Oracle® Real User Experience Insight

Installation Guide

13.5
F37658-04
August 2023

Oracle Real User Experience Insight Installation Guide, 13.5

F37658-04

Contents

J Setting up RUEI Against a Remote Database Service

Preface

Oracle Real User Experience Insight (RUEI) provides you with a powerful analysis of your network and business infrastructure. RUEI helps you to monitor real-user experience, set Key Performance Indicators (KPIs) and Service Level Agreements (SLAs), and sends alerts when it reaches the threshold.

Audience

This document is intended for the following people:

- System administrators with good Linux knowledge for the installation of RUEI. RUEI Super Administrator (that is, the admin user) who is responsible for post-installation configuration and system maintenance.
- RUEI Super Administrator (that is, the admin user) who is responsible for post-installation configuration and system maintenance.

It is expected that the person using this book is familiar with network and web technology. You should have good knowledge of the network topology and knowledge of your organization's network and application environment.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

Refer to the following documents in the Oracle Real User Experience Insight (RUEI) documentation set:

- *Oracle Real User Experience Insight Release Notes*.
- *Oracle Real User Experience Insight User's Guide.*
- *Oracle Real User Experience Insight Administrator's Guide*.

For the latest version of this document and other RUEI documentation, see https://docs.oracle.com/cd/cloud-control-13.3/nav/associated_products.htm.

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 (RUEI). In particular, it describes how RUEI monitors data traffic, its operational requirements, and the available deployment options. Also, the chapter discusses the ways of how you can increase the amount of information available within the RUEI Reporter database.

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. It also includes the utilization of web services which implement clearly defined business functions. Applications can be accessed from mobile devices and there are many cloud based deployment options including on-premises, SaaS and hybrid. RUEI is designed for measuring, analyzing, and improving the availability and performance of all the deployment scenarios. To achieve this, RUEI is capable of performing data collection from network traffic, ADF servers, and data collection using Javascript browser instrumentation.

To view a visual demonstration about using RUEI, go to the following URL, and click **Begin Video**:

`https://apex.oracle.com/pls/apex/f?p=44785:24:0::NO:24:P24_CONTENT_ID,P24_PREV_PAGE:5783,1`

Data Collection

Figure 1-1 shows the Network Data Collector (available in previous RUEI releases) and Figure 1-2 shows the Tag Data Collector which is an option that allows you to collect data using Javascript and does not require network monitoring.

Figure 1-1 Network Data Collector

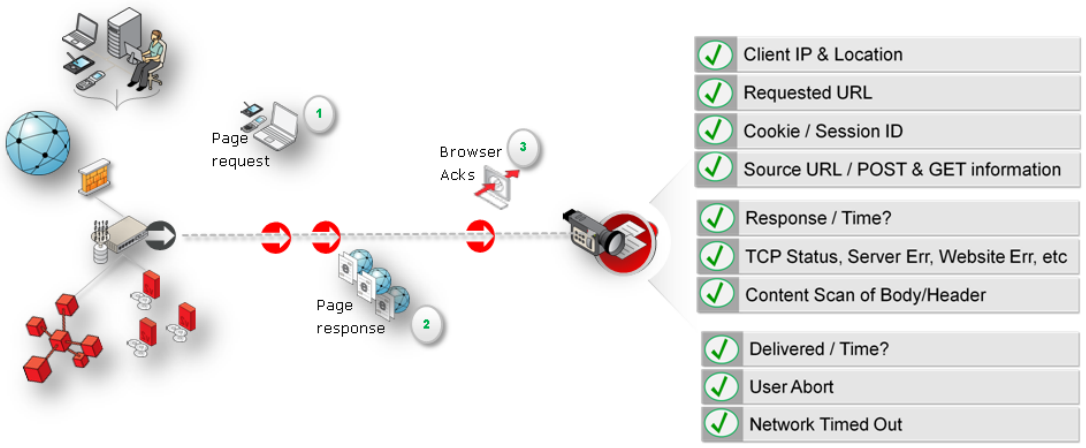


Figure 1-2 Tag Data Collector

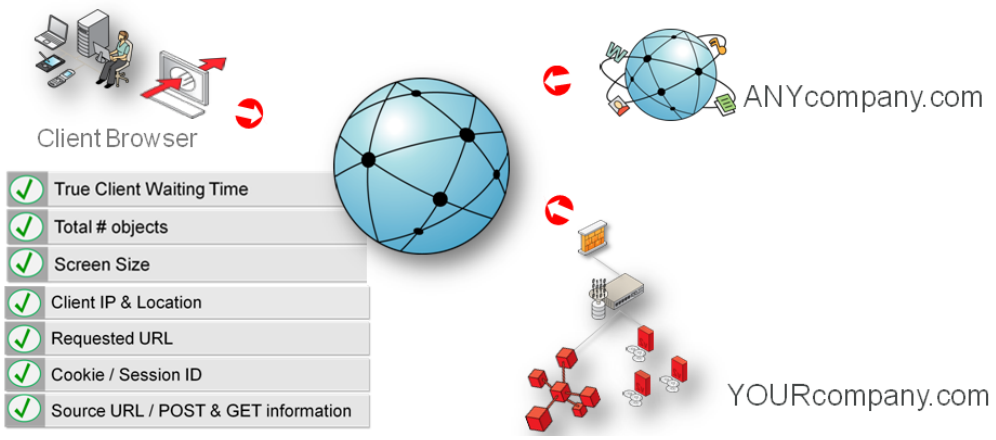


Table 1-1 outlines the different data collections that are available with RUEI.

Table 1-1 Data Collection Methods

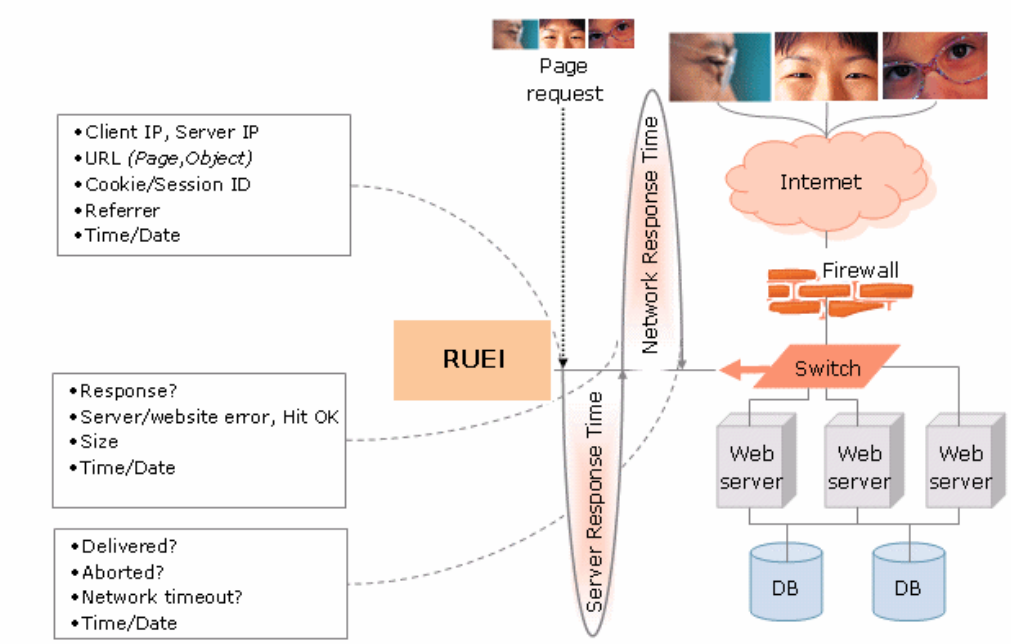
	Network	Tag
Overview	This option collects data that passes through the network and was the default option in previous releases and requires either a local or remote collector. It monitors all network traffic in promiscuous mode.	This option, also called tag based monitoring, collects data by monitoring the request and processing of a specific web URL (the tag) which is inserted into all pages and requires either a local or remote collector. It monitors only the traffic related to a local IP address.
Applications	You must define an application. See *Identifying and Reporting Web Pages* chapter of *User's Guide*.	You must define an onload object and use the generated javascript in your application. For more information, see *Identifying and Reporting Web Pages* in the *Real User Experience Insight User Guide*.
Suites	You must define a Suite. See *Working With Suites and Web Services* chapter of *User's Guide*.	Only WebCenter Sites can be monitored using tag-based data collection. For more information, see *Working With Suites and Web Services* in *Real User Experience Insight User Guide*.
Further Information	Planning the Software Installation Security for Network Data Collection Connection Options for Network Data Collection	Planning the Software Installation

The options are further described in Planning the Software Installation.

The network 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. Typically, RUEI is installed before the web servers, behind a firewall in the DMZ (as shown in Figure 1-3).

Figure 1-3 How RUEI Collects Data with a Network Data Collector



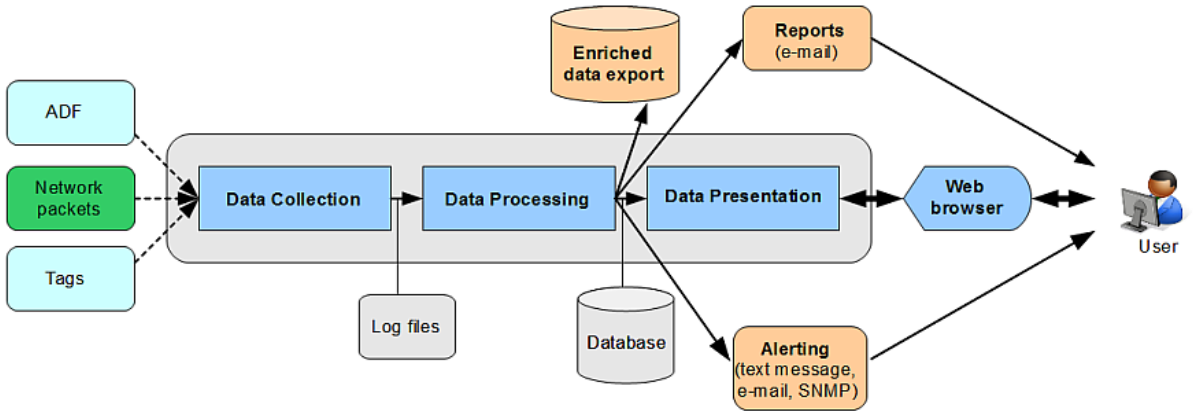
When an object is requested by a visitor, RUEI sees the request and measures the time the web server requires to present the visitor with the requested object. At this point, RUEI knows who requested the page (the client IP), which object was requested, and from which server the object was requested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

When the web server responds and sends the requested object to the visitor. RUEI 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). RUEI can determine the time taken for the object to traverse the internet to the visitor and calculate the output between the visitor and the server (connection speed of the visitor).

Product Architecture

RUEI is based on a three-layer product architecture, as shown in Figure 1-4.

Figure 1-4 RUEI Product Architecture



The monitored data packets are processed by the layers shown in Table 1-2.

Table 1-2 Product Architecture Layers

Layer	Description
Data Collection	This layer is responsible for acquiring raw data and delivering it to the Data Processor layer. 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 the OLAP data sets. These comprise the multi-dimensional data structure that is viewable with 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 supported browser.

Each of these layers can be deployed on the same system, or for scalability issues, on separate systems.

Security for Network Data Collection

To read HTTP(S) data streams, a proprietary software module reassembles TCP/IP packet streams. Because the network 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).

Connection Options for Network Data Collection

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 on options.

Monitoring SSL and Forms Traffic

> **Note:**
>
> 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 recommended that you regular review the information available through the Collector Statistics window (select **System**>**Status**>**Collector Statistics** for each collector node) to verify the integrity of the TCP packet stream. Keep a check on the reported TCP and SSL connection errors. Also, the Collector software needs direct access to the physical network interface and that a configuration where multiple servers share a single physical network interface, for example certain blade server types, may not work reliably. Contact your hardware vendor for any queries related to your configuration.

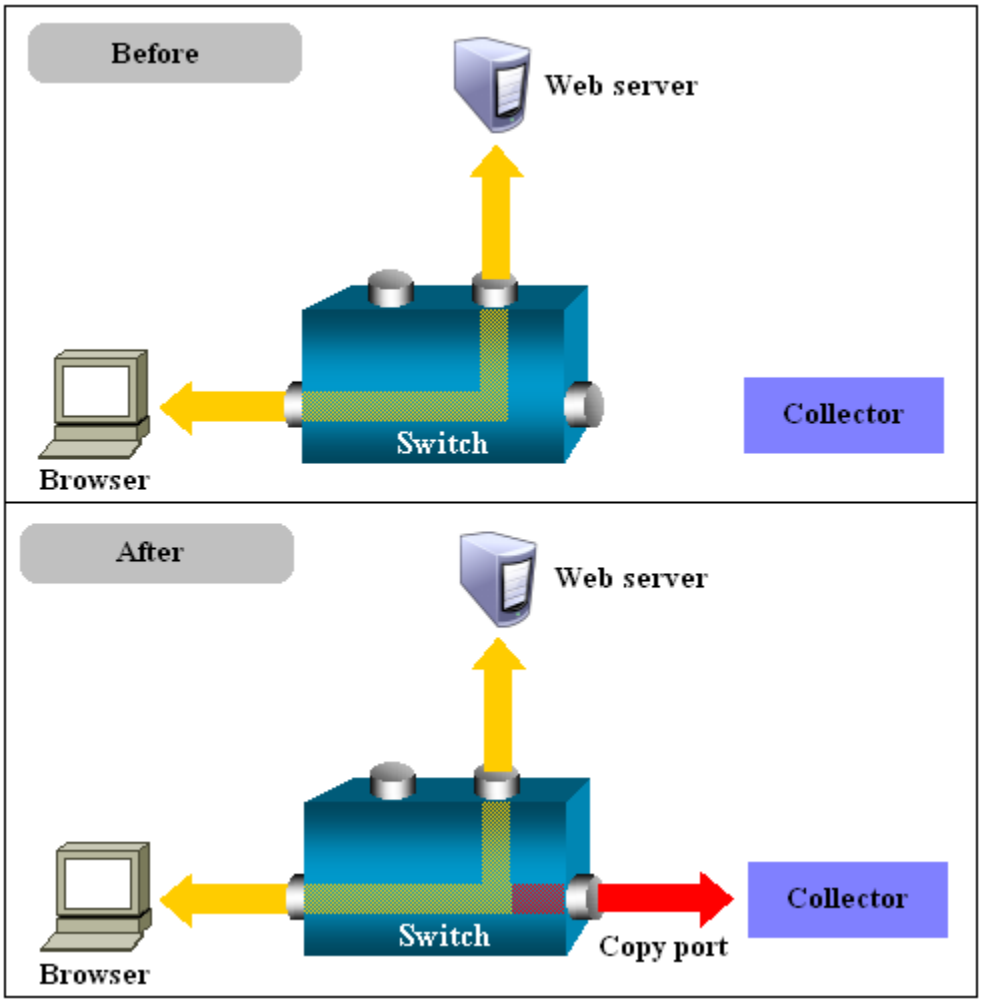
Copy Ports

Copy Port is a switch that builds the Layer 2 forwarding table based on the source MAC address that the switch receives. Once the forwarding table is built, the switch forwards the traffic that is destined for a MAC address directly to the corresponding port.

For example, after the web server MAC in Figure 1-5 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 1-5 Network Connection Using a Copy Port



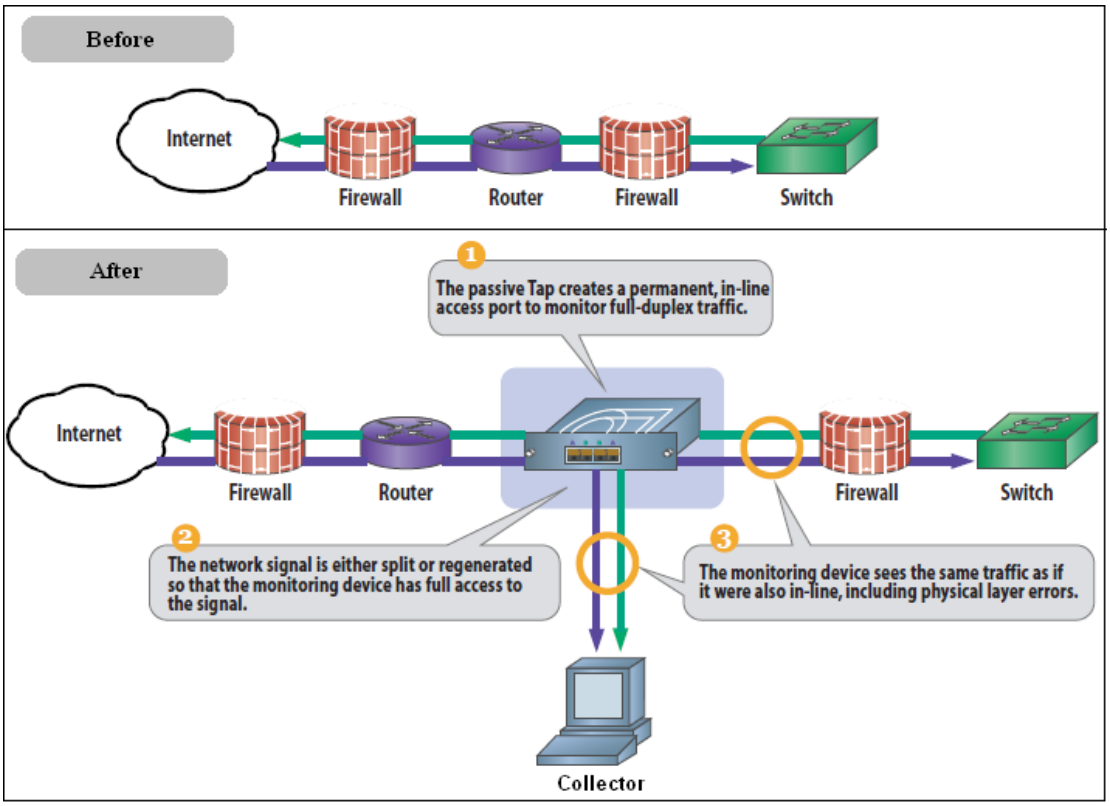
In the configuration shown in the lower part of Figure 1-5, the Collector is attached to a port that is configured to receive a copy of every packet that the browser sends and receives. This port is called a copy port. Copy ports can copy traffic from any or all data ports to a single unused port and prevent bi-directional traffic on the port to protect against backflow or traffic into the network.

Activating a copy port on a switch can have a performance impact. Typically, copy ports support a wide range of configuration options. For more information, about these options, consult your switch documentation or contact the vendor.

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 1-6 illustrates a typical TAP deployment for one Collector.

Figure 1-6 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. During heavy loads, copy ports are prone to packet loss. 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. Aggregation taps are only supported if they maintain the ordering of packets in the packet stream. Reporting accuracy can be impacted when using aggregation taps if the monitor port gets saturated, resulting in packet loss and inaccurate timing information. When capturing data with a network TAP, the use of cascaded TAP configurations is not supported.

It is possible in RUEI to monitor and process data from multiple networks, by either deploying a tap on each network segment and connecting those to a central collector, or by deploying multiple collectors, one on each monitored segment. For more information, see Scaling Scenarios.

Installation Options

A RUEI system can be installed either through a Reporter or a Collector option. Each of these installation options is reviewed in the following sections.

Reporter

A Reporter system processes the data gathered by the Collectors attached to it. After processing, this data is stored in an Oracle database, referred to as the Reporter database. System users can review the collected data through a browser-based interface.

For RUEI to be able to accurately monitor network traffic, and report its results, it needs certain information about your network and application infrastructure. This includes how pages, service function calls, and end users will be identified, the scope of monitoring in your network environment, the monitoring of specific KPIs and SLAs, and the roles and permissions assigned to system users. This information is held in a separate Configuration database.

Collector

A Collector gathers data and submits the data to a Reporter. Multiple Collectors can be attached to the same Reporter. A direct connection is required between the Collector systems and the Reporter system. A collector can be either network based or tag based as described in Planning the Software Installation.

Each Reporter installation also contains a local Collector instance. The Reporter can be configured to just process information gathered by this local Collector (this is a single-server configuration), or to receive information from additional Collectors. The local Collector instance on the Reporter system can also be disabled if not required.

Local and Remote Database Installations

The data available through the Reporter system is stored in an Oracle database, called the Reporter database. The information required by RUEI in order to correctly monitor and report on your web infrastructure, such as information about monitored applications and system users, is held in a separate Configuration part of the database. The 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.

For supported database versions please see the certification list in My Oracle Support.

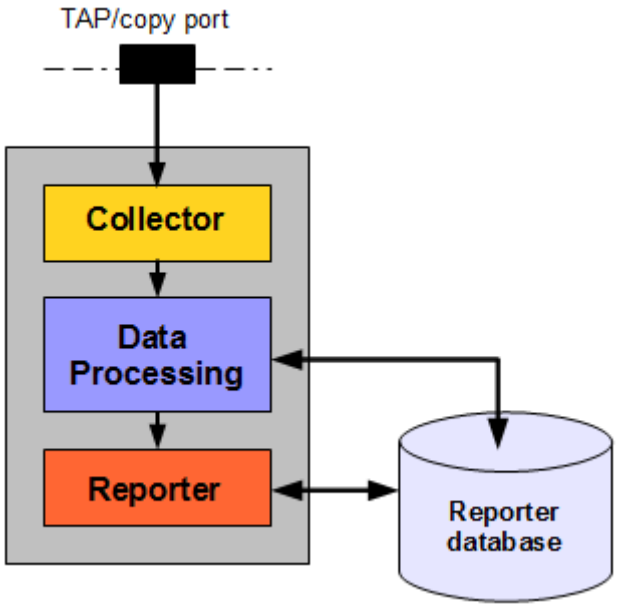
Scaling Scenarios

This section highlights the different deployment scenarios available to you. The selection of the most appropriate deployment scenario is primarily determined by the level of monitored network traffic, your reporting requirements, and the hardware specifications of your deployment systems.

Single-Server Deployment

This is the simplest deployment, and is suitable for monitoring web environments with low to medium levels of traffic. An example is shown in Figure 1-7.

Figure 1-7 Single-Server Deployment

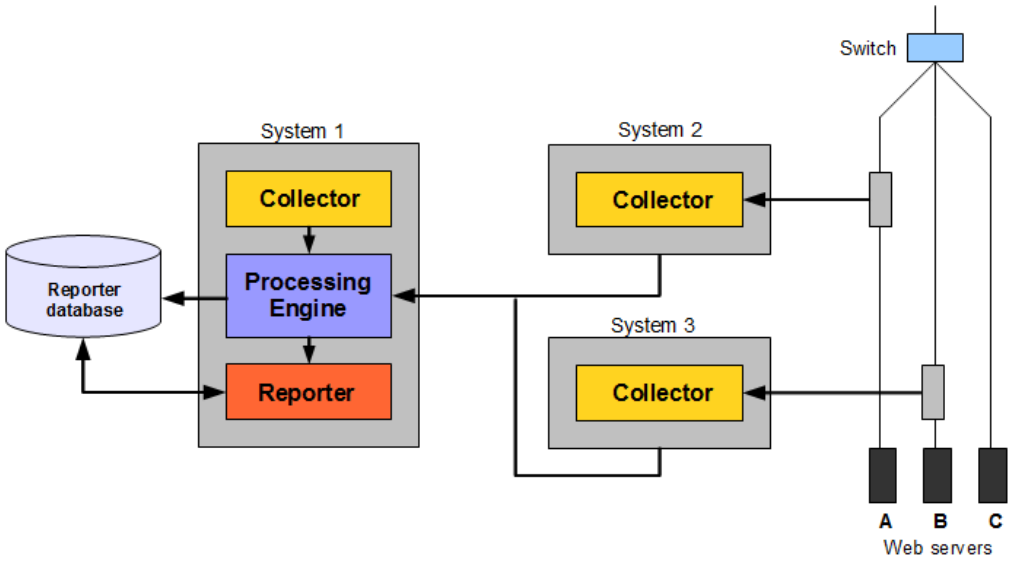


In this deployment, a single system serves as both Collector and Reporter. As explained in the previous section, the Reporter database can reside locally on the Reporter system or on a remote database server.

Multiple-Server Deployment

The use of multiple servers may be considered when there is a need to monitor very high level of 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. Figure 1-8 shows an example of a multiple-Collector deployment.

Figure 1-8 Multiple-Collector Deployment



This features a deployment in which both data lines are monitored in the same reporting environment. This deployment assumes that the traffic on each line is mutually exclusive. It also illustrates 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. Collector instance on the Reporter system (system 1) is disabled.

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 within the DMZ.

The application and infrastructure configuration information held in the database is maintained by the Reporter based on information provided by system users through its browser-based interface. Each Collector uses this information to determine how the data it gathers should be reported.

Server Requirements

The required minimum system specifications for the selected configuration (as explained in Installation 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 Connection Options for Network Data Collection, both copper and fibre-based network cards may be required. If necessary, consult both your network and systems management teams.

Network Cards Within Bonded Groups

Monitoring of network traffic using network cards that are part of a bonded group is not supported.

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

Single-Server Requirements

Table 1-3 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 1 TB HDD free space.[1,2,3]
Network interfaces	When using a network-TAP device[4], a minimum of three network interfaces are required: • Two interfaces for network traffic capturing. • One interface for network services.
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-10 or equivalent storage configurations are strongly recommended.

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

3 The use of an NFS share for local data (that is, *$RUEI_DATA* and *$RUEI_HOME*) is not supported. This restriction does not apply to *$RUEI_DATA*`/processor/data` and *$RUEI_DATA*`/collector/wg/REPLAY`.

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

Reporter Requirements

Table 1-4 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 1 TB HDD free space[1,2,3].
Network interfaces	A minimum of one 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-10 or equivalent storage configurations are strongly recommended.
2 This may need to be increased if Enriched data exchange is enabled.
3 The use of an NFS share for local data (that is, *$RUEI_DATA* and *$RUEI_HOME*) is not supported. This restriction does not apply to *$RUEI_DATA*/processor/data and *$RUEI_DATA*/collector/wg/REPLAY.

Collector Requirements

The requirements for Collector systems are shown in Table 1-5.

Table 1-5 Collector System Minimum Requirements

Element	Requirement
CPU	64-bit Intel or AMD dual-core processor or equivalent.
Memory	16 GB.
Disk space	Minimum 250 GB HDD free space[1].
Network interfaces	When using a network-TAP[2] device, a minimum of three network interfaces are required: • Two interfaces for network traffic capturing[3]. • 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 The use of an NFS share for local data (that is, *$RUEI_DATA* and *$RUEI_HOME*) is not supported. This restriction does not apply to *$RUEI_DATA*/processor/data and *$RUEI_DATA*/collector/wg/REPLAY.
2 Capturing data with a network-TAP device prevents the use of a cascaded TAPs configuration.
3 For up and down stream traffic. The use of TAPs that integrate up and down stream traffic on one line (that is, link aggregation TAPs) is not recommended.

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 the traffic. Any physical deployment requirements (such as space limitations, distances, power planning, rack space and layout, or cabling) should be identified.

You can use the checklist presented in Installation Checklist to capture the information.

Forms-Based Traffic

If you are planning to monitor Forms-based traffic, the memory requirements may be higher than those outlined in Server Requirements. 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 (FSR) facility, you need to configure additional storage capacity. This is explained in Full Session Replay Storage Requirements.

Encrypted Traffic

If a significant level of the monitored traffic is encrypted, it 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), it is *strongly* recommended that you consider a split-server deployment. Alternatively, consider the use of a remote database server. 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 server.

Data Retention Policies

The availability of specific data within the Data Browser, as well as reports based on that data, depends on the amount of available disk space on the Collector and Reporter systems, as well as the amount of database space available on the Reporter system.

Data gathered during monitoring is first written to log files, stored on the Collector system. These files are copied to and processed by, the Reporter to populate the database that holds the multi-dimensional data structure viewable through the Data Browser and reports. These temporary log files are automatically removed from the Collector system after three days, and from the Reporter system (by default) after seven days.

The size of the database user quota for the Reporter system is configurable during installation. By default, it is set to 500 GB. It is important to understand that data is consolidated when it is no longer required by the Reporter's defined retention policy. For example, by default, daily information about the last 32 days is retained. Daily information older than this is consolidated into the monthly information. Similarly, monthly information is consolidated into yearly information.

RUEI maintains data at several aggregation levels, whose retention is configured in days. The following describes the various aggregation levels and their default values:

- Instance: 8 days
- 5-minute: 15 days
- Hourly: 32 days
- Daily: 90 days
- Monthly: 60 months

These numbers can be fine-tuned per category of data (app, suite, service, SLA) and beyond that per individual type (for example, All Pages or Failed Pages). The default value for enriched data exchange is 8 days for each type.

DB space is about 5 GB per period each. This is heavily dependent on load and diversity of traffic. You should occasionally check the reporter data retention screen, especially in the first month, to verify enough disk space is available.

Statistics data is configurable from the CLI. However, statistics retention is not configurable, while User flow completion and fusion product retention are only configurable from the command line.

Minimum and maximum values for data retention settings are automatically determined. Less-detailed aggregation levels must always have at least as much retention as more-detailed aggregation levels.

Be aware that a new RUEI installation will grow quickest during the first 32 days. The growth rate will slow down. The growth rate depends on monitored traffic levels.

Full Session Replay Storage Requirements

If you are planning to make use of the Full Session Replay (FSR) 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 and the guidance on storage requirements, is described in the rest of this section. This procedure must be repeated for each Collector for which full session replay information is required.

Configuring Additional Storage for Full Session Replay

The procedure described below assumes that you have a fully operational system, and that FSR has been enabled. 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 running 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 running the following command:

   ```
   appsensor start wg
   ```

6. Calculate the required storage capacity. To do so, multiply 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

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

Memory Requirements

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

For each Collector system, each 100 concurrent hits require 2 MB, and each 1000 SSL connections require 1 MB. In addition, up to 600 MBps of network traffic can be buffered before individual TCP sessions start to be dropped. Up to 600 MBps should also be assumed for content checks (such as XPath queries and error strings). If you define a large number of content checks, or specify that they contain NLS character sets, the memory required may increase.

Software Requirements

The following GNU/Linux distributions are supported:

Oracle Linux

- Oracle Linux 7, 64-bit, both Intel and AMD compatible.
- Oracle Linux 8, 64-bit, both Intel and AMD compatible.

RedHat Enterprise Linux

- RedHat Enterprise Linux 7, 64-bit, both Intel and AMD compatible.
- RedHat Enterprise Linux 8, 64-bit, both Intel and AMD compatible.

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.

Network Requirements

- All server system clocks should be synchronized through 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 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 Configuring a Failover Collector System), the primary and secondary Collector systems need to be able to contact each other using ICMP.

Collector-Reporter Bandwidths

The amount of 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. 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.

Client Requirements

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

- Mozilla Firefox 75 (and above)
- Internet Explorer 11
- Microsoft Edge
- Safari 12 and 13.
- Google Chrome 81 (and above).

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).

> **Note:**
>
> 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.

2
Installing the RUEI Software

This chapter describes the prerequisites and the procedure for installing each of the RUEI components. The procedure for upgrading an existing RUEI 13.x.x.x installation to release 13.5.1.0 is described in Upgrading to RUEI 13.5.The post-installation configuration procedure is described in Configuring RUEI

> **Note:**
>
> Before attempting to install RUEI components on any system, make sure that the latest OpenSSL patches are applied for your operating system using the appropriate commands (for example, `yum update` or `up2date`). Applying the latest OpenSSL patches helps improve the security of the system.

Prerequisites

This section describes the steps that should be taken before installing the RUEI software. Ensure that *all* preconditions described in this section are met before proceeding with the installation process.

> **Note:**
>
> RUEI installation is supported for RedHat Enterprise/Oracle Linux 7.x, 8.x and 9.x. However for maximum reliability and security, upgrade the system to the latest patch version before installing RUEI.

Planning the Software Installation

For an introduction to RUEI data collection, see Data Collection. The following installation data collection options are available:

- Network data collector: This option collects data that passes through the network and was the default option in previous releases and requires either a local or remote collector.
- Tag data collector: This option, also called tag based monitoring, collects data by monitoring the request and processing of a specific web URL (the tag) which is inserted into all pages.

Table 2-1 Installation Overview and Data Collection Methods

	Network	Tag
Requirement	Access to network traffic to perform Network Protocol Analysis.	Access to application templates to insert Javascript code.
Single Server (as in Figure 1-7)	Use the `reporter` option when running the installer as described in Installing the Reporter Software (installs network data collector automatically).	Use the `reporter-tag` option when running the installer as described in Installing the Reporter Software (installs tag based data collector automatically).

Planning the Software Installation Location

Depending on the installation location of the Reporter 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 for the disk partitioning phase.

The following table shows the disk space requirements for the RUEI installation components.

Table 2-2 Required Disk Space Specifications

Partition	Min. Required Disk Space (GB)	Component
Reporter / Single Server	.	.
ORACLE_BASE (default /u01/app/oracle) 1	600	Database
RUEI_HOME (default /opt/ruei)	5	RUEI Software
RUEI_DATA (default /var/opt/ruei/)	400	RUEI Data
Collector / Tag Collector	.	.
RUEI_HOME (default /opt/ruei)	5	RUEI Software
RUEI_DATA (default /var/opt/ruei/)	200	RUEI Data
Database	.	.
ORACLE_BASE (default /u01/app/oracle) 1	600	Database

This means that for a stand-alone RUEI server installation, a minimum of 1005 GB is required.

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

Configuring the Network Interface for Network Data Collection

If you want to use network data collection:

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.

> **Note:**
>
> 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 the `/etc/sysconfig/network-scripts/ifcfg-ethX` file (where *X* represents the necessary network interface). Alternatively, use the graphical utility **system-config-network** to perform the above actions.

Configuring Operating System Security

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

You must ensure that Security Enhanced Linux (SELinux) is disabled. To disable SELinux set `SELINUX=disabled` in the `/etc/selinux/config` file. This is necessary for the correct operation of RUEI. Changing the SELinux setting requires rebooting the system so that the entire system can be re-labelled.

Please configure the operating system's firewall, if enabled, to allow access to the respective services, like (by default) TCP port 1521 for the database listener TCP port 443 for the web interface and TCP port 22 for the SSH server.

For security reasons, it is recommended that you select the **Encrypt System** check box during operating system installation so that all sensitive data is stored in a secure manner. A passphrase is required during booting the system.

Verify NTP Daemon Operation for Network Data Collection

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

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

RedHat Enterprise/Oracle Linux

In RedHat Enterprise/Oracle Linux, NTP synchronization, timezone and other clock related settings are managed through the **timedatectl** tool:

> **Note:**
>
> This command will enable the *NTP enabled* option, which should also enable *NTP synchronized* option as well if the time server is set properly in the following chrony config file:
>
> `/etc/chrony.conf`

```
# timedatectl
Local time: Wed 2017-10-04 09:42:09 BST
Universal time: Wed 2017-10-04 08:42:09 UTC
RTC time: Wed 2017-10-04 08:42:09
Time zone: Europe/London (BST, +0100)
NTP enabled: yes
NTP synchronized: yes
RTC in local TZ: no
DST active: yes
Last DST change: DST began at
Sun 2017-03-26 00:59:59 GMT
Sun 2017-03-26 02:00:00 BST
Next DST change: DST ends (the clock jumps one hour backwards) at
Sun 2017-10-29 01:59:59 BST
Sun 2017-10-29 01:00:00 GMT
```

Verify that **NTP enabled** and **NTP synchronized** show **yes**.

By default, the `chrony` package is installed to provide NTP synchronization. If time is not synchronized, in `/etc/chrony.conf`, provide at least one valid (and reachable) timeserver through at least one `server` directive.

After editing `/etc/chrony.conf`, restart the `chronyd` daemon:

```
systemctl restart chronyd
```

After that, the `timedatectl` command should display **NTP synchronized** as **yes**.

To see whether the service is active and which time server is used, run `systemctl status chronyd.service -l` as shown in the following example.

```
systemctl status chronyd.service -l

chronyd.service - NTP client/server
   Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled; vendor
preset: enabled)
   Active: active (running) since Tue 2020-04-14 12:59:17 PDT; 2h 14min ago
     Docs: man:chronyd(8)
           man:chrony.conf(5)
 Main PID: 12783 (chronyd)
   Memory: 324.0K
   CGroup: /system.slice/chronyd.service
           \u2514\u250012783 /usr/sbin/chronyd

Apr 14 12:59:17 host1 systemd[1]: Starting NTP client/server...
Apr 14 12:59:17 host1 chronyd[12783]: chronyd version 3.2 starting (+CMDMON
+NTP +REFCLOCK +RTC +PRIVDROP +SCFILTER +SECHASH +SIGND +ASYNCDNS +IPV6
+DEBUG)
Apr 14 12:59:17 host1 chronyd[12783]: Frequency -8.954 +/- 7.631 ppm read
from /var/lib/chrony/drift
Apr 14 12:59:17 host1 systemd[1]: Started NTP client/server.
Apr 14 13:01:27 host1 chronyd[12783]: Selected source 10.128.128.1
```

Installing the RUEI Prerequisites

The procedure described in this section is only required for a Reporter system. The procedure depends on whether you are using RedHat Enterprise/Oracle Linux 7.*x*, 8.*x* or 9.*x*.

Installing All Requirements Using a Yum Repository

Depending on the OS flavor (RedHat or Oracle) and version you use, you may also need to enable the use of the "optional" (or "optional latest") repository to satisfy all dependencies.

The procedure depends on whether you are using RedHat Enterprise/Oracle Linux 7.*x*, 8.*x* or 9.*x*.

- Installing RedHat Enterprise/Oracle Linux 7.x Prerequisites
- Installing RedHat Enterprise/Oracle Linux 8.x Prerequisites
- Installing RedHat Enterprise/Oracle Linux 9.x Prerequisites

Installing RedHat Enterprise/Oracle Linux 7.x Prerequisites

After performing a minimum RedHat Enterprise / Oracle Linux 7.x installation, complete the following. A graphic environment is not required.

Install the necessary Reporter prerequisite packages running the following commands:

```
yum -y install httpd \
mod_ssl \
php \
php-ldap \
```

```
php-soap \
php-mbstring \
librsvg2-tools \
rsync \
libpcap \
ncurses \
zlib \
net-snmp \
net-snmp-libs \
net-snmp-utils \
*-fonts
```

Installing RedHat Enterprise/Oracle Linux 8.x Prerequisites

After performing a minimum RedHat Enterprise / Oracle Linux 8.x installation, complete the following. A graphic environment is not required.

Install the necessary Reporter prerequisite packages running the following commands:

```
yum -y install httpd \
mod_ssl \
php \
php-ldap \
php-soap \
php-mbstring \
php-json \
php-xml \
librsvg2-tools \
rsync \
libpcap \
ncurses \
zlib \
net-snmp \
net-snmp-libs \
net-snmp-utils \
*-fonts
```

Installing RedHat Enterprise/Oracle Linux 9.x Prerequisites

After performing a minimum RedHat Enterprise / Oracle Linux 9.x installation, complete the following. A graphic environment is not required.

Install the necessary Reporter prerequisite packages running the following commands:

```
yum -y install httpd \
mod_ssl \
php \
php-ldap \
php-soap \
php-mbstring \
php-json \
php-xml \
librsvg2-tools \
rsync \
```

```
libpcap \
ncurses \
zlib \
net-snmp \
net-snmp-libs \
net-snmp-utils \
*-fonts \
compat-openssl11
```

Installing Oracle Database

Download and install Oracle Database Enterprise Edition from the Oracle database software downloads page at the following location:

https://www.oracle.com/database/technologies/oracle-database-software-downloads.html

The procedure for installing the Oracle database is fully described in the product documentation. It is available from the Oracle Database Documentation Library. The path user and group names used in this guide are based on the Oracle database product documentation.

> **Note:**
>
> For supported database versions, please see the certification list in My Oracle Support.

> **Note:**
>
> While Oracle Database is also available as an RPM package, instructions and scripts in this guide assume the .zip packages and Universal Installer are used to install the database software.

Obtaining the RUEI Software

The RUEI software is available from the Oracle Software Delivery Cloud web site (`http://edelivery.oracle.com`). To download the software, do the following:

1. Sign in to the Oracle Software Delivery Cloud web site.
2. From the Category search text field, enter "Oracle Real User Experience Insight" and select it from the drop-down list.
3. From the search results, click " DLP: Oracle Real User Experience Insight 13.5.1.0.0". It will be added to your Cart.
4. Click **Checkout**.
5. Check to make sure the contents of your Cart are correct. Click **Continue**.
6. Accept the *Oracle License Agreement* and click **Continue**.

7. Click **Download**.

Unpacking the RUEI Software

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

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

The following directories and files are extracted and provide the software required to complete the RUEI installation:

- `/root/ruei/db_templates/ruei_database.dbt`
- `/root/ruei/mkstore/mkstore-11.2.0.4.0.tar.gz`
- `/root/ruei/extra/oracledb`
- `/root/ruei/extra/ruei-clean.sh`
- `/root/ruei/extra/ruei-collector-failover.sh`
- `/root/ruei/extra/ruei-migrate`
- `/root/ruei/extra/ruei-reporter-failover.sh`
- `/root/ruei/extra/ruei.conf`
- `/root/ruei/extra/upgradeCheck.php`
- `/root/ruei/rpms/ux-*.rpm`
- `/root/ruei/ruei-check.sh`
- `/root/ruei/ruei-install.sh`
- `/root/ruei/ruei-prepare-db.sh`
- `/root/ruei/ruei-upgrade.sh`
- `/root/ruei/sql_scripts/*.sql`

Generic Installation Tasks

The 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).

Check The RUEI Configuration File

The `/etc/ruei.conf` file specifies the settings used within your installation. A template of this file is provided in the `/root/ruei/extra` directory of the RUEI distribution zip. All components in your RUEI environment (such as the remote database and Collectors) require the same global `/etc/ruei.conf` configuration file.

> **Note:**
>
> Be aware that all variables specified in the following table are the values used throughout this guide, and can be modified as required.

Table 2-3 RUEI Configuration Settings

Setting	Description	Value
RUEI_HOME	Home directory of the RUEI software. Do not set to any path beginning with /var/opt/ruei.	/opt/ruei

> **Note:**
>
> The directory name cannot exceed 50 characters in length. RUEI_HOME and RUEI_DATA must be independent paths. For example, if RUEI_HOME is /opt/ruei, then RUEI_DATA cannot be set to /opt/ruei/data. Also, RUEI_HOME cannot be set to a subdirectory of /var/opt/ruei and that RUEI_DATA cannot be set to a subdirectory of /opt/ruei.

Table 2-3 (Cont.) RUEI Configuration Settings

Setting	Description	Value
RUEI_DATA	Directory for RUEI data files. Do not set to any path beginning with /opt/ruei. **Note:** The directory name cannot exceed 50 characters in length. RUEI_HOME and RUEI_DATA must be independent paths. For example, if RUEI_HOME is /opt/ruei, then RUEI_DATA cannot be set to /opt/ruei/data. Also, RUEI_HOME cannot be set to a subdirectory of /var/opt/ruei and that RUEI_DATA cannot be set to a subdirectory of /opt/ruei.	/var/opt/ruei
RUEI_USER	The RUEI operating system user.	moniforce
RUEI_GROUP	The RUEI operating system group.	moniforce
RUEI_DB_INST	The database instance name. **Note:** The database instance name cannot exceed 8 characters in length.	ux

Table 2-3 (Cont.) RUEI Configuration Settings

Setting	Description	Value
RUEI_DB_TSCONF	The configuration tablespace name **Note:** A database table space name cannot exceed 30 characters in length.	UXCONF
RUEI_DB_TSSTAT	The statistics tablespace name **Note:** A database table space name cannot exceed 30 characters in length.	UXSTAT
RUEI_DB_USER	The database user name. **Note:** The database user name cannot exceed 30 characters in length.	UXINSIGHT
RUEI_DB_TNSNAME	The Reporter database connect string. **Note:** The alias name cannot exceed 255 characters in length.	uxinsight

Table 2-3 (Cont.) RUEI Configuration Settings

Setting	Description	Value
RUEI_DB_TNSNAME_CFG	The Reporter database connect string. **Note:** *RUEI_DB_TNSNAME* is the default for a Reporter system.	$RUEI_DB_TNSNAME or config
RUEI_DB_TNSNAME_BI	The export database connect string. **Note:** The database user name cannot exceed 30 characters in length.	uxinsight
MKSTORE_BIN	The location of the mkstore utility.	/usr/local/mkstore/mkstore

Table 2-3 (Cont.) RUEI Configuration Settings

Setting	Description	Value
TZ	The PHP timezone setting.	Europe/Amsterdam

> **Note:**
>
> This should be the appropriate timezone setting, and must be valid for Linux, PHP and the Oracle Database. For Linux, you can use the `tzselect` utility, and for PHP use the following location: http://www.php.net/manual/en/timezones.php. See the Oracle Database Globalization Support Guide for more information on time zones for the Oracle Database. Please note that it is required to set `ORA_SDTZ` (the database session time zone) to TZ in *ruei.conf*. See the *ruei.conf* installation template file in `/root/RUEI/extra` for instructions on how to do this.

DEFAULT_TABLESPACE	The name for the default RUEI tablespace.	

Table 2-3 (Cont.) RUEI Configuration Settings

Setting	Description	Value
REMOTE_DB	Default is 0. Set to 1 for remote database. **Note:** Necessary when you do not have command-line access to the remote database host and running ruei-prepare-db.sh there is not an option. (See Setting up RUEI Against a Remote Database Service)	
DBCONNECT	Fully qualified database connection string to remote database	
INSTANTCLIENT_DIR	The path to the Oracle Instant Client library, needed for data processing and the UI. **Note:** The default value corresponds to Oracle Instant Client version 21.	`/usr/lib/oracle/21/client64`
JAVA_HOME	The path to your Java 8 Runtime Environment installation.	`/usr/java/jre`

Important

The `TZ`, `RUEI_HOME`, `RUEI_DATA`, `RUEI_USER` and `RUEI_GROUP` settings described in Table 2-3 *must* be specified in terms of literal values. Therefore, the following is not permitted:

```
RUEI_BASE=/my/ruei/dir
export RUEI_HOME=$RUEI_BASE/home
```

> **Note:**
>
> If you change settings in `/etc/ruei.conf` after the installation of a RUEI system, you must restart system processing to make these changes effective (System > Maintenance > System reset > Restart system processing).

Failover Reporter Configuration Settings

Table 2-4 shows the settings that are used to configure a failover Reporter, and are only relevant to Reporter systems. For information on the configuration procedure, see Configuring a Failover Reporter System.

Table 2-4 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 2-5 shows the settings that are used to configure a failover Collector, and are only relevant to Collector systems. For information on the configuration procedure, see Configuring a Failover Collector System.

Table 2-5 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.

An example of the configuration file is included in the RUEI distribution pack. You can copy it to /etc by issuing the following command:

```
cp /root/ruei/extra/ruei.conf /etc/
```

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

Creating a RUEI User and Directories

1. Create the `moniforce` group and *`RUEI_USER`* 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
   ```

   > **Note:**
   >
   > The login shell for the `moniforce` (*`RUEI_USER`*) user must be set to `/bin/bash`.

2. The RUEI directory locations are flexible, however it is necessary to use the *exact* directory name described as configured in the `/etc/ruei.conf` file. Create the RUEI application root directory running the following commands:

   ```
   mkdir -p /opt/ruei
   chmod 755 /opt/ruei
   ```

   > **Note:**
   >
   > The specified $RUEI_HOME and $RUEI_DATA directories must have 755 permissions defined for them. For more information on these directories, see Table 2-3 .

3. Ensure the file is readable by the RUEI_USER user by issuing the following commands:

   ```
   chmod 644 /etc/ruei.conf
   chown moniforce:moniforce /etc/ruei.conf
   ```

Installing Java

For Reporter and Collector systems, you need to install the Java Runtime Environment (JRE) version 8. Please download a 64 bit (x64) Linux version from https://www.java.com/en/download/linux_manual.jsp

The installation instructions below (and default value of `JAVA_HOME` in `/etc/ruei.conf`) are based on the non-RPM (`.tar.gz`) version

1. Run the following commands:

   ```
   mkdir -p /usr/java
   chmod 755 /usr/java
   cd /usr/java
   tar xzf <path-of-download>/jre-8u*-linux-x64.tar.gz
   ```

2. This installs the necessary Java software in the directory `/usr/java/jre1.8.0_<version>`. To make the install directory version independent, create a more generic symlink running the following command:

   ```
   ln -s /usr/java/jre1.8.0_* /usr/java/jre
   ```

System Pre-installation Check

To verify if the system is ready for RUEI to be installed, it is advised to run the RUEI system check.

Running the System Check

To run the system check:

1. `cd /root/ruei`
2. `./ruei-check.sh <installation option> <check>`

Depending on the installation option for the system, the check will need to be called with different arguments. The following table shows a list of available arguments.

Table 2-6 RUEI System Check Command Line Arguments

Installation Option	System pre-installation check
Single Server	./ruei-check.sh *reporter* system --role *reporter*
Reporter	.
• With local Database	./ruei-check.sh *reporter* system --role *reporter*
• Without local Database	./ruei-check.sh *reporter* system --role *reporter* --with-remote-db
Collector	./ruei-check.sh *collector* pre-install --role *collector*
Database	./ruei-check.sh *database* pre-install --role *database*

Note 1: Single Server and Reporter have the same ruei-check.sh command line because of the similar system requirements.

Note 2: In case of installation issues, please provide Oracle Customer Support with the RUEI check log file `/tmp/ruei-check.log`.

Note 3: Make sure you had set up and checked the `/etc/ruei.conf` file on each system as described in Check The RUEI Configuration File.

Reporter Installation

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

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.

PHP Configuration

1. Ensure that the web server starts automatically after re-boot by running the following command:
   - **RedHat Enterprise / Oracle version 7.x/8.x:**

     ```
     systemctl enable httpd
     ```

   - **RedHat Enterprise / Oracle version 9.x:**

     ```
     systemctl enable httpd
     systemctl enable php-fpm
     ```

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

   ```
   session.gc_maxlifetime = 14400
   memory_limit = 192M
   upload_max_filesize = 128M
   post_max_size = 128M
   ```

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
```

Securing Apache Web Server

In order to protect sensitive data on RUEI, it is *strongly* recommended that access to the Reporter interface is restricted to HTTPS. Use the following command as the `root` user:

```
sed -i -e 's/^Listen 80/#Listen 80/' /etc/httpd/conf/httpd.conf
```

In addition to the already disabled SSLv2, also disable support for SSLv3 in the web server using the following command as the `root` user, if neccessary.

```
sed -i -e 's/^SSLProtocol all -SSLv2/SSLProtocol all -SSLv2 -SSLv3/' /etc/httpd/
conf.d/ssl.conf
```

Changing MPM Module in Apache Configuration

In order to enable PHP execution, you will need to modify the `/etc/httpd/conf.modules.d/00-mpm.conf` file.

> **Note:**
>
> When running on RedHat Enterprise / Oracle Linux 9.*x*, it is not required to change the MPM Module.

Run the following commands as the `root` user:

```
sed -i -e 's/^LoadModule mpm_event_module/#LoadModule
mpm_event_module/' /etc/httpd/conf.modules.d/00-mpm.conf


sed -i -e 's/^#LoadModule mpm_prefork_module/LoadModule
mpm_prefork_module/' /etc/httpd/conf.modules.d/00-mpm.conf
```

Installing the Oracle Database Instant Client

Download the Oracle Database Instant Client (Basic) and SQL*Plus (version 19.x and above) package from Oracle Instant Client Downloads for Linux x86-64 (64-bit), and install by running the following commands as the `root` user:

```
cd /root/ruei/ic
rpm -Uhv oracle-instantclient*-basic-*.rpm
rpm -Uhv oracle-instantclient*-sqlplus-*.rpm
```

Installing the php-oci8 Module

As a prerequisite download and install the Oracle database Instant Client SDK (devel) package for your version of PHP, based on your yum, for your version of Instant Client from Oracle Instant Client Downloads for Linux x86-64 (64-bit).

You can find detailed installation instructions for the `php-oci8` module at https://www.php.net/manual/en/oci8.installation.php

> **Note:**
>
> The version of oci8 you need to install depends on your PHP version. Consult the **Description** field at https://www.php.net/manual/en/oci8.installation.php .

Example commands:

1. Install the Oracle database Instant Client SDK (devel) package:

   ```
   yum install php-pear php-devel
   yum install <path-of-download>/oracle-instantclient-devel-*.x86_64.rpm
   ```

2. `pear config-set http_proxy <url_of_proxy>:<port>`

   > **Note:**
   >
   > This step is optional, if a proxy is needed for internet access.

3. `pecl install oci8-<version>`

> **Note:**
>
> When prompted for a path to the library, you can choose the default of `autodetect`.

4. Create a file named `/etc/php.d/oci8.ini` and add the following to it:

```
#enable oci8 extension module
extension=oci8.so
```

5. Restart httpd:

```
systemctl restart httpd
```

> **Note:**
>
> If your OS is RedHat Enterprise / Oracle version 9.x, also restart php-fpm:
>
> ```
> systemctl restart php-fpm
> ```

Creating the Reporter Database Instance

> **Note:**
>
> If you intend to use RUEI with Enterprise Manager, you require the RUEI wallet password described below. Without the correct wallet password you cannot associate RUEI with Enterprise Manager.

The procedure described in this section should be skipped if you are installing a secondary (failover) Reporter system (see Configuring a Failover Reporter System), and you should continue at Installing the Reporter Software.

The Reporter 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 Generic Database Instance Setup.

If you are using a remote database and you do not have command-line access to the remote database server because, for example, you want to configure RUEI using a “Pluggable Database", see Setting up RUEI Against a Remote Database Service.

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. This script will only run on Linux. If you are installing the Oracle database on a different operating system, see Generic Database Instance Setup.
- `sql_scripts`: this directory contains a number of SQL scripts that are called by the `ruei-prepare-db.sh` script.
- `db_templates`: this directory contains templates for the RUEI database instance that is created by the `ruei-prepare-db.sh` script.
- `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 RUEI System Check Tool.

For creating the database autologin wallet in this section and, optionally, for the integration with Enterprise Manager later on, a specific version of the "mkstore" utility is needed. You can set up this utility as follows. This needs to be done on the system where the database instance (RUEI_DB_INST) will be created as well as the reporter if those are separate systems.

- Run the following commands:

```
cd /usr/local
tar xzf /root/ruei/mkstore/mkstore-11.2.0.4.0.tar.gz
```

- This installs the mkstore utility to /usr/local/mkstore-11.2.0.4.0. To make the install directory version independent, create a more generic symlink using the following command:

```
ln -s /usr/local/mkstore-11.2.0.4.0 /usr/local/mkstore
```

- Make the following change to /etc/ruei.conf:

```
* export MKSTORE_BIN=/usr/local/mkstore/mkstore
```

- If you are executing these steps on a database server separate from the reporter system, make the following change to /etc/ruei.conf:

```
* export JAVA_HOME=$ORACLE_HOME/jdk/jre
```

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

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

> **Note:**
>
> These files will be created in the RUEI_DATA directory.

The RUEI configuration file (`/etc/ruei.conf`) also needs to be present on the database server and configured as described in Check The RUEI Configuration File and the instructions for setting up `mkstore`, given earlier in this section.

Do the following:

1. Copy the `ruei-prepare-db.sh` and `ruei-check.sh` scripts, and the `sql_scripts` and `db_templates` directories to the server on which you intend to run the database instance, and make them executable for the `oracle` user. These scripts and directories can be found in the RUEI distribution zip (`/root/ruei/`).
2. Review the settings in the `/etc/ruei.conf` file to match your needs as described in Check The RUEI Configuration File. If you want to use different names for the configuration and statistics tablespaces make sure these names are set before continuing. The same tablespace names must be used on the RUEI reporter and on the remote database.
3. Log in 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 Reporter database user password.

   > **Note:**
   >
   > The database password is also used as the Oracle wallet password. Both passwords must be 8-30 characters in length, and contain both numbers and letters. For information on changing the Oracle wallet password, please consult the appropriate Oracle documentation.

   . This enables the RUEI application to login to the database automatically. The script also creates the "connection data" files for you now.

   The script also prompts you for a default tablespace name to be used for this installation, and then creates the connection data files.

   Run the following commands:

   ```
   chmod +x ruei-prepare-db.sh ruei-check.sh
   chmod -R +r /home/oracle/sql_scripts/
   chmod -R +r /home/oracle/db_templates/
   export ORACLE_HOME=/u01/app/oracle/product/12.1.0/dbhome_1
        Note: This line requires customization based on your database
   version and installation path.
   ./ruei-prepare-db.sh create
   ```

   You are prompted whether you want the installation script to check your system. It is recommended that you do so. The checks performed are fully described in RUEI System Check Tool.

   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 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. Log in 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 through `cron` running 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'
```

To validate the Database Instance creation, run the RUEI post-installation check using the following commands:

For Reporter with local Database or a Single Server system:

```
cd /root/ruei/
 ./ruei-check.sh database post-install --role reporter
```

For a Database server system:

```
cd /root/ruei/
./ruei-check.sh database post-install --role database
```

Installing the Reporter Software

The procedure described in this section is relevant to all configurations described in Scaling Scenarios and Planning the Software Installation. Installing the reporter software also installs the collector and processor software.

1. Make the `apache` and `moniforce` members of two additional groups running the following commands:

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

2. Go to the directory that holds the RUEI software, and run the following commands:

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

3. Use one of the following options to run the pre installation check and install the reporter software:

   - If you are installing a reporter in a split server configuration or you want to use only network based data collection as described in Planning the Software Installation:

```
./ruei-check.sh reporter pre-install
./ruei-install.sh reporter
```

> **Note:**
>
> Investigate and fix any issues reported by the per installation check, before continuing with the RUEI reporter software installation.

- If you are installing on a single server and you want to use tag based data collection as described in Planning the Software Installation (This option also supports network based data collection):

```
./ruei-check.sh reporter,tag-server pre-install
./ruei-install.sh reporter-tag
```

> **Note:**
>
> Investigate and fix any issues reported by the per installation check, before continuing with the RUEI reporter software installation.

For information on monitoring an application based on tagging, see Defining Applications in the *Identifying and Reporting Web Pages* chapter of the *RUEI Users Guide*.

4. Re-start the Apache web server running the following command:

   For Linux 7.x/8.x

   ```
   /bin/systemctl restart httpd.service
   ```

5. As the `root` user, add the following lines to the `.bash_profile` file of the *`RUEI_USER`* (*`RUEI_DATA`*`/.bash_profile`):

   ```
   source /etc/ruei.conf
   source $RUEI_HOME/bin/env.sh
   ```

6. Verify that the RUEI software was correctly installed:

   - If you are installing a reporter in a split server configuration or you want to use only network based data collection as described in Planning the Software Installation:

     ```
     ./ruei-check.sh reporter post-install
     ```

   - If you are installing a reporter in a split server configuration or you want to use only tag based data collection as described in Planning the Software Installation:

     ```
     ./ruei-check.sh reporter,tag-server post-install
     ```

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

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

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

You are prompted to enter and confirm the password.

Password Requirements

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.

Remote Tag Data Collector Installation

The procedure described in this section is only relevant to remote tag-based data Collector systems, see Planning the Software Installation and Scaling Scenarios.

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

1. Make sure that the rsync and libpcap packages are installed. For example, enter the following commands to install the packages using Yum:

   ```
   yum -y install rsync
   yum -y install libpcap
   ```

2. Install Apache running the following command:

   ```
   rpm -Uhv httpd-2.2.15-*..x86_64.rpm
   ```

3. Ensure that the web server starts automatically after re-boot by running the following command:

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

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

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

5. Install the tag based data collector as described in Planning the Software Installation:

   ```
   ./ruei-check.sh collector pre-install --role collector
   ./ruei-install.sh tag-server
   ```

   > **Note:**
   >
   > Investigate and fix any issues reported by the per installation check, before continuing with the RUEI reporter software installation.

6. Re-start the Apache web server running the following command:

   ```
   /bin/systemctl restart httpd.service
   ```

7. As the `root` user, add the following lines to the .bash_profile file of the RUEI_USER (RUEI_DATA/.bash_profile):

   ```
   source /etc/ruei.conf
   source $RUEI_HOME/bin/env.sh
   ```

8. Verify that the RUEI software is correctly installed by running the following command:

```
./ruei-check.sh reporter,tag-server post-install
```

9. Set up a password-less remote login from the Reporter system to the newly created Collector system. The necessary configuration steps are described in Configuring Reporter Communication (Split-Server Setup Only).

Remote Network Data Collector Installation

The procedure described in this section is only relevant to remote network data Collector systems, see Planning the Software Installation and Scaling Scenarios.

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

1. Make sure that the rsync and libpcap packages are installed. For example, enter the following commands to install the packages using Yum:

```
yum -y install rsync
yum -y install libpcap
```

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

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

3. Install the network based collector as described in Planning the Software Installation:

```
./ruei-check.sh collector pre-install --role collector
./ruei-install.sh collector
```

> **Note:**
>
> Investigate and fix any issues reported by the per installation check, before continuing with the RUEI reporter software installation.

4. As the `root` user, add the following lines to the `.bash_profile` file of the RUEI_USER (RUEI_DATA/.bash_profile):

```
source /etc/ruei.conf
source $RUEI_HOME/bin/env.sh
```

5. Configure the network interfaces as described in Configuring the Network Interface.

6. Verify that the RUEI software is correctly installed by running the following command:

```
./ruei-check.sh collector post-install
```

7. Set up a password-less remote login from the Reporter system to the newly created Collector system. The necessary configuration steps are described in Configuring Reporter Communication (Split-Server Setup Only)

Configuring the Network Interface

This section is only relevant to network data 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 the `/etc/sysconfig/network-scripts/ifcfg-eth`*X* file (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**.

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 delivers the E-mail directly to the destination MTA. If this behavior is not according to your needs or policies, sending mail through 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 running the following command for RedHat Enterprise/Oracle Linux 7 and 8.*x*:

   ```
   yum install sendmail-cf
   ```

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 running the following command:

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

4. Restart Sendmail running the following command:

   ```
   service sendmail restart
   ```

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

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>
```

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. Log in to the Reporter server as `root`. Run the following commands:

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

   Press **Enter** to accept the defaults.

2. Log in as `root` to each of the Collector systems and become the `moniforce` user by running 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 running 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 running 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 if it is now possible to execute a remote command (as `moniforce` user) on the Reporter system without using a password. For example:
   - Log in as `root` on the Reporter server.
   - Log in 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.

Verifying Successful Installation of RUEI

After completing the **Initial Setup Wizard** (described in Performing Initial RUEI Configuration), verify your installation by running the following commands on the **Reporter** system:

```
cd /root/ruei
./ruei-check.sh diagnostics
```

Note 1: The RUEI systems may require some time to settle after completing the **Inital Setup Wizard**. Once settled, the check *"Reporter ~ post-install-settled" >> "System Status Overview"* should report **[OK]**, as shown below:

```
[2.4] Reporter ~ post-install-settled
      [m] System status overview                                    [ OK ]
        Reporter
          Connectivity with Collectors                 [ OK ]
          Connectivity with Configuration Database     [ OK ]
          Connectivity with Enriched Data Exchange     [ OK ]
          Daemon status                                [ OK ]
          Data Aggregation                             [ OK ]
          Database Usage                               [ OK ]
          Data Processor Output                        [ OK ]
          Disk Usage                                   [ OK ]
          Enriched Data Exchange                       [N/A ]
          KPI Alerting                                 [ OK ]
          Status Reporting Self-Test                   [ OK ]
          Event Log                                    [ OK ]
        System network data Collectors
          System (localhost)                           [ OK ]
            Buffer Overrun                             [ OK ]
            Connectivity with Reporter                 [ OK ]
            CPU Usage Status                           [ OK ]
            Daemon Status                              [ OK ]
            Disk Usage                                 [ OK ]
            In-Memory Configuration Status             [ OK ]
            On-Disk Configuration Status               [ OK ]
            Output Generation                          [ OK ]
```

Note 2: The RUEI system check, verifies many parts of the system, including the "System Status Overview". The "System Status Overview" can also be accessed using the UI by selecting **System**, then **Status**.

Note 3: For more information on the RUEI system check see RUEI System Check Tool.

Using RUEI with Oracle Enterprise Manager

You can set up a connection to the Oracle Enterprise Manager Repository so that KPIs defined for the applications, suites, and services that comprise your business applications can be reported as events in Incident Manager. The use of the business application facility is described in *Oracle Enterprise Manager Cloud Control Oracle Fusion Middleware Management Guide.*

3
Upgrading to RUEI 13.5

This chapter describes the procedure for upgrading an existing RUEI 13.x.x.*x* installation to release 13.5. The post-installation configuration procedure is described in Configuring RUEI . Before upgrading RUEI, check that your system conforms to the prerequisites outlined in Prerequisites .

Migrating Users with Enterprise Manager Access

As of Release 13.1.2.1, RUEI does not allow user accounts (as distinct from system accounts) to have the Enterprise Manager access role. When upgrading from a release prior to 13.1.2.1, non-system accounts that have this privilege will have that privilege revoked and a message will be displayed. You need to create new system accounts with the Enterprise Manager access permission as described in the *Managing Users and Permissions* chapter of the *RUEI User's Guide*. The revocation of the privilege happens during "rpm_post_install" phase, for example:

```
2020-01-13 23:28:29 check_em_access_permissions ...
[User Permissions] EM access has been revoked, for the following user account(s):
[User Permissions] - em_user
[User Permissions] To restore, the user(s) must first be converted to a system
account. This can be accomplished via the edit user wizard in the UI.
2020-01-13 23:28:30 check_em_access_permissions done
...
```

Patching the Operating System

Upgrade the system to the latest patch version before upgrading RUEI for maximum reliability and security.

Downlad and Install the latest Java Runtime Environment (JRE) version 8, x64 version, from Java Downloads for Linux.

Upgrading From RUEI 13.x.x.x to 13.5

This section describes the procedure for upgrading from an existing RUEI 13.x.x.x installation to release 13.5

Before proceeding with the upgrade, make a backup of your configuration, the main database, and the databases on each processor separately. To perform a configuration backup, select **System** >**Maintenance**, and then click **Backup and restore**. The configuration backup is required in case of a rollback.

For more information on how to back up your database, see the Backup and Recovery User's Guide .

Verifying the Environment is Ready to Upgrade to RUEI 13.5

Before starting the upgrade, you should verify your current RUEI environment is ready to upgrade to this RUEI release. This can safely be done before you enter the maintenance window for your upgrade.

Do the following:

1. Log in to the Reporter as root. Within the /root directory, unzip the RUEI zip file, and go to the directory containing the application files. Run the following commands:

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

2. Run the pre-installation readiness check by running the following commands:

   ```
   cd /root/ruei
   chmod +x ruei-upgrade.sh
   ./ruei-upgrade.sh verify_pre_upgrade
   ```

If any issues are reported, these should be resolved before the upgrade. You can run the same steps again to verify the issues are resolved.

Upgrading the Reporter System from RUEI 13.x.x.x

To upgrade the Reporter system from RUEI 13.x.x.x, perform the procedures shown in the following sections:

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

Perform the Upgrade

1. Upgrade to the latest Java Runtime Environment (JRE) version 8. Please download a 64 bit (x64) Linux version from https://www.java.com/en/download/linux_manual.jsp. You can see detailed instructions for installing JRE, in the Installing Java section.

2. > **Note:**
   >
   > This step should be executed when upgrading from a version prior to 13.5 and not having php-xml installed already

   ```
   yum -y install php-xml
   ```

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

```
cd /root/ruei
chmod +x ruei-upgrade.sh
./ruei-upgrade.sh stop_ruei
```

4. Perform the necessary pre-upgrade actions by running the following commands:

```
cd /root/ruei
./ruei-upgrade.sh rpm_pre_install
```

5. Update RUEI database instance.

> **Note:**
>
> When using a remote Pluggable Database or in other instances where you are using the REMOTE_DB=1 and DBCONNECT options in /etc/ruei.conf, you can execute the below steps as the RUEI_USER user on the reporter system. You will need the password of the global SYS user.

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

```
cd /root/ruei
cp ruei-prepare-db.sh /home/oracle
cp -r sql_scripts /home/oracle
chmod +x /home/oracle/ruei-*.sh
chmod +r /home/oracle/sql_scripts/*
su - oracle
export ORACLE_HOME=/u01/app/oracle/product/12.1.0/dbhome_1 (See Footnote 1)
./ruei-prepare-db.sh sql_packages
```

Upon completion, you should again become the root user on the reporter system.

Footnote 1: Replace "12.1.0" in the ORACLE_HOME path with the database version applicable in your setup.

6. For each required Collector system, perform the steps indicated in Upgrading the Remote Collector System(s) from RUEI 13.x.x.x .

7. > **Note:**
>
> This step should be executed when upgrading from a version prior to 13.2.3.1.

As the root user, run the following commands and changes in order to upgrade the `Oracle InstantClient` and `php-oci8`.

```
rpm -e --nodeps php-oci8-11gR2
rpm -e --nodeps oracle-instantclient11.2-sqlplus
rpm -e --nodeps oracle-instantclient11.2-basic
```

Install the `Oracle InstantClient` by following the steps in the Installing the Oracle Database Instant Client chapter.

In `/etc/ruei.conf` , change the value of `INSTANTCLIENT_DIR` to `/usr/lib/oracle/<version>/client64`, where *<version>* should correspond to the version of `Instant Client`.

Build the latest version of `php-oci8` by following the steps in the Installing the php-oci8 Module chapter.

8. Install the new versions of the RPMs running the following commands:

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

9. Perform the necessary post-upgrade actions by running the following commands:

```
cd /root/ruei
./ruei-upgrade.sh rpm_post_install
```

> **Note:**
>
> This can take several hours on a large system when upgrading from a version prior to 13.4, due to the reorganization of indexes.

10. Restart processing running the following commands:

```
cd /root/ruei
./ruei-upgrade.sh reinitialize
./ruei-upgrade.sh start_ruei
```

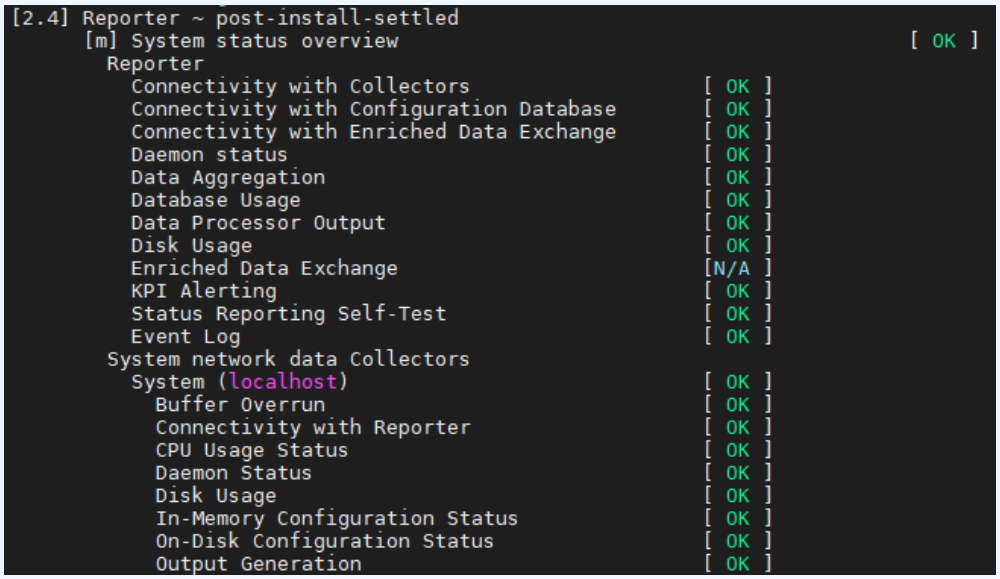
Verify the Upgrade

After completing the upgrade, verify your installation by running the following commands on the Reporter system:

```
cd /root/ruei
./ruei-check.sh diagnostics
```

Note:

The RUEI systems may require some time to settle after completing the upgrade. Once settled, the check *"Reporter ~ post-install-settled" >> "System Status Overview"* should report **[OK]**, as shown in the following graphic.



Note:

The RUEI system check, verifies many parts of the system, including the "System Status Overview". The "System Status Overview" can also be accessed using the UI by selecting **System**, then **Status**.

Note:

For more information on the RUEI system check see RUEI System Check Tool for more information.

Upgrading the Remote Collector System(s) from RUEI 13.x.x.x

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 running the following commands:

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

2. Upgrade to the latest Java Runtime Environment (JRE) version 8. Please download a 64 bit (x64) Linux version from https://www.java.com/en/download/linux_manual.jsp. You can see detailed instructions for installing JRE, in the Installing Java section.
3. Upgrade the Collector RPMs running the following commands:

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

4. Verify the Collector upgrade.

   To verify the collector upgrade, please run the RUEI post-installation check using the following commands:

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

After completing the above procedure for each required Collector system, you should continue with the upgrade of the Reporter system. For more information, see Upgrading the Reporter System from RUEI 13.x.x.x.

Improved Database Performance

Starting with release 13.2.3.1, you will experience better database performance by disabling use of the PARALLEL hint. You can apply the new defaults to your configuration by running the following commands as the RUEI_USER user:

```
execsql config_set_value processor db_core_dop 1
execsql config_set_value processor db_core_dop_kpi 1
execsql config_set_value processor db_gui_dop 1
execsql config_set_value processor cubr_fact_hints ''
```

Steps After Upgrading From RUEI 13.x.x.x

For All Sessions data, to make pre-upgrade data available again in the data browser, run the following command:

> **Note:**
>
> These post-upgrade steps should only be executed when upgrading from versions prior to 13.2.1.1.

```
./ruei-upgrade.sh migrate_visit_data
```

After migrating the pre-upgrade data successfully, run the following command to delete the old data:

```
./ruei-upgrade.sh drop_visit_cube
```

For Sessions Diagnostic data, to make pre-upgrade data available again in the data browser, run the following command:

```
./ruei-upgrade.sh migrate_session_data
```

After migrating the pre-upgrade data successfully, run the following command to delete the old data:

```
./ruei-upgrade.sh drop_session_cube
```

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).

Important

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

Introduction to Configuring RUEI

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 Installing the RUEI Software. After that, you are required to specify the installation type and mail setup (described in Performing Initial RUEI Configuration), and then perform some post-installation configuration (described in 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 Authorizing Initial Users. if you are installing a split-server configuration, you will need to configure each Collector system. This is described in Configuring Collector Systems.

Important

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

Performing Initial RUEI Configuration

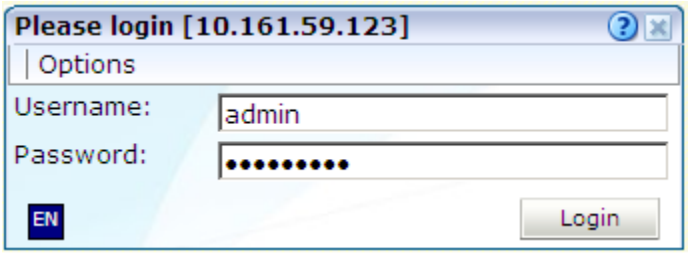
RUEI must be configured with information about your network infrastructure to start data monitoring and reporting. Once completed, user traffic reporting is available. This initial configuration can be changed later, as necessary. It is only intended to provide RUEI with sufficient information to start 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 the following URL: `https://`***`Reporter`***`/ruei`.

   Where, *`Reporter`* specifies the host name or IP address of your RUEI installation. The dialog shown in Figure 4-1 appears.

Figure 4-1 Logon Dialog



2. Specify the `admin` user, and the password defined with the `set-admin-password` script (defined in Installing the Reporter Software). Click **Login**. The dialog shown in Figure 4-2 appears.

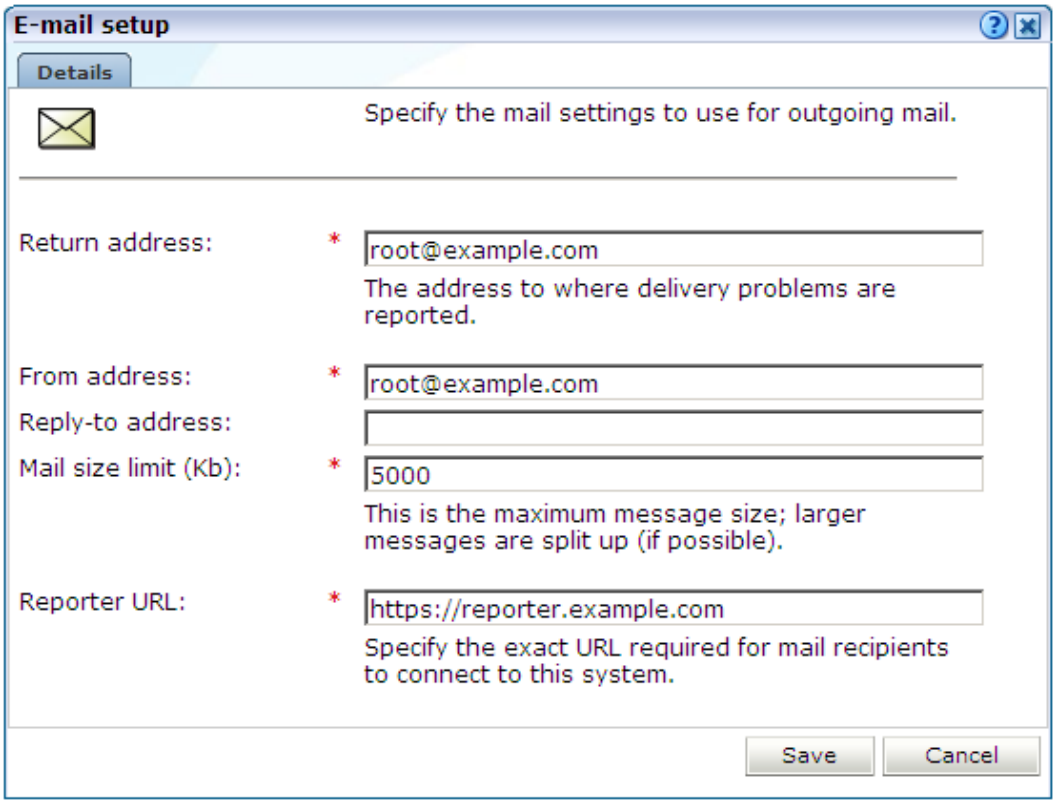
Figure 4-2 Initial Setup Wizard

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. For more information, see

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

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

Figure 4-3 Mail Setup Dialog



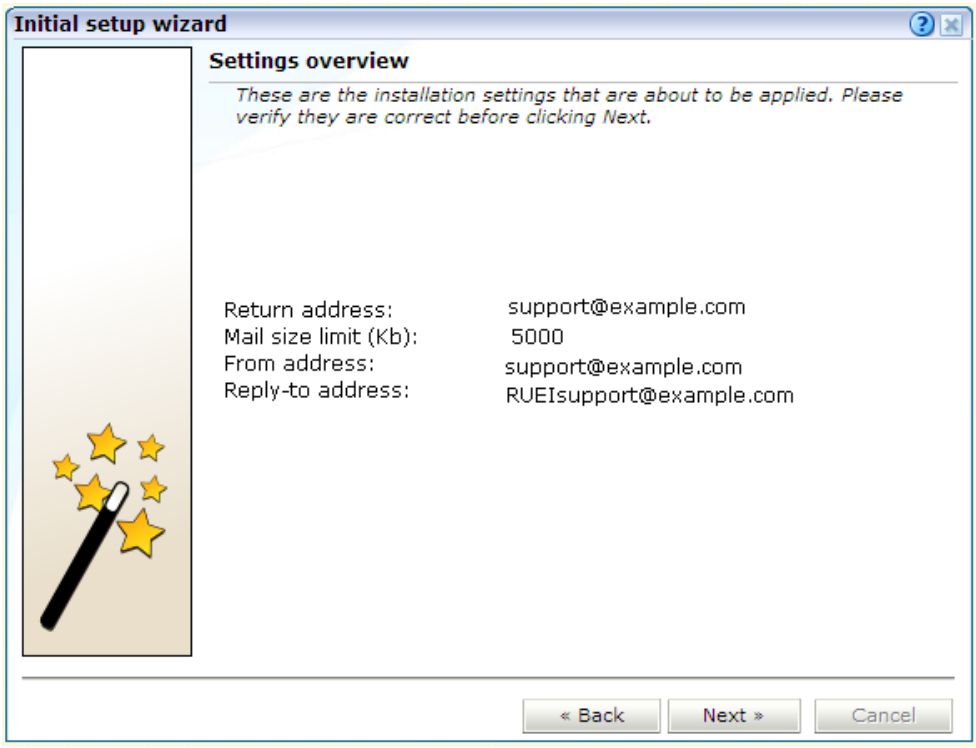
4. Specify the requested information as explained in Table 4-1.

Table 4-1 E-mail Setup Fields

Field	Description
Return address	Specifies the e-mail address to which failed or problem e-mails are reported. It is recommended that this an address that is regularly checked.
From address	Specifies the address the recipient sees in their mail client.
Reply-to address	Specifies the address that users can click within an e-mail to reply to an e-mail. If this is not specified, the **From address** setting is used.
Mail size limit	Specifies the maximum message size (in kilobytes) allowed for e-mails. If an e-mail contains reports that exceed this limit, the system will try to split up the reports into individuals e-mails to overcome this limitation. Reports that are too large to be sent individually are not sent, and the user is informed of the problem. The default mail size limit is 5000 Kb.
Reporter URL	Specifies the exact URL required for e-mail recipients to connect to the Reporter system. Typically, this is the same URL used by RUEI users to access the Reporter system.

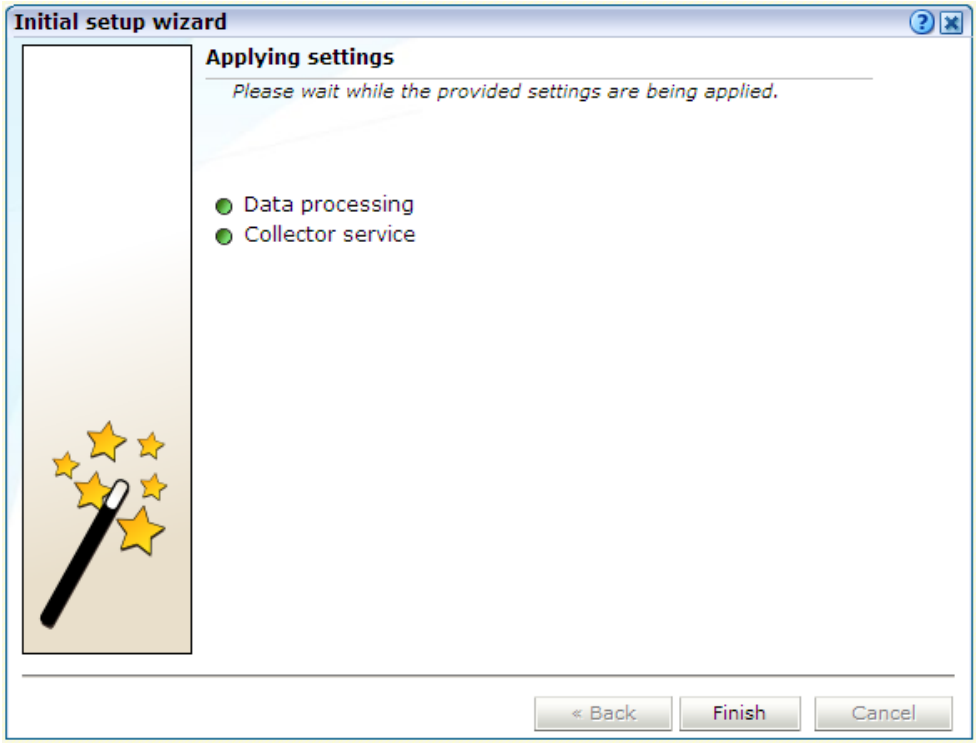
The e-mail information is used to configure RUEI's interface to your internal network, and will be used for reporting problems. When you have entered the required information, click **Next**. The dialog shown in Figure 4-4 appears.

Figure 4-4 Settings Overview Dialog



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

Figure 4-5 Applying Settings Dialog



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

Configuring Collector Systems

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

1. Install the Collector software on the required systems. This is described in Installing the RUEI Software.
2. Register the Collector systems with the Reporter. The procedure to do this is described in the *Oracle Real User Experience Insight User's Guide*.
3. If you expect high volumes of traffic and have installed the collector on a powerful system (minimum of 12 cores, 32GB RAM or more), and RUEI is not monitoring servlet forms traffic, you can configure the collector to take advantage of the more powerful hardware using the procedure described in the *Configuring Collector Systems* chapter of the *Real User Experience Administration Guide*.

Resetting Collector Systems

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

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

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

2. Follow the procedure described in the *Oracle Real User Experience Insight User's Guide* to register the Collector with the required Reporter.

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.

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, together with the structure of supported cookie technologies, is described 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.

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*.

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*.

Defining Applications and Page Identification

Page identification within RUEI is based on defined 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. 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 Insight User's Guide*.

Suites

In addition to generic applications, dedicated support is available for the monitoring of certain Oracle Enterprise architectures (such as Oracle E-Business suite, Siebel, and WebLogic Portal). If you are using any of the currently supported architectures within your monitored environment, it is *strongly* recommended that you make use of this facility. It not only saves you time in defining your applications, and makes applications within suites more compatible, but also ensures that these architectures are monitored correctly.

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*.

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 Installing 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, and the creation and management of user accounts are described in the *Oracle Real User Experience Insight User's Guide*.

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.

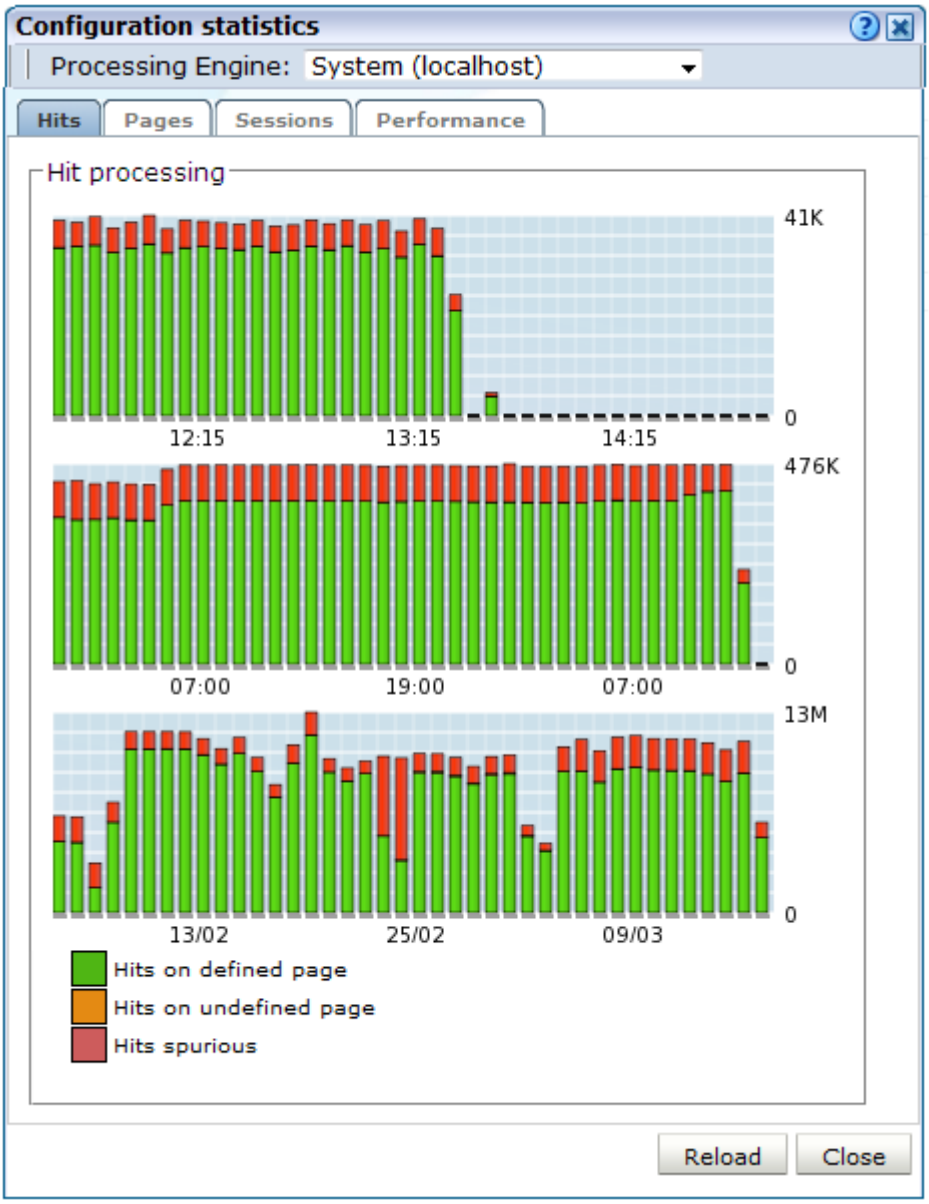
Verifying and Evaluating Your Configuration

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.

Viewing Traffic Summary

You can open an overview of the monitored network traffic by selecting **System** >**Status**>**Reporter**, and then **Statistics**. This provides you with immediate information about hits, pages, and session processing, as well as the system load. An example is shown in Figure 4-6.

Figure 4-6 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.

> **Note:**
>
> 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 Server Requirements

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 Statistics**. This opens the Collector Statistics window. For more information, see 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.

Configuring Support for the T3 Protocol

RUEI 13.3.1.0 includes limited support for the T3 protocol. T3 is an Oracle proprietary protocol for communication to and between Oracle WebLogic Server instances. With this release of RUEI you can monitor service calls between Oracle WebLogic Server instances, however future releases of RUEI might change how T3 is supported and any 13.3.1.0 configuration might not be backwards compatibility.

To configure support for the T3 protocol:

1. Configure the T3 port in RUEI. Select **Configuration**, then Security, and select the **Protocols** option. The resulting screen is described in the *Managing Security-Related Information* chapter of the *RUEI User's Guide*. Select HTTP for the T3 protocol or HTTPS for the ST3 protocol and enter the port number, typically 7001.
2. Create a suite of the type **T3 Java RMI** as described in the *Working With Suites and Web Services* chapter of the *RUEI User's Guide*. The **T3 Java RMI** type will only be available option after you have configured the T3 protocol port as described in step 1.
3. Modify the newly defined suite as required to monitor T3 traffic. Data masking and identification using content messages are not supported for the T3 protocol.

5

Configuring the Oracle Access Manager

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. The procedure may need to be modified to reflect the specific configuration of your OAM server.

Configuring OAM 11g

This section describes the procedure for configuring OAM 11g. For information on configuring OAM 10g, see OAM 10.

RUEI is able to monitor OAM 11g (R2PS3 BP02) secured web applications in order to report on user identification information provided by OAM. OAM provides this information for each user session in an encrypted cookie which, once properly configured, is monitored and decrypted by RUEI. The user identification (user id) is extracted from the decrypted content and used within RUEI.

Exporting and Importing the OAM 11g AES key

A shared AES key is available for each OAM server which can be used by RUEI to decrypt the OAM 11g cookie (OAM_DIAG_CTS). This key needs to be extracted from the OAM server and uploaded to the RUEI Reporter. RUEI allows you to upload a 'global' OAM AES key and and allows key uploads per application. An application OAM AES key overrides the global OAM AES key.

Exporting an OAM 11g AES key

Export the key using the following procedure:

1. Start the WebLogic Server console, running the following command:

   ```
   $MW_HOME/Oracle_IDM1/common/bin/wlst.sh
   ```

2. Connect to the WebLogic Server, running the following command:

   ```
   Connect('user','password','t3://hostname:port')
   ```

3. Run the following WLST command to retrieve the key:

   ```
   retreiveDiagnosticCookieKey( keystoreLocation="keystoreLocation",
   password="password")
   ```

   Where,

   `keystoreLocation` is an existing directory where the output JKS file will be stored, and `password` is the password used to encrypt the JKS file.

Importing an OAM 11g AES key

On the RUEI side use the `oam-key.sh` tool to add or remove OAM AES keys. Either import a global key, or import one or more application specific keys.

1. You must specify a collector profile name during the import process, to list all profiles, running the following command:

   ```
   execsql config_get_profiles
   ```

2. If you want to use an application specific key, you must specify an application name during the import process, to list all application names, running the following command:

   ```
   execsql get_matches
   ```

3. Gather the required passwords. During import the following passwords are requested:
   - original key password - This is the password provided during the JSK export from the OAM server. This password is used to decrypt the JKS keystore file.
   - key storage passphrase - This is the password RUEI uses to safely store and encrypt the AES key.

4. To import a global key, run the following command:

   ```
   oam-key.sh install PATH_TO_JKS_FILE 'Collector Profile Name'
   ```

   Where, *PATH_TO_JKS_FILE* is the location of the JKS file created during export.

5. To import an application specific key, run the following command:

   ```
   oam-key.sh install PATH_TO_JKS_FILE 'Collector Profile Name' 'Application Name'
   ```

   Where, `Application Name` is the name of the application.

Removing an OAM 11g AES Key

To remove a global key, run the following command:

```
oam-key.sh delete 'Collector Profile Name'
```

To remove an application specific key, run the following command:

```
oam-key.sh delete 'Collector Profile Name' 'Application Name'
```

Configuring an Application to Use OAM

After configuring OAM 11g, you can add a user id source to an application based on Oracle Access Manager 11g. For more information, see Monitoring OAM and SSO-Based Traffic in the *Oracle RUEI User's Guide.*

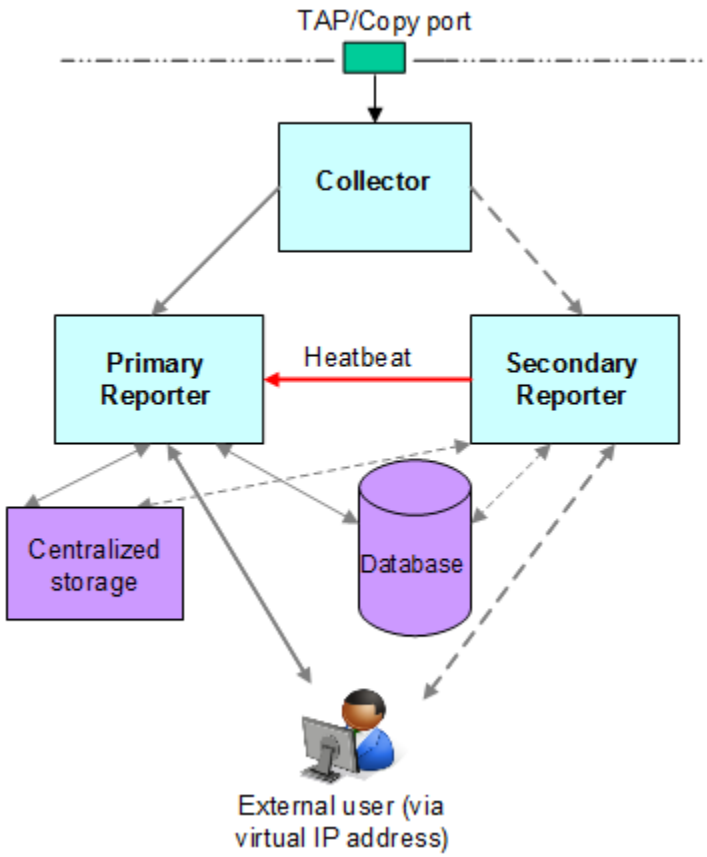
6
Configuring a Failover Reporter System

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. The described procedure assumes that the primary Reporter system has been installed, configured, and is fully operational. The installation procedure for a primary Reporter is identical to that of a standalone Reporter. For more information, see Configuring a Failover Collector System.

Introduction to Failover Reporter Systems

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 6-1.

Figure 6-1 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.

The failback (that is, the process of restoring the RUEI installation to its original state), must be performed manually. For more information, see Initiating 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.

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 running the following command as the *`RUEI_USER`* user:

   ```
   project -stop
   ```

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.

Installing the Secondary Reporter

The installation procedure for a secondary Reporter system is almost identical to that of a standalone Reporter system. 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. For more information, see Configuring RUEI .

   You must ensure that you do the following:

   - Follow the instructions described in Installing the RUEI Software.
   - 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 Installing the Reporter Software.
   - Follow the instructions described in Configuring the Network Interface.
   - If you performed the instructions described in Configuring Automatic Browser Redirection (Optional) for the primary Reporter system, then you will need to repeat them for the secondary Reporter system.

Configuring Reporter Failover

To configure the 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 run the following command to stop all processing of monitored traffic:

   ```
   project -stop
   ```

2. Copy the `.ssh` directory of the *`RUEI_USER`* user on the primary Reporter system, created while performing the procedure described in Configuring Reporter Communication (Split-Server Setup Only), to the secondary Reporter system. 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 running 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. Log in to the secondary Reporter system as the *RUEI_USER* user, and run the following command:

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

   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. For more information, see Check The RUEI Configuration File. The settings specified on both Reporter systems must be identical except for the `RUEI_REP_FAILOVER_VIRTUAL_DEV` setting.

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

   ```
   project -start
   ```

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. For more information, see 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 for 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. After doing so, you must perform a failback to return your RUEI installation to its original state.
17. Select **System**>**Maintenance**, and then **E-mail setup**) to update the Reporter URL with the virtual Reporter host name or IP address.

Initiating 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 on the secondary server running 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 running the following commands:

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

7

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. The described procedure assumes that the primary Collector system has been installed, configured, and is fully operational.
For more information, see Configuring a Failover Reporter System.

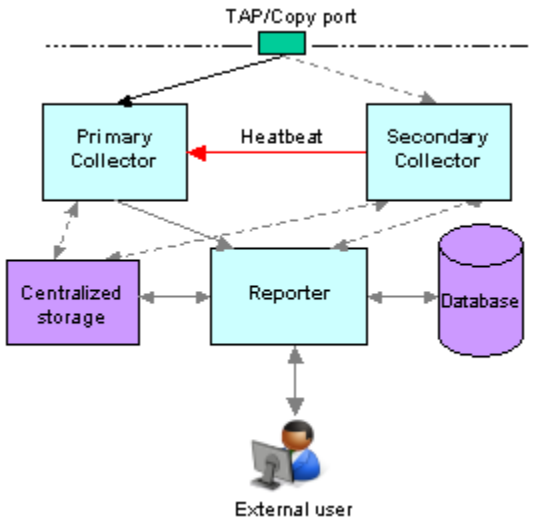
SSL and Forms Traffic

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. Therefore, during a failover or fallback, traffic may be lost.

Introduction to Failover Collector Systems

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. This facility is only available for remote Collectors. For more information on configuration of a failover collector system, see Figure 7-1.

Figure 7-1 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.

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

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. For more information, see 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.

Configuring the Secondary Collector

To configure the secondary Collector, do the following:

1. Copy the `.ssh` directory (created when following the procedure described in Configuring Reporter Communication (Split-Server Setup Only) on the primary Collector to the secondary Collector. It must be copied to the same location.
2. On the primary Collector system, run 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, run 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. 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 running 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:

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

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

     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`.
   - Run 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
   ```

   > **Note:**
   >
   > 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.

   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 Check The RUEI Configuration File for an explanation of these settings. 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. 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. For more information, see 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 for 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. After doing so, you must perform a failback to return your RUEI installation to its original state.

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, run 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, run 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), run 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 manually set up an Oracle database instance for use by the RUEI Reporter. RUEI supports Oracle database version 11gR2 and 12c Release 1.

> **Note:**
>
> While RUEI is supported on Oracle Database releases 11gR2 and later, the best performance for RUEI 13.3.1.0 is achieved with Oracle Database 12c Release 1.

You can download Oracle Database (12c Release 1 or 11g Release 2) Standard Edition, Standard Edition One, or Enterprise Edition from the Oracle database home page at the following location:

http://www.oracle.com/technetwork/database/enterprise-edition/downloads

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 platforms designed for large queries by comparatively few users offer the best deployment solutions.

Overview of Database Setup

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). For more information, see Check The RUEI Configuration File.
- 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. You are required to have `sysdba` authorization.

Location of SQL Scripts

The SQL scripts referred to as alternatives to the procedures described in the rest of this appendix can found in the `/root/ruei/sql_scripts/` directory after extraction of the RUEI distribution zip.

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.

Using the `ruei_database.dbt` template (32K blocksize) which can be found in the `/root/ruei/db_templates/` directory, they should be consistent with the following:

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

Alternatively, on Linux platforms, the `ruei-prepare-db.sh` script can also be run (as the Oracle user) to create the Oracle database instance as follows:

```
./ruei-prepare-db.sh create_database
```

In addition to the *TSDEFAULT* tablespace, two additional tablespaces must be created for the RUEI Reporter system.

Creating Tablespaces

Before continuing make sure you have chosen names for the default tablespace (named *TSDEFAULT* below for reference), the configuration tablespace (default is `UXCONF`) and the statistics tablespace (default is `UXSTAT`). The latter two names should also be set in the `/etc/ruei.conf` file using the `RUEI_DB_TSCONF` and `RUEI_DB_TSSTAT` variables respectively. Note that the same tablespace names must be used for all components in your RUEI environment, such as the remote database and Processors.

For performance reasons, it is *strongly* recommended that you use compressed tablespaces. The following command can be used to create the TSDEFAULT tablespace. The default datafiles location is used, and you may want to specify a different location for the datafiles:

```
create tablespace TSDEFAULT datafile 'uxdefault01.dbf' size 5M reuse autoextend
on default compress;
```

The following command line instruction can be used to enable compression on the *TSDEFAULT* tablespace:

```
alter tablespace TSDEFAULT default compress;
```

Select **Configuration**> **General**>**Advanced settings**, and then **Reporter data retention policy** to create the table space. The size of the required database instance is 500 GB (or larger). The required disk space depends on the specified Reporter data retention policy.

For most RUEI deployments, you will require more than a single datafile in the *TSDEFAULT* tablespace.The default datafiles location is used, and you may want to specify a different location for the datafiles. Run the following command to add additional datafiles:

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

In addition to the *TSDEFAULT* tablespace, two additional tablespaces must be created for the Reporter system:

- RUEI_DB_TSCONF: contains RUEI configuration information. Typically, less than 1 GB in size.
- RUEI_DB_TSSTAT: contains RUEI statistics information used for internal purposes. Typically, only a few GB in size.

The names of these two tablespaces are fixed and not configurable. The required tablespaces can be created running the following commands:

```
create tablespace RUEI_DB_TSCONF datafile 'uxconf01.dbf' size 5M reuse autoextend on
default compress;
create tablespace RUEI_DB_TSSTAT datafile 'uxstat01.dbf' size 5M reuse autoextend on
default compress;
```

Alternatively, instead of using the commands described in this section, the table set up can be performed by running the prepdb_tablespaces.sql SQL script. The script requires three input variables to be set, one for each configurable table space name.

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, 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, see the Oracle Database Administrator's Guide.

The documented procedure can also be performed by running the prepdb_maintenance_schedule.sql SQL script.

Installing SQL Packages

RUEI requires additional packages to be installed. These can be installed by running the following command:

```
./ruei-prepare-db.sh sql_packages
```

Alternatively, you can install the packages manually with the ux_dbms_lock.sql and ux_dbms_session.sql scripts in the sql_scripts directory.

Creating the RUEI Database User

This section explains the creation of the RUEI database user, and the 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 TSDEFAULT
         temporary tablespace TEMP
```

```
        profile DEFAULT
        quota 500G on TSDEFAULT;

alter user RUEI_DB_USER
        quota unlimited on RUEI_DB_TSCONF
        quota unlimited on RUEI_DB_TSSTAT;

alter profile DEFAULT
        limit PASSWORD_LIFE_TIME unlimited;

grant   create session,
        create sequence,
        create table,
        create trigger,
        create view,
        create synonym,
        create database link,
        create procedure,
        create materialized view,
        create type
        to RUEI_DB_USER;

grant execute on dbms_crypto to RUEI_DB_USER;
grant execute on ux_dbms_lock to RUEI_DB_USER;
grant execute on ux_dbms_session to RUEI_DB_USER;
```

Alternatively, instead of using the commands described in this section, the RUEI database user configuration can be performed by running the `prepdb_user.sql` SQL script. The script requires three input variables to be set, one for each configurable table space name.

Creating Database Triggers

RUEI requires additional database triggers to be created. Create these triggers using the following command:

```
./ruei-prepare-db.sh create_triggers
```

Alternatively, you can create the triggers manually running the `prepdb_triggers.sql` scripts located in the `sql_scripts` directory.

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)))
```

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.

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.

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

```
mkstore -wrl /tmp -create
```

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 running the following command:

```
mkstore -wrl /tmp -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`*.`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 running 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 appendix describes how you can set up an 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. To back up your configuration, select **Configuration**>**System**> **Maintenance**, and then **Backup and restore**.

Introduction to Enriched Data Export Setup

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 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 particular 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, 11gR2 or 12c Release1, and installation of the Oracle database software should have been completed before starting the setup procedure described in the rest of this appendix. Be aware that advanced knowledge of Oracle database administration is assumed.

The setup procedure described in this appendix refers to a number of settings (such as `RUEI_DB_TNSNAME_BI`). These are explained in Table 2-3.

Migration to an Alternative Enriched Data Export Database

When migrating enriched data export from one database to another, the export data currently stored in the previous database is not automatically 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 particular period. In particular, try to avoid querying the same data more than once.

Setting up the Alternative Database Instance

This section describes the procedure that must be followed in order to setup the database instance on the alternative database server.

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. Do the following:

1. Log in to the alternative database system as the `oracle` user, and run the following commands:

```
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`.

Using Compressed Tablespaces

For performance reasons, it is recommended that you use compressed tablespaces. Do the following:

1. Run the following SQL command as the System Administrator on the alternative database server 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 add additional table space by running the following SQL command:

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

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

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). For more information, see Oracle Database Administrator's Guide.

Creating the RUEI Database User

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

1. Run the following commands on the alternative database server 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.

Connecting the RUEI Systems to the Alternative Database Server

This section describes the procedure that must be followed in order for the Reporter and Processing Engine systems to connect to the alternative database server. This procedure must be followed on the Reporter system.

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 directory (*RUEI_DATA*) on the Reporter system. Do the following:

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=Act number :
12061130003875Name : Pavithra Mendon IFSC -
      hdfc0001206)))
DIAG_SIGHANDLER_ENABLED = FALSE
```

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

2. Edit the `tnsnames.ora` files on the Reporter system. You should add the following:

```
RUEI_DB_TNSNAME_BI =(DESCRIPTION=
  (ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=BI_database_server)
     (PORT=1521)))
  (CONNECT_DATA=(SERVICE_NAME=RUEI_DB_INST_BI)))
```

Where,

- *`BI_database_server`* specifies the network address (hostname or IP address) of the alternative Enriched data export database server.
- *`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.

Setting up the Oracle Wallet

The Reporter requires non-interactive access to the alternative Enriched data export 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. Do the following:

1. Run the following command to add the new credentials to the existing wallet files `ewallet.p12` and `cwallet.sso`:

   ```
   mkstore -wrl RUEI_DATA -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.

   You are prompted for the wallet password and the database password for *`RUEI_DB_USER_BI`*.

2. 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.

Editing the RUEI Configuration File

1. Edit the `/etc/ruei.conf` configuration file on the Reporter from which you intend to export enriched data. Use the `RUEI_DB_TNSNAME_BI` setting to specify the export database connect string. For more information, see Check The RUEI Configuration File.

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

2. Logout and login again as the `moniforce` user.
3. Restart processing on the Reporter system by running the following command:

   ```
   project -restart
   ```

C

Setting up a Connection to the Enterprise Manager Repository

This appendix describes how you can set up a connection to the Oracle Enterprise Manager Repository. This is necessary when you want KPIs defined for the applications, suites, and services that comprise your business applications to be reported as events in Incident Manager. The use of Incident Manager is described in Oracle Enterprise Manager Cloud Control Administrator's Guide. The use of the business application facility is described in Oracle Enterprise Manager Cloud Control Oracle Fusion Middleware Management Guide.

Introduction to Enterprise Manager

Oracle Enterprise Manager supports the monitoring of business applications. These represent logical services or applications, and unify the dedicated performance monitoring, diagnostics, and reporting capabilities available through RUEI with that available through Oracle Enterprise Manager. The alerts generated by KPIs defined for the applications, suites, and services that comprise your business applications are reported as events in Incident Manager. For more information about the advantages of using Enterprise Manager to monitor KPIs, see the Oracle Enterprise Manager Cloud Control Oracle Fusion Middleware Management Guide.

After completing the procedure described here, register the RUEI system in Enterprise Manager using the procedure described in Monitoring Business Applications in the *Oracle Enterprise Manager Cloud Control Oracle Fusion Middleware Management Guide*.

If you change any setting described in this Appendix, you must restart the system using the RUEI System Reset Wizard:

1. Select **System**>**Maintenance**, and then **System** reset.
2. Select **Reapply latest configuration** option and click **Next** to apply the changes you have made.

Creating a RUEI User for Communication with Enterprise Manager

In order for RUEI to communicate with Enterprise Manager, you must create a RUEI user with the **Enterprise Manager access** permission. For more information, see Managing Users and Permissions in the *Oracle Real User Experience Insight User's Guide*.

1. Log in to RUEI as an `administrator` user.
2. Select **System**> **User management**, and click the **Add new user** command button in the taskbar.
3. Complete the wizard, ensuring that you create a **system** user, with the **Enterprise Manager access** permission.

> **Note:**
>
> You are not prompted to enter this user's credentials when registering RUEI with Enterprise Manager.

Creating a non-sysman Enterprise Manager Repository User

During the process of registering RUEI with Enterprise Manager 12c, you must provide the credentials of an Enterprise Manager repository user. If you do not want to use the `sysman` user credentials, you can create a non-sysman user as follows:

> **Note:**
>
> With Oracle Enterprise Manager 13c, a database user is automatically created (EUS_ENGINE_USER). When this user is first used, you are prompted to set a password for this user, and this password is stored in the RUEI wallet. By default this password will expire after 180 days. See the Configuring Authentication chapter of the *Database Security Guide* for information on configuring this user.

1. Log in to the RUEI server as the `ruei` user.
2. Unpacking the RUEI Software describes how to unpack the RUEI software. Copy the resulting `/root/ruei/sql_scripts` directory from the RUEI server to the Enterprise Manager repository server.
3. Run SQL*Plus as the `sysman` user in the `sql_scripts` directory on the Enterprise Manager repository server and create the user using the following script:

   ```
   SQL> @create_em_user_for_event.sql
   ```

> **Note:**
>
> After completing the procedure described here, set up RUEI using the username and password you entered in step 3. For more information, see Monitoring Business Applications chapter of the *Oracle Enterprise Manager Cloud Control Oracle Fusion Middleware Management Guide*.

Setting Up a Connection to Oracle Enterprise Manager

In order to connect with Enterprise Manager, a specific version of the `mkstore` utility is needed. The required procedure consists setting up RUEI to use the `mkstore` utility and restarting RUEI.

You can set up this utility as follows.

1. Run the following commands to install the `mkstore` utility to `/usr/local/mkstore-11.2.0.4.0`.

   ```
   cd /usr/local
   tar xzf /root/RUEI/mkstore/mkstore-11.2.0.4.0.tar.gz
   ```

2. To make the install directory version independent, create a more generic symlink using the following command:

   ```
   ln -s /usr/local/mkstore-11.2.0.4.0 /usr/local/mkstore
   ```

3. Make the following change to `/etc/ruei.conf`:

   ```
   * export MKSTORE_BIN=/usr/local/mkstore/mkstore
   ```

4. If you are executing these steps on a database server separate from the reporter system, make the following change to `/etc/ruei.conf`:

   ```
   * export JAVA_HOME=$ORACLE_HOME/jdk/jre
   ```

Clearing a Connection to Oracle Enterprise Manager

If you remove a RUEI registration from Oracle Enterprise Manager, you may see a message indicating there are some data in RUEI side that must be removed manually. If you see this message, complete the following procedure:

> **Note:**
>
> The wallet password is required to complete this procedure.

1. Change directory to the location of the `mkstore` utility. This utility is included with the Oracle Database and Oracle Client runtime. In both cases, it is located in `$ORACLE_HOME/bin`.
2. Determine the credential you want to delete by listing the current credentials running the following command:

   ```
   ./mkstore -wrl ewallet.p12 -listCredential
   ```

3. Delete the wallet credential running the following command:

   ```
   ./mkstore -wrl ewallet.p12 -deleteCredential 'CREDENTIAL_NAME'
   ```

   Where, `CREDENTIAL_NAME` is the name of the credential you want to delete.

4. Clear the database entries running the following SQL command:

   ```
   delete from C_EM_SYSTEM where HOST_NAME='Host_Name';
   ```

   Where, `Host_Name` is the hostname of the RUEI instance.

D

RUEI System Check Tool

This appendix covers how to run the RUEI System Check Tool. It is recommended that you use this tool to verify successful installation and to troubleshoot any installation issues. The RUEI system check tool is used to run various checks before, during and after a RUEI installation or a RUEI upgrade, or in case of run-time issues with the RUEI system.

> **Note:**
>
> Please provide the output of the RUEI system check tool when in contact with Oracle Customer Support.

To re-run the RUEI system check tool, use the following commands as *root*:

```
cd /root/ruei
./ruei-check.sh diagnostics
```

> **Note:**
>
> The diagnostics mode will automatically detect which components have been installed and perform the appropriate checks.

The tool will save the output also to the logfile `/tmp/ruei-check.log`. The automatic system configuration backup / saveall will automatically included this logfile.

Please consult the relevant sections of this guide for related information when the RUEI System Check Tool reports a warning or an error.

E

Verifying Monitored Network Traffic

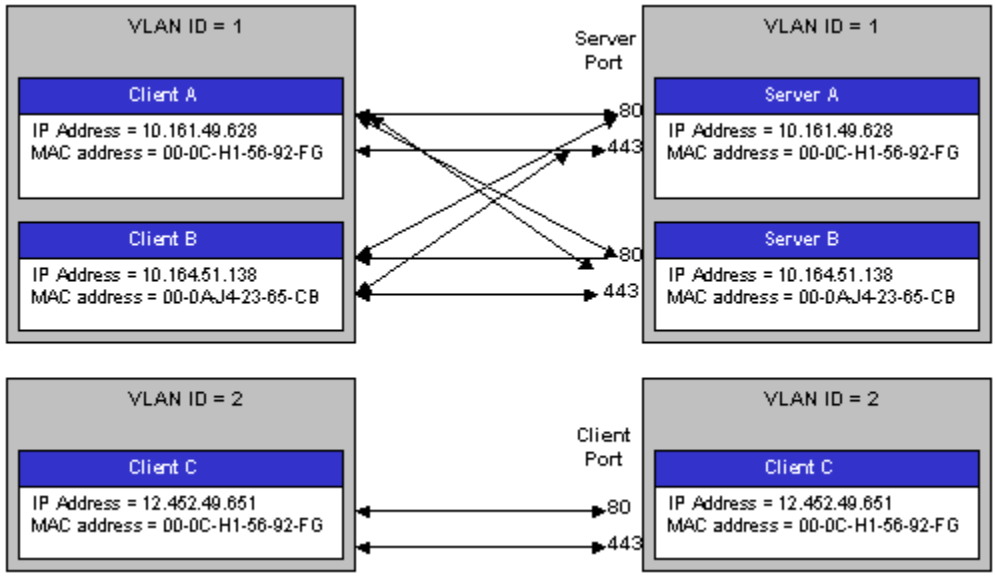
This appendix describes how you can use the TCP diagnostic facility to verify that RUEI sees all required network traffic. It is recommended that a network engineer within your organization validates collected network traffic after installation and configuration of RUEI.

Introduction to Network Traffic

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 E-1.

Figure E-1 Example Network Topology

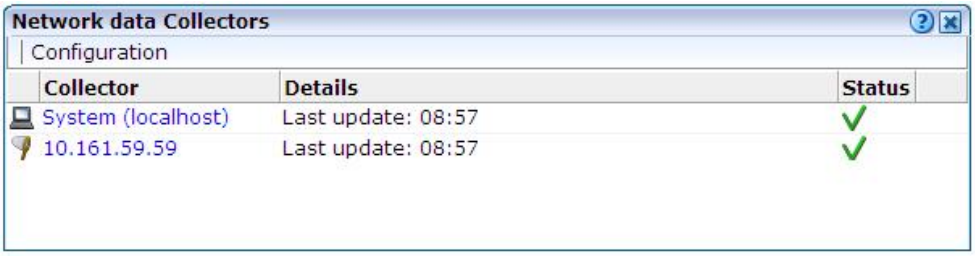


Creating Traffic Snapshots

To create a TCP traffic snapshot, do the following:

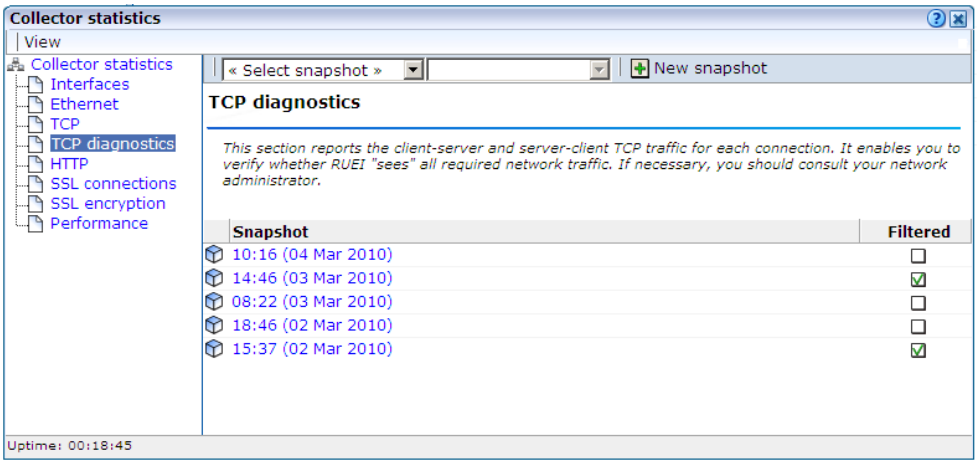
1. Within the **Configuration** facility, click the **Show Collector status** icon. Alternatively, select **System**> **Status**, and then **Collector Statistics**. The Network data Collectors window shown in Figure E-2 opens. For more information, see Oracle Real User Experience Insight User's Guide.

Figure E-2 Network Data Collectors



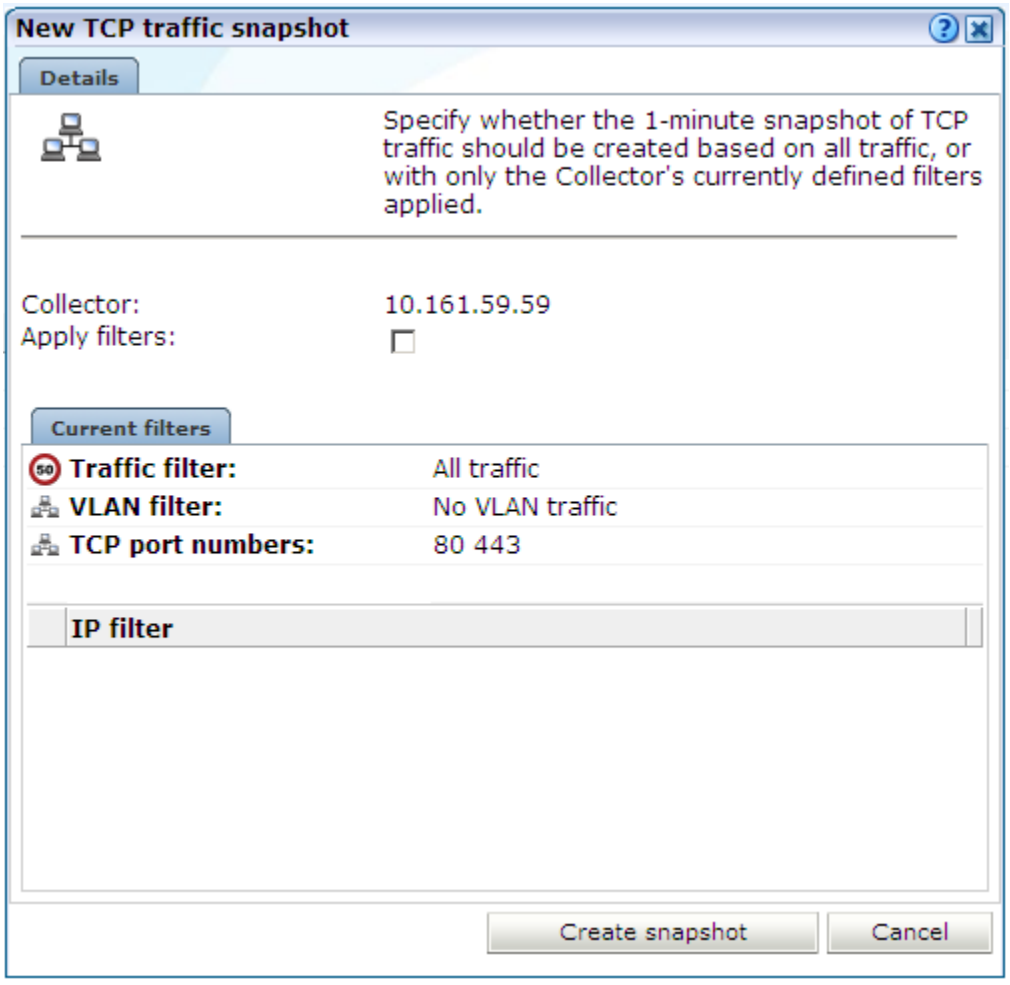
2. Click the required Collector. The **System (localhost)** item refers to the Collector instance running on the Reporter system. Other Collectors within the network are represented by their IP address.
3. Click the **TCP diagnostics** tab. A panel similar to the one shown in Figure E-3 appears.

Figure E-3 TCP Diagnostics



4. Click the **New snapshot** icon in the toolbar. The dialog shown in Figure E-4 appears.

Figure E-4 New TCP Traffic Snapshot Dialog

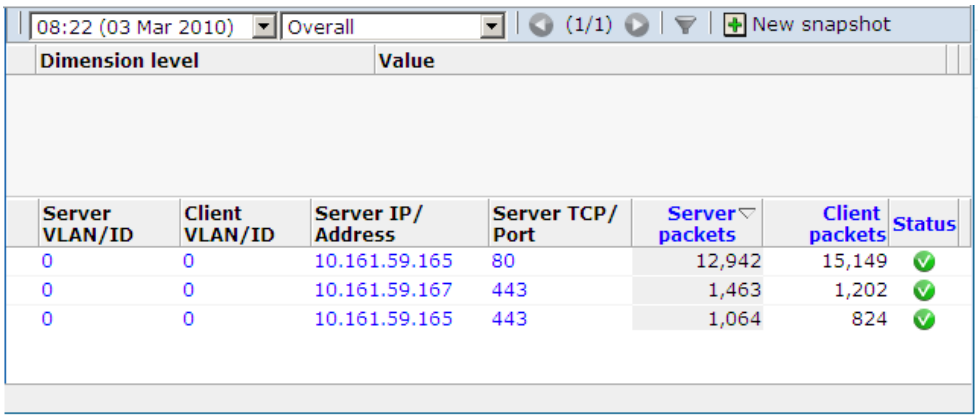


5. Use the **Apply filters** check box to specify whether the create traffic snapshot should be created to report all traffic seen by the selected Collector, or only that traffic that fits the Collector's currently defined filters. For more information, see Oracle Real User Experience Insight User's Guide. These are shown in the lower part of the dialog. 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 E-5.

Figure E-5 TCP Traffic Snapshot Overview



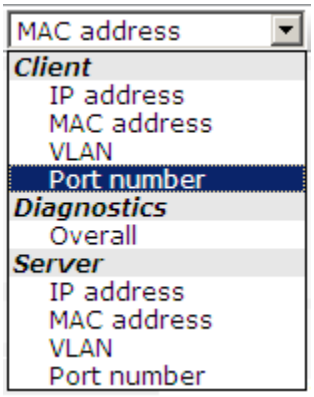
Analyzing Traffic Information

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. For more information, seeFigure E-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, as shown in Figure E-5appears. 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 E-6) to the right of the snapshot menu to select the primary column used for the displayed items.

Figure E-6 Sort Menu



3. The **Status** column shown in Figure E-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 E-1.

Table E-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.

F

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

Note the following:

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

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

- 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 recommended that you create a Helpdesk report file of your installation. To do so, select **System**>**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. Please note that this file contains information in a proprietary format. Do not try to modify its contents.

In addition, extended information about internal errors is available by enabling Session debugging. To do so, select the **Session debug** option from the **Help** menu. For more information, see Oracle Real User Experience Insight User's Guide.

Running the RUEI System Check

It is recommended you use the RUEI system check tool to troubleshoot installation issues. See RUEI System Check Tool for usage of this tool

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 `delete` option to remove the current database and install a new one.

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**>**Maintenance**>**Network data collectors**, select each attached Collector, and select the **Restart** option from the menu.
- Review your network filter definitions. 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.
- Verify that the Collector interfaces are `up`.

For more information, see the Oracle Real User Experience Insight User's Guide

Resources and Log Files

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

- *`RUEI_DATA`*`/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**>**Status**, and then **Collector Statistics**. 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**>**Status**,and then **Reporter Statistics**. A screen similar to the one shown in Figure 4-6 appears. It should indicate some activity.

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 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 ethN` (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
```

  You may want to repeat the above command to view changes in network traffic while diagnosing network issues.
- If the network interface is not available, make sure the `ONBOOT` parameter is set to `YES`.
- 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.

Data Processing Problems

If, for any reason, data processing does not start, try to restart it by selecting **System**>**Maintenance**, and then **System reset**. The System reset wizard appears. Select the **Restart system processing** option. 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 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** and **Status**. A failing Collector can become a block to further data processing of the system's data.

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.

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 expand the collector for which you want SSL decryption analysis and click **Collector Statistics**.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 running 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
```

Check the collector statistic page of RUEI for issues, specifically searching for sessions labelled:

- Ephemeral - These sessions provide forward secrecy and therefore cannot be monitored by RUEI.
- Anonymous - These sessions do not have a long-lived server key and therefore cannot be monitored by RUEI.

Missing Packages and Fonts Error Messages

It is recommended that you 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

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 running 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 libpcap \
sendmail-cf httpd php php-pear php-mbstring phpldap librsvg2 xorg-x11-xinit \
net-snmp-utils perl-XML-Twig
```

For RedHat Enterprise/Oracle Linux 6.*x*, run the 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 \
libpcap sendmail-cf httpd php php-pear php-mbstring phpldap librsvg2 \
xorg-x11-xinit net-snmp-utils perl-XML-Twig rsync ksh openssl098e wget bc \
bind-utils
```

However, be aware that additional RPMs shipped with the RUEI installation zip file still need to be installed.

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 running 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 running 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.

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

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 /@connect-string
```

Where, *`connect-string`* is either *`RUEI_DB_TNSNAME`* or *`RUEI_DB_TNSNAME_CFG`*.

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 running the following command:

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

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**>**Status**, and verify correct operation of the core components. If any of these components are in error, try to resolve them using the advice provided in this appendix.

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 running the following command:

```
ifconfig ethN up
```

Where, *N* represents the necessary network interface.

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
```

ORA-00020: maximum number of processes (%s) exceeded

If this error is reported, you will need to increase the maximum number of processes available to the databases within your environment. To increase the maximum number of processes from the default (150) to 300, do the following:

1. Log in as the `oracle` user to each database within your RUEI deployment.
2. Obtain an SQL*Plus prompt by running the following command:

   ```
   sqlplus / as sysdba
   ```

3. Run the following commands:

   ```
   SQL> alter system set processes=300 scope=spfile;
   System altered.

   SQL> shutdown immediate
   Database closed.
   Database dismounted.
   ORACLE instance shut down.
   SQL> startup
   ORACLE instance started.
   ```

rsync Fails When user@ Argument not Specified

Version 3.0.6-4 of the `rsync` utility distributed as part of RedHat Linux 5.7 is known to contain the bug BZ# 726060. This leads to a failure and error when specifying the source or destination argument of the `rsync` command without the optional `user@` argument. If you encountered this issue, it is recommended that you upload and install the RedHat update 2011:1112-1. It is available from the following location:

http://rhn.redhat.com/errata/RHBA-2011-1112.html

ORA-00600 Error Reported

The following error is reported when restoring a RUEI backup or deleting certain configuration items (for example, application, user id source, framework exception):

```
ORA-00600: internal error code, arguments: [kkmmctbf:bad intcoln]
```

This is caused by a known bug in Oracle database version 11.2.0.3.0. It can be fixed by downloading and installing the patch 13582702 available at the following location:

https://support.oracle.com/epmos/faces/ui/patch/PatchDetail.jspx?_afrLoop=33337295036267&patchId=13582702

Dropped Segments and Bad Checksums

If the collector is reporting a large number of dropped segments or segments with bad checksums, this could indicate a problem with the network card settings. This is because large segments, also referred to as Jumbo frames, are typically created by the network interface card driver due to an optimization feature called "receive offload". Typically, such segments created by the driver do not have a checksum (blank checksum) or have a random (junk) value as the checksum.

The dropped segments and bad checksums counters can be inspected by selecting **System**>**Status**, then expand the collector host, and select **Collector Statistics**, then **TCP**.

To see if large frames are present on the network card, select **Interfaces** on the collector status screen. Look at the value of the **Largest Encountered Frame** field for each interface and compare it with the value of the **Configured Max Frame Size** field. If the configured size is less than the largest encountered frame, then the collector is dropping these frames as they are too large for its internal capture buffers. In addition, the collector will issue a warning event in the Event Log when it encounters a frame larger than the maximum configured size.

In RUEI 12.1.0.6, the maximum configured frame size has been set to 64KB by default. In addition, checksum validation rules have been relaxed to accept both frames with blank checksums, and large frames with a junk checksum. Therefore, the rest of this section is only applicable if you have reduced the frame size for any reason and are running into drops due to bad checksums.

Background to Receive Offload and Checksum Offload Settings

Some network drivers have provisions to combine multiple physical frames into a single, large frame (of anything up to 64Kb) that is then passed on to the kernel network stack in a single operation. Network card vendors may refer to this as **frame coalescing**, **large receive offload** or **generic receive offload**. The goal is to improve efficiency by reducing the number of interrupts and copy operations from driver to kernel.

In addition to frame coalescing, some network drivers also perform TCP checksum offloading, that is, they perform TCP checksum validations for incoming packets and compute and set the checksums for outgoing packets. The goal is to improve efficiency by offloading these tasks from the kernel software to the network card hardware.

To view the current offload settings of a network interface, run the following command (you may need to do this as the root user):

```
# ethtool -k eth1
Offload parameters for eth1:
Cannot get device udp large send offload settings: Operation not supported
rx-checksumming: on
tx-checksumming: on
scatter-gather: on
tcp segmentation offload: on
udp fragmentation offload: off
generic segmentation offload: on
generic-receive-offload: on
```

The actual interpretation of the fields might differ per driver, but typically, **generic-receive-offload** indicates that the network driver is coalescing frames. In addition, the driver may or may not be filling in checksums for the resulting large frames, this can depend on other offload settings, such as **rx-checksumming** or **tcp-segmentation-offload** or simply differ per driver implementation.

Frames for which the checksum was not filled in correctly are dropped because they fail the checksum validations performed by the collector.

Checksum validation is only be attempted on frames that are not coalesced, and that have a checksum field which is not blank.

Disable Offloading Settings

To avoid large frame issues, disable the **offload settings** of the network card in order to stop it from coalescing frames altogether. Disable the **generic-receive**, **tcp-segmentation** and **generic-segmentation** offloads running the following command for each interface that the Collector is monitoring:

```
# ethtool -K eth1  tso off gso off gro off
```

Enable Jumbo Frames

If you are still observing Jumbo frames after disabling offloading for all capture interfaces, then you need to increase the maximum frame size of the collector. Go to the **Configuration** tab, and click the **Security** button on the left. Next, click **Jumbo frames** in the Security panel in the lower left of the screen. Follow the instruction on screen to set the maximum frame size.

Disable TCP Checksum Validation in Collector

To disable TCP checksum validation on the reporter system, enter the following commands as the RUEI user:

```
execsql config_set_profile_value System_name tcp TcpDoChecksum replace
    no
```

Where, *System_name* is the collector profile you want to configure. Replace this with the actual collector profile name.

Disable TCP Checksums Offloading

If the driver is not filling in TCP checksums properly due to checksum offloading, and the collector statistics show checksum errors, disable it via the command:

```
# ethtool -K eth1 rx off tx off
```

The driver implementations might differ for different vendors, to the point that some might not even let you change any of these settings. Contact Oracle Support if you are unable to change the settings of your drivers successfully and are still observing packet loss in the collector.

Errors During Installation on RedHat Enterprise/Oracle Linux 6.*x*

Installing RedHat Enterprise/Oracle Linux 6.x Prerequisites of this guide instructs you to run the following command to install all optional fonts.

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

This command may fail with a message similar to the following:

```
Transaction Check Error:
file /usr/share/fonts/opensymbol/opens___.ttf conflicts between attempted
installs of openoffice.org-opensymbol-fonts-1:3.2.1-19.6.0.1.el6_2.7.noarch
and libreoffice-opensymbol-fonts-1:4.0.4.2-9.0.1.el6.noarch
```

To workaround this issue, run the following command to install fonts:

```
yum install -y *-fonts --exclude=libreoffice*
```

SSL Error on RedHat Enterprise/Oracle Linux 6.*x*

An error similar to the following may be displayed:

```
appSensor, version ux-collector-12.1.0.6.1-20140818-collector (Aug 18
2014(11:41:41), adc4150376) RUEI_12.1.0.6.0_LINUX.X64_140818 , 64-bit
Copyright (c) 2003, 2014, Oracle, All rights reserved.
Running as instance wg
Reading configuration in "wg/config".
Finished loading configuration.
Device "eth0" initialized for capture
OK
#####   Cannot open /u01/ruei/opt/collector/lib64/libssl.so:
/u01/ruei/opt/collector/lib64/libssl.so: symbol EVP_aes_128_gcm, version
libcrypto.so.10 not defined in file libcrypto.so.10 with link time reference
#####   Plugin "libssl" failed to load
Loading plugin "libssl"
FAILED
#####   Error reading plugin configuration
 Cannot open /u01/ruei/opt/collector/lib64/libssl.so:
/u01/ruei/opt/collector/lib64/libssl.so: symbol EVP_aes_128_gcm, version
libcrypto.so.10 not defined in file libcrypto.so.10 with link time reference
 Plugin "libssl" failed to load
 wg/config/plugins.cfg, 15: User give up
 Error reading plugin configuration
 Collector exited, initialization failed
```

This indicates that the incorrect version of OpenSSL is running. Make sure that you have applied the latest OpenSSL patches for your operating system using the appropriate commands (for example, `yum update` or `up2date`). Applying the latest OpenSSL patches helps improve the security of the system.

G

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 1005 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* or 6.*x*.
Oracle Database 11g or 12c 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).
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.
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.

H

Removing RUEI From Systems

This appendix describes the procedure for uninstalling RUEI from Reporter and Collector systems.
To uninstall RUEI from each Reporter and Collector system, do the following:

1. Log in to the required system as the *RUEI_USER* user, and clear all `crontab` entries by running the following command:

   ```
   echo "" | crontab
   ```

2. Stop all processing on the Reporter systems by running the following command as the *RUEI_USER* user:

   ```
   project -stop
   ```

   In the case of Collector systems, stop data collection by running the following command:

   ```
   appsensor stop wg
   ```

3. Remove the installed RUEI RPMs by running the following command as the `root` user:

   ```
   rpm -qa | grep ^ux- | xargs rpm -e
   ```

   If parts of the installed RPMs were removed manually or corrupted, errors might be encountered in the above step. In this case, you should run the following command:

   ```
   rpm -qa | grep ^ux- | xargs rpm -e --noscripts
   ```

   Part of the installation may remain after running the above command.

4. On the Reporter system, unistall the `php-oci8` module, Oracle database Instant client, PHP configuration, and SQLplus extension by running the following commands as the `root` user:

   ```
   rm /etc/php.d/ruei.ini
   rpm -e php-oci8-11gR2
   rpm -e oracle-instantclient11.2-sqlplus
   rpm -e oracle-instantclient11.2-basic
   ```

5. Ensure that all RUEI daemons are deactivated by running the following commands as the `root` user:

   ```
   . /etc/ruei.conf
   killall -u $RUEI_USER
   ```

6. Remove all RUEI data files by running the following commands as the `root` user:

   ```
   rm -rf $RUEI_HOME
   rm -rf $RUEI_DATA
   ```

7. Remove each database instance by logging into the required database server(s) as the `oracle` user, and running the following commands:

   ```
   . /etc/ruei.conf
   . oraenv
   dbca -silent -deleteDatabase -sourceDB ${RUEI_DB_INST}
   ```

When prompted for the Oracle SID, you should specify the same value as that for the `RUEI_DB_INST` setting in the `/etc/ruei.conf` file.

8. For Reporter and Collector systems, remove the Java Runtime Environment (JRE) by running the following commands as the `root` user:

```
rm -fr /usr/java/jre1.8.0_241
rm -fr /usr/java/jre
```

9. On the Reporter system, edit the `/etc/sysconfig/httpd` file, and remove the following line that loads the RUEI environment:

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

10. Revert the changes made to user and group settings by running the following commands as the `root` user:

```
. /etc/ruei.conf
/usr/sbin/userdel $RUEI_USER
/usr/sbin/groupdel $RUEI_GROUP
/usr/sbin/usermod -G apache apache
```

11. Remove the RUEI configuration file `/etc/ruei.conf` running the following command as the `root` user:

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

During the installation procedure, you may have installed several additional RPMs. Which of these can safely be removed depends on the original Linux installation. A database installation will remain on each database server. The procedure for uninstalling the Oracle database is fully described in the product documentation. See Removing Database Software for more information about database deinstallation.

Third-Party Licenses

This appendix contains licensing information about certain third-party products included with this version 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 © 1998-2011 The OpenSSL Project. All rights reserved. It is distributed under the license available at the following location:

http://www.openssl.org/source/license.html

PHP

Copyright © 1999-2013 The PHP Group. All rights reserved.

This product includes PHP software, freely available from http://php.net/software/. It is distributed under the license available at the following location:

http://creativecommons.org/licenses/by/3.0/legalcode

Java Runtime Environment

ORACLE AMERICA, INC. ("ORACLE"), FOR AND ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES UNDER COMMON CONTROL, IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT CAREFULLY. BY SELECTING THE "ACCEPT LICENSE AGREEMENT" (OR THE EQUIVALENT) BUTTON AND/OR BY USING THE SOFTWARE YOU ACKNOWLEDGE THAT YOU HAVE READ THE TERMS AND AGREE TO THEM. IF YOU ARE AGREEING TO THESE TERMS ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE LEGAL AUTHORITY TO BIND THE LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO BE BOUND BY THE TERMS, THEN SELECT THE "DECLINE LICENSE AGREEMENT" (OR THE EQUIVALENT) BUTTON AND YOU MUST NOT USE THE SOFTWARE ON THIS SITE OR ANY OTHER MEDIA ON WHICH THE SOFTWARE IS CONTAINED.

1. DEFINITIONS. "Software" means the software identified above in binary form that you selected for download, install or use (in the version You selected for download, install or use) from Oracle or its authorized licensees, any other machine readable

materials (including, but not limited to, libraries, source files, header files, and data files), any updates or error corrections provided by Oracle, and any user manuals, programming guides and other documentation provided to you by Oracle under this Agreement. "General Purpose Desktop Computers and Servers" means computers, including desktop and laptop computers, or servers, used for general computing functions under end user control (such as but not specifically limited to email, general purpose Internet browsing, and office suite productivity tools). The use of Software in systems and solutions that provide dedicated functionality (other than as mentioned above) or designed for use in embedded or function-specific software applications, for example but not limited to: Software embedded in or bundled with industrial control systems, wireless mobile telephones, wireless handheld devices, netbooks, kiosks, TV/STB, Blu-ray Disc devices, telematics and network control switching equipment, printers and storage management systems, and other related systems are excluded from this definition and not licensed under this Agreement. "Programs" means: (a) Java technology applets and applications intended to run on the Java Platform, Standard Edition platform on Java-enabled General Purpose Desktop Computers and Servers, and (b) JavaFX technology applications intended to run on the JavaFX Runtime on JavaFX-enabled General Purpose Desktop Computers and Servers. “README File" means the README file for the Software set forth in the Software or otherwise available from Oracle at or through the following URL:

http://www.oracle.com/technetwork/java/javase/documentation/index.html

2. LICENSE TO USE. Subject to the terms and conditions of this Agreement including, but not limited to, the Java Technology Restrictions of the Supplemental License Terms, Oracle grants you a non-exclusive, non-transferable, limited license without license fees to reproduce and use internally the Software complete and unmodified for the sole purpose of running Programs.

3. RESTRICTIONS. Software is copyrighted. Title to Software and all associated intellectual property rights is retained by Oracle and/or its licensors. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. You acknowledge that the Software is developed for general use in a variety of information management applications; it is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use the Software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Oracle or its licensors is granted under this Agreement. Additional restrictions for developers and/or publishers licenses are set forth in the Supplemental License Terms.

4. DISCLAIMER OF WARRANTY. THE SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ORACLE FURTHER DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT.

5. LIMITATION OF LIABILITY. IN NO EVENT SHALL ORACLE BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF ORACLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ORACLE'S ENTIRE LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS (U.S. $1,000).

6. TERMINATION. This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate

immediately without notice from Oracle if you fail to comply with any provision of this Agreement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon termination, you must destroy all copies of Software.

7. EXPORT REGULATIONS. You agree that U.S. export control laws and other applicable export and import laws govern your use of the Software, including technical data; additional information can be found on Oracle's Global Trade Compliance web site (http://www.oracle.com/products/export-regulations.html). You agree that neither the Software nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

8. TRADEMARKS AND LOGOS. You acknowledge and agree as between you and Oracle that Oracle owns the ORACLE and JAVA trademarks and all ORACLE- and JAVA-related trademarks, service marks, logos and other brand designations ("Oracle Marks"), and you agree to comply with the Third Party Usage Guidelines for Oracle Trademarks currently located at http://www.oracle.com/us/legal/third-party-trademarks/index.html. Any use you make of the Oracle Marks inures to Oracle's benefit.

9. U.S. GOVERNMENT LICENSE RIGHTS. If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation shall be only those set forth in this Agreement.

10. GOVERNING LAW. This agreement is governed by the substantive and procedural laws of California. You and Oracle agree to submit to the exclusive jurisdiction of, and venue in, the courts of San Francisco, or Santa Clara counties in California in any dispute arising out of or relating to this agreement.

11. SEVERABILITY. If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

12. INTEGRATION. This Agreement is the entire agreement between you and Oracle relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

SUPPLEMENTAL LICENSE TERMS

These Supplemental License Terms add to or modify the terms of the Binary Code License Agreement. Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement. These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

A. SOFTWARE INTERNAL USE FOR DEVELOPMENT LICENSE GRANT. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the README File incorporated herein by reference, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Oracle grants you a non-

exclusive, non-transferable, limited license without fees to reproduce internally and use internally the Software complete and unmodified for the purpose of designing, developing, and testing your Programs.

B. LICENSE TO DISTRIBUTE SOFTWARE. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the README File, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Oracle grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software, (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that protects Oracle's interests consistent with the terms contained in this Agreement, and (vi) you agree to defend and indemnify Oracle and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software. The license set forth in this Section B does not extend to the Software identified in Section D.

C. LICENSE TO DISTRIBUTE REDISTRIBUTABLES. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the README File, including but not limited to the Java Technology Restrictions of these Supplemental Terms, Oracle grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute those files specifically identified as redistributable in the README File ("Redistributables") provided that: (i) you distribute the Redistributables complete and unmodified, and only bundled as part of Programs, (ii) the Programs add significant and primary functionality to the Redistributables, (iii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README File), (iv) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (v) you only distribute the Redistributables pursuant to a license agreement that protects Oracle's interests consistent with the terms contained in the Agreement, (vi) you agree to defend and indemnify Oracle and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software. The license set forth in this Section C does not extend to the Software identified in Section D.

D. JAVA TECHNOLOGY RESTRICTIONS. You may not create, modify, or change the behavior of, or authorize your licensees to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "javafx", "sun", “oracle" or similar convention as specified by Oracle in any naming convention designation. You shall not redistribute the Software listed on Schedule 1.

E. SOURCE CODE. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.

F. THIRD PARTY CODE. Additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME file set forth in the Software or otherwise available from Oracle at or through the following URL: `http://www.oracle.com/technetwork/java/javase/documentation/index.html`. In addition to any terms and conditions of any third party opensource/freeware license identified in the THIRDPARTYLICENSEREADME file, the disclaimer of warranty and limitation of liability

provisions in paragraphs 4 and 5 of the Binary Code License Agreement shall apply to all Software in this distribution.

G. TERMINATION FOR INFRINGEMENT. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right.

H. INSTALLATION AND AUTO-UPDATE. The Software's installation and auto-update processes transmit a limited amount of data to Oracle (or its service provider) about those specific processes to help Oracle understand and optimize them. Oracle does not associate the data with personally identifiable information. You can find more information about the data Oracle collects as a result of your Software download at http://www.oracle.com/technetwork/java/javase/documentation/index.html.

For inquiries please contact: Oracle America, Inc., 500 Oracle Parkway, Redwood Shores, California 94065, USA.

License for Archived Java SE Technologies; Last updated 13 March 2012.

The MIT License (MIT)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Daniel Veillard

Except where otherwise noted in the source code (e.g. the files hash.c, list.c and the trio files, which are covered by a similar license but with different Copyright notices) all the files are:

Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sub-license, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FIT- NESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

MaxMind

```
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:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) 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

   (d) 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.
```

J

Setting up RUEI Against a Remote Database Service

This appendix contains information on setting up RUEI against a remote database service including the pluggable database.
In a **standard** setup, the Reporter Database Instance is created using ruei-prepare-db.sh which, along with other helper scripts, is to be executed on the host on which the Oracle Database software is installed. There are cases, however, in which you do not have access to the command-line of the database server, or where having to copy the scripts over is inconvenient. This includes Pluggable Database setups.

The sections in this appendix describe the following:

Prerequisites

- An existing database instance or Pluggable Database. The database instance or Container Database (if using a Pluggable Database) needs to be configured using paragraph B.1 and B.2 of Generic Database Instance Setup as a reference for the required options (e.g. Character Set).
- The fully-qualified connection string to the remote database service. In case of a pluggable database setup, this should be the name of the pluggable database, not the container database.
- The password for the SYS user who has **sysdba** rights. In case of a pluggable database setup, this should be the `-global- SYS` user.

Setting Up

To set up RUEI, do the following:

- As the `root` user, run the following commands:
  - `cd /usr/local`
  - `tar xzf /root/RUEI/mkstore/mkstore-11.2.0.4.0.tar.gz`
- This installs the mkstore utility to `/usr/local/mkstore-11.2.0.4.0`. To make the install directory version independent, create a more generic symlink running the following command:
  - `ln -s /usr/local/mkstore-11.2.0.4.0 /usr/local/mkstore`
- Add/change the following settings in `/etc/ruei.conf`:
  - `export DEFAULT_TABLESPACE=<name_of_default_tablespace>`

- `export REMOTE_DB=1`
- `export DBCONNECT="(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(Host=<databasehostname>)(Port=<port>))(CONNECT_DATA=(service_name=<service name>)))"`
- `export RUEI_DB_INST=<name of service or sid>`
- `export MKSTORE_BIN=/usr/local/mkstore/mkstore`

All values between <> serve as an example. Replace them with values appropriate to your setup.

Running ruei-prepare-db.sh

Running `ruei-prepare-db.sh` on the reporter system:

Make `ruei-prepare-db.sh` and the `sql_scripts` subdirectory available to the `$RUEI_USER user (e.g. /tmp)` and set the proper permissions by running the following commands:

- `cd /tmp`
- `chmod +x ruei-prepare-db.sh`
- `chmod -R +r sql_scripts/`

As the `$RUEI_USER` user, run the following commands:

- `cd /tmp`
- `export ORACLE_HOME=/usr/lib/oracle/12.1/client64`
- `./ruei-prepare-db.sh create`

The `ruei-prepare-db.sh` script will execute all regular steps, except creating the instance and will prompt for the password of the database `SYS` user, a password for the RUEI user, and a password for the wallet.