	TCP	Y	The RUEI user interface is accessible over HTTPS.

[1] Optional, but *strongly* recommended.

1.8 Client Requirements

The workstations that will access the RUEI user interface must have one of the following browsers installed:

- Mozilla Firefox 3 or 4.
- Internet Explorer 6 SP2.
- Internet Explorer 7 or 8.

Note that JavaScript must be enabled. No other browser plug-ins are required.

In addition, the workstation should have a screen resolution of 1024 * 768 (or higher).

Important: Ensure that any pop-up blocker within the browser has been disabled.

AJAX Support

RUEI uses AJAX to enhance its user interaction. Internet Explorer relies on the MSXML control to facilitate AJAX. The AJAX dependencies can trigger a security warning when using strict security settings.

Internet Explorer 6 does not properly support transparent images in the PNG format. RUEI uses a well know fix (AlphaImageLoader) for this problem which relies on DirectX. If you are experiencing browser crashes with IE 6, you may need to update your version of DirectX. The PNG fix can trigger a security warning when using strict security settings.

2

Installing the RUEI Software

This chapter describes the procedure and prerequisites for installing the Apache Web server and RUEI software. The procedure for upgrading an existing RUEI 6.*x* installation to release 11.1 is described in Chapter 3, "Upgrading to RUEI 11.1". The post-installation configuration procedure is described in Chapter 4, "Configuring RUEI".

2.1 Prerequisites

This section describes the steps that should be taken before starting to install the RUEI software. Ensure that all preconditions described in this section should be meet before proceeding with the installation process.

2.1.1 Planning the Software Installation Location

Depending on installation location of the database and the RUEI software, the necessary disk space needs to be carefully planned. During operating system installation, you will need this information at hand during the disk partitioning phase.

Table 2–1 shows the disk space requirements for the RUEI installation components.

Table 2–1 Required Disk Space Specifications

Partition	Minimum Required Disk Space (GB)	Component
ORACLE_BASE (default `/u01/app/oracle`)[1]	300	Database server
RUEI_HOME (default `/opt/ruei`)	1	Reporter, Collector
RUEI_DATA (default `/var/opt/ruei/`)	100	Reporter, Collector

[1] This is the example location of the database used throughout this guide.

This means that for a stand-alone RUEI server installation, a minimum of 400 GB is required. In the case of a high-traffic implementation, involving a dedicated remote Collector, a minimum of 200 GB of disk space is recommended for `/var/opt/ruei` (RUEI_DATA).

Important: The Reporter and database servers require high performance data storage. RAID-10 or RAID-5 (or equivalent) storage configurations with high performance disks are *strongly* recommended.

2.1.2 Configuring the Network Interface

1. Ensure that a static IP address is assigned to the interface used to access the RUEI Web interface. In addition, the assigned IP address and host name should be configured in the `/etc/hosts` file. If necessary, ensure that all Reporter and Collector systems are correctly defined in the DNS system.
2. Ensure that the network interface(s) used for network packet monitoring are administratively *up*, but *without* an IP address.

> **Important:** Make the network interface *up* status permanent (after a reboot) by setting the ONBOOT parameter of the capturing interfaces to *yes*. The network interfaces configuration can be found in `/etc/sysconfig/networking/devices/ifcfg-eth`*X* (where *X* represents the necessary network interface). Alternatively, use the graphical utility **system-config-network** to perform the above actions.

2.1.3 OS Security Configuration

When the system boots for the first time, a post-installation wizard appears, and allows you to finalize the operating system configuration settings. Ensure that:

1. Ensure that the RUEI firewall rules shown in Table 1–7 are correctly configured.
2. Security Enhanced Linux (SELinux) is disabled. This is necessary for the correct operation of RUEI. Note that changing the SELinux setting requires rebooting the system so that the entire system can be relabeled.
3. For security reasons, it is *strongly* recommended you check the **Encrypt System** check box during operating system installation so that all sensitive data is stored in a secure manner. A passphase is required during booting the system.

2.1.4 Verify NTP Daemon Operation

Ensure that the date and time settings are correctly specified. The use of NTP is *strongly* recommended, and is required in a split-server deployment. In addition, all time zones specified for Reporter and Collector systems *must* be identical.

Because the NTP daemon is a critical component of RUEI, especially in a split Reporter-Collector configuration, it is recommended that you verify that it is activated in at least run level 5 during boot. Use the following commands:

```
chkconfig --list | grep ntp
ntpd     0:off   1:off   2:off   3:off   4:off   5:off   6:off
chkconfig ntpd on
chkconfig --list | grep ntp
ntpd     0:off   1:off   2:on    3:on    4:on    5:on    6:off
/etc/init.d/ntpd start
Starting ntpd:                                        [  OK  ]
```

Note that if the NTP daemon is not already running, you can start it with the command

```
/etc/init.d/ntpd restart
```

The following sample output show when the NTP daemon is synchronized (indicated by an "*").

```
ntpq -pn
       remote           refid      st t when poll reach   delay   offset  jitter
```

```
==============================================================================
*194.171.167.130     .PPS.          1 u 994 1024 377     6.429   0.041   0.093
+80.85.129.25        130.235.20.3   3 u 725 1024 377     4.435   0.673   0.129
+82.94.235.106       135.81.191.59  2 u 678 1024 377     1.709   1.774   0.020
 127.127.1.0         .LOCL.        10 l   8   64 377     0.000   0.000   0.001
```

Important: In distributed environments, all time zones specified for Reporter and Collector systems *must* be identical.

2.1.5 Installing the RUEI Prerequisites

Note that the procedure described in this section is only required for a Reporter system.

1. The required packages are available from the Oracle Linux or RedHat Enterprise Linux distribution sets. Issue the following command to install all prerequisites for the Reporter:

```
rpm -Uhv httpd-2.2.3-*.el5.x86_64.rpm \
apr-1.2.7-11.*.x86_64.rpm \
apr-util-1.2.7-*.x86_64.rpm \
php-5.1.6-*.x86_64.rpm \
mod_ssl-2.2.3-*.el5.x86_64.rpm \
distcache-1.4.5-*.x86_64.rpm \
php-common-5.1.6-*.x86_64.rpm \
php-cli-5.1.6-*.x86_64.rpm \
php-mbstring-5.1.6-*.x86_64.rpm \
php-ldap-5.1.6-*.x86_64.rpm \
gmp-4.1.4-*.el5.x86_64.rpm \
postgresql-libs-8.1.11-*.el5_1.1.x86_64.rpm \
lm_sensors-2.10.7-*.el5.x86_64.rpm \
net-snmp-5.3.2.2-*.el5.x86_64.rpm \
net-snmp-utils-5.3.2.2-*.el5.x86_64.rpm \
perl-XML-Twig-3.26-*.fc6.noarch.rpm \
perl-XML-Parser-2.34-*.x86_64.rpm
```

2. Issue the following the commands to install all optional fonts. Alternatively, install the multi-byte character sets necessary to meet your NLS requirements.

```
rpm -Uhv fonts-*
```

2.1.6 Installing All Requirements Using a Yum Repository (Alternative)

As an alternative to manual installation, you can use a Yum repository to install the required RPMs. This requires a working Yum repository. For information on Yum repositories, see http://linux.duke.edu/projects/yum/. Install the necessary Oracle database packages using the following commands:

```
yum -y install gcc
yum -y install gcc-c++
yum -y install compat-libstdc++-33
yum -y install libstdc++-devel
yum -y install elfutils-libelf-devel
yum -y install glibc-devel
yum -y install libaio-devel
yum -y install sysstat
```

Install the necessary Reporter packages using the following commands:

```
yum -y install perl-URI
```

```
yum -y install perl-XML-Twig
yum -y install net-snmp-utils
yum -y install sendmail-cf
yum -y install httpd
yum -y install mod_ssl
yum -y install php
yum -y install php-mbstring
yum -y install php-ldap
yum -y install bitstream-vera-fonts
yum -y install librsvg2
yum -y install xorg-x11-xinit
yum -y install fonts-*
```

2.1.7 Oracle Database Installation

Download and install Oracle Database 11g EnterpriseF Edition from the Oracle database home page at the following location:

http://www.oracle.com/technology/software/products/database/index.html

The procedure for installing the Oracle database is fully described in the product documentation. It is *strongly* recommended that you download and review the appropriate *Oracle Database 11g Quick Installation Guide*. It is available from the Oracle Database Documentation Library.

2.2 Obtaining the RUEI Software

The RUEI software is available from the Oracle E-Delivery Web site (`http://edelivery.oracle.com`). Select the following media pack criteria:

- Oracle Enterprise Manager
- Linux x86-64

2.3 Unpacking the RUEI Software

Copy the downloaded RUEI zip file to `/root` directory on the server, and unzip it. Use the following commands:

```
cd /root
unzip package_name.zip
```

The following directories are created which contain the software needed to complete the RUEI installation:

- `/root/RUEI/111`
- `/root/RUEI/ZendOptimizer`
- `/root/RUEI/IC`
- `/root/RUEI/PHP`
- `/root/RUEI/Java`
- `/root/RUEI/extra`

2.4 Generic Installation Tasks

All steps described in this section must be performed regardless of your planned installation (that is, a Reporter with local database, a Reporter with remote database, or a Collector).

2.4.1 The RUEI Configuration File

The `/etc/ruei.conf` file specifies the settings used within your installation. Note that all components in your RUEI environment (such as the remote database and Collectors) require the same global `/etc/ruei.conf` configuration file. The settings shown in Table 2–2 are defined.

Table 2–2 RUEI Configuration Settings

Setting	Description	Value[1]
RUEI_HOME[2]	Home directory of the RUEI software.	`/opt/ruei`
RUEI_DATA[2]	Directory for RUEI data files.	`/var/opt/ruei`
RUEI_USER	The RUEI operating system user.	`moniforce`
RUEI_GROUP	The RUEI operating system group.	`moniforce`
RUEI_DB_INST[3]	The database instance name.	`ux`
RUEI_DB_USER[4]	The database user name.	`UXINSIGHT`
RUEI_DB_TNSNAME[5]	The database connect string.	`uxinsight`
RUEI_DB_TNSNAME_BI[4]	The export database connect string.	`uxinsight`

1 Be aware that all variables specified in this table are the values used throughout this guide, and can be modified as required.
2 The directory name cannot exceed 50 characters in length.
3 The database instance name cannot exceed 8 characters in length.
4 The database user name cannot exceed 30 characters in length.
5 The alias name cannot exceed 255 characters in length.

Failover Reporter Configuration Settings

Table 2–3 shows the settings that are used to configure a failover Reporter, and are only relevant to Reporter systems. See Chapter 7, "Configuring a Failover Reporter System" for information on the configuration procedure.

Table 2–3 RUEI Failover Reporter Configuration Settings

Setting	Description
RUEI_REP_FAILOVER_PRIMARY_IP	The primary Reporter IP address.
RUEI_REP_FAILOVER_STANDBY_IP	The secondary Reporter IP address.
RUEI_REP_FAILOVER_VIRTUAL_IP	The virtual Reporter IP address.
RUEI_REP_FAILOVER_VIRTUAL_DEV	The network interface used to connect to the virtual Reporter IP address.
RUEI_REP_FAILOVER_VIRUAL_MASK	The network mask of the virtual Reporter IP address.

Failover Collector Configuration Settings

Table 2–4 shows the settings that are used to configure a failover Collector, and are only relevant to Collector systems. See Chapter 8, "Configuring a Failover Collector System" for information on the configuration procedure.

Table 2–4 RUEI Failover Collector Configuration Settings

Settings	Description
RUEI_COL_FAILOVER_PRIMARY_IP	The primary Collector IP address.
RUEI_COL_FAILOVER_STANDBY_IP	The secondary Collector IP address.
RUEI_COL_FAILOVER_VIRTUAL_IP	The virtual Collector IP address.
RUEI_COL_FAILOVER_VIRTUAL_DEV	The network interface used to connect to the virtual Collector IP address.
RUEI_COL_FAILOVER_VIRTUAL_MASK	The network mask of the virtual Reporter IP address.

There is no need to change the settings for JAVA_HOME and INSTANTCLIENT_DIR if you intend to use the software contained on the RUEI distribution pack.

1. Create the `moniforce` group and user. The home directory of `moniforce` should be set to `/var/opt/ruei`, with read permissions for group members.

```
/usr/sbin/groupadd moniforce
/usr/sbin/useradd moniforce -g moniforce -d /var/opt/ruei
chmod -R 750 /var/opt/ruei
chown -R moniforce:moniforce /var/opt/ruei
```

2. An example of the configuration file is included in the RUEI distribution pack. Ensure the file is readable by the RUEI_USER user by issuing the following commands:

```
cp /root/RUEI/extra/ruei.conf /etc/
chmod 644 /etc/ruei.conf
chown moniforce:moniforce /etc/ruei.conf
```

In case of a remote database installation, the `ruei.conf` file needs to be identical with that of the Reporter system.

2.4.2 Installing Java

For both Reporter and Collector systems you need to install the Java Runtime Environment (JRE). Java is bundled within the RUEI distribution pack.

1. Issue the following commands:

```
cd /root/RUEI/Java
chmod +x ./jre-1_5_0_22-linux-amd64-rpm.bin
./jre-1_5_0_22-linux-amd64-rpm.bin
```

   Note you are prompted to accept the Java licence agreement. You cannot continue until you have done so.

2. This installs the necessary Java software in the directory `/usr/java/jre1.5.0_22`. To make the install directory version independent, create a more generic symlink using the following command:

```
ln -s /usr/java/jre1.5.0_22 /usr/java/jre
```

2.5 Remote Collector Installation

This section can be skipped for Reporter or remote database servers.

Logon to the Collector system as the `root` user, and do the following:

1. The RUEI file and directory locations are fixed. Therefore, it is necessary to use the exact directory name described below. Create the RUEI application root directory using the following command:

```
mkdir -p /opt/ruei
chmod 750 /opt/ruei
```

2. Change to the RUEI root directory and run the `ruei-install.sh` script using the following commands:

```
cd /root/RUEI/11.1
chmod +x ruei-install.sh ruei-check.sh
./ruei-install.sh collector
```

3. In addition to the actions described above, you need to configure the network interfaces. This is fully described in Section 2.7, "Configuring the Network Interface". Moreover, you also need to setup a password-less remote login from the Reporter system to the newly created Collector system. The necessary configuration steps are described in Section 2.12, "Configuring Reporter Communication (Split-Server Setup Only)".

2.6 Reporter Installation

This section describes the procedure for installing the required components for a Reporter system. These include the Apache Web server, the Oracle database Instant Client, and the Zend Optimizer.

2.6.1 Installing the Apache Web Server and PHP

This section describes the installation and configuration of the Apache Web server, and the components that use it.

2.6.1.1 PHP Configuration

1. Ensure that the Web server starts automatically after re-boot by issuing the following command:

```
/sbin/chkconfig httpd on
```

2. Edit the `/etc/sysconfig/httpd` file to include the following line at the bottom of the file:

```
source /etc/ruei.conf
```

3. Create the following settings in the `/etc/php.d/ruei.ini` file:

```
session.gc_maxlifetime = 14400
memory_limit = 96M
upload_max_filesize = 128M
post_max_size = 128M
```

2.6.1.2 Avoiding rsvg Warnings

RUEI uses rsvg for graph generation. In order to avoid warnings about a missing directory, create the empty `.gnome2` directory using the following command:

```
mkdir -p /var/www/.gnome2
```

2.6.2 Installing the Oracle Database Instant Client

Install the Oracle database Instant Client and SQLplus extension with the following commands as the `root` user:

```
cd /root/RUEI/IC
rpm -Uhv oracle-instantclient11.2-basic-*.rpm
rpm -Uhv oracle-instantclient11.2-sqlplus-*.rpm
```

2.6.3 Installing the php-oci8 Module

Install the `php-oci8` module (this is part of the RUEI distribution set) using the following commands:

```
cd /root/RUEI/PHP
rpm -Uhv php-oci8-11gR2-*
```

2.6.4 Installing the Zend Optimizer

Go to the directory containing the Zend Optimizer code, unpack the tar file, and run the Zend optimizer installer. Read the license agreement. You will not be able to proceed until you have accepted the license terms. Accept all default settings, and allow the installer to restart the Apache Web server. Issue the following commands:

```
cd /root/RUEI/ZendOptimizer
tar zxvf ZendOptimizer-3.3.3-linux-glibc23-x86_64.tar.gz
cd ZendOptimizer-3.3.3-linux-glibc23-x86_64
./install
```

Note: If you upgrade your system packages (for example, using Yum), this can overwrite changes you previously made to the `/etc/php.ini` file. Therefore, you should be prepared to re-install the Zend Optimizer. When doing so, ensure the Zend Optimizer installer indicates the location of the `php.ini` file as `/etc/php.ini` and not `/usr/local/Zend/etc/php.ini`.

Additional Information

It is recommended you move the Zend configuration lines created in the `/etc/php.ini` file to the RUEI-specific PHP configuration file `/etc/php.d/ruei.ini` to prevent PHP upgrade issues. If you performed a default installation of the Zend Optimizer, this involves moving the following lines:

```
[Zend]
zend_extension_manager.optimizer=/usr/local/Zend/lib/Optimizer-3.3.3
zend_extension_manager.optimizer_ts=/usr/local/Zend/lib/Optimizer_TS-3.3.3
zend_optimizer.version=3.3.3

zend_extension=/usr/local/Zend/lib/ZendExtensionManager.so
zend_extension_ts=/usr/local/Zend/lib/ZendExtensionManager_TS.so
```

2.6.5 Creating the RUEI Database Instance

The procedure described in this section should be skipped if you are installing a secondary (failover) Reporter system (see Chapter 7, "Configuring a Failover Reporter System"), and you should continue at Section 2.6.6, "Installation of the Reporter Software".

The RUEI database can reside either locally (that is, on the Reporter server) or on a remote database server. In this section you will create the database instance required for RUEI, and generate the "connection data" required for the Reporter to connect to this database instance. As an alternative for the database setup described in this chapter, you can follow the procedure described in Appendix A, "Generic Database Instance Setup".

You will need the following scripts to be present on the system where the database instance (RUEI_DB_INST) will be created:

- `ruei-prepare-db.sh`: creates the database instance, Oracle wallet, and database connect files.
- `ruei-check.sh`: this is a hardware and environment check utility, and is automatically invoked by `ruei-prepare-db.sh`. The script can also be used as a stand-alone troubleshooting utility. For a complete description of the script, refer to Appendix C, "The ruei-check.sh Script".

The four "connection data" files created during the procedure described in this section are as follows:

- `cwallet.sso`
- `ewallet.p12`
- `sqlnet.ora`
- `tnsnames.ora`

The RUEI configuration file (`/etc/ruei.conf`) also needs to be present on the database server and configured as described in Section 2.4.1, "The RUEI Configuration File".

Do the following:

1. Copy the `ruei-prepare-db.sh` and `ruei-check.sh` scripts to the server on which you intend to run the database instance, and make them executable for the `oracle` user. These scripts can be found in the RUEI distribution zip (`/root/RUEI/111`).
2. Review the settings in the `/etc/ruei.conf` file to match your needs as described in Section 2.4.1, "The RUEI Configuration File".
3. Logon to the database server as the `oracle` user on the database server, and set the ORACLE_HOME environment variable. You need to run the `ruei-prepare-db.sh` script as the `oracle` user. This script creates the RUEI_DB_INST database, but only after a number of hardware and software environment checks have been performed. The actual checks performed depend on the system type you are currently installing.

   The script prompts you for the RUEI database user password[1]. This enables the RUEI application to login to the database automatically. The script also creates the "connection data" files for you now.

   If you run the `ruei-prepare-db.sh` script for a combined Reporter/Database server, all files are placed automatically in the correct location[2]. In case of a remote

[1] The database password is also used as the Oracle wallet password. Both passwords must be between 8 and 30 characters in length, and contain both numbers and letters. For information on changing the Oracle wallet password, please consult the appropriate Oracle documentation.

[2] If you do not know the root password, you can select the "remote database" option, and manually extract the connection tar file. This is described in step 4.

database, a separate .tar file is generated, and you will need to perform the extra step 4.

Issue the following commands:

```
chmod +x ruei-prepare-db.sh ruei-check.sh
export ORACLE_HOME=/u01/app/oracle/product/11.1.0/db_1[3]
./ruei-prepare-db.sh
```

If you ran the above commands on a combined Reporter/Database server you can skip step 4 and proceed to step 5.

4. This step only applies when using a remote database.

   In the case of a Reporter system using a remote database, you will need to copy the generated /tmp/ruei-database-configuration.tar file in step 3 from the database server to the Reporter system. The /tmp/ruei-database-configuration.tar file must be extracted on the Reporter server in the directory /var/opt/ruei (RUEI_DATA). The permissions of the files need to be set so that the specified RUEI_USER (moniforce) can use them.

   Copy the generated .tar file, which holds connection data files to the Reporter system. Logon to the Reporter server and extract the .tar file using the following commands:

   ```
   cd /var/opt/ruei
   tar xvf path-to-tar-file/ruei/database-configuration.tar
   chown moniforce:moniforce cwallet.sso ewallet.p12 sqlnet.ora tnsnames.ora
   ```

5. Because logging of the database can consume a large amount of disk space, it is recommended that you install a clean-up script to avoid the usage of unnecessary disk space. Copy the (example) script to the oracle user directory and activate it via cron using the following commands:

   ```
   mkdir -p /home/oracle/bin
   cp /root/RUEI/extra/ruei-clean.sh /home/oracle/bin
   chmod +x /home/oracle/bin/ruei-clean.sh
   su - oracle -c 'echo "10 0 * * * /home/oracle/bin/ruei-clean.sh" | crontab'
   ```

2.6.6 Installation of the Reporter Software

1. The RUEI directory locations are flexible. Therefore, it is necessary to use the exact directory name described as configured in the /etc/ruei.conf file. Create the RUEI application root directory using the following command:

   ```
   mkdir -p /opt/ruei
   chmod 750 /opt/ruei
   ```

   Note: The specified RUEI_HOME and RUEI_DATA directories must have 750 permissions defined for them.

2. Make the apache and moniforce members of two additional groups using the following commands:

   ```
   /usr/sbin/usermod -aG moniforce apache
   /usr/sbin/usermod -aG uucp apache
   /usr/sbin/usermod -aG uucp moniforce
   ```

[3] This line requires customization based on your database version and installation path.

3. Go to the directory which holds the RUEI software, and install the RUEI packages. You can specify `reporter` or `collector` to the `ruei-install.sh` script depending on the required installation:

```
cd /root/RUEI/111
chmod +x ruei-install.sh
./ruei-install.sh reporter
```

4. Re-start the Apache Web server using the following command:

```
/sbin/service httpd restart
```

5. Verify that the RUEI software was correctly installed by issuing the following command:

```
./ruei-check.sh postinstall
```

6. This step should not be performed if you are installing a secondary (failover) Reporter system (see Chapter 7, "Configuring a Failover Reporter System"). You should continue at Section 2.7, "Configuring the Network Interface".

   As the `moniforce` user, set the RUEI `admin` user password to enable logging onto the RUEI interface with the following commands:

```
su - moniforce
set-admin-password
```

   You are prompted to enter and confirm the password.

Note: When defining the `admin` user password, bear the following in mind:

- The password must have at least eight characters, and contain at least one non-alphanumeric character (such as $, @, &, and !).
- The initial password must be changed within seven days.
- The user name and password are case sensitive.

2.7 Configuring the Network Interface

This section is only relevant to Reporter and Collector systems.

Make the monitoring network interface *up* status permanent (after a reboot) by setting the ONBOOT parameter of the capturing interfaces to *yes* in the interface configuration files. The network interfaces configuration can be found in `/etc/sysconfig/network-scripts/ifcfg-eth`*X* (where *X* represents the necessary network interface). Alternatively, use the graphical utility **system-config-network** to set the appropriate interfaces to "activate device when computer starts".

2.8 Enabling Multibyte Fonts (Optional, but Recommended)

This section is only relevant to the Reporter system.

For PDF generation with multibyte character content, additional fonts need to be enabled. These fonts need to be made available to Java. Use the following command to copy (or move) the RUEI-installed fonts to the appropriate Java directory:

```
cp RUEI_HOME/bi_publisher/fonts/* \
/usr/java/jre/lib/fonts/
```

2.9 Mail (MTA) Configuration (Optional, Reporter Only)

This section is only relevant to the Reporter system.

RUEI assumes a working local MTA for sending PDF reports and E-mail alerts. By default, Linux uses the Sendmail MTA. By default, Sendmail will deliver the E-mail directly to the destination MTA. If this behavior is not according to your needs or policies, sending mail via a SmartHost (relay) might be an alternative. To configure a SmartHost in Sendmail, do the following:

1. Install the Sendmail configuration utility by going to the directory containing the uploaded RPM and issuing the following command:

   ```
   rpm -Uhv sendmail-cf-8.13.8-*.el5.x86_64.rpm
   ```

2. Find the line which contains the Smart Host setting in `/etc/mail/sendmail.mc`. Modify the SMART_HOST setting to your needs. For example:

   ```
   define('SMART_HOST', 'my.example')dnl
   ```

3. Generate the new configuration into a new `sendmail.cf` by executing the following command:

   ```
   make -C /etc/mail
   ```

4. Restart Sendmail. For example:

   ```
   /etc/init.d/sendmail restart
   ```

> **Note:** Extensive information about the configuration of the Sendmail MTA is available at http://www.sendmail.org.

2.10 SNMP (Reporter Only)

You can download the RUEI MIB definition file through the Reporter interface. This definition file can be added to the SNMP manager. The procedure for downloading the MIB file is described in the *Oracle Real User Experience Insight User's Guide*.

2.11 Configuring Automatic Browser Redirection (Optional)

This section is only relevant to Reporter systems.

To have the browser automatically redirected to the correct RUEI path, create the file `/var/www/html/index.html` with the following content:

```
<head>
<meta http-equiv="REFRESH" content="0;URL=/ruei/">
</head>
```

2.12 Configuring Reporter Communication (Split-Server Setup Only)

This section is only relevant to a Reporter system with remote Collector(s).

A password-less SSH connection must be setup between the `Moniforce` user from the Reporter system to each Collector system. Do the following:

1. Logon to the Reporter server as `root`. Issue the following commands:

   ```
   su - moniforce
   ssh-keygen -P ""
   ```

   Press **Enter** to accept the defaults.

2. Logon as `root` to each of the Collector systems and become the `moniforce` user by issuing the following command:

   ```
   su - moniforce
   ```

3. Create the `.ssh` directory (if it does not already exist) for the `moniforce` user on each Collector system by issuing the following commands:

   ```
   mkdir ~/.ssh
   chmod 700 ~/.ssh
   ```

4. Copy the SSH key on the Reporter system to the required location on the Collector system by issuing the following commands:

   ```
   cd ~/.ssh
   ssh root@Reporter cat /var/opt/ruei/.ssh/id_rsa.pub >> authorized_keys
   ```

   (you will need to specify the Reporter system `root` password)

   ```
   chmod 600 authorized_keys
   ```

5. Check that it is now possible to execute a remote command (as `moniforce` user) on the Reporter system without using a password. For example:

   - Logon as `root` on the Reporter server.
   - Logon as `moniforce` user: `su - moniforce`.
   - Execute a remote pwd command: `ssh Collector pwd`.
   - Enter yes to the question "Are you sure you want to continue connecting (yes/no)?".
   - The command should return `/var/opt/ruei`.

6. The above steps must be performed for each Collector!

> **Note:** If the connection between the Reporter and the Collector(s) has not been correctly configured, you will receive an authorization error when you try to register the remote Collector.

2.13 Verifying Successful Installation of RUEI

On completion of the Initial Setup Wizard (described in Section 4.2, "Performing Initial RUEI Configuration"), you can verify your installation by selecting **System**, the **Status**. All system indicators should report OK. Note Status notification will indicate "Unknown" because no system alerts have yet been configured. This is fully described in the *Oracle Real User Experience Insight User's Guide*.

3

Upgrading to RUEI 11.1

This chapter describes the procedure for upgrading an existing RUEI 6.*x* installation to release 11.1. The post-installation configuration procedure is described in Chapter 4, "Configuring RUEI".

If the Linux DVD is not automatically mounted, use the following commands to mount it:

```
mkdir -p /mnt/dvd
mount /dev/dvd /mnt/dvd
```

> **Note:** In the rest of this chapter it is assumed that the Linux DVD is mounted on `/mnt/dvd`.

Troubleshooting Upgrade or Rollback Problems

The upgrade and rollback scripts log their actions in the files `/tmp/ruei-upgrade-x.log` and `/tmp/ruei-rollback-x.log`. If you encountered any problems during the upgrade or rollback, please attach the relevant file to any request to Customer Support.

3.1 XPath Support

As of version 11.1, support for the use of XPath queries has been extended to provide full XPath 1.0 functionality for content scanning. This has important implications when upgrading an existing RUEI installation.

The upgrade script reports all namespaces found in the current configuration. These *must* be explicitly defined upon completion of the upgrade process. Otherwise, your configuration will no longer work correctly.

In addition, be aware that XPath expressions executed against content that is not well-formed XHTML code can return different results than in previous versions. Therefore, it is *strongly* recommenced that you carefully review all XPath expressions used in your RUEI installation. For further information on XPath support, see the *Oracle Real User Experience Insight User's Guide*.

3.2 Upgrading From RUEI 6.*x* to 11.1

This section describes the procedure for upgrading from an existing RUEI 6.*x* installation to release 11.1.

Important: Before proceeding with the upgrade, make a backup of your configuration. Select **System**, then **Maintenance**, and then **Backup and restore**. The configuration backup is required in case of a rollback.

3.2.1 Upgrading Accelerator packages

As of version 6.5.1, all supported accelerators are automatically installed as part of the Reporter installation procedure. Note that the use of some accelerators requires additional Oracle product licenses. You should ensure that you are licensed to use a product before configuring suites based upon it. For further information, please consult your Oracle representative.

3.2.2 Upgrading the Reporter System

The Reporter upgrade procedure described in this section applies to both single server installations as well as dedicated Reporter systems.

Do the following:

1. Login to the Reporter as `root`. Within the `/root` directory, unzip the RUEI zip file, and go to the directory containing the application files. Use the following commands:

   ```
   cd /root
   unzip Vxxxx.zip
   ```

2. Stop all processing on the Reporter and Collector system(s) using the following commands:

   ```
   cd /root/RUEI/extra
   chmod +x ruei-upgrade-6.x-11.1.sh
   ./ruei-upgrade-6.x-11.1.sh stop_ruei
   ```

3. Note that if you are upgrading from version 6.5.1 or 6.5.2, you should not perform this step, but continue at step 8.

   Install the new Oracle Instant client by issuing the following commands:

   ```
   cd /root/RUEI/IC
   rpm -Uhv oracle-instantclient11.2-*
   ```

4. Install the new PHP OCI module by issuing the following commands:

   ```
   cd /root/RUEI/PHP
   rpm -Uhv php-oci8-11gR2-*
   ```

5. Update the logical links by issuing the following commands:

   ```
   ln -sf /usr/lib64/oracle/11.2/php-oci8/oci8.ini /etc/php.d/oci8.ini
   ln -sf /usr/lib64/oracle/11.2/php-oci8/oci8.so /usr/lib64/php/modules/oci8.so
   ```

   Note the use of the `force` (`-f`) option.

6. Update the `/etc/ruei.conf` configuration file to use the new Oracle Instant client. Replace the line

   ```
   export INSTANTCLIENT_DIR=/usr/lib/oracle/11.1/client64
   ```

   with the line

```
export INSTANTCLIENT_DIR=/usr/lib/oracle/11.2/client64
```

7. Restart the Apache Web server by issuing the following command:

   ```
   service httpd restart
   ```

8. Perform the necessary pre-upgrade actions by executing the following commands:

   ```
   cd /root/RUEI/extra
   ./ruei-upgrade-6.x-11.1.sh rpm_pre_install
   ```

9. Make the `ruei-prepare.sh` and `ruei-check.sh` scripts available to the Oracle user (for example, by extracting the RUEI distribution zip on the Oracle database) on the system where the database resides. Update the RUEI database instance by issuing the following commands as the Oracle user:

   ```
   cd /root/RUEI/111
   cp ruei-prepare-db.sh /home/oracle
   cp ruei-check.sh /home/oracle
   chmod +x /home/oracle/ruei-*.sh
   su - oracle
   export ORACLE_HOME=/u01/app/oracle/product/11.1.0/db_1[1]
   ./ruei-prepare-db.sh
   exit
   ```

   Upon completion, you should again be the `root` user.

10. For each required Collector system, perform the steps indicated in the following section. Upon completion, proceed to step 11.

11. Install the new versions of the RPMs using the following commands:

    ```
    cd /root/RUEI/111
    chmod +x ruei-install.sh
    ./ruei-install.sh *.rpm
    ```

12. Perform the necessary post-upgrade actions by executing the following commands:

    ```
    cd /root/RUEI/extra
    ./ruei-upgrade-6.x-11.1.sh rpm_post_install
    ```

13. This step should be performed *only* if you are upgrading from RUEI version 6.0.*x*. Otherwise, it should be skipped.

    Important: if you do not perform the action described in this step, the currently defined Error Page Replay (EPR) and Full Session Replay (FSR) settings are applied for *each* monitored application. Depending on the number of monitored applications, and your previous settings, the amount of required disk space can significantly increase. For example, if data retention was set to 50 GB, and five applications are monitored by a Collector, the Collector will reserve up to 50 GB per application upon upgrading to this version (that is, a total Collector disk space of 250 GB).

    If this would require too much disk space to be reserved on a Collector system, you can issue the following command to limit the total reserved disk space to its currently defined settings:

    ```
    ./ruei-upgrade-6.x-11.1.sh resize_replay_store
    ```

[1] This line requires customization based on your database version and installation path.

In this case, the total reserved disk space for each application becomes the current setting divided by the current number of applications. For example, if the current data retention setting was 100 GB, and there are currently 10 monitored applications, this would result in 10 GB of disk space being available for each application. Note that, if you choose to use the above command, it may result in the loss of existing (the oldest) replay data.

14. Restart processing using the following commands:

```
cd /root/RUEI/extra
./ruei-upgrade-6.x-11.1.sh reinitialize
./ruei-upgrade-6.x-11.1.sh start_ruei
```

Note: During and after the upgrade procedure, if error or information messages appear in the event log (select **System**, then **Status**, and then **Event log**), you should mark them as read after completing the upgrade procedure, and monitor whether new messages are reported. In the event of re-occurring error messages, you should contact Customer Support.

3.2.3 Upgrading the Remote Collector System(s)

For each required remote Collector system, login as `root`. Within the `/root` directory, unzip the RUEI zip file, go to the directory containing the application files, and install the new versions of the RPMs. Do the following:

1. Unzip the RUEI distribution package using the following commands:

```
cd /root
unzip Vxxxx.zip
```

2. Upgrade the Collector RPMs using the following commands:

```
cd /root/RUEI/111
chmod +x ruei-install.sh
./ruei-install.sh collector
```

3. This step should be performed *only* if you are upgrading from RUEI version 6.0.*x*. Otherwise, it should be skipped.

   Convert the Replay store by issuing the following commands:

```
cd /root/RUEI/extra
chmod +x ruei-upgrade-6.x-11.1.sh
./ruei-upgrade-6.x-11.1.sh convert_replay_store
```

Note: The script may fail if there is no replay data on the system, or if executed twice.

3.3 Rolling Back to Version 6.5.*x*

This section describes the procedure to rollback to version 6.5.*x* after upgrading to version 11.1. Note that the Collector included in the Reporter installation is automatically rolled back during the described procedure. However, remote Collector systems must be individually rolled back. The procedure to do this is described later in this section.

Important: Be aware that it may not be possible to restore your system to its exact state prior to upgrading. It is *strongly* recommended that you contact Customer Support before rolling back an upgrade.

1. Login to the Reporter system as `root`. Within the `/root` directory, unzip the RUEI 6.5.*x* distribution zip file, and go to the directory containing the application files. Use the following commands:

   ```
   cd /root
   unzip Vxxx.zip
   ```

2. Stop all processing on the Reporter system by issuing the following commands:

   ```
   cd /root/RUEI/extra
   ./ruei-rollback-11.1-6.5.x.sh stop_ruei
   ```

3. This step only applies to rollback to version 6.5.0. Remove all unused accelerator packages. Use the following command to list all installed accelerators:

   ```
   rpm -qa | grep ^ux-suites
   ```

   Use the following command to remove any appropriate accelerator:

   ```
   rpm -e ux-suites-name
   ```

   where *name* is the appropriate accelerator.

4. Execute the RPM pre-installation phase by issuing the following command:

   ```
   ./ruei-rollback-11.1-6.5.x.sh rpm_pre_install
   ```

5. Restore the previous RPMs by issuing the following commands:

   ```
   cd /root/RUEI/65
   chmod +x ruei-install.sh
   ./ruei-install.sh *.rpm
   ```

6. Execute the post-installation script by executing the following command:

   ```
   ./ruei-rollback-11.1-6.0.x.sh rpm_post_install
   ```

7. Rollback all required remote Collectors (using the procedure described in the next section). Upon completion, continue to step 8. If your installation does not make use of a remote Collector, proceed directly to step 8.

8. Restore the RUEI configuration backup you created prior to upgrading by selecting **System**, then **Maintenance**, then **Backup and restore**, and then select **Restore system from file**.

9. Restart processing by issuing the following commands:

   ```
   cd /root/RUEI/extra
   ./ruei-rollback-11.1-6.5.x.sh start_ruei
   ```

Rolling Back Remote Collector Systems

Do the following:

1. Login to the remote Collector system as `root`. Within the `/root` directory, unzip the 6.5.*x* distribution zip file, and go to the directory containing the application files. Issue the following commands:

```
cd /root
unzip Vxxx.zip
```

2. Restore the previous RPMs by issuing the following commands:

```
cd /root/RUEI/extra
chmod +x ruei-rollback-11.1-6.5.x.sh
cd /root/RUEI/65
chmod +x ruei-install.sh
./ruei-install.sh ux-collector-*.rpm
```

Upon completion for all required Collectors, return to step 8 above.

3.4 Rolling Back to Version 6.0.*x*

This section describes the procedure to rollback to version 6.0.*x* after upgrading to version 11.1. Note that the Collector included in the Reporter installation is automatically rolled back during the described procedure. However, remote Collector systems must be individually rolled back. The procedure to do this is described later in this section.

Important: Be aware that it may not be possible to restore your system to its exact state prior to upgrading. It is *strongly* recommended that you contact Customer Support before rolling back an upgrade.

---

1. Login to the Reporter system as `root`. Within the `/root` directory, unzip the RUEI 6.0.*x* distribution zip file, and go to the directory containing the application files. Use the following commands:

```
cd /root
unzip Vxxx.zip
```

Important: If your RUEI installation makes use of accelerator packages (such as Oracle E-Business Suite or Siebel), repeat the unzipping for all previously installed accelerator packages.

---

2. Stop all processing on the Reporter system by issuing the following commands:

```
cd /root/RUEI/extra
./ruei-rollback-11.1-6.0.x.sh stop_ruei
chmod +x ruei-rollback-11.1-6.0.x.sh
./ruei-rollback-11.1-6.0.x.sh convert_replay_store
```

3. Remove all unused accelerator packages. Use the following command to list all installed accelerators:

```
rpm -qa | grep ^ux-suites
```

Use the following command to remove any appropriate accelerator:

```
rpm -e ux-suites-name
```

where *name* is the appropriate accelerator.

4. Issue the following commands:

```
sqlplus system/<password>@uxinsight
```

```
SQL> alter tablespace USERS default nocompress;
```

5. Execute the RPM pre-installation phase by issuing the following command:

```
./ruei-rollback-11.1-6.5.x.sh rpm_pre_install
```

6. Restore the previous RPMs by issuing the following commands:

```
cd /root/RUEI/60
rpm -e ux-lang-zh_cn
chmod +x ruei-install.sh
./ruei-install.sh *.rpm
```

   Note that errors reported during this step can be safely ignored. They will be resolved upon completion of step 8.

7. Execute the post-installation script by executing the following command:

```
./ruei-rollback-11.1-6.0.x.sh rpm_post_install
```

8. Rollback all required remote Collectors (using the procedure described in the next section). Upon completion, continue to step 9. If your installation does not make use of a remote Collector, proceed directly to step 9.
9. Restore the RUEI configuration backup you created prior to upgrading by selecting **System**, then **Maintenance**, then **Backup and restore**, and then select **Restore system from file**.
10. Restart processing by issuing the following commands:

```
cd /root/RUEI/extra
./ruei-rollback-11.1-6.0.x.sh start_ruei
```

> **Note:** The `admin` password needs to be reset using the `set-admin-password` script after rolling back to version 6.0.*x*.

Rolling Back Remote Collector Systems

Do the following:

1. Login to the remote Collector system as `root`. Within the `/root` directory, unzip the 6.0.*x* distribution zip file, and go to the directory containing the application files. Issue the following commands:

```
cd /root
unzip Vxxx.zip
```

2. Restore the previous RPMs by issuing the following commands:

```
cd /root/RUEI/extra
chmod +x ruei-rollback-11.1-6.0.x.sh
./ruei-rollback-11.1-6.0.x.sh convert_replay_store
cd /root/RUEI/60
chmod +x ruei-install.sh
./ruei-install.sh ux-collector-*.rpm
```

Upon completion for all required Collectors, return to step 9 above.

4

Configuring RUEI

This chapter describes the procedure for initially configuring RUEI. This task is performed by the individual within your organization who has been assigned the role of RUEI Super Administrator (this is, the `admin` user). For more information about roles, see the *Oracle Real User Experience User's Guide*.

Important

It is *strongly* recommended that a network engineer within your organization validates collected network traffic after configuring RUEI. The procedure to do this is described in Appendix D, "Verifying Monitored Network Traffic".

4.1 Introduction

In order to get RUEI up and running, you will need to have prepared the server systems for RUEI, and installed the RUEI software. This is described in Chapter 2, "Installing the RUEI Software". After that, you are required to specify the installation type and mail setup (described in Section 4.2, "Performing Initial RUEI Configuration"), and then perform some post-installation configuration (described in Section 4.4, "Performing Post-Installation Configuration"). This is necessary in order to start reporting. It includes deciding how pages and users will be identified, and specifying the scope of monitoring in your network environment. Finally, you will need to define the system's initial users, as described in Section 4.4.6, "Authorizing Initial Users". Note that if you are installing a split-server configuration, you will need to configure each Collector system. This is described in Section 4.3, "Configuring a Collector System".

Caution: The configuration of RUEI should be discussed with someone with a detailed knowledge of your organization's network topology.

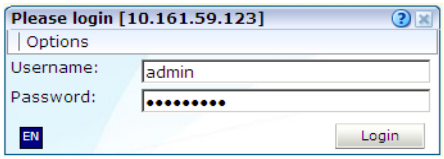
4.2 Performing Initial RUEI Configuration

In order for RUEI to start data monitoring and reporting, it must be configured with some information about your network infrastructure. Once completed, user traffic reporting is available. Note that this initial configuration can be changed later, as necessary. It is only intended to provide RUEI with sufficient information to start real-user monitoring and reporting.

To perform the initial RUEI configuration, do the following:

1. Start the Initial setup wizard by pointing your browser at `https://Reporter/ruei`. The dialog shown in Figure 4–1 appears:

Figure 4–1 Logon Dialog Box



Specify the `admin` user, and the password defined with the `set-admin-password` script (defined in Section 2.6.6, "Installation of the Reporter Software"). When ready, click **Login**. The dialog shown in Figure 4–2 appears.

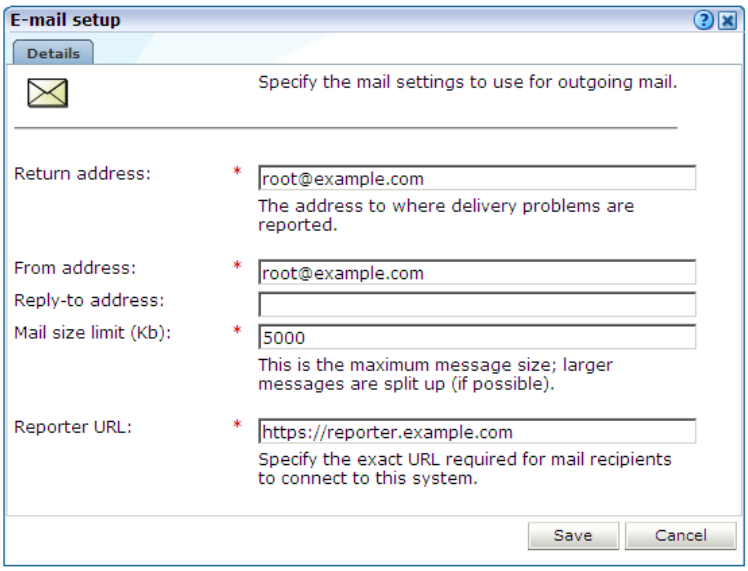
Note that the first time a user logs on, they receive a warning that the Web server was unable to verify the identify of the site's certificate. Depending on your security policies, you can either choose to accept this certificate permanently, temporarily for this session, or reject the certificate. Alternatively, you can purchase a certificate from a Certificate Authority (CA). You can also create an SSL certificate. More information at the following location:

`http://httpd.apache.org/docs/2.2/ssl/ssl_faq.html#realcert`

Figure 4–2 Initial Setup Wizard Dialog

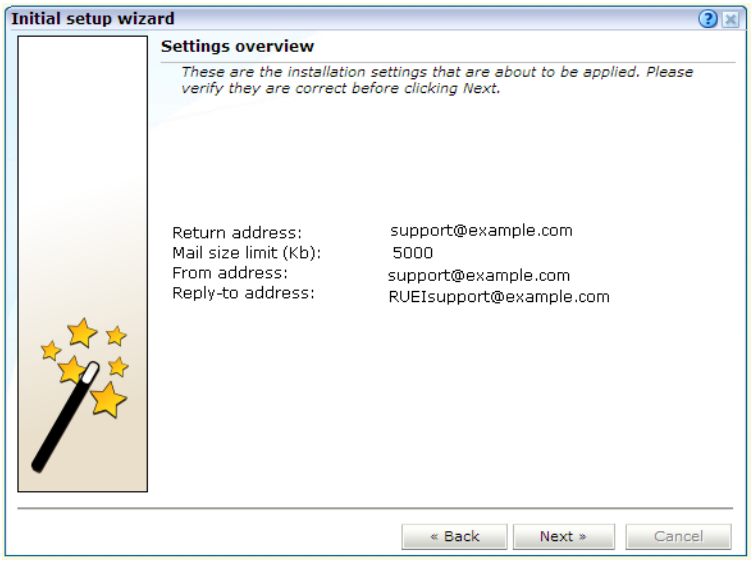
2. Click **Next** to proceed with configuration. The dialog shown in Figure 4–3 appears:

Figure 4–3 Mail Setup Dialog



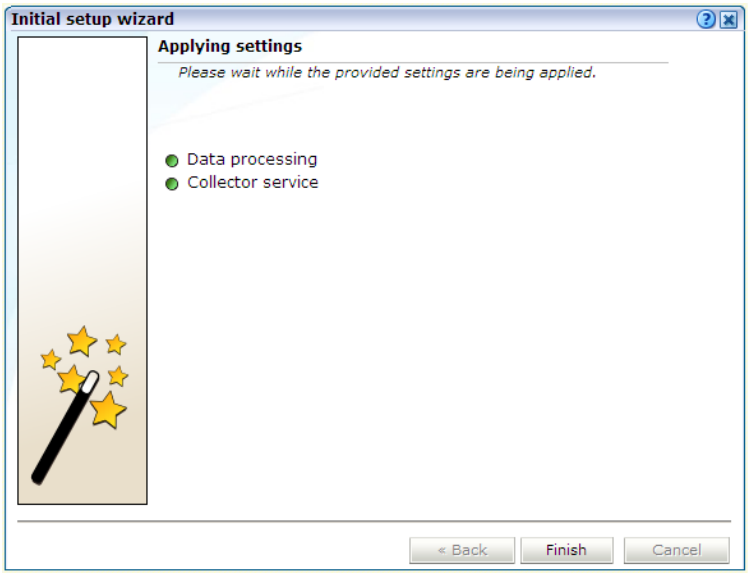
3. Specify the requested information. The e-mail information is used to configure RUEI's interface to your internal network, and will be used for reporting problems. When you have entered the required information, click **Next**. The dialog shown in Figure 4–4 appears.

Figure 4–4 Settings Overview Dialog



4. Check that the information specified in the settings overview is correct. You can use **Back** and **Next** to move between dialogs as necessary. When ready, click **Next**. The dialog shown in Figure 4–5 appears.

Figure 4–5 Applying Settings Dialog



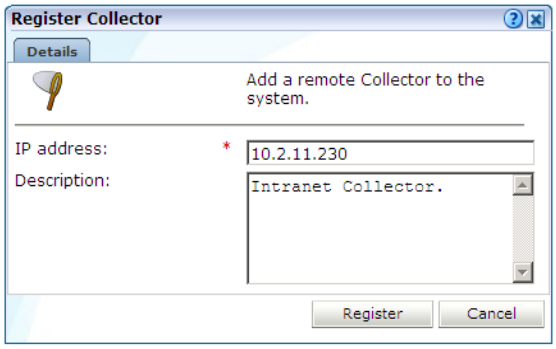
5. This dialog indicates how far the system has got in applying your specified settings. Typically, this process takes a maximum of 15 minutes. When finished, click **Finish** to close the dialog.

4.3 Configuring a Collector System

To register a Collector to a Reporter system, do the following:

1. Within the Reporter system, select **System**, then **Maintenance**, and then **Network data collectors**. The Network data collectors window appears.
2. Select **Configuration**, and then **Register remote Collector**. The Register Collector dialog shown in Figure 4–6 appears.

Figure 4–6 Register Collector Dialog



3. Enter the IP address of the Collector. Optionally, you can also specify a brief description of the attached Collector. When ready, click **Register**. On return to the Network data collectors window, the new Collector should be listed.

4.3.1 Resetting a Collector System

If for any reason you need to register a Collector system with a different Reporter system than earlier configured, do the following:

1. Logon to the Collector system as the `moniforce` user, and remove the Collector's currently defined Reporter assignment by issuing the following commands:

```
su - moniforce
appsensor delete wg
```

2. Follow the procedure described in Section 4.3, "Configuring a Collector System" to register the Collector with the required Reporter.

4.4 Performing Post-Installation Configuration

In order to start reporting, the RUEI needs certain information about the monitored network environment. It is important to understand that RUEI is designed to work within a wide range of network environments. Therefore, the configuration choices you make will affect the accuracy and usability of the reported data. It is strongly recommended that you carefully review the settings described in this section.

4.4.1 Specifying the Cookie Technology

Within RUEI, session information is based on cookies. Therefore, RUEI needs to know and understand the cookie technology (or technologies) your organization is using. The procedure to configure this is described in the *Oracle Real User Experience Insight User's Guide*. The structure of supported cookie technologies is also explained in the *Oracle Real User Experience Insight User's Guide*.

If cookie information is not available, user tracking is based on visitor IP address. This can lead to unreliable session information. For example, in the case of users behind a proxy server, all users coming from that network would be identified as the same user.

4.4.2 Adding/Uploading HTTPS SSL Keys

Uploading SSL keys to the system is extremely important if most of your HTTP traffic is based on SSL sessions. Without the SSL keys being available to the system, the Collector will not be able to decrypt the SSL session traffic. In these circumstances, further configuration of cookies, user identification, and application pages would make little sense. Ensure that you upload and activate your HTTPS SSL keys as early on as possible in the configuration process. The management of SSL keys is fully described in the *Oracle Real User Experience Insight User's Guide*.

4.4.3 Specifying How Users are Identified

Within RUEI, user identification is first based on the HTTP Authorization field. After that, it is derived from the supplied GET/POST argument within URLs. Therefore, if you are using arguments within URLs, the item within these used for user identification must be specified in order to provide reliable results. This is fully described in the *Oracle Real User Experience Insight User's Guide*.

4.4.4 Naming Pages

Page identification within RUEI is based on applications. Essentially, an application is a collection of Web pages. This is because pages on a Web site are typically bound to a particular application. For each page that the system detects, it uses the available application definitions to assign a name to it. Note that information about any pages that could not be identified using these definitions is discarded, and, therefore, not available through reports and the data browser. This is fully described in the *Oracle Real User Experience User's Guide*.

4.4.5 Specifying the Scope of Monitoring

Within RUEI, you control the scope of traffic monitoring by specifying which TCP ports the SYSTEM should monitor. Obviously, no information is available for non-monitored ports. In addition, you can restrict monitoring to specific servers and subnets. This is fully described in the *Oracle Real User Experience Insight User's Guide*.

4.4.6 Authorizing Initial Users

In order for users to start working with RUEI, you will need to authorize the required users. Only one user, `admin`, is available after installation. The procedure to set the initial `admin` user password is described in Section 2.6.6, "Installation of the Reporter Software". All other required users must be created and assigned the necessary roles and access permissions through the Reporter GUI. In particular, it is recommended that you create a dedicated Security Officer account to finalize the security-related configuration. User roles, creation and management are fully described in the *Oracle Real User Experience Insight User's Guide*.

Note that user names and passwords are case sensitive. For ease of entry, it is recommended that you do not include any diacritic characters, such as umlauts, within passwords.

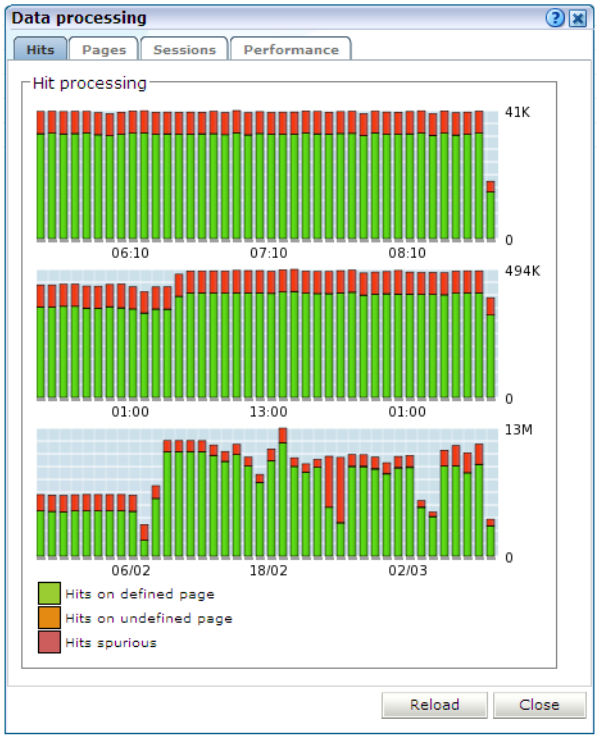
4.5 Verifying and Evaluating Your Configuration

To ensure the quality and quantity of data being collected and analyzed by your RUEI system, it is strongly advised that you verify the system's configuration using some core metrics. These are described in the following sections.

4.5.1 Viewing a Traffic Summary

You can open an overview of the monitored network traffic by selecting **System**, then **Status**, and then **Data processing**. This provides you with immediate information about hits, pages, and session processing, as well as the system load. An example is shown in Figure 4–7:

Figure 4–7 Data Processing Dialog



The precise number of percentage of identified sessions, page views, and hits relies heavily on your exact configuration. If you intend to measure all traffic, it is recommended that at least 80% of sessions, page views, and hits are reported as "identified". It is also recommended that you regularly review the reported numbers and percentages to ensure the quality and quantity of reported data.

Important: After initial configuration of cookies, user identification, and application page structure, the system will take at least 5 - 10 minutes before the **Sessions**/**Hits**/**Page views** tabs are updated with green bars. If, after 20 - 30 minutes after initial configuration, there are no green bars showing on any of the tabs, please review your initial RUEI configuration. If the bars do not indicate any activity at all, please review your system's network card configuration as outlined in Section 1.7, "Network Requirements"

4.5.2 Confirming Data Collection

At this point, RUEI should be collecting data from each of its associated Collectors. You can easily check the status of these Collectors by selecting **System**, then **Status**, and then **Collector status**. This opens the Network data collectors window. This is fully described in the *Oracle Real User Experience Insight User's Guide*.

It is important to understand that the data being collected by Collector system(s) is offered to the RUEI data processing module for further analysis. If no data is collected, there is no means by which it can be processed.

5

Installing and Configuring SSO Authentication Integration

This chapter describes the procedure for installing and configuring the Oracle HTTP server. This is an optional part of the RUEI installation process, and is only required if you intend to use the Oracle Single Sign-On (SSO) service to authenticate RUEI users. Note that the Oracle SSO service must be fully installed and configured before it can be used for RUEI user authentication.

The procedure to configure the Reporter system for Oracle SSO user authentication is described in the *Oracle Real User Experience Insight User's Guide*. Note that RUEI must be fully installed before it can be configured for Oracle SSO user authentication.

5.1 Turning off the Default Web Server

The Oracle SSO server uses its own Web server in order to prevent conflicts with the currently installed Web server. Therefore, the currently installed Web server needs to be turned off by issuing the following commands:

```
/sbin/service httpd stop
/sbin/chkconfig --del httpd
```

Note: It is recommended that you do *not* un-install the default Linux Apache Web server because this would also un-install the PHP module.

5.2 Reporter System Without Local Database

The procedure described in this section should only be followed if you are installing and configuring the oracle HTTP server for a Reporter that does not a local database. Otherwise, the procedure described in Section 5.3, "Reporter System With Local Database" should be followed.

5.2.1 Creating the Oracle User

This section is only relevant for RUEI installations configured to use a remote database. In this case, the `oracle` user does not yet exist, and so must be created by issuing the following commands:

```
/usr/sbin/groupadd oinstall oinstall
/usr/sbin/useradd -g oinstall oracle
```

5.2.2 Setting up the Oracle HTTP Server Environment

This section is only relevant for RUEI installations configured to a remote database. In this case, the following lines need to be added to the `/etc/security/limits.conf` file:

```
oracle soft nofile 16384
oracle hard nofile 65536
```

5.2.3 Creating the Installation Directory

Issue the following commands:

```
mkdir -p /u01/app/oracle
chown -R oracle:oinstall /u01/app/oracle
```

5.3 Reporter System With Local Database

The procedure described in this section should only be followed if you are installing and configuring the oracle HTTP server for a Reporter that with a local database. Otherwise, the procedure described in Section 5.2, "Reporter System Without Local Database" should be followed.

Increase the number of open files limit. Edit the following line in the `/etc/security/limits.conf` file:

```
oracle soft nofile 16384
```

5.4 Installing Oracle HTTP Server

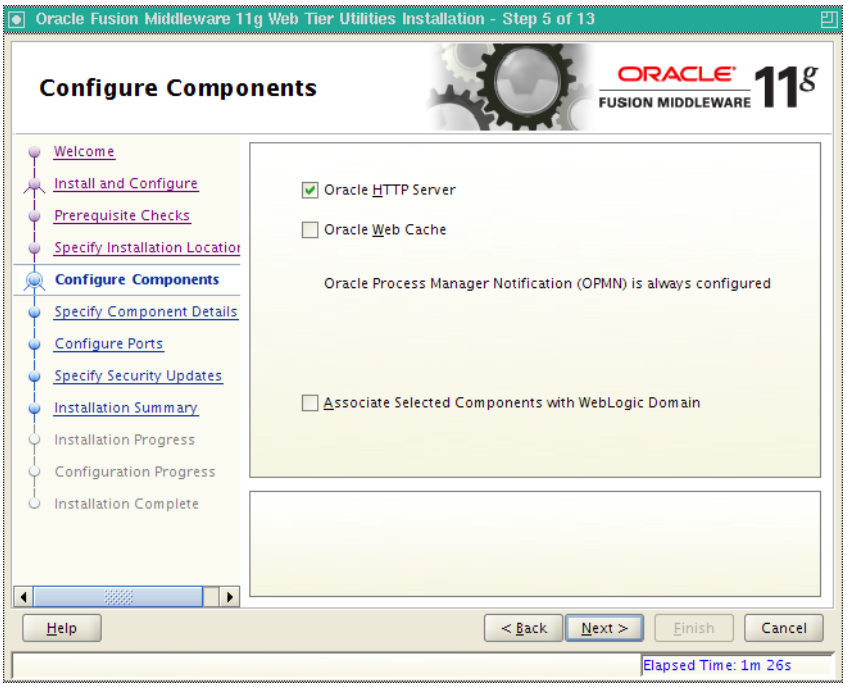
Do the following:

1. Login to the Reporter server as the `oracle` user, and unzip the Oracle HTTP Server zip file. Ensure that you have you display environment setup correctly (reference or copy a piece about setting up the X server in other part of the install manual). The installation of Oracle HTTP server needs to be performed as the `oracle` user (only some parts in this chapter require `root` privileges).

   ```
   unzip ofm_webtier_11.1.1.1.0_64_disk1_10f1.zip
   cd webtier/Disk1
   export ORACLE_BASE=/u01/app/oracle
   ./runInstaller
   ```

2. As the installation script runs, you should accept all default values, except for step 5. Here, you must uncheck the two check boxes **Oracle Web Cache** and **Associate selected components with weblogic domain** shown in Figure 5–1.

Figure 5–1 Configure Components Dialog



3. After exiting the installation script, set the following environment variables:

```
export ORACLE_HOME=$ORACLE_BASE/product/11.1.1/as_1
export ORACLE_INSTANCE=$ORACLE_HOME/instances/instance1
```

4. Stop the Oracle HTTP server and Oracle Process Manager Notification (OPMN) using the following command:

```
$ORACLE_INSTANCE/bin/opmnctl stopall
```

5. Edit the `$ORACLE_HOME/ohs/bin/apachectl` file to fix the bug 8327898. Change the `prefork` as follows:

```
case ${MPM} in

async   ) _httpd="httpd.async" ;;
prefork  ) _httpd="httpd.prefork" ;;
*        ) _httpd="httpd.worker" ;;
esac
```

   Note more information about this bug is available at https://support.oracle.com/CSP/ui/flash.html.

6. Edit the `$ORACLE_INSTANCE/config/OPMN/opmn/opmn.xml` file to use the `httpd.prefork` in order so that the PHP module can be loaded. In addition, set the following variables from the `/etc/ruei.conf` configuration file:

```
<environment>
      <variable id="TEMP" value="/tmp"/>
      <variable id="TMP" value="/tmp"/>
      <variable id="OHSMPM" value="prefork"/>
      <variable id="TNS_ADMIN" value="/var/opt/ruei"/>
      <variable id="RUEI_DB_TNSNAME" value="uxinsight"/>
      <variable id="RUEI_DB_USER" value="uxinsight"/>
      <variable id="RUEI_HOME" value="/opt/ruei"/>
```

```
      <variable id="RUEI_DATA" value="/var/opt/ruei"/>
      <variable id="JAVA_HOME" value="/usr/java/jre">
</environment>
```

7. Logon as the `root` user, and change the permissions for the `.apachectl` file so that the Oracle HTTP server can run as the Apache user. Issue the following commands:

   ```
   chown root $ORACLE_HOME/ohs/bin/.apachectl
   chmod 6750 $ORACLE_HOME/ohs/bin/.apachectl
   ```

8. Add `apache` to the `oinstall` group using the following command:

   ```
   usermod -aG oinstall apache
   ```

9. Logon as the `oracle` user and edit the `$ORACLE_INSTANCE/config/OHS/ohs1/httpd.conf` file for the Oracle HTTP server to run as the Apache user. Edit the following lines:

   ```
   User apache
   Group apache
   ```

10. Create the `$ORACLE_INSTANCE/config/OHS/ohs1/moduleconf/php5.conf` file, and edit it to contain the following:

    ```
    LoadModule php5_module "/usr/lib64/httpd/modules/libphp5.so"
    AddHandler php5-script php
    AddType    text/html   php
    ```

11. Copy the `/etc/httpd/conf.d/uxinsight.conf` file and make it available to the Oracle HTTP server using the following command:

    ```
    cp /etc/httpd/conf.d/uxinsight.conf $ORACLE_INSTANCE/config/OHS/ohs1/moduleconf
    ```

12. Start Oracle Process Manager Notification (OPMN) and the Oracle HTTP server using the following command:

    ```
    oracle$ $ORACLE_INSTANCE/bin/opmnctl startall
    ```

13. Stop the HTTP server using the following command:

    ```
    $ORACLE_INSTANCE/bin/opmnctl stopproc ias-component=ohs1
    ```

14. In order to have RUEI running on the default HTTPS port, edit the `$ORACLE_INSTANCE/config/OHS/ohs1/ssl.conf` file, and change the line with the `Listen` directive to the following:

    ```
    Listen 443
    ```

    In addition, edit the `VirtualHost` definition as follows:

    ```
    <VirtualHost *:443>
    ```

15. Start the Oracle HTTP server using the following command:

    ```
    $ORACLE_INSTANCE/bin/opmnctl startproc ias-component=ohs1
    ```

16. Stop the Oracle HTTP server using the following command:

    ```
    oracle$ $ORACLE_INSTANCE/bin/opmnctl stopproc ias-component=ohs1
    ```

17. Create the `$ORACLE_INSTANCE/config/OHS/ohs1/moduleconf/mod_osso.conf` file:

```
LoadModule osso_module "${ORACLE_HOME}/ohs/modules/mod_osso.so"

<IfModule osso_module>
   OssoConfigFile /u01/app/oracle/product/11.1.1/as_
1/instances/instance1/config/OHS/ohs1/osso.conf
   OssoIpCheck off
   OssoIdleTimeout off
</IfModule>
```

18. Copy the `osso.conf` file that you received after registering RUEI with the Oracle SSO server to the `$ORACLE_INSTANCE/config/OHS/ohs1` directory.
19. Start the Oracle HTTP server using the following command:

```
$ORACLE_INSTANCE/bin/opmnctl startproc ias-component=ohs1
```

5.5 Verifying the Oracle HTTP Server Configuration

You can test the Oracle HTTP server for integration with RUEI by directing your browser to `https://`***`Reporter`***`/ruei`. When you select **System**, then **User management**, the **Configure SSO connection** option should be enabled.

For information about enabling Oracle SSO user authentication within RUEI, see the *Oracle Real User Experience User's Guide*.

6

Configuring the Oracle Access Manager (OAM)

This chapter describes the procedure for configuring the Oracle Access Manager (OAM) for identifying user IDs within OAM-based traffic. The procedure described assumes that you already have a working OAM server. Note that the procedure may need to be modified to reflect the specific configuration of your OAM server.

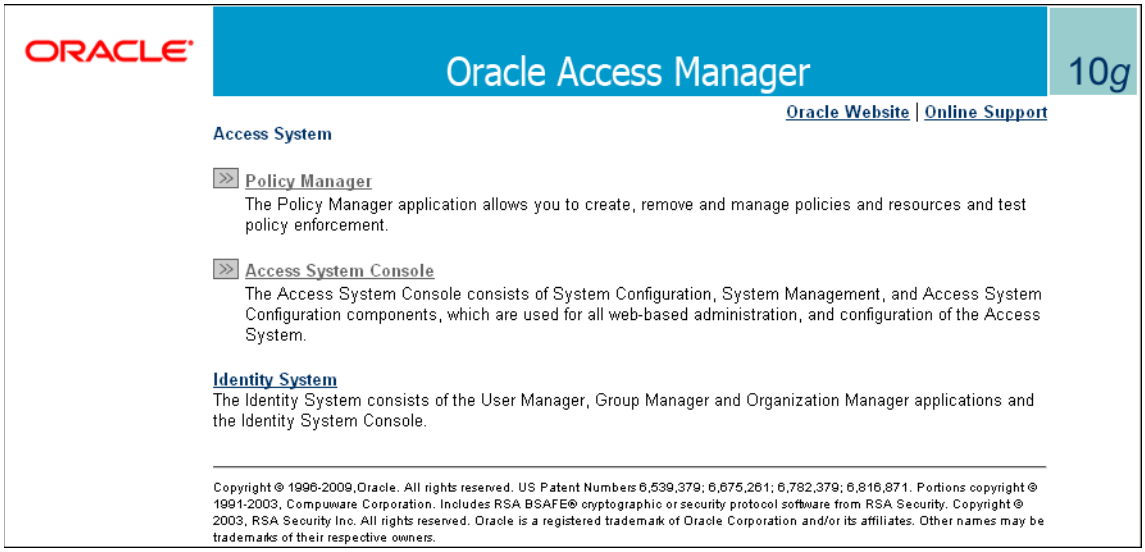
Be aware that RUEI only supports the monitoring of OAM version 10.1.4.*x* (or higher), and that the load placed on the OAM infrastructure by RUEI is the equivalent of the monitored Web server.

6.1 Creating an OAM Access Gate for RUEI

Do the following:

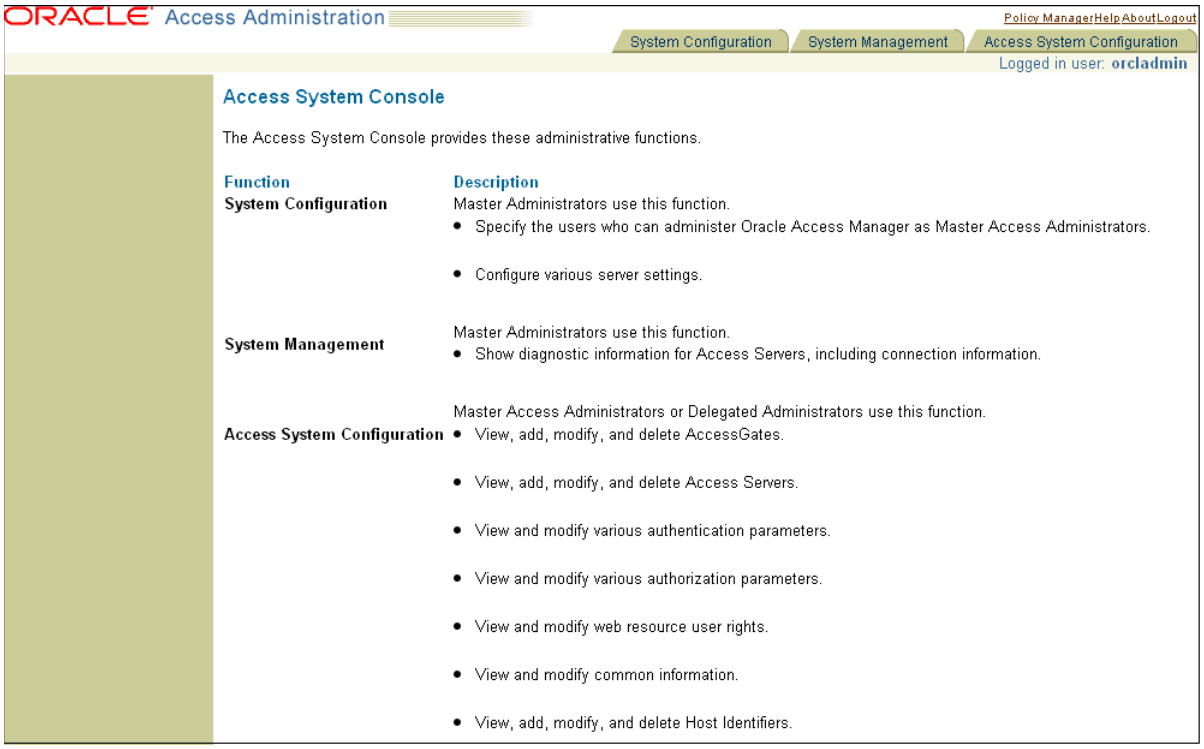
1. Direct your Web browser to The Access Manager server interface. If you are unsure of the required URL, you should contact the OAM system administrator. The page shown in Figure 6–1 appears.

Figure 6–1 OAM Server Interface.



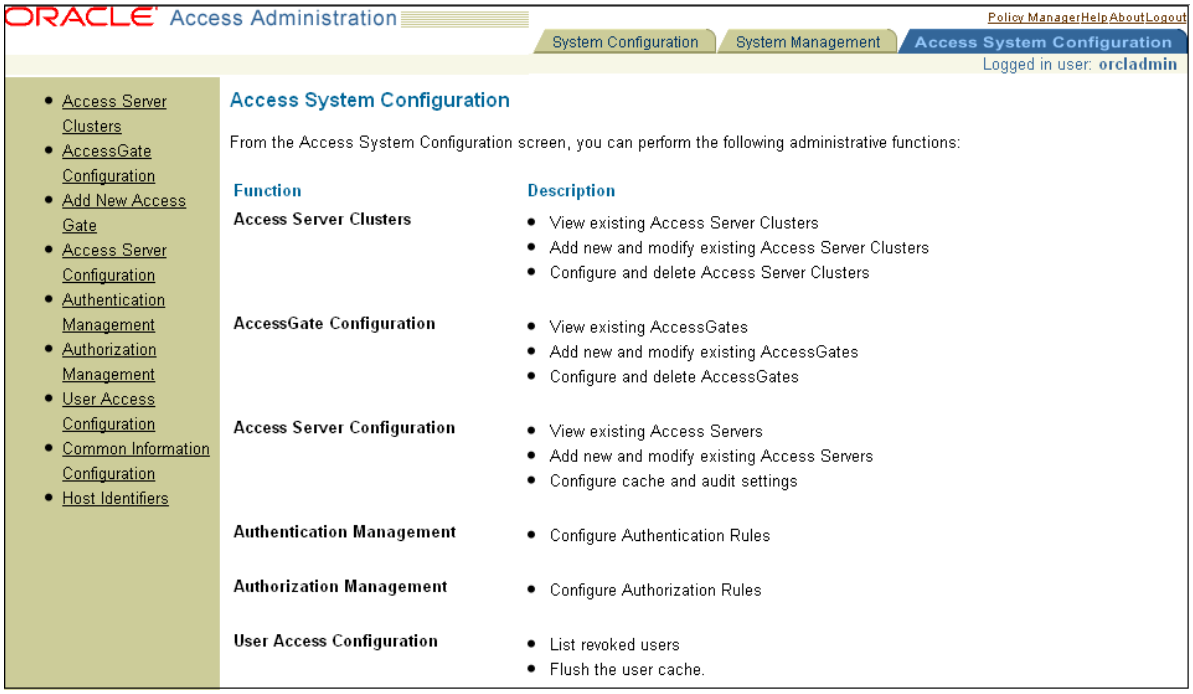
2. Click the **Access System Console** link. The page shown in Figure 6–2 appears.

Figure 6–2 OAM Access Administration.



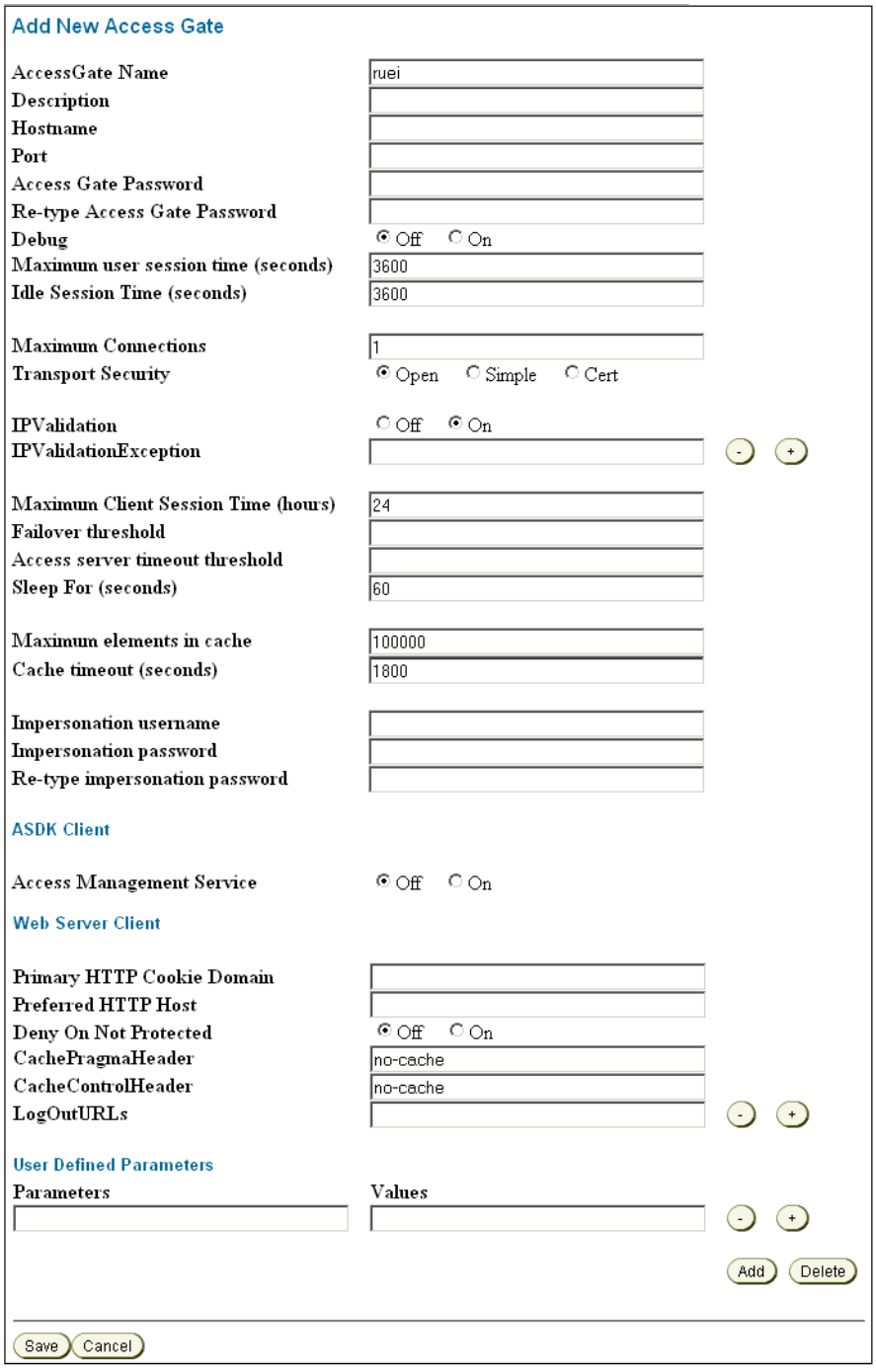
3. Click the **Access System Configuration** tab. The page shown in Figure 6–3 appears.

Figure 6–3 OAM Access System Configuration Page.



4. Click the **Add New Access Gate** option on the left-hand side of the page. The page shown in appears.

Figure 6–4 Add New Access Gate Page



5. Provide the following information:

   - **Access Gate Name**: specify a unique ID for the new access gate. For example, `ruei`.
   - **Hostname**: specify the hostname of the RUEI reporter system.

- **Port**: specify the port RUEI should monitor for OAM-based traffic. This should be port 443.
- **Access Gate Password**: specify the password that should be used to authorize the RUEI Reporter system to access the OAM server.
- **Re-Type Access Gate Password**: confirm the authorization password.
- **Preferred HTTP Host**: specify `SERVER_NAME`.

Note that the remaining fields can left blank or with default values specified.

When ready, click **Save**.

6. Click the **List Access Servers** command button to connect the newly created access gate with the required access server. Select the required access server from the displayed list and, when ready, click **Add**.

   Note that if no access server is listed, Click **Add** and add the new access gate to the default access server.

6.2 Downloading and Installing the Access Gate Software

Do the following:

1. Download and install the GCC libraries. These can be obtained from either your operating system vendor or `http://gcc.gnu.org`. Note that a description of the contents of the Oracle Access Manager 10.1.4 third-party integration disks is available at the following location:

   `http://www.oracle.com/technetwork/middleware/ias/downloads/10gr3-webgates-integrations-readme-154689.pdf`

2. Download the 64-bit OAM Access Server SDK from the following location:

   `http://download.oracle.com/otn/linux/ias/101401/oam_int_linux_v7_cd3.zip`

3. Extract, unzip, and copy the GCC libraries using the following commands:

```
cat as_linux_x86_gcc_runtime_lib_access_manager_101401.cpio | cpio -idmv
unzip Oracle_Access_Manager10_1_4_0_1_linux_GCClib.zip
cp lib* /usr/local/lib/
```

6.3 Configuring the Access Gate Software on the RUEI Server

Do the following:

1. Unzip the OAM Access Server SDK distribution set, and run the installer, by issuing the following commands:

```
unzip oam_int_linux_v7_cd3.zip
./Oracle_Access_Manager10_1_4_2_5_linux64_AccessServerSDK
```

   By default, the OAM Access Server SDK is installed in `/opt/netpoint/AccessServerSDK/`.

Note: The user specified while running the Access Gate SDK installation wizard should be the same as that specified for RUEI_USER in the `ruei.conf` file (see Table 2–2).

---

2. Create a trust between RUEI and the access server by creating XML files using the `configureAccessGate` utility. Issue the following commands:

```
cd  /opt/netpoint/AccessServerSDK/oblix/tools/configureAccessGate
./configureAccessGate -i /opt/netpoint/AccessServerSDK/ -t AccessGate
```

3. As the utility runs, specify the following information based on the configuration of the access gate you created earlier:

```
Please enter the Mode in which you want the AccessGate to run : 1(Open)
2(Simple) 3(Cert) : 1

Please enter the AccessGate ID : short_name

Please enter the Password for this AccessGate :

Please enter the Access Server ID : accessSrv1

Please enter the Access Server Host Machine Name : fully_qualified_hostname

Please enter the Access Server Port : 6021

Preparing to connect to Access Server.  Please wait.

AccessGate installed Successfully.

Press enter key to continue ...
```

   Where *short_name* specifies the Access Gate ID, and *fully_qualified_hostname* is the Access server system host name.

4. At this point, the RUEI Reporter system is connected to the OAM access server. Update the `OBACCESS_INSTALL_DIR` variable in the `/etc/ruei.conf` configuration file to reflect the installation path of the Access Server SDK. In the case of the default installation path, the required line would be as follows:

```
export OBACCESS_INSTALL_DIR=/opt/netpoint/AccessServerSDK/
```

5. Re-start RUEI processing by selecting **System**, then **Maintenance**, then **System reset**, and select the **Restart system processing** option. When ready, click **Next**. When prompted, confirm the restart.

6.4 Configuring the Required Session Traffic Definitions

In order to enable correct tracking of OAM-based sessions, you need to specify the following configuration information within RUEI:

1. Configure all required applications for user identification based on OAM. To do so, click the **User ID** tab within each required application overview, and then click **Add new source**. Within the **Source type** menu, select the "Oracle Access Manager" option. When ready, click **Save**.

2. Select **Configuration**, then **Applications**, and then **Session tracking**. Ensure that the "Oracle Access Manager" is included in the list of cookie technologies configured for your RUEI installation. By default, this uses the cookie name `ObSSOcookie`.

Note: In order for OAM-based traffic to be correctly reported, the masking of the OAM cookie must be configured as "Plain" within the Cookie masking facility (Select **Configuration**, then **Security**, then **Masking**, and then **Cookie masking**).

Note that until an OAM request has been processed by the RUEI system access gate, the following message is shown when requesting the access servers listing for your access gate:

```
Not Responding
AM service status mismatch
```

7

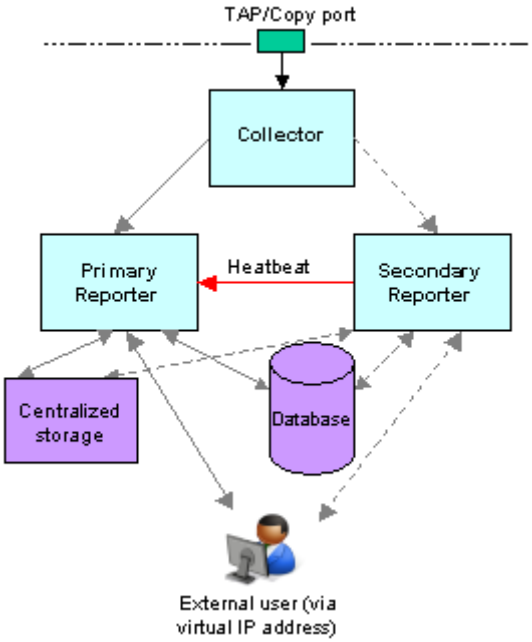
Configuring a Failover Reporter System

This chapter describes the procedure for configuring a failover Reporter system that will immediately take over processing of network traffic in the event that the primary Reporter system becomes unavailable. Note that the described procedure assumes that the primary Reporter system has been installed, configured, and is fully operational. Note that the installation procedure for a primary Reporter is identical to that of a standalone Reporter. The procedure to configure a failover Collector system is described in Chapter 8, "Configuring a Failover Collector System".

7.1 Introduction

The configuration of a secondary (or failover) Reporter system offers the advantage that it can seamlessly take over processing of monitored traffic in the event that the primary Reporter system becomes unavailable. In this way, a high level of operational reliability is achieved. The configuration of a failover Reporter system is shown in Figure 7–1.

Figure 7–1 Failover Reporter Configuration



At server level, a crossover cable connects the primary and secondary Reporter systems. As long as a regular "heartbeat" continues between the primary and secondary servers, the secondary server will not initiate processing of traffic. However, the secondary server will immediately take over the processing task of the primary server as soon as it detects an alteration in the "heartbeat" of the primary server. This process is referred to as failover.

Note that failback (that is, the process of restoring the RUEI installation to its original state, must be performed manually. The procedure is described in Section 7.5, "Instigating Reporter Failback".

Prerequisites

In order to configure a failover Reporter installation, the following conditions must be met:

- The primary and secondary Reporter systems must be directly connected via a crossover cable. In addition, both systems must also be connected to a local or public network to in order to connect to the remote Collector and database systems.
- The database and Collector instances used by the RUEI installation must both be remote.
- The primary and secondary Reporter systems must share the same storage (such as SAN or NFS). In particular, the `RUEI_DATA/processor/data` and `RUEI_DATA/processor/data/sslkeys` directories.

7.2 Preparing the Primary Reporter

Make the `RUEI_DATA/processor/data` and `RUEI_DATA/processor/sslkeys` directories available on a shared storage location.

1. Stop all processing on the primary Reporter system by issuing the following command as the *`RUEI_USER`* user:

   ```
   project -stop wg
   ```

2. Mount the shared Reporter location on the primary Reporter system. To do so, edit the `/etc/fstab` file so that it is mounted at `boot`. For example:

   ```
   10.6.5.9:/home/nfs /reporter_share nfs rsize=1024,wsize=1024  0 0
   ```

3. Move the existing `data` and `sslkey` directories to the shared Reporter location. For example:

   ```
   mv RUEI_DATA/processor/data /reporter_share
   mv RUEI_DATA/processor/sslkeys /reporter_share
   ```

   where *`reporter_share`* specifies the shared location for data and SSL keys on the primary and secondary Reporter systems.

7.3 Installing the Secondary Reporter

The installation procedure for a secondary Reporter system is almost identical to that of a standalone Reporter system. Note that Initial Setup Wizard should *not* be run. Do the following:

1. When starting the installation procedure for the secondary Reporter system, ensure that the `/etc/ruei.conf` file is identical to that of the primary Reporter system.
2. Install the Linux operating system and RUEI Reporter software on the secondary Reporter system. The procedure to do this is described in Chapter 2, "Installing the RUEI Software". Specifically:
   - Follow the instructions described in Chapter 2, "Installing the RUEI Software" up to and including Section 2.6.4, "Installing the Zend Optimizer".
   - Copy the following files from the *RUEI_DATA* directory on the primary Reporter system to the secondary Reporter system: `cwallet.sso`, `ewallet.p12`, `sqlnet.ora`, and `tnsnames.ora`. You should ensure that the ownerships and permissions of these files are identical on both Reporter systems.
   - Follow the instructions described in steps 1-5 in Section 2.6.6, "Installation of the Reporter Software".
   - Follow the instructions described in Section 2.7, "Configuring the Network Interface".
   - If you performed the instructions described in Section 2.8, "Enabling Multibyte Fonts (Optional, but Recommended)" through Section 2.11, "Configuring Automatic Browser Redirection (Optional)" for the primary Reporter system, then you will need to repeat them for the secondary Reporter system.

7.4 Configuring Reporter Failover

Do the following:

1. If you have not already done so, login to the primary Reporter system as the *RUEI_USER* user, and issue the following command to stop all processing of monitored traffic:

   ```
   project -stop wg
   ```

2. Copy the `.ssh` directory of the *RUEI_USER* user on the primary Reporter system, created while performing the procedure described in Section 2.12, "Configuring Reporter Communication (Split-Server Setup Only)", to the secondary Reporter system. Note that it *must* be copied to the same location.
3. Ensure that the `uid` and `gid` settings of the *RUEI_USER* user are the same on both the primary and secondary Reporter systems. For example:

   ```
   id moniforce
   uid=501(moniforce) gid=502(moniforce) groups=502(moniforce)
   ```

4. Configure the static IP addresses on both Reporter systems used for the crossover cable. This can be done using a utility such as `system-config-network`.
5. Edit the `/etc/fstab` file so the `RUEI_DATA/processor/data` and `RUEI_DATA/processor/sslkeys` directories are mounted at `boot`. For example:

   ```
   10.6.5.9:/home/nfs /reporter_share nfs rsize=1024,wsize=1024  0 0
   ```

   where *reporter_share* specifies the shared location for data and SSL keys on the primary and secondary Reporter systems.
6. Move the local `data` and `sslkeys` directories for the secondary Reporter system to the shared Reporter location by issuing the following commands:

```
rm -rf RUEI_DATA/processor/data
rm -rf RUEI_DATA/processor/sslkeys
ln -s /reporter_share/data RUEI_DATA/processor/data
ln -s /reporter_share/sslkeys RUEI_DATA/processor/sslkeys
```

7. Login to the secondary Reporter system as the *RUEI_USER* user, and issue the following command:

   ```
   project -new -fromdb UX wg
   ```

   This creates the secondary Reporter's on-disk configuration files using the primary Reporter's database configuration.

8. Edit the `/etc/ruei.conf` file on both the primary and secondary Reporters to specify the virtual, primary, and standby IP addresses. For example:

   ```
   export RUEI_REP_FAILOVER_PRIMARY_IP=192.168.56.201
   export RUEI_REP_FAILOVER_STANDBY_IP=192.168.56.202
   export RUEI_REP_FAILOVER_VIRTUAL_IP=10.11.12.23
   export RUEI_REP_FAILOVER_VIRTUAL_DEV=eth0
   export RUEI_REP_FAILOVER_VIRTUAL_MASK=255.255.255.0
   ```

   THE RUEI_REP_FAILOVER_PRIMARY_IP and RUEI_REP_FAILOVER_STANDBY_IP settings should specify the IP addresses of the crossover cable between the two Reporter systems. See Section 2.4.1, "The RUEI Configuration File" for an explanation of these settings. Note that the settings specified on both Reporter systems *must* be identical except for the RUEI_REP_FAILOVER_VIRTUAL_DEV setting.

9. Issue the following command to restart processing of monitored traffic on the primary Reporter system:

   ```
   project -start wg
   ```

10. Install the `ruei-reporter-failover.sh` script on both Reporter systems. For example, in the `/usr/local/sbin` directory. It is located in the RUEI zip file (see Section 2.3, "Unpacking the RUEI Software").

11. Add the following entry to the `root` user's `crontab` file of both the primary and secondary Reporter systems:

    ```
    * * * * * /usr/local/sbin/ruei-reporter-failover.sh
    ```

    This causes the secondary Reporter to send a heartbeat signal to the primary Reporter every 60 seconds, and take over processing of RUEI monitored traffic in the event that the Primary Reporter becomes unavailable.

    Wait at least 60 seconds.

12. Ensure that *all* user access to the Reporter GUI is via the specified virtual IP address. This is necessary to ensure automatic failover to the secondary Reporter system in the event that the primary Reporter system becomes unavailable.

13. Check the `RUEI_DATA/processor/log/failover.log` file on both Reporter systems. These files contain the results of the "ping" commands. Ensure that there are no error messages. For example, about unspecified failover configuration settings.

14. Check the output of the `/sbin/ifconfig` command on the primary Reporter to ensure that the virtual IP address has been correctly configured. For example:

    ```
    /sbin/ifconfig
    eth0      Link encap:Ethernet  HWaddr 08:00:27:F7:B0:14
    ```

```
          inet addr:192.168.56.201  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef7:b014/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:80 errors:0 dropped:0 overruns:0 frame:0
          TX packets:311 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12793 (12.4 KiB)  TX bytes:26268 (25.6 KiB)

eth0:0    Link encap:Ethernet  HWaddr 08:00:27:F7:B0:14
          inet addr:10.11.12.23  Bcast:192.168.56.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

15. Unregister all remote Collectors with the primary Reporter, and re-register them using the virtual IP address.
16. Shutdown the primary Reporter system, and verify that the secondary Reporter begins processing monitored traffic. A warning that the primary system is unreachable and that the secondary system is being activated is reported in the event log. Note that after doing so, you must perform a failback to return your RUEI installation to its original state.
17. Update the Reporter URL (select **System**, then **Maintenance**, and then **E-mail setup**) with the virtual Reporter host name or IP address.

7.5 Instigating Reporter Failback

Failback to the primary Reporter system must be performed manually in order to return your RUEI installation to its original state. Do the following:

1. Load your global RUEI configuration settings using the following command as the `root` user:

   ```
   . /etc/ruei.conf
   ```

2. Ensure that the heartbeat mechanism between the primary and secondary Reporter systems is functioning correctly. To do so, verify that they can 'ping' each other on the RUEI_REP_FAILOVER_PRIMARY_IP and RUEI_REP_FAILOVER_ STANDBY_IP IP addresses.
3. To instigate the fallback, remove the `active-failover-server` file, and shutdown the virtual interface on the secondary server by issuing the following commands:

   ```
   rm $RUEI_DATA/processor/data/active-failover-server
   ifconfig $RUEI_REP_FAILOVER_VIRTUAL_DEV:0 down
   ```

8

Configuring a Failover Collector System

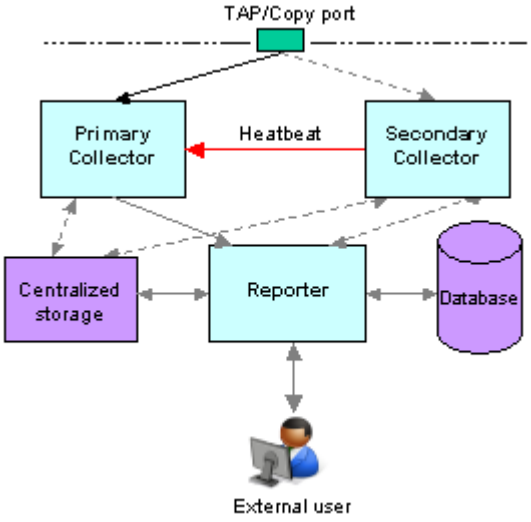
This chapter describes the procedure for configuring a failover remote Collector system that will take over monitoring of network traffic in the event that the primary Collector system becomes unavailable. Note that the described procedure assumes that the primary Collector system has been installed, configured, and is fully operational.

The procedure to configure a failover Reporter system is described in Chapter 7, "Configuring a Failover Reporter System".

8.1 Introduction

The configuration of a secondary (or failover) Collector system offers the advantage that it can seamlessly take over monitoring of network traffic in the event that the primary Collector system becomes unavailable. In this way, a high level of operational reliability is achieved. Note that this facility is only available for remote Collectors. The configuration of a failover Collector system is shown in Figure 8–1.

Figure 8–1 Failover Collector Configuration



At server level, a crossover network cable connects the primary and secondary Collector systems.As long as a regular "heartbeat" continues between the primary and secondary servers, the secondary server will not initiate monitoring of the network traffic. However, the secondary server will take over the monitoring task of the primary Collector as soon as it detects a failure in the "heartbeat" of the primary server.

This process is referred to as failover. The secondary Collector will take over the primary Collector's virtual IP address, and it is through this that the Reporter system will communicate with it.

Note that failback (that is, the process of restoring the primary Collector to its original state), must be performed manually. The procedure is described in Section 8.4, "Initiating Collector Failback".

Prerequisites

In order to configure a failover Collector installation, the following conditions must be met:

- A secondary TAP or copy port must be inserted at the same location as the primary one within the monitored network.
- The RUEI software version of the primary and secondary Collectors must be identical.
- The primary and secondary Collector systems must be directly connected via a crossover cable. In addition, both systems must also be connected to a local or public network in order to connect to the Reporter system.
- Both the primary and secondary Collector systems must have direct access to the same shared storage on which log files and replay data is written. In particular, the `$RUEI_DATA/collector` directory must be accessible by both systems.

Important

When configuring a failover Collector system, be aware of the following:

- When failover to the secondary Collector is initiated, the data that is currently being recorded by the primary Collector is lost. Typically, this represents information about traffic for up to a 1-minute period.
- When failover is initiated, state information that needs to be maintained for the duration of the connection for TCP, HTTP, SSL and Oracle Forms-based sessions is lost. Therefore, details of these sessions during failover are not available.
- Because of the above points, some page views are lost. It is possible that these pages contain session logon details. In this case, the session is reported as anonymous. In addition, specific user flow steps can be lost.

8.2 Installing the Secondary Collector

The installation procedure for a secondary Collector system is identical to that of a remote Collector system.

1. Install the Linux operating system and the RUEI Collector software on both Collector systems. The procedure to do so is described in Section 2.1, "Prerequisites".
2. When starting the installation procedure for the secondary Collector system, ensure that the `/etc/ruei.conf` file is identical to that of the primary Collector system.

8.3 Configuring the Secondary Collector

Do the following:

1. Copy the .ssh directory (created when following the procedure described in Section 2.12, "Configuring Reporter Communication (Split-Server Setup Only)" on the primary Collector to the secondary Collector. Note that it must be copied to the same location.

2. On the primary Collector system, issue the following commands to add the "host keys" for the Collector to the global known_hosts file on the Reporter system:

```
. /etc/ruei.conf
ifconfig ${RUEI_COL_FAILOVER_VIRTUAL_DEV}:0 $RUEI_COL_FAILOVER_VIRTUAL_IP \
netmask $RUEI_COL_FAILOVER_VIRTUAL_MASK up
sleep 2
arping -c 3 -A -I $RUEI_COL_FAILOVER_VIRTUAL_DEV $RUEI_COL_FAILOVER_VIRTUAL_IP
```

   On the Reporter system, use an arp -a or ping command to check that you can reach the virtual IP address on the primary Collector system.

   Then, issue the following command:

```
ssh-keyscan -t rsa,dsa Collector-virt-ip-address >> /etc/ssh/ssh_known_hosts
```

   As the *RUEI_USER* user, ensure that the virtual Collector IP address is not specified in the ~/.ssh/known_hosts file.

   Attempt to establish an SSH connection as the *RUEI_USER* user from the Reporter system to the primary Collector system. Note that you should not receive any warning or prompt about the host key, and you should be logged in automatically.

   On the primary Collector system, bring down the virtual IP address using the following command:

```
ifconfig ${RUEI_COL_FAILOVER_VIRTUAL_DEV}:0
$RUEI_COL_FAILOVER_VIRTUAL_IP netmask $RUEI_COL_FAILOVER_VIRTUAL_MASK down
```

   Repeat the above procedure for the secondary Collector system. Upon completion, four keys should be specified in the /etc/ssh/ssh_known_hosts file for the virtual IP address.

3. Ensure that the uid and gid settings of the *RUEI_USER* user are the same on both the primary and secondary Collector systems. For example:

```
id moniforce
uid=501(moniforce) gid=502(moniforce) groups=502(moniforce)
```

   Important

   If you need to change the UID of the *RUEI_USER* user on an operational Collector system, you should:

   - Issue the following commands as the *RUEI_USER* user:

```
appsensor stop wg
sslloadkeys -f
```

     Note that you should enter yes (written in full) when prompted.

   - Change the user:group ownership of all files and directories under /var/opt/ruei/collector to the new UID.

   - Issue the following command as the root user:

```
/etc/init.d/crond restart
```

4. Configure the static IP addresses on both Collector systems used for the crossover cable. This can be done using a utility such as `system-config-network`.

5. Mount the shared storage on the *`RUEI_DATA`*`/collector` directory, and edit the `/etc/fstab` file so that it is mounted at boot. For example:

```
10.6.5.9:/home/nfs /var/opt/ruei/collector/data nfs rsize=1024,wsize=1024  0 0
```

> **Important:** Note that if the Collector is already operational before this step, and the `$RUEI_DATA/collector` directory is not shared, the existing directory content must be copied to the mount point specified above. Security Officers should be aware that this copying process includes server SSL keys.

   Note that if the Collector is already operational before this step, and the `$RUEI_DATA/collector` directory is not shared, the existing directory content must be copied to the mount point specified above. Security Officers should be aware that this copying process includes server SSL keys.

   Alternatively, if your shared storage does not provide sufficient bandwidth to keep up with the storage of replay data, you can symlink the `REPLAY` directories to a local location instead. In this case, only the HTTP log files and logs will be written to the shared disk. However, be aware that if you specify this configuration, replay data recorded before failover is initiated will be lost, and only sessions after the failover are accessible. In addition, these links will be reset to factory defaults and, therefore, the directories do not currently exist in the initial Collector setup.

6. Edit the `/etc/ruei.conf` file on both the primary and secondary Collector systems to specify the virtual, primary, and standby IP addresses. For example:

```
RUEI_COL_FAILOVER_PRIMARY_IP=192.168.56.201 # crossover cable primary
RUEI_COL_FAILOVER_STANDBY_IP=192.168.56.202 # crossover cable secondary
RUEI_COL_FAILOVER_VIRTUAL_IP=10.11.12.23    # (virtual) IP to access Collector
RUEI_COL_FAILOVER_VIRTUAL_DEV=eth0
RUEI_COL_FAILOVER_VIRTUAL_MASK=255.255.255.0
```

   The RUEI_COL_FAILOVER_PRIMARY_IP and RUEI_COL_FAILOVER_STANDBY_IP settings should specify the IP addresses of the crossover cable between the two Collector systems. See Section 2.4.1, "The RUEI Configuration File" for an explanation of these settings. Note that the settings specified on both Collector systems must be identical.

7. Ensure that *all* communication between the Reporter and the Collector is via the specified virtual IP address. This is necessary to ensure automatic failover to the secondary Collector system in the event that the primary Collector system becomes unavailable. Note that this may require you to reconfigure existing Collector systems.

8. Install the `ruei-collector-failover.sh` script on both Collector systems. For example, in the `/usr/local/bin` directory. It is located in the RUEI zip file (see Section 2.3, "Unpacking the RUEI Software").

9. Add the following entry to the `root` user's `crontab` file of both the primary and secondary Collector systems:

```
* * * * * /usr/local/bin/ruei-collector-failover.sh
```

This causes the secondary Collector to send a heartbeat signal to the primary Collector every 60 seconds, and take over processing of RUEI monitored traffic in the event that the Primary Collector becomes unavailable.

Wait at least 60 seconds

10. Check the output of the `/sbin/ifconfig` command on the primary Collector to ensure that the virtual IP address has been correctly configured. For example:

```
$ /sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:F7:B0:14
          inet addr:192.168.56.201  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef7:b014/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:80 errors:0 dropped:0 overruns:0 frame:0
          TX packets:311 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12793 (12.4 KiB)  TX bytes:26268 (25.6 KiB)
eth0:0    Link encap:Ethernet  HWaddr 08:00:27:F7:B0:14
          inet addr:10.11.12.23  Bcast:192.168.56.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

11. Unregister the primary remote Collector with the Reporter, and re-register it using the virtual IP address.

12. Shutdown the primary Collector system, and verify that the secondary Collector begins processing monitored traffic. A warning that the primary system is unreachable and that the secondary system is being activated should be reported in the event log. Note that after doing so, you must perform a failback to return your RUEI installation to its original state.

8.4 Initiating Collector Failback

Failback to the primary Collector system must be performed manually in order to return your RUEI installation to its original state. Do the following:

1. On the primary Collector system, issue the following commands:

```
. /etc/ruei.conf
echo $RUEI_COL_FAILOVER_PRIMARY_IP > \
/var/opt/ruei/collector/active-failover-server
```

2. On the secondary Collector system, issue the following commands:

```
. /etc/ruei.conf
ifconfig ${RUEI_COL_FAILOVER_VIRTUAL_DEV}:0 $RUEI_COL_FAILOVER_VIRTUAL_IP \
netmask $RUEI_COL_FAILOVER_VIRTUAL_MASK down
```

3. On the primary Collector system (with the `/etc/ruei.conf` file still loaded), issue the following commands:

```
ifconfig ${RUEI_COL_FAILOVER_VIRTUAL_DEV}:0 $RUEI_COL_FAILOVER_VIRTUAL_IP \
netmask $RUEI_COL_FAILOVER_VIRTUAL_MASK up
sleep 2
arping -c 3 -A -I $RUEI_COL_FAILOVER_VIRTUAL_DEV $RUEI_COL_FAILOVER_VIRTUAL_IP
```

A

Generic Database Instance Setup

This appendix describes how you can setup an Oracle database instance for use by the RUEI Reporter that is running on a platform other than Oracle Linux 5.*x* or RedHat Enterprise Linux 5.*x*. RUEI supports Oracle database version 11gR1 and 11gR2.

Note that the approach taken in this appendix is to describe the requirements for a generic database instance, rather than a detailed procedural description. Therefore, a sound working knowledge of Oracle database administration is required.

Platform Support

While a wide range of platforms are supported for deployment of a remote database, high performance single-threaded platforms designed for large queries by comparatively few users offer the best deployment solutions.

A.1 Overview

Upon completion, the following parameters and settings should be specified for the new Oracle database instance:

- RUEI_DB_INST: the name of the new database instance (as specified in the `/etc/ruei.conf` file). See Section 2.4.1, "The RUEI Configuration File" for more information.
- The instance should be based on the `Data_Warehouse.dbc` template.
- The character set of the instance should be set to `AL32UTF8`.
- The `recyclebin` and `audit_trail` features should be disabled for performance reasons.
- Monitor the `redolog` file size, and adjust the size if necessary.

Each of these requirements is discussed in more detail in the following sections.

A.2 Creating the Database Instance

The following discussion assumes that the Oracle database instance is created on the command line. However, you are free to use any suitable utility to specify the required parameters. They should be consistent with the following:

```
dbca -silent -createDatabase -gdbName RUEI_DB_INST -sid RUEI_DB_INST \
-characterSet AL32UTF8 -templateName Data_Warehouse.dbc -databaseType DATA_WAREHOUSING \
-redoLogFileSize 500 -initParams recyclebin=off -initParams audit_trail=none
```

A.3 Using Compressed Tablespaces

For performance reasons, it is *strongly* recommended that you use compressed tablespaces. The following command line instruction can be used to enable compression on the `USERS` tablespace:

```
alter tablespace USERS default compress;
```

The size of the required database instance is 200 GB (or larger). The required disk space depends on the specified Reporter data retention policy (select **Configuration**, then **General**, then **Advanced settings**, and then **Reporter Data Retention Policy**).

For most RUEI deployments, you will require more than a single datafile in the `USERS` tablespace. Note that the default datafiles location is used, and you may want to specify a different location for the datafiles. Use the following command to add additional datafiles:

```
alter tablespace USERS add datafile 'user02.dbf' size 5M autoextend on;
```

A.4 Creating Additional Tablespaces

In addition to the `USERS` tablespace, three additional tablespaces must be created for the RUEI Reporter system:

- `UXCONF`: contains RUEI configuration information. Typically, less than 1 GB in size.
- `UXSTAT`: contains RUEI statistics information used for internal purposes. Typically, only a few GB in size.
- `UXTEMP`: contains RUEI temporary tables. Typically, several GB in size.

Note that the names of these three tablespaces are fixed and not configurable. The required tablespaces can be created using the following commands:

```
create tablespace UXCONF datafile 'uxconf01.dbf' size 5M reuse autoextend on default compress;
create tablespace UXSTAT datafile 'uxstat01.dbf' size 5M reuse autoextend on default compress;
create tablespace UXTEMP datafile 'uxtemp01.dbf' size 5M reuse autoextend on default compress;
```

A.5 DRCP Connection Pooling

For performance reasons, it is *strongly* recommended that you use a shared pool for all connection to the database. The following is an example of how to activate a shared pool for the database:

```
exec dbms_connection_pool.start_pool;
exec dbms_connection_pool.configure_pool(inactivity_timeout=>3600, max_think_time=>3600);
```

A.6 Rescheduling Oracle Database Maintenance

By default, Oracle database maintenance tasks are schedule to run at 22:00. These can have a significant impact on the overall database performance. Therefore, depending on traffic levels on the monitored environment, you may need to reschedule these maintenance tasks to a period with low traffic/load levels (for example, 03:00). For information on how to reschedule planned maintenance tasks, refer to the *Oracle Database Administrator's Guide* available at the following location:

```
http://download.oracle.com/docs/cd/B28359_01/server.111/b28310/memory003.htm#ADMIN11200
```

A.7 Creating the RUEI Database User

This section explains the creation of the RUEI database user, and permissions it must be assigned.

The RUEI database user is specified in the RUEI_DB_USER setting (in the `/etc/ruei.conf` file). It receives the minimum required permissions. However, note that the `dbms_crypto` permission is required for encryption of the SSL private keys that a Collector is using. In addition, because RUEI typically operates in an unattended 7x24 environment, the `PASSWORD_LIFE_TIME` permission should be set to unlimited.

The following examples show how the RUEI database user can be created with the minimum required permissions.

```
create user RUEI_DB_USER
         identified by PASSWORD
         default tablespace USERS
         temporary tablespace TEMP
         profile DEFAULT
         quota 200G on USERS;

alter user RUEI_DB_USER
         quota unlimited on UXCONF
         quota unlimited on UXSTAT
         quota unlimited on UXTEMP;

alter profile DEFAULT
         limit PASSWORD_LIFE_TIME unlimited;

grant    create session,
         create sequence,
         create table,
         create trigger
         to RUEI_DB_USER;

grant execute on dbms_crypto to RUEI_DB_USER;
```

A.8 Setting up the Connection Data

After the Oracle database instance has been defined, the connection data needs to be set up. This requires two files, `sqlnet.ora` and `tnsnames.ora`, in the RUEI home directory (RUEI_DATA).

The following is an example of the contents of the `sqlnet.ora` file:

```
NAMES.DIRECTORY_PATH = (TNSNAMES)
SQLNET.WALLET_OVERRIDE = TRUE
WALLET_LOCATION = (SOURCE=(METHOD=FILE)(METHOD_DATA=(DIRECTORY=/var/opt/ruei)))
DIAG_SIGHANDLER_ENABLED = FALSE
```

Ensure that the DIRECTORY setting points to the directory for RUEI data files (RUEI_DATA) specified in the `/etc/ruei.conf` file.

The following is an example of the contents of the `tnsnames.ora` file:

```
uxinsight=(DESCRIPTION=
  (ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=localhost.localdomain)(PORT=1521)))
  (CONNECT_DATA=(SERVICE_NAME=ruei)(SERVER=POOLED)))
```

In the example above, `uxinsight` is the database alias (RUEI_DB_TNSNAME) specified in the `/etc/ruei.conf` file. Ensure that the `HOST` setting specifies your

database. If you specify a host name, ensure that it is also specified in the `/etc/hosts` setup. However, you can also specify an IP address.

A.9 Setting up the Oracle Wallet

The processing part of RUEI requires non-interactive access to the Oracle database. In order to achieve this, the Oracle `autologin` wallet is used to store passwords securely.

Use the following command to create the Oracle wallet on the database system:

```
mkstore -wrl /dev/shm -create
```

Note that you are prompted for the wallet password.

After the (empty) wallet has been created, you must add the credentials of RUEI_DB_TNSNAME and RUEI_DB_USER to the Oracle wallet using the following command:

```
mkstore -wrl /dev/shm -createCredential RUEI_DB_TNSNAME RUEI_DB_USER
```

Two wallet files, `ewallet.p12` and `cwallet.sso`, must be moved to the RUEI_DATA directory on the Reporter system. Both files should have the ownership of RUEI_USER and RUEI_GROUP. Note that `ewallet.p12` only needs to be readable by RUEI_USER, while *`cwallet.sso`* needs to be readable by both RUEI_USER and RUEI_GROUP. On Linux, this can be accomplished by issuing the following commands:

```
chown RUEI_USER:RUEI_GROUP *wallet*
chmod 600 ewallet.p12
chmod 640 cwallet.sso
```

If the Oracle database instance has been set up correctly, it should now be possible to enter the database without being prompted for the password. The RUEI_USER on the Reporter system can access the database instance as follows:

```
sqlplus /@RUEI_DB_TNSNAME
```

If this last step fails, you should carefully review the information in this appendix before proceeding with your RUEI deployment.

B

Setting up an Alternative Enriched Data Export Database Instance

This chapter describes how you can set up a alternative Oracle database instance for use by the Enriched data export facility. The use of this facility is fully described in the *Oracle Real User Experience Insight User's Guide*.

> **Note:** Before proceeding with the configuration of the alternative database, it is recommended that you make a backup of your configuration. Select **Configuration**, then **System**, then **Maintenance**, and then **Backup and restore**.

B.1 Introduction

By default, when using the Enriched data export facility, the data is exported to the same database instance as used by the Reporter. However, it is *strongly* recommended that you configure an alternative database instance for enriched data export. This is due to the following reasons:

- The SQL queries used to access the exported data can place a significant performance overhead on the database. Be aware that if large amounts of data need to be handled, complex SQL queries need to be executed, or a number of queries need to be run against the exported data within a 5-minute period, the use of a separate database will provide a significant performance improvement.
- The use of a separate export database instance will minimize the impact on your RUEI deployment, as well as provide for easier management of it. Particularly in the case of database sizing and backup.

If you intend to use an alternative export database, this must be an Oracle database version 11gR1 or 11gR2, and installation of the Oracle database software should have been completed before starting the setup procedure described in the rest of this chapter. Be aware that advanced knowledge of Oracle database administration is assumed.

The setup procedure described in this chapter refers to a number of settings (such as RUEI_DB_TNSNAME_BI). These are explained in Table 2–2.

Migration to an Alternative Enriched Data Export Database

Be aware that when migrating Enriched data export from one database to another, the export data currently stored in the previous database is *not* migrated to the new database. Because the defined data retention policy is no longer enforced on the

previous database, any historical data will remain on the previous database. If required, the necessary tables can be manually purged from the previous database.

Accessing the Export Data

Access to the data in the export database is available via SQL. Be aware that the SQL queries used to access exported data can place a significant performance overhead on the export database. Therefore, it is recommended that you carefully review the design of your SQL queries to minimize their overhead. In particular, you should ensure that table columns not required for external analysis are dropped from the returned data. In addition, you should try to minimize the number of SQL queries run during a 5-minute period. In particular, try to avoid querying the same data more than once.

B.2 Creating the Database Instance

The following discussion assumes that the Oracle database instance is created on the command line. However, you are free to use any suitable utility to specify the required parameters.

1. Logon to the export database system as the `root` user, and issue the following command:

```
dbca -silent -createDatabase -gdbName EXPORT_DATABASE_NAME \
   -sid EXPORT_DATABASE_NAME -characterSet AL32UTF8 \
   -templateName Data_Warehouse.dbc -databaseType DATA_WAREHOUSING \
   -redoLogFileSize 500 -initParams recyclebin=off -initParams audit_trail=none
```

   where:

   - *EXPORT_DATABASE_NAME* specifies the literal export database instance name.
   - For performance reasons, it is recommended that the `recyclebin` and `audit_trail` features are disabled.
   - The character set instance should be specified as `ALT32UTF8`.

B.3 Using Compressed Tablespaces

For performance reasons, it is *strongly* recommended that you use compressed tablespaces.

1. Issue the following SQL command as the System Administrator to enable compression on the USERS tablespace:

```
alter tablespace USERS default compress;
```

2. By default, a single 32 GB datafile is created for the USERS tablespace. For most deployments, you will need to be increase this by using the following SQL command:

```
alter tablespace USERS add datafile 'user02.dbf' size 5M autoextend on;
```

   Note that in the command shown above, the default datafile location is specified. You are free to specify an alternative location.

B.4 Rescheduling Oracle Database Maintenance

By default, Oracle database maintenance tasks are schedule to run at 22:00. These can have a significant impact on the overall database performance. Therefore, depending on traffic levels within the monitored environment, and the scheduled processes

reading the export database tables, you may need to reschedule these maintenance tasks to a period with low traffic/load levels (for example, 03:00). Information on how to reschedule planned maintenance tasks is provided in the *Oracle Database Administrator's Guide* available at following location:

http://download.oracle.com/docs/cd/B28359_01/server.111/b28310/memory003.htm#ADMIN11200

B.5 Creating the RUEI Database User

Access to the alternative database requires the creation of an authorized user.

1. Issue the following commands to create the RUEI database user with the minimum required privileges:

```
create user RUEI_DB_USER_BI
         identified by "password"
         default tablespace USERS
         temporary tablespace TEMP
         profile DEFAULT
         quota 50G on USERS;

alter profile DEFAULT
         limit PASSWORD_LIFE_TIME unlimited;

grant    create session,
         create table
         to RUEI_DB_USER_BI;
```

   where:

   - *RUEI_DB_USER_BI* specifies the export database user name.
   - *password* specifies the required password variable.

B.6 Setting up the Connection Data

After the alternative Oracle database instance has been defined, the connection data needs to be set up. This requires two files, `sqlnet.ora` and `tnsnames.ora`, in the RUEI data files directory (RUEI_DATA) of the RUEI home directory (RUEI_USER) on the Reporter system.

1. Ensure that the `sqlnet.ora` file contains the following:

```
NAMES.DIRECTORY_PATH = (TNSNAMES)
SQLNET.WALLET_OVERRIDE = TRUE
WALLET_LOCATION = (SOURCE=(METHOD=FILE)(METHOD_DATA=(DIRECTORY=/var/opt/ruei)))
DIAG_SIGHANDLER_ENABLED = FALSE
```

   Ensure that the DIRECTORY setting points to the directory for RUEI data files (RUEI_DATA) specified in the `/etc/ruei.conf` file.

2. Create the `tnsnames.ora` file. It should contain the following:

```
RUEI_DB_TNSNAME_BI =(DESCRIPTION=
  (ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=localhost.localdomain)
     (PORT=1521)))
  (CONNECT_DATA=(SERVICE_NAME=RUEI_DB_INST_BI)(SERVER=POOLED)))
```

   where:

   - *RUEI_DB_TNSNAME_BI* specifies the export database connect string.

- *RUEI_DB_INST_BI* specifies the export database instance name.

Ensure that the HOST setting specifies your database. If you use a host name, ensure that it is also specified in the /etc/hosts setup. However, you can also specify an IP address.

B.7 Setting up DRCP Connection Pooling

For performance reasons, you may want to use a shared pool for all connections to the database.

1. Within Oracle Database Resident Connection Pooling (DRCP), use the following command to enable shared pooling:

```
exec dbms_connection_pool.start_pool;
exec dbms_connection_pool.configure_pool(inactivity_timeout=>3600, max_think_
time=>3600);
```

B.8 Setting up the Oracle Wallet

The processing part of RUEI requires non-interactive access to the Oracle database. In order to achieve this, the Oracle autologin wallet is used to store passwords securely. A wallet should already exist to connect to the Reporter database.

1. Use the following command to create a temporary copy of the ewallet.p12 and cwallet.sso files in the RUEI_DATA directory, and add the new database credentials to the wallet:

```
mkstore -wrl /dev/shm -createCredential RUEI_DB_TNSNAME_BI RUEI_DB_USER_BI
```

where:

- *RUEI_DB_TNSNAME_BI* specifies the export database connect string.
- *RUEI_DB_USER_BI* specifies the user of the remote database.

Note that you are prompted for the wallet password and the database password for RUEI_DB_USER_BI.

2. Move back the ewallet.p12 and cwallet.sso files to the RUEI_DATA directory. Ensure that the permissions for these files are set correctly. Both files should have the ownership of RUEI_USER and RUEI_GROUP. The ewallet.p12 file only needs to be readable by the RUEI_USER, but both files need to be readable by RUEI_GROUP.
3. If the database instance has been set up correctly, it should now be possible to access the export database without being prompted for the password. The RUEI_USER on the Reporter system can access the database instance as follows:

```
sqlplus /@RUEI_DB_TNSNAME_BI
```

If this step fails, you should carefully review the procedure described so far before proceeding.

B.9 Editing the RUEI Configuration File

Edit the /etc/ruei.conf configuration file on the Reporter system from which you intend to export enriched data.

1. Use the RUEI_DB_TNSNAME_BI setting to specify the database connect string to be used by the Enriched data export facility.

Important: Other than the modification described above, do *not* make any other changes to the `ruei.conf` file.

2. Within the Reporter, select **System**, then **Maintenance**, then **System reset**, and click the **Reapply latest configuration** radio button. When ready, click **Next**. You are prompted to confirm the re-application.

   This forces a reload of the `ruei.conf` file, and the changes that you have made to it during the setup procedure to take effect. The tables described in Appendix R of the *Oracle Real User Experience Insight User's Guide* will now be created and populated in the alternative database.

   Note that in period between setting RUEI_DB_TNSNAME_BI and the reloading of the `ruei.conf` file, messages can appear in the Event log. If these messages do not persist after re-loading of the `ruei.conf` file, they can be ignored.

C

The ruei-check.sh Script

This appendix provides a detailed explanation of the checks performed by the `ruei-check.sh` script. It is *strongly* recommended that you use this script to verify successful installation, and to troubleshoot any installation issues.

When started, the script prompts you to specify which role or roles the system is required to perform. For example:

```
1 - Reporter + Collector + Database
2 - Reporter + Collector
3 - Reporter + Database
4 - Collector only
5 - Reporter only
6 - Database only

Please specify which role(s) this system should perform: x
```

In the above example, the script will check the system to verify that it meets the requirements for both a Reporter and Collector installation with a local database.

The checks performed in the order shown in Table C–1, and are divided into three types: pre-installation, system, and post-installation checks. Whether a specific check is performed depends on the selected role(s).

Table C–1 ruei-check.sh Checks.

	Role						
Check	**1**	**2**	**3**	**4**	**5**	**6**	**Description**
System checks							
Architecture	•	•	•	•	•	•	Must be x86_64.
Operating system	•	•	•	•	•	•	Must be Oracle/RedHat Linux 5.*x*.
Memory	•	•	•	•	•	•	Must be at least 4 GB. Recommended 16 GB for Reporter installation. Recommended 8 GB for a Collector only or remote database installation.
Swap space	•	•	•	•	•	•	Must be at least 3/4 of the installed system memory[1].
Disk space for $RUEI_HOME	•	•	•	•	•		The disk space for the specified $RUEI_HOME location must be at least 512 MB.
Disk space for $RUEI_DATA	•	•	•	•	•		The disk space for the specified $RUEI_DATA location must be at least 100 GB.
Disk containing $RUEI_DATA	•	•	•	•	•		The specified $RUEI_DATA location must be local. Remote file systems (such as NFS) are not supported.

Table C–1 (Cont.) ruei-check.sh Checks.

Check	Role 1	2	3	4	5	6	Description
Disk speed on $RUEI_DATA	•	•	•	•	•		The disk speed of the specified $RUEI_DATA location must be at least 40 MB/s (120 MB/s or more is recommended).
SELinux	•	•	•	•	•	•	SELinux must be disabled.
Network interfaces	•	•		•			Must have at least one interface must be Up without an IP address (as described in Section 2.5, "Network Configuration").
Hostname	•	•	•	•	•	•	The system's configured IP address and hostname must be specified in the `/etc/hosts` file.
DNS	•	•	•	•	•	•	The configured DNS server must resolve the system's configured hostname to its IP address.
HTTPD autostart	•	•	•		•		Must be configured to start automatically.
HTTPD up	•	•	•		•		Must be up.
Database autostart	•		•			•	Must be configured to start automatically.
SSHD autostart	•	•	•	•	•	•	Must be configured to start automatically.
SSHD up	•	•	•	•	•	•	Must be up.
SSHD	•	•	•	•	•	•	Attempts to check if the SSH is not firewalled.
NTPD autostart	•	•	•	•	•	•	Must be configured to start automatically.
NTPD up	•	•	•	•	•	•	Must be up.
NTPD	•	•	•	•	•	•	Must be synchronized with a time server.
PHP CLI	•	•	•		•		PHP must be available on the command line.
PHP settings	•	•	•		•		`session.gc_maxlifetime` must be set to 14400. `memory_limit` must be set to 96M. `post_max_size` must be set to 128M. `upload_max_filesize` must be set to 128M. Zend Optimizer must be available. (These appear as individual checks, and are only performed if the above check is passed).
PHP timezone	•	•	•		•		PHP must return the same timezone as the Reporter operating system. See Section E.15, "ruei-check.sh Script Reports PHP Timezone Error" for additional information.
RSVG	•	•	•		•		The `~apache/.gnome2` directory must exist.
Pre-install checks							
Disk space for database data directory	•		•			•	Must be 300 GB. (If on the same partition as $RUEI_DATA, must be 400 GB).
Disk containing database data directory	•		•			•	Must be local. (Remote file systems, such as NFS, are not supported).
Disk speed of database data directory	•		•			•	Must be at least 40 MB/s (120 MB/s is recommended).
$RUEI_USER user exists	•	•	•	•	•		The specified $RUEI_USER user must exist.
`apache` user exists	•	•	•		•		User `apache` must exist.
User `apache` in group $RUEI_GROUP	•	•	•		•		User `apache` must be a member of the specified group $RUEI_GROUP.

Table C–1 (Cont.) ruei-check.sh Checks.

Check	Role 1	2	3	4	5	6	Description
User `apache` in group `uucp`	•	•	•		•		User `apache` must be a member of the group `uucp`.
User $RUEI_USER in group `uucp`	•	•			•		The specified $RUEI_USER user must be in group `uucp`.
User `root` must have `umask` of 0022	•	•	•	•	•	•	User `root` must have the `umask` 0022.
User `root` can write to `/etc/http/conf.d`	•	•	•		•		User `root` must be able to write to the `/etc/http/conf.d` directory.
User `root` can write to `/etc/init.d`	•	•	•		•		User `root` must be able to write to the `/etc/init.d` directory.
User `root` can write to `/etc/ld.so.conf.d`	•	•		•			User `root` must be able to write to the `/etc/ld.so.conf.d` directory.
User `root` can write to $RUEI_HOME	•	•	•	•	•		User `root` must be able to write to the specified $RUEI_HOME directory.
User `root` can write to $RUEI_DATA	•	•	•	•	•		User `root` must be able to write to the specified $RUEI_DATA directory.
User `root` can write to `/tmp`	•	•	•	•	•	•	User `root` must be able to write to the `/tmp` directory.
`/etc/sysconfig/httpd` must call `/etc/ruei.conf`	•	•	•		•		The `/etc/sysconfig/httpd` script must call the `/etc/ruei.conf` configuration file.
$RUEI_USER user able to contact database	•	•	•		•		The specified $RUEI_USER user must be able to connect to the database.
`oci8` PHP extension available	•	•	•		•		The `oci8` PHP extension must be available.
$RUEI_USER user able to contact database via PHP	•	•	•		•		The specified $RUEI_USER user must be able to connect to the database via PHP.
$RUEI_USER user must have `umask` 0027	•	•	•	•	•		The specified $RUEI_USER user must have a `umask` of 0027.
$RUEI_USER user able to read $RUEI_HOME	•	•	•	•	•		The specified $RUEI_USER user must be able to read the specified $RUEI_HOME directory.
$RUEI_USER user able to write to $RUEI_DATA	•	•	•	•	•		The specified $RUEI_USER user must be able to read the specified $RUEI_DATA directory.
Permissions and ownership of $RUEI_DATA	•	•	•	•	•		The Apache user must be able to read from the specified $RUEI_DATA directory.
`/etc/ruei.conf` syntactically correct	•	•	•		•		The `/etc/ruei.conf` configuration file must be a syntactically correct shell script.
User `root` able to contact database after loading `ruei.conf`	•	•	•	•	•		The `root` user must be able to connect to the database after the environment specified in the `ruei.conf` configuration file has been loaded.
`wm_concat` available	•	•	•		•		The `wm_concat` database function (used by suites) must be available.
$JAVA_HOME value valid	•	•	•		•		The value specified for $JAVA_HOME in the `/etc/ruei.conf` configuration file must be valid.
Post-install checks							
Reporter RPM check	•	•	•		•		The `ux-collector`, `ux-bi-publisher`, `ux-core`, `ux-generic`, `ux-ipdb`, `ux-gui`, `ux-lang-en` `ux-adf`, `ux-lang-zh_cn`, `ux-wlp`, `ux-suites-ebs`, `ux-suites-jde`, `ux-suites-sbl`, `ux-suites-psft`, and `ux-suites-flex` RPMs must be installed and have the same version (for example, 5.1.0).

Table C–1 (Cont.) ruei-check.sh Checks.

Check	Role 1	2	3	4	5	6	Description
Collector RPM check				•			The `ux-collector` RPM must have been installed.
Java shared objects	•	•		•			The Java path must have been correctly added to the LD_LIBRARY_PATH (see Section 2.4, "Generic Installation Tasks").
GUI reachable	•	•	•		•		The Reporter GUI must be reachable via the local hostname on the secure interface (note if a self-signed certificate is found, a warning is generated).
Reporter GUI can reach database	•	•	•		•		The Reporter GUI must be able to contact to the database.
Permissions and ownership of Oracle wallet	•	•	•		•		The Oracle wallet must be readable by the Apache and $RUEI_USER user.
Core binaries in path	•	•	•		•		The specified $RUEI_USER user must be able to call the core binaries without specifying a full name.

[1] If memory is added to meet the memory requirement, this check may start failing.

D

Verifying Monitored Network Traffic

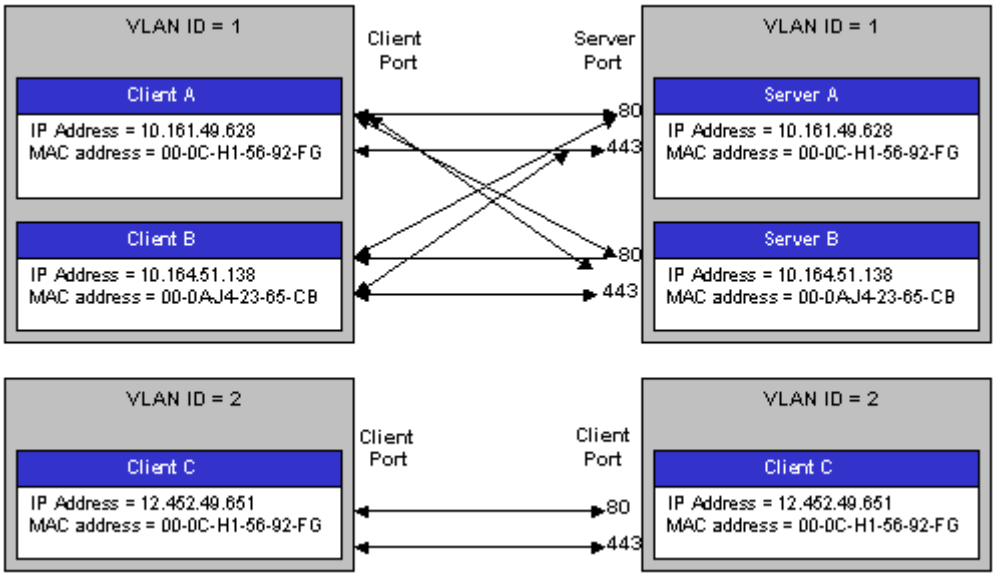
This appendix describes how you can use the TCP diagnostic facility to verify that RUEI "sees" all required network traffic. It is *strongly* recommended that a network engineer within your organization validates collected network traffic after installation and configuration of RUEI.

D.1 Introduction

The TCP diagnostics utility allows you to create 1-minute snapshots of the network traffic seen by a selected Collector. This snapshot can then be used to help determine whether there are gaps in the expected traffic flow. For example, there could be unconfigured port numbers, or an incorrectly specified VLAN ID.

The TCP traffic can be analyzed across client and server IP and MAC address, as well as port number and VLAN ID. Each snapshot's scope in terms of network traffic information is shown in Figure D–1.

Figure D–1 Example Network Topology

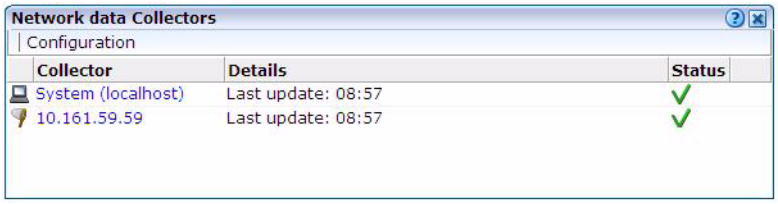


D.2 Creating Traffic Snapshots

To create a TCP traffic snapshot, do the following:

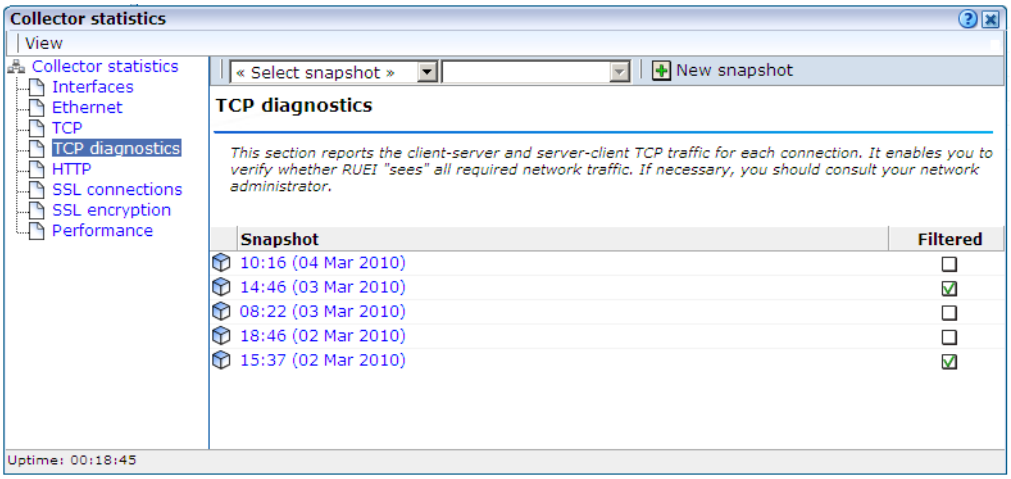
1. Within the **Configuration** facility, click the **Show Collector status** icon. Alternatively, select **System**, then **Status**, and then **Collector status**. The Network data Collectors window shown in Figure D–2 opens. This is fully explained in the *Oracle Real User Experience User's Guide*.

Figure D–2 Network Data Collectors



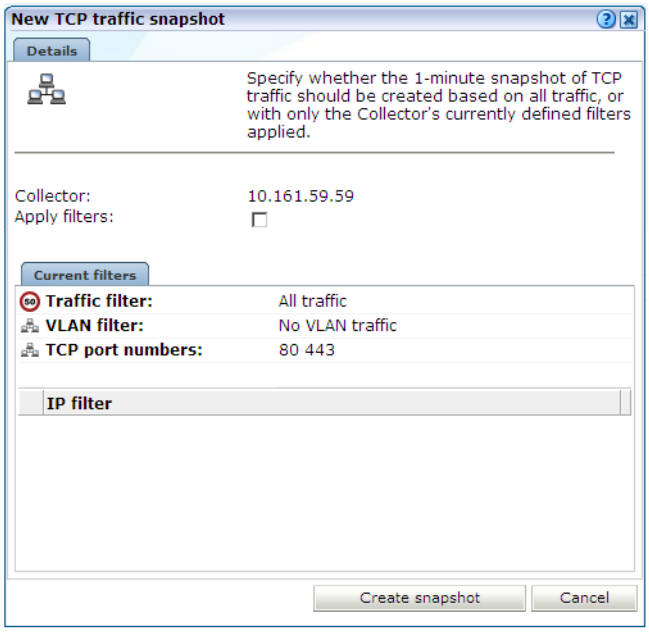
2. Click the required Collector. The **System (localhost)** item refers to the Collector instance running on the Reporter system. Other Collectors within the network are represented by their IP address.
3. Click the **TCP diagnostics** tab. A panel similar to the one shown in Example D–3 appears.

Figure D–3 TCP Diagnostics



4. Click the **New snapshot** icon in the toolbar. The dialog shown in Figure D–4 appears.

Figure D–4 New TCP Traffic Snapshot Dialog

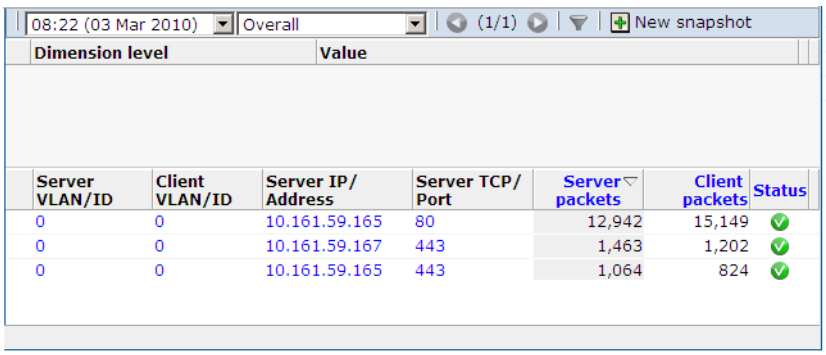


5. Use the **Apply filters** check box to specify whether the create traffic snapshot should be created to report all traffic seen by the selected Collector, or only that traffic that fits the Collector's currently defined filters (see the *Oracle Real User Experience Insight User's Guide* for more information). These are shown in the lower part of the dialog. Note that you can also view them by clicking the **View snapshot filters** icon on the toolbar. When ready, click **Create snapshot**.

> **Note:** The maximum number of traffic snapshots across all Collector systems in your RUEI installation is 15. When this maximum is reached, the oldest snapshot is automatically replaced by the newly created snapshot.

6. There is a 1-minute delay while the snapshot is created. Upon completion, an overview of the newly created snapshot's details is presented. An example is shown in Figure D–5.

Figure D–5 TCP Traffic Snapshot Overview



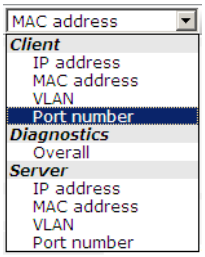
D.3 Analyzing Traffic Information

To analysis a created snapshot, do the following:

1. Select the required snapshot from the snapshot menu, or click it via the TCP diagnostics main panel (shown in Figure D–3). Snapshots created with applied filters are indicated with a tick character in the **Filtered** column. You can view the applied filters by clicking the tick character.
2. An overview of the selected snapshot (similar to the one shown in Figure D–5) appears. Note that you can click a selectable item to filter on it. For example, the list of reported items should be restricted to those that include a particular server IP address. You can remove a filter by clicking the **Remove** icon beside it in the filters section of the panel.

   Optionally, use the sort menu (shown in Figure D–6) to the right of the snapshot menu to select the primary column used for the displayed items.

Figure D–6 Sort Menu



3. The **Status** column shown in Figure D–5 indicates whether a possible problem may exist with the TCP traffic monitored during the snapshot. In the event of a fail status being reported, you can mouse over the status icon to see additional information. Possible identified problems are explained in Table D–1.

Table D–1 Identify Problems and Possible Causes

Status	Description
Client/server packet ratio is too high.	The number of client packets compared to server packets seems to be unusually large. This could indicate that the Collector cannot see both directions of traffic due (or is seeing duplicate traffic in one direction), or there is a server-related issue (for example, it is switched off).
Server/client packet ratio is too high.	The number of server packets compared to client packets seems to be usually large. This could indicate that the Collector cannot see both directions of traffic due (or seeing duplicate traffic in one direction), or there is a client-related issue (for example, unacknowledged server packets).
Insufficient number of server and client packets for analysis.	There was insufficient traffic (TCP packets) to perform a reliable client/server ratio analysis. A minimum of 100 packets is required. This may because normal traffic levels to the server are low. Otherwise, it may indicate routing issues with RUEI being unable to see some portions of network traffic.
Server VLAN ID does not match client VLAN ID.	This would normally indicate a routing issue. For example, traffic from the client to the server is being routed via one VLAN, but the traffic back from the server to the client is being routed via another VLAN. Be aware that RUEI can only monitor traffic on one VLAN segment at a time.

E

Troubleshooting

This appendix highlights the most common problems encountered when installing RUEI, and offers solutions to locate and correct them. The information in this appendix should be reviewed before contacting Customer Support.

More Information

- Information on Oracle Enterprise Manager is available at the following location:

  `http://www.oracle.com/us/products/enterprise-manager/index.html`

- Detailed technical information is available from My Oracle Support:

  `https://support.oracle.com`

Contacting Customer Support

If you experience problems with the installation or configuration of the RUEI, you can contact Customer Support. However, before doing so, it is strongly recommended that you create a Helpdesk report file of your installation. To do so, select **System**, then **Configuration**, and then **Helpdesk report**. This file contains extended system information that is extremely useful to Customer Support when handling any issues that you report.

E.1 Running the ruei-check.sh Script

It is recommended you use the `ruei_check.sh` script to troubleshoot installation issues. When first run, the script requires you to specify an installation type (`reporter`, `collector`, or `database`). Be aware this selection is saved to file. Therefore, if you want to run the script and be able to specify a different installation type, you need to delete the file `/tmp/ruei-system-type` using the following command:

```
rm /tmp/ruei-system-type
```

You can specify the parameters shown in Table E–1.

Table E–1 ruei-check.sh Parameters

Parameter	Description
`system`	Performs basic system checks, as well as a a number of prerequisites checks. These include interfaces that can be monitorable interfaces, that the Oracle database starts correctly, and that the Apache Web server, PHP, and Zend optimizer are correctly configured.
`preinstall`	Checks whether the Oracle database is correctly configured.

Table E–1 (Cont.) ruei-check.sh Parameters

Parameter	Description
`postinstall`	Checks if the RUEI RPMs have been installed correctly.
`all`	Performs all the above checks in the indicated sequences.

For example:

```
cd /root/RUEI/111
./ruei-check.sh all
```

E.2 The ruei-prepare-db.sh Script Fails

If the `ruei-prepare-db.sh` script fails, this can be because the database listener has not been started correctly due to a failing DNS look up. To resolve this problem, do the following:

- Ensure the `/etc/hosts` file includes your host.
- Ensure entries in the `/etc/nsswitch.conf` file are specified in the required (sequence hosts: files DNS).

> **Note:** The `ruei-prepare-db.sh` script can be run with the `--clean` option to remove the current database and install a new one.

E.3 Starting Problems

If the system does not seem to start, or does not listen to the correct ports, do the following:

- Restart each Collector service. To do so, select **System**, then **Maintenance**, then **Network data collectors**, select each attached Collector, and select the **Restart** option from the menu. This is described in more detail in the *Oracle Real User Experience Insight User's Guide*.
- Review your network filter definitions. This is described in the *Oracle Real User Experience Insight User's Guide*. In particular, ensure that no usual network filters have been applied. This is particularly important in the case of VLANs.
- Ensure that RUEI is listening to the correct protocols and ports. This is described in the *Oracle Real User Experience Insight User's Guide*.
- Verify that the Collector interfaces are *up*. This is described in the Section 2.5, "Network Configuration".

Resources and Log Files

If during, or directly after running the Initial setup wizard (described in Section 4.2, "Performing Initial RUEI Configuration"), the system returns an error, there are the following resources and log files available to help you in debugging:

- `/var/opt/ruei/processor/log/gui_debug.log`: a proprietary debug and log file that shows low-level system information. Although it contents may be difficult to read, you can find standard system error messages listed here.
- `/var/log/httpd/access_log` and `/error_log`: the Apache daemon access and error log files. If any part of the HTTP or PHP execution of the RUEI user

interface is in error, it will show up in these log files. (Note that these are *not* the log files used by RUEI for HTTP data analysis).

Root-Cause Analysis

Before starting to address specific issues, it is important to understand the basic operation of data collection, data processing, and data reporting. Any root-cause analysis of RUEI problems should take the following:

- Verify data collection. Select **System**, then **Status**, and then **Collector status**. Select a Collector from the displayed list, and verify that the system interfaces are showing traffic activity on TCP, Ethernet, and HTTP level.
- In addition, verify that there are no problems with the SSL data decryption. It is normal that some errors occur (especially shortly after startup). But if SSL traffic is to be decrypted, the error rate can never be 100%.
- Verify data processing. Select **System**, then **Status**, then **Data processing**. A screen similar to the one shown in Figure 4–7 appears. It should indicate some activity.

E.4 Data Collection Problems

If the data collection service is not running, or will not start, do the following:

- Use the TCP diagnostics facility to verify that RUEI "sees" all required network traffic. The use of this tool is described in Appendix D, "Verifying Monitored Network Traffic".
- Ensure the network cards used for data collection are running in promiscuous mode. This can be verified by issuing the command `ifconfig eth`*`N`* (where *`N`* is the number of the network interface being used for data collection). It should return an output similar to the following:

```
ethn      Link encap:Ethernet  HWaddr 00:15:17:3E:26:AF
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 GiB)  TX bytes:0 (0.0 GiB)
          Memory:b9120000-b9140000
```

- If the network interface is not available, make sure the ONBOOT parameter is set to YES, as described in Section 2.5, "Network Configuration".
- If the network interface is not yet in promiscuous mode, set it by issuing the following command: `ifconfig eth`*`N`*`promisc` (where *`N`* is the number of the network interface being used for data collection).
- Verify there is *no* IP address assigned to the network interface being used for data collection. If there is a configured IP address, remove it.

> **Note:** Do not set to 0.0.0.0 or 127.0.0.1. Remove the configured IP address completely.

E.5 Data Processing Problems

If, for any reason, data processing does not start, try to restart it by selecting **System**, then **Maintenance**, and then **System Reset**. The System reset wizard appears. Select

the **Restart system processing** option. Note that restarting system processing can take between 5 and 30 minutes.

In general, if no data is being processed, verify your system's configuration as described in Section 4.5, "Verifying and Evaluating Your Configuration". If you do not apply any configuration to the system, no data processing will take place.

If you are using an environment with multiple Collectors, ensure all Collectors are up and running normally. To do so, select **System**, then **Status**, and then **Collector status**. A failing Collector can become a block to further data processing of the system's data.

E.6 E-Mail Problems

Sending E-mails is RUEI functionality that is handled on a system level, together with your Mail Transfer Agent (MTA), such as Sendmail or Postfix. If problems occur when sending E-mails, do the following:

- If mail is sent correctly by RUEI to your MTA, the user interface will report "Message sent successfully" when you attempt to send a daily, weekly, or monthly report manually.
- If mail could not be sent correctly by RUEI to your MTA, verify that the MTA is up and running. Alternatively, analyze the mail settings by selecting **System**, then **Maintenance**, and **E-mail configuration**.
- If the mail was sent successfully, but not delivered to the recipient, analyze the operation of your MTA to further identify the root cause of the mails that are not delivered.
- Refer to the `/var/log/maillog` file for reported mailing issues.

Common issues with E-mail delivery often involve an incorrectly configured MTA, or an MTA that is not allowed to send E-mail within the Data Center or corporate network.

E.7 SSL Decryption Problems

In order to decrypt SSL traffic, the Collector needs to have the SSL key and certificate available. To enable SSL decryption, you should do the following:

- Upload the SSL key through the appropriate Collector.
- Enable the SSL key by entering the required decryption passphase (when applicable).

The certificate needs to be uploaded to the Collector(s) by selecting **Configuration**, then **Security**, and then **SSL keys**. To check the status of the SSL decryption, select **System**, then **Status**, and then **Collector status**, and select the Collector for which you want SSL decryption analysis. Within the **SSL encryption** page, note the following:

- Decryption errors will occur if there is no SSL key uploaded.
- The percentage of successful decryption will be a low number shortly after uploading and activating the appropriate SSL keys.
- This percentage should rise in the first minutes and hours after uploading the SSL keys.

RUEI accepts PKCS#12 and PEM/DER encoding of SSL keys and certificates. Basically, this means both the certificate and key should be concatenated into one file. If you have separate key and certificate files, you can create a PKCS#12-compliant file by issuing the following command:

```
openssl pkcs12 -export -in certificate.cer -inkey key.key -out pkcs12file.p12
-passout pass:yourpassphrase
```

Where:

- *certicate.cer* is your CA root certificate file.
- *key.key* is the server's SSL key file.
- *pkcs12file.p12* is the output file name for the PKCS#12-encoded file.
- *yourpassphrase* is the passphrase you want to use to protect the file from unwanted decryption.

For example, consider the situation where the CA root certificate filename is `ca_mydomainroot.cer`, the server's SSL key is `appsrv12.key`, you want the output file to be called `uxssl.p12`, and want to protect this file with the passphrase `thisismysecretpassphrase`. The following command is required:

```
Openssl pkcs12 -export -in ca_mydomainroot.cer -inkey appsrv12.key -out uxssl.p12
-passout pass:thisismysecretpassphrase
```

E.8 Missing Packages and Fonts Error Messages

It is *strongly* recommended that you follow the installation procedure and settings described in Section 2.6, "Package Installation". In particular, you should not perform a "minimal" installation of Oracle Linux. If you do so, it can lead to a wide range of reported problems, depending on the components not included in the installation, but required by RUEI.

The most common of these are reported `fontconfig` error messages in the `/var/log/http/error_log` file. These can be fixed by installing the following fonts:

- urw-fonts-noarch v2.3
- ghostscript-fonts-noarch v5
- dejavu-lgc-fonts-noarch v2
- liberation-fonts v0.2
- bitmap-fonts v0.3
- bistream-vera-fonts-noarch v1.10

Depending on your language settings, install all other required fonts.

However, other possible error messages include reported missing packages (such as `librsvg2`).

When a Yum repository is available, all dependencies available on the Linux 5.*x* DVD can be installed by issuing following command:

```
yum -y install gcc gcc-c++ compat-libstdc++-33 glibc-devel libstdc++-devel \
elfutils-libelf-devel glibc-devel libaio-devel sysstat perl-URI net-snmp \
sendmail-cf httpd php php-pear php-mbstring phpldap bitstream-vera-fonts \
librsvg2 xorg-x11-xinit net-snmp-utils perl-XML-Twig
```

However, be aware that additional RPMs shipped with the RUEI installation zip file still need to be installed according to the procedure described in Section 2.6, "Package Installation".

E.9 ORA-xxxxx Errors

If you receive any Oracle database errors, do the following:

- Ensure that the `/etc/sysconfig/httpd` file contains the following lines:

  ```
  source /etc/ruei.conf
  ```

  If you have to add these lines, restart the Apache Web server using the following command:

  ```
  service httpd restart
  ```

- Ensure that the `ewallet.p12` file is readable by the RUEI_USER specified user. Additionally, the `cwallet.sso` file should also be readable by the RUEI_GROUP specified group. On Linux/UNIX, this can by accomplished by issuing the following commands:

  ```
  chmod 600 ewallet.p12
  chmod 640 cwallet.sso
  ```

- Ensure the same host name is specified in the `/var/opt/ruei/tnsnames.ora`, `/etc/sysconfig/network`, and `/etc/hosts` files.

  Note if you make changes to any of these files, you may need to reboot the server.

E.10 Oracle DataBase Not Running

Verify the Oracle database is up and running by changing to the `moniforce` user and obtaining an SQL*Plus prompt with the following commands:

```
su - moniforce
sqlplus /@uxinsight
```

You should receive the SQL*Plus command line without being prompted for a password. This indicates that the Oracle wallet authentication was successful.

If necessary, re-start the Oracle database using the following command:

```
/etc/init.d/oracledb
```

E.11 General (Non-Specific) Problems

If you are experiencing problems with the reporting module, or find its interface unstable, it is recommended that you do the following:

- Clear all content caching within your browser, and re-start your browser.
- Examine the error log. This is described in the *Oracle Real User Experience Insight User's Guide*.
- Select **System**, then **Status**, and verify correct operation of the core components by then selecting **Data Collection**, **Logfile processing**, and **Data processing**. If any of these components are in error, try to resolve them using the advice provided in this appendix.

E.12 Network Interface Not Up

If the network interface you intend to use for data collection is not *Up* (that is, the `ONBOOT=YES` parameter was not set), you can bring it immediately using the following command:

```
ifconfig ethN up
```

where *N* represents the necessary network interface.

E.13 Memory Allocation Error During Upgrade Procedure

The following memory allocation error is received while updating the Reporter RPMs as part of the procedure for upgrading from version 5.1 to 6.0:

```
Cannot allocate memory
```

Make more memory for a socket connection available to the Collector in order for it to start. Issue the following command as the `root` user:

```
/sbin/sysctl -w net.core.optmem_max=65535
```

E.14 OAM-Related Problems

In order to start isolating OAM-related problems, you should do the following:

1. Logon to the Reporter system as the `moniforce` user.
2. To obtain a sample value of the cookie, issue the following command:

   ```
   EXAMPLE_VALUE=$(zgrep ObSSOCookie \
   $WEBSENSOR_HOME/data/wg_localhost/http/`date +"%Y%m%d"`/*/http-*|\
   tail -1 |sed 's,^.*ObSSOCookie=\([^;[:space:]]*\)[;[:space:]].*$,\1,g')
   ```

3. To view the obtained sample value, issue the following command:

   ```
   echo $EXAMPLE_VALUE
   ```

   You should check that the returned output is not empty and does not contain errors. The following is an example of the possible output:

   ```
   2bTxIrJxIGg%2FMrntHeRuhI1bADtml%2FNPXMho%2FuXK1S3PmiqdsQy4QAgcq0JiQbLfabIs1FBQc
   %2Bq1Nadjw7naVCqAyT7ir883GoGkSTX8ODtW7S1HQlbATMahOSYsTn8wshgg%2Fg5vi0d18%2F3Zw6
   tOdPevrhE0wTCk069p%2FkeIS8ftPBUSe6p9rEKiWBqyptQpUzW4SwfTz89iNxOoNULPkG4I5B%2BVa
   2ac4pgA4rc%2Bre%2BdFk3Gcm7dyu5XC%2BiQKRznERRE1t7wQb7RF5zjFL8hD6Jl0yquJytYPV3x7u
   fa%2BWatYE5uIHq3NdUKzuLq0214
   ```

4. To specify the obtained value as the OAM cookie, issue the following commands:

   ```
   project -
   cp $WEBSENSOR_INI/../evt/OAM2* $WEBSENSOR_INI
   mklookup --match $EXAMPLE_VALUE '%' '%1[$OAM2UserName] %0
   ```

Reported Errors

If the following error is received:

```
*ERROR* - obssocookie: could not dlopen()
/opt/netpoint/AccessServerSDK//oblix/lib/libobaccess.so:
/opt/netpoint/AccessServerSDK//oblix/lib/libobaccess.so: cannot open shared
object file: Permission denied
```

This indicates that the `moniforce` user does not have the necessary permissions. You should logon to the Reporter system as the `moniforce` user, and issue the following commands:

```
find /opt/netpoint/AccessServerSDK -type d -exec chmod o+rx {} \;
find /opt/netpoint/AccessServerSDK -type f -exec chmod o+r {} \;
```

If the following error is received:

```
*ERROR* - obssocookie: could not dlopen()
/opt/netpoint/AccessServerSDK//oblix/lib/libobaccess.so:
/opt/netpoint/AccessServerSDK//oblix/lib/libobaccess.so: wrong ELF class:
ELFCLASS32
```

This indicates that the 32-bit version of the Access Gate SDK was installed instead of the required 64-bit version. The procedure to download and install the required Access Gate SDK is described in Section 6.2, "Downloading and Installing the Access Gate Software".

Note that the Access Gate SDK installation package includes a utility to uninstall the 32-bit version (`_uninstAccessSDK/uninstaller.bin`).

If the following error is received:

```
Server is not authenticated to access the the OAM environment
```

This indicates that the creation of a trust between RUEI and the access server (described in Section 6.3, "Configuring the Access Gate Software on the RUEI Server") was not successfully performed, and should be repeated.

If the following error is received:

```
*ERROR* - obssocookie: environment variable OBACCESS_INSTALL_DIR not set
```

This indicates that the procedure described in Chapter 6, "Configuring the Oracle Access Manager (OAM)" was not followed.

E.15 ruei-check.sh Script Reports PHP Timezone Error

The following error is reported by the `ruei-check.sh` script:

```
Checking if the PHP timezone has been set correctly:   [FAIL]
PHP and OS timezones do not match (os: winter +0000, summer +0100. php:
winter +0100, summer +0200)
```

This can easily be fixed by setting the TZ environment variable at the bottom of the `/etc/ruei.conf` file on the Reporter system as follows:

```
export TZ=Europe/Lisbon
```

F

Installation Checklist

This appendix provides a checklist of actions that should be complete, and information gathered, before starting to install the RUEI software. These include server and infrastructure readiness and configuration, as well as HTTPS encrypted traffic and alerting issues.

Server readiness Base hardware and operating system requirements.	
Intel/AMD 64-bit platform (minimum 2 dual-core CPUs). Network connectivity: ■ 10/100 MB NIC for office network connectivity. ■ 10/100/1000 MB NIC for data collection connectivity. Disk space: at least 400 GB (on high-performance RAID-5, RAID-10, or similar). Memory: at least 16 GB RAM for single server. OS: Oracle Linux 64-bit or RedHat Enterprise Linux 64-bit 5.*x*. Oracle Database 11g Enterprise Edition. The `ruei-check.sh` script reports no errors. The EBS, JD Edwards, FLEXCUBE, and PeopleSoft configuration zip files are available.	

Infrastructure readiness Ensure easy placement and accessibility of the system.	
Prepare rackspace in the Data Center cabinet with power sockets. The server is accessible through remote ports: ■ Port 80/443 for HTTP(S) traffic to the RUEI Web server. ■ Port 22 for remote management over SSH/SCP. ■ Port 25 (E-mail). ■ Port 123 (NTP). ■ Port 161/162 (SNMP). ■ Port 1521 (for remote database setup). Access to the Data Center on the appropriate day and time is arranged. Network preparation for TAP/copy port is done and cables available in cabinet. Server configuration completed (see below).	

Infrastructure readiness	
Main topology with proxies, load balancers, routers, switches, and so on, is known.	
Main traffic flows throughout the infrastructure are known.	
VLAN topology, VLAD IDs, and IP addresses are known.	
The monitoring position for the RUEI server is located as close as possible to the firewall.	
The domains, applications, server farm(s), and/or VLANs to be monitored are identified.	

Server configuration

Complete the details below to for reference during server configuration.

Host name and domain name (optional).	
Data Center name.	
Placement date and time.	
Server IP, netmask, and default gateway.	
Server type (Collector/Reporter).	
NTP server IP and backup.	
DNS server IP and backup.	
Mail server and sender mail.	
Socket 0: collection port to TAP/switch name.	
Socket 1: collection port to TAP/switch name.	
Socket 2: rescue/maintenance interface.	<reserved>
Socket 3: Office network to switch name.	
Socket 4: collection port to TAP/switch name.	
Socket 5: collection port to TAP/switch name.	

Data collection configuration

Once in place, the server will start collecting data. Specify how much data is expected, and the technologies used.

HTTP traffic (in MB, pageviews, or hits per hour).	
Base technology for Web applications.	
Limits on amount of traffic to be captured: ■ HTTP and HTTPS ports (if other than 80/443 HTTP/HTTPS). ■ VLAN traffic and VLAN IDs (optional).	
Cookie technology.	
Page-labelling technology.	
Blind POST field names (such as `passwd`).	
User identification in URL (if other than login).	
Web service domains or networks.	

Data collection configuration	
XML/SOAP envelopes (max 10).	
Chronos/EUM URL (for EBS and Forms).	

HTTPS enablement	
Specify the contact(s) for the required SSL keys to monitor encrypted traffic.	
Name:	Name:
Function:	Function:
E-mail:	E-mail:
Phone/Mobile:	Phone/Mobile:
Keys (if not all):	Keys (if not all):

System health notifications	
The system can trigger and send alerts for various components. Specify the users, notification methods, and details for each component.	
Name:	Name:
Function:	Function:
E-mail:	E-mail:
Mobile:	Mobile:
Text message:	Text message:

Alerting via SNMP (optional)[1]
SNMP management server.
SNMP community name.
SNMP version.

[1] RUEI provides a standard MIB to be imported into the SNMP manager.

G

Third-Party Licenses

This appendix contains licensing information about certain third-party products included with this release of RUEI. Unless otherwise specifically noted, all licenses herein are provided for notice purposes only.

The sections in this appendix describe the following third-party licenses:

Apache Software License, Version 2.0

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. **Definitions**. "License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. **Grant of Copyright License**. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. **Grant of Patent License**. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. **Redistribution**. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

- You must give any other recipients of the Work or Derivative Works a copy of this License; and
- You must cause any modified files to carry prominent notices stating that You changed the files; and
- You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
- If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices

that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. **Submission of Contributions**. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. **Trademarks**. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. **Disclaimer of Warranty**. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. **Limitation of Liability**. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. **Accepting Warranty or Additional Liability**. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

OpenSSL

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org).

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

THIS SOFTWARE IS PROVIDED BY THE OPENSSL PROJECT "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENSSL PROJECT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA OR PROFITS; OR BUSINESS INTERRUPTION) HOWVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

PHP

Copyright © 1999-2006 The PHP Group. All rights reserved.

This product includes PHP software, freely available from http://php.net/software/.

"THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE."

Java Runtime Environment

Oracle is required to provide the following notice as part of the license terms for the Sun JRE that the field of use for the JRE is: (i) general purpose desktop computers, laptops and servers, and (ii) embedded systems (by way of example: embedded applications, cell phones, PDAs, TV devices, digital set top boxes, telematics devices and home gateway devices), provided that the Java Runtime Environment (JRE) is licensed only to run Licensee applications, middleware and database products and the JRE is not licensed to directly run any third party applications. This shall not be understood to prevent third party applications from indirectly and incidentally utilizing the JRE, but only as such is required to enable other Licensee Product functionality.

After installing the JRE, the complete terms of the Sun Microsystems license agreement are available in the file `/usr/java/jre/THIRDPARTYLICENSEREADME.txt`.

Index