

Administering Composite Applications at Run Time

Objectives

After completing this lesson, you should be able to:

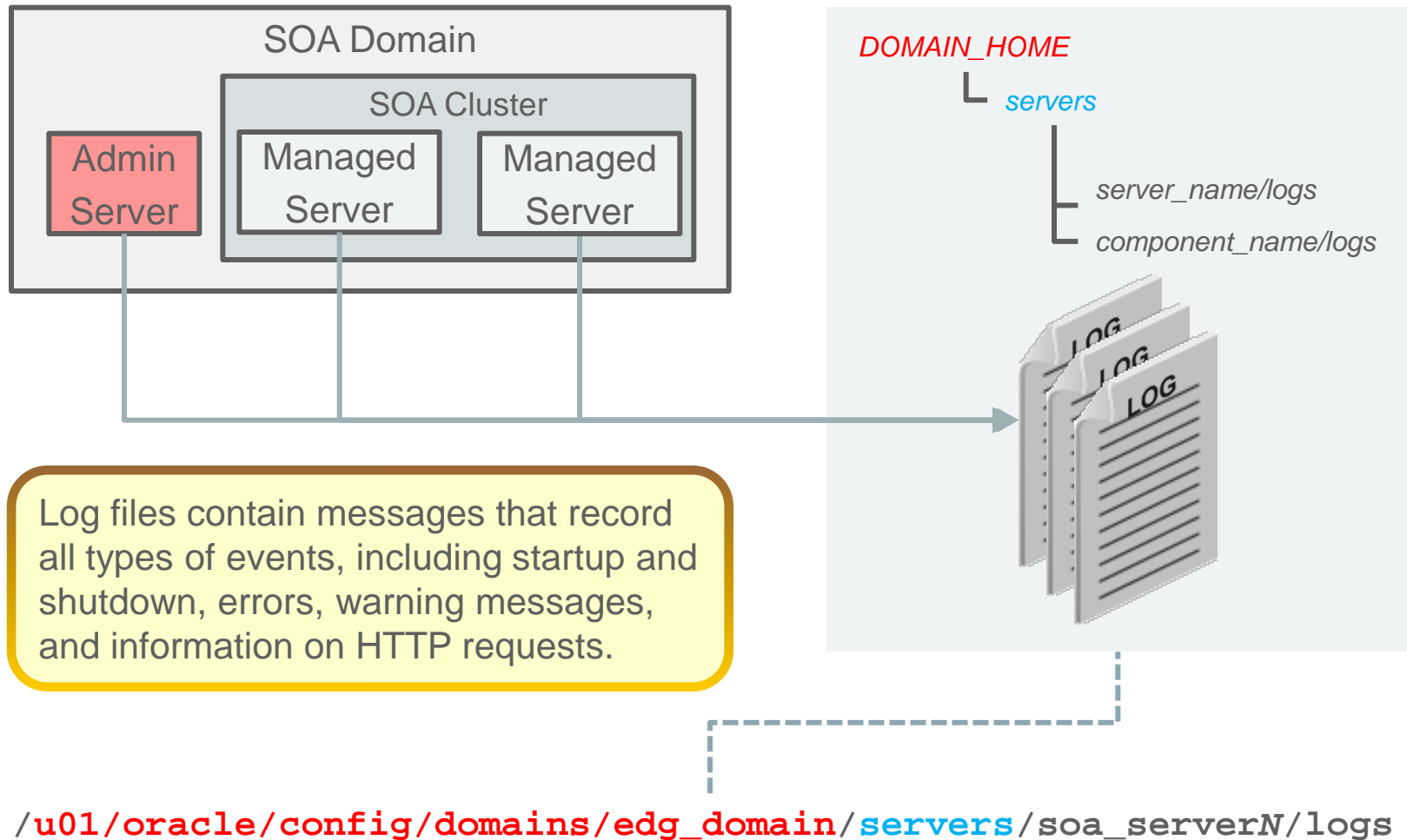
- Configure logging, audit levels, and sensors
- Manage faults in the error hospital



Agenda

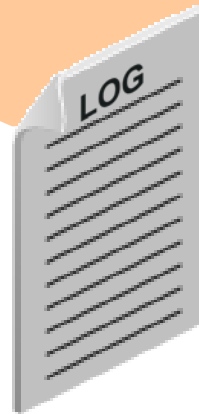
- Configuring Logging, Audit Levels, and Sensors
- Managing Faults in the Error Hospital

Log Files: Overview



ODL Log File Format

```
[2015-05-13T12:31:29.0584-07:00] [OHS]  
[NOTIFICATION:16] [OHS-9999]  
[mod_weblogic.c] [host_id: example] [host_addr:  
nn.nnn.nn.nn] [pid: 12789]  
[tid: 46919953675776] [user: username VirtualHost: main  
WebLogic Server Plugin version 12.1.2  
<WLSPLUGINS_MAIN_LINUX.X64_130502.1731>
```



Logging Levels

| Message Type | Level | Description |
|----------------|-------|---|
| INCIDENT_ERROR | 1 | A serious problem that may be caused by a bug in the product and that should be reported to Oracle Support. Examples are errors from which you cannot recover or serious problems. |
| ERROR | 1 | A serious problem that requires immediate attention from the administrator and is not caused by a bug in the product. An example is if Oracle Fusion Middleware cannot process a log file, but you can correct the problem by fixing the permissions on the document. |
| WARNING | 1 | A potential problem that should be reviewed by the administrator. Examples are invalid parameter values or a specified file does not exist. |
| NOTIFICATION | 1 | A major lifecycle event such as the activation or deactivation of a primary sub-component or feature. This is the default level for NOTIFICATION. |
| NOTIFICATION | 16 | A finer level of granularity for reporting normal events |
| TRACE | 1 | Trace or debug information for events that are meaningful to administrators, such as public API entry or exit points |
| TRACE | 16 | Detailed trace or debug information that can help Oracle Support diagnose problems with a particular subsystem |
| TRACE | 32 | Very detailed trace or debug information that can help Oracle Support diagnose problems with a particular subsystem |

Configuring Logging Levels

The screenshot shows the Oracle SOA Suite configuration interface. On the left, the 'Target Navigation' pane shows the hierarchy: SOA Infrastructure > Logs > Log Configuration. The main area displays the 'Log Levels' configuration page for 'soa-infra'.

Log Levels Configuration Page:

Use this page to configure basic and advanced log configuration settings.

Log Levels | Log Files

This page allows you to configure the log level for both persistent loggers and active runtime loggers. Persistent loggers are logs that become active when the component is started. The log levels for these loggers are persisted across component restarts. Runtime loggers become active when a particular feature area is exercised. For example, oracle.j2ee.ejb.deployment.Logger is a runtime module is deployed. Log levels for runtime loggers are not persisted across component restarts.

View: Runtime Loggers

Search: All Categories

| Logger Name | Oracle Diagnostic Logging Level (Java Level) | Log File |
|------------------------------|--|-------------|
| oracle.integration | NOTIFICATION:1 (INFO) [Inheri] | odi-handler |
| oracle.sdp | NOTIFICATION:1 (INFO) [Inheri] | odi-handler |
| oracle.sdp.internal | NOTIFICATION:1 (INFO) [Inheri] | odi-handler |
| oracle.soa | NOTIFICATION:1 (INFO) [Inheri] | odi-handler |
| oracle.soa.adapter | NOTIFICATION:1 (INFO) [Inheri] | odi-handler |
| oracle.soa.adapter.apps | NOTIFICATION:1 (INFO) [Inheri] | odi-handler |
| oracle.soa.adapter.aq | NOTIFICATION:1 (INFO) [Inheri] | odi-handler |
| oracle.soa.adapter.coherence | NOTIFICATION:1 (INFO) [Inheri] | odi-handler |
| oracle.soa.adapter.db | NOTIFICATION:1 (INFO) [Inheri] | odi-handler |
| oracle.soa.adapter.file | NOTIFICATION:1 (INFO) [Inheri] | odi-handler |
| oracle.soa.adapter.ftp | INCIDENT_ERROR:1 (SEVERE+100) ERROR:1 (SEVERE) WARNING:1 (WARNING) NOTIFICATION:1 (INFO) NOTIFICATION:16 (CONFIG) NOTIFICATION:32 TRACE:1 (FINE) TRACE:16 (FINER) TRACE:32 (FINEST) NOTIFICATION:1 (INFO) [inherited from parent] | odi-handler |
| oracle.soa.adapter.jdworl | | |

☐ Persist log level state across component restarts

Configuring Log Files

Log Configuration

Use this page to configure basic and advanced log configuration settings.

Log Levels **Log Files**

Use this page to create and edit log file configurations. A log file configuration specifies the log file where the log messages will be logged to, the format as well as other parameters depending on the log file configuration class.

Create... Create Like... **Edit Configuration...** View Configuration... Delete Configuration...

| Handler Name | Log Path | Log File Format | Rotation Policy |
|-----------------------|---|-----------------------------------|-----------------|
| em-log-handler | \${domain.home}/servers/\${weblogic.Name}/sysman/log/em... | Oracle Diagnostics Logging - Text | Size Based |
| em-trc-handler | \${domain.home}/servers/\${weblogic.Name}/sysman/log/em... | Oracle Diagnostics Logging - Text | Size Based |
| odl-handler | \${domain.home}/servers/\${weblogic.Name}/logs/\${weblogic... | Oracle Diagnostics Logging - Text | Size Based |
| owsm-message-h... | \${domain.home}/servers/\${weblogic.Name}/logs/c | | |
| soa-tracking-trc-h... | \${domain.home}/servers/\${weblogic.Name}/logs/\$ | | |

Edit Log File

Log File: soa-tracking-trc-handler
Handler Class: oracle.core.ojdl.logging.ODLHandlerFactory
* Log Path: \${domain.home}/servers/\${weblogic.Name}/logs/\${weblogic.Name}-soa-trac
Log File Format: ☒ Oracle Diagnostics Logging - Text ☐ Oracle Diagnostics Logging - XML
Log Level:
Use Default Attributes: ☐
Supplemental Attributes: J2EE_APP.name,J2EE_MODULE.name,WEBSERVICE.name,WEBSERVIC
Loggers To Associate: oracle.soa.sql.trc.fabric

Rotation Policy

☒ Size Based ☐ Time Based
* Maximum Log File Size (MB): 5.0
Maximum Size Of All Log Files (MB): 50.0
Start Time:
* Frequency: ☒ Minutes ☐ Hourly ☐ Day
Retention Period: ☒ Minutes ☐ Day

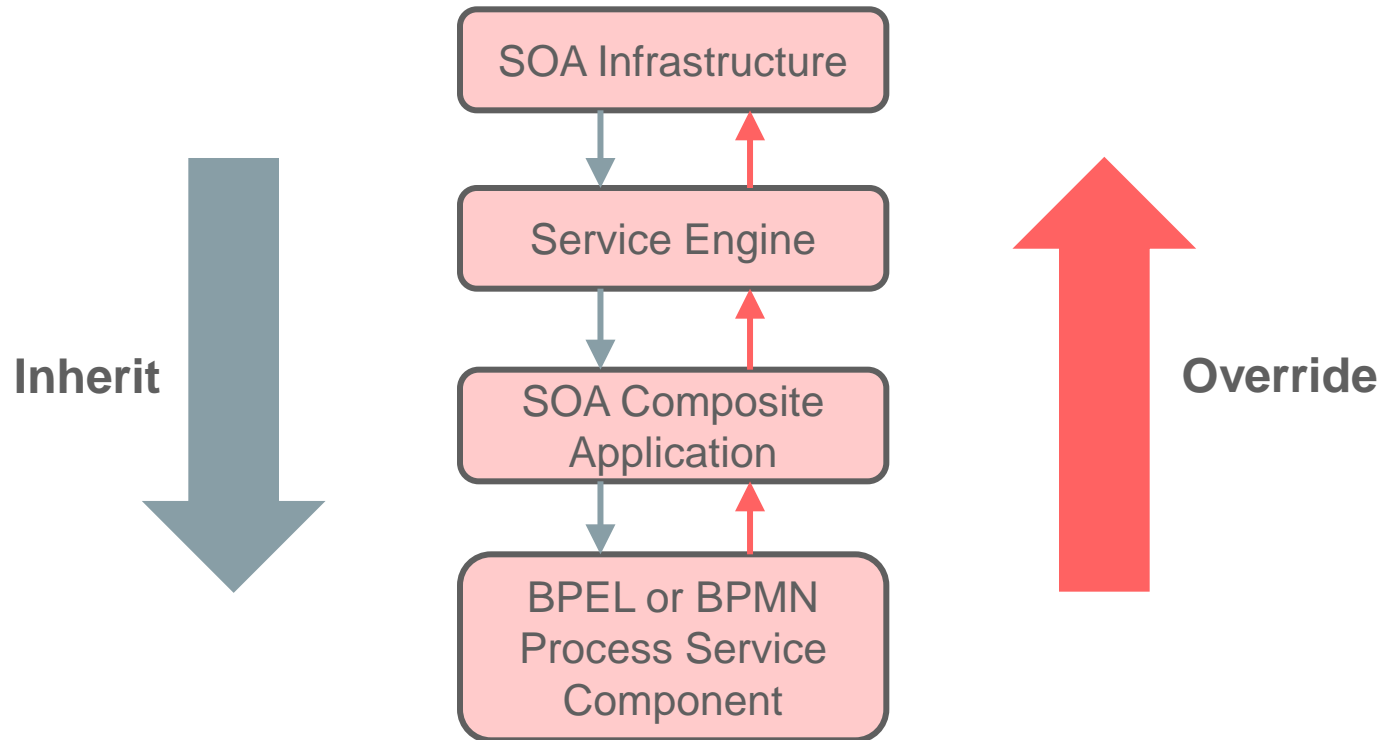
Cancel OK

Audit Levels

| Audit Level | Composite Instance Tracking | Message Payload Tracking |
|-------------|-----------------------------|---------------------------|
| Off | No | No |
| Production | Yes | Partial |
| Development | Yes | Yes, with all the details |

Setting the *audit level* allows you to select the amount of message data to be collected by the message tracking infrastructure.

Order of Precedence for Audit Level Settings



Properties set at the SOA Infrastructure level impact all service engines and deployed SOA composite applications, except those for which you explicitly set different audit level values.

Managing the Audit Level of BPEL Components

soa-infra SOA Infrastructure

Logged in as weblogic_soa | soavh01.example.com
Page Refreshed Mar 24, 2015 5:36:42 PM GMT

System MBean Browser

Application Defined MBeans: SCAComposite.SCAComponent:BPELProcess1

Show MBean Information

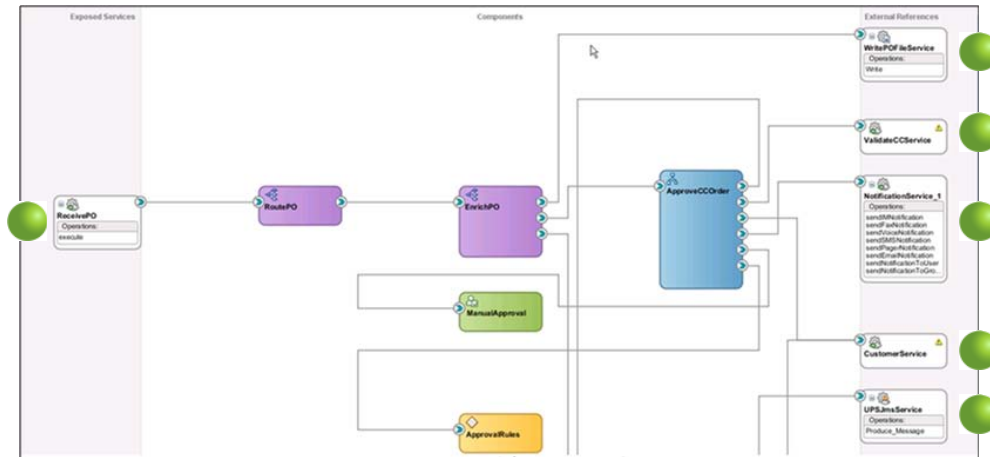
Attributes Operations Notifications

| Name | Description | Access | Value |
|---------------------------------|--|--------|------------|
| 1 ConfigMBean | If true, it indicates that this MBean is a Config MBean. | R | false |
| 2 eventProvider | If true, it indicates that this MBean is an event provider as defined by JSR-77. | R | true |
| 3 Events | Component Business Event Subscription | RW | [Ljavax.ma |
| 4 eventTypes | All the event's types emitted by this MBean. | R | save.invol |
| 5 Implementation | Component Implementation | R | javax.man |
| 6 Name | Component Name | R | BPELProc |
| 7 objectName | The MBean's unique JMX name | R | oracle.soa |
| 8 PolicyAttachmentSupport | Determine the class of supported policies | R | componer |
| 9 PolicySubjectName | The name of the policy subject | R | Versioning |
| 10 PolicySubjectResourcePattern | The resource pattern of the policy subject | R | /WLS/edg |
| 11 PolicySubjectType | The type of the policy subject | R | SCACOM |
| 12 Properties | Component Properties | RW | [Ljavax.ma |
| 13 ReadOnly | If true, it indicates that this MBean is a read only MBean. | R | false |
| 14 References | Component References | R | javax.man |
| 15 RestartNeeded | Indicates whether a restart is needed. | R | false |

State M

Sensors

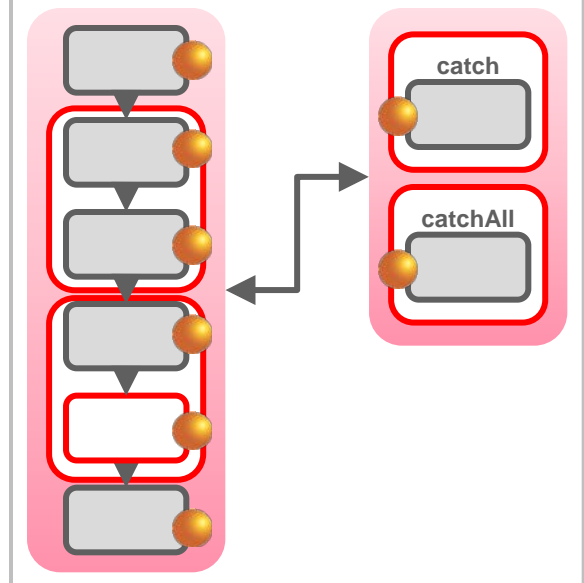
Composite Application



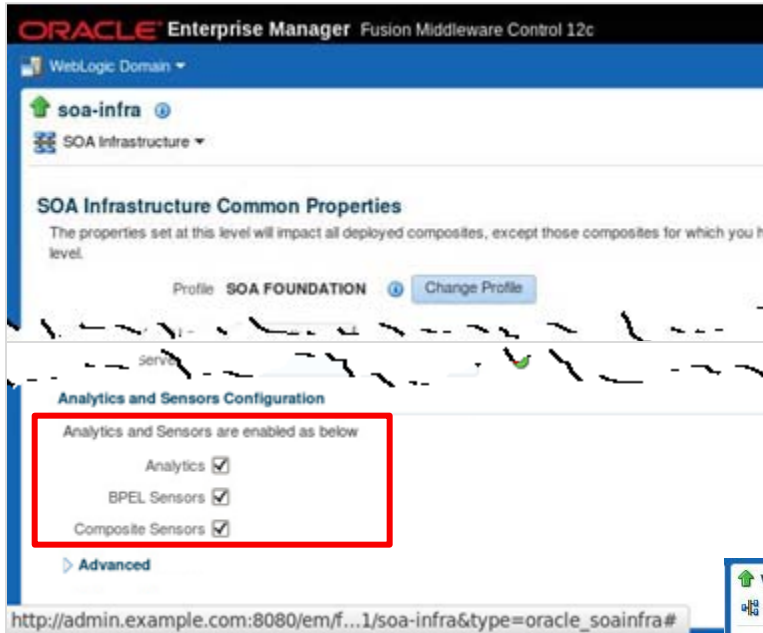
Composite Sensors enable you to monitor incoming and outgoing messages.

BPEL Sensors enable you to collect data in BPEL faults, activities, and variables.

BPEL Process

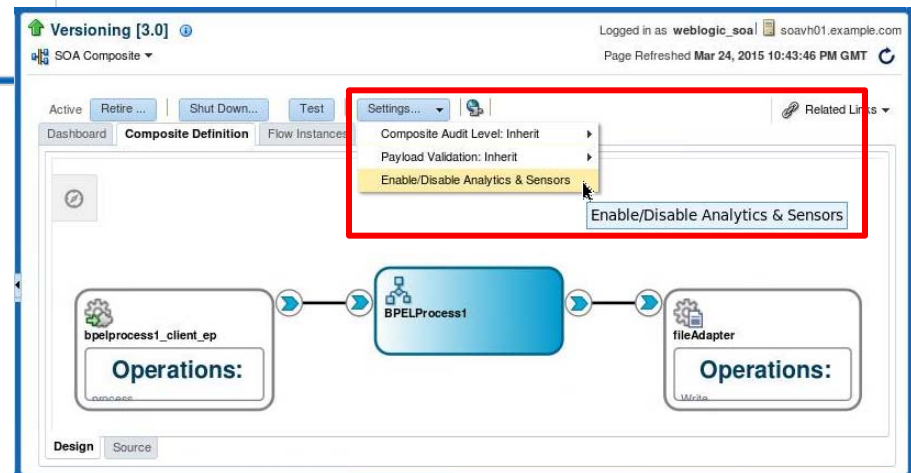


Enabling and Disabling Sensors



Enable or disable sensors at the soa-infra level from the Common Properties page.

Enable or disable sensors at the composite level from the home page for the composite.



Monitoring Composite Instances and Faults

The screenshot displays the SOA Infrastructure monitoring dashboard. At the top, it shows the user is logged in as 'weblogic_soa' and the page was refreshed on Mar 23, 2015 at 5:07:52 PM GMT. The dashboard is divided into several sections:

- Key Configuration:** Includes settings for Profile (SOA FOUNDATION), Instance Tracking (Production), Default Query Duration (Last 24 Hours), and Auto Purge (Enabled).
- Business Transaction Faults:** A section highlighted with a red box, showing a 'Last*' filter set to 24 Hours and a message to 'Refresh region to show the latest data. Click graph to drill down.'
- SOA Runtime Health:** Shows the status of 'soa_cluster1' as 'Initialized Successfully' and lists components like 'soa-infra (soa_server2)' and 'soa-infra (soa_server1)'.
- System Backlogs:** Displays a 'Last*' filter set to 24 Hours and a message to 'Refresh region to show the latest data.' Below this, it lists messages in queues: 'BPEL Invoke --', 'BPEL Callback --', and 'Mediator Parallel Routing --'.
- Composites and Adapters Availability:** Shows a filter for 'soa_server1' and a list of status messages: 'No Composite Start-Up Errors', 'No EIS Connectivity Errors', 'All Composites are UP', and 'Adapter Downtime 1'.
- Search:** Includes radio buttons for 'Instances' and 'Bulk Recovery Jobs', a 'Recent Instances - Last 24 Hours' section with 'With Faults' and 'All' filters, and a search form with fields for 'Composite', 'Instance Name or ID', 'Sensor Name', and 'Sensor Value', along with a 'Search Instances' button.
- Fault Alerts:** Includes radio buttons for 'Rules', 'All', 'System', and 'Partition', and a message 'No alerts found.'

Quiz



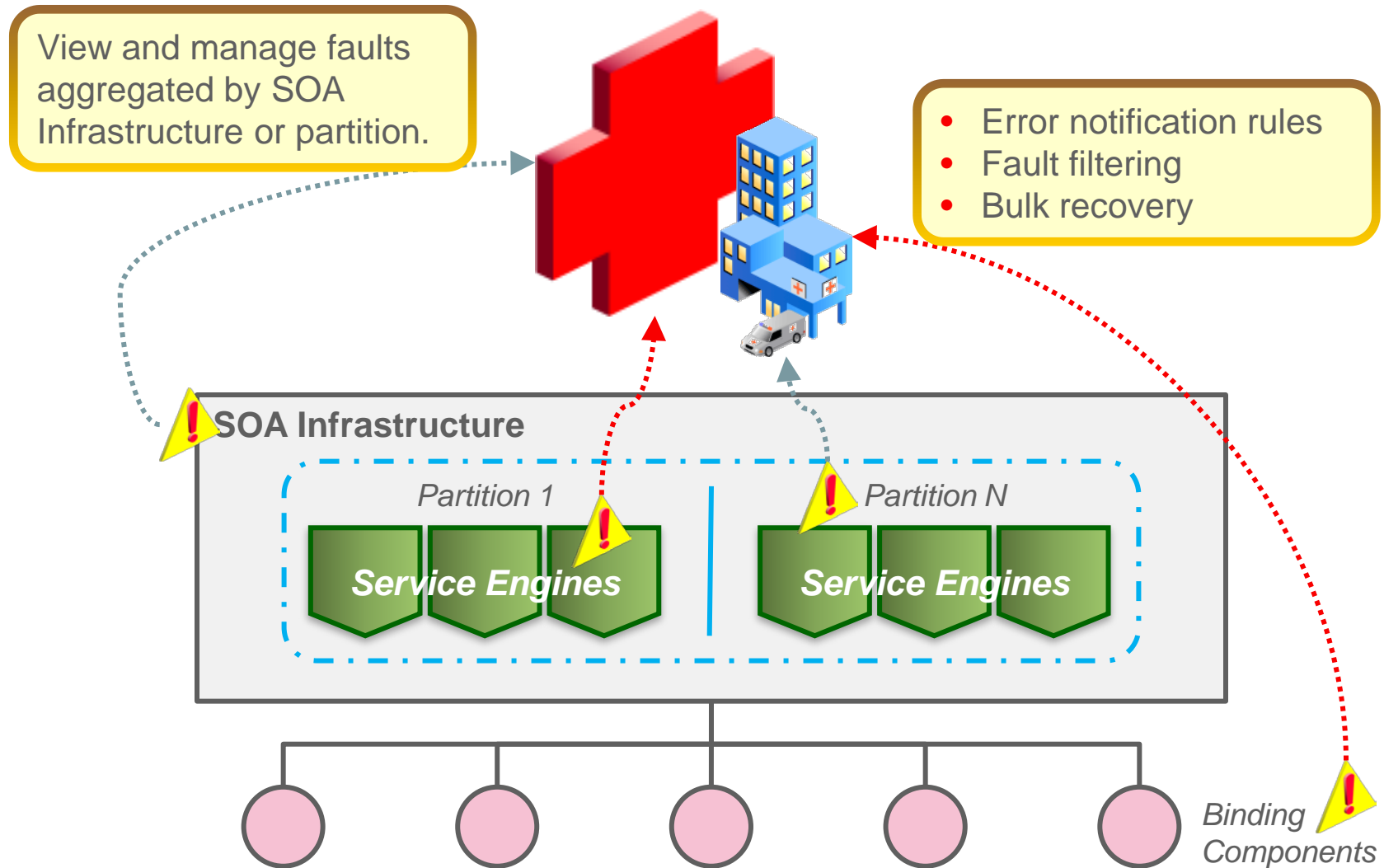
Audit level is used to select the amount of information to be collected by the log files.

- a. True
- b. False

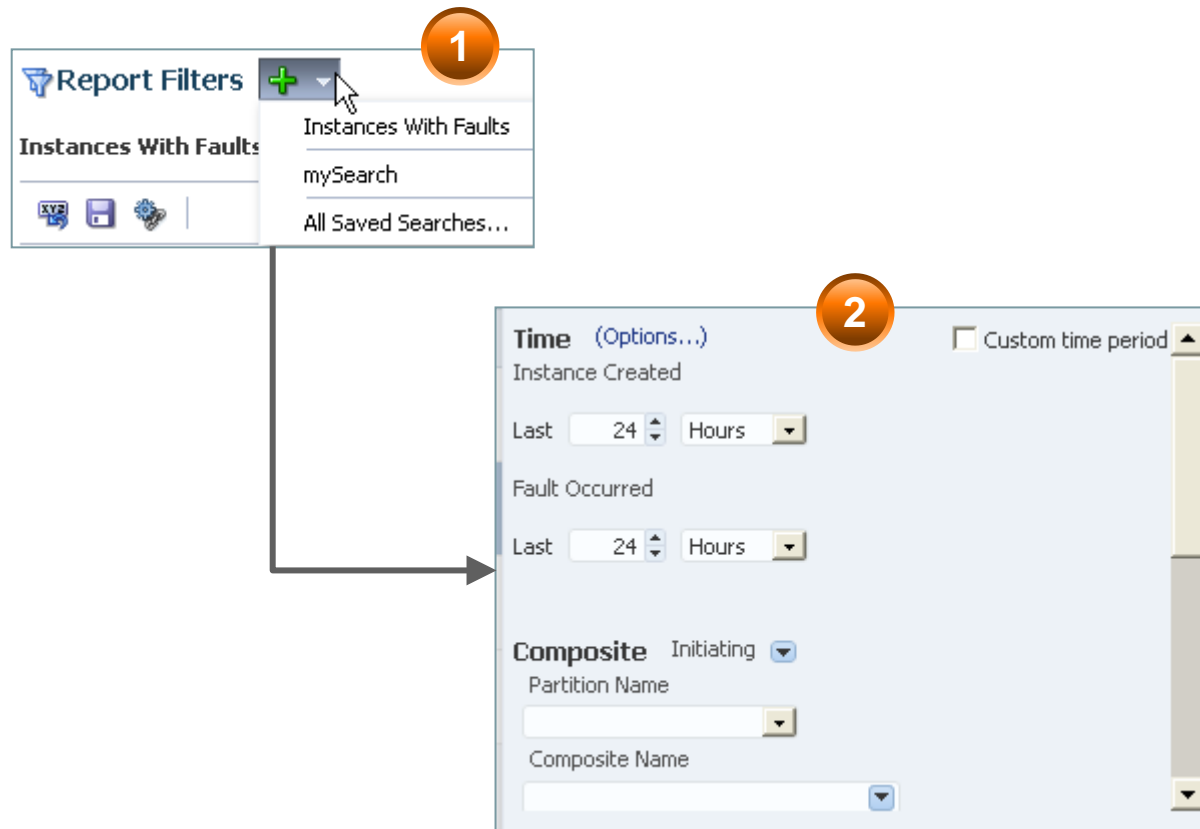
Agenda

- Configuring Logging, Audit Levels, and Sensors
- Managing Faults in the Error Hospital

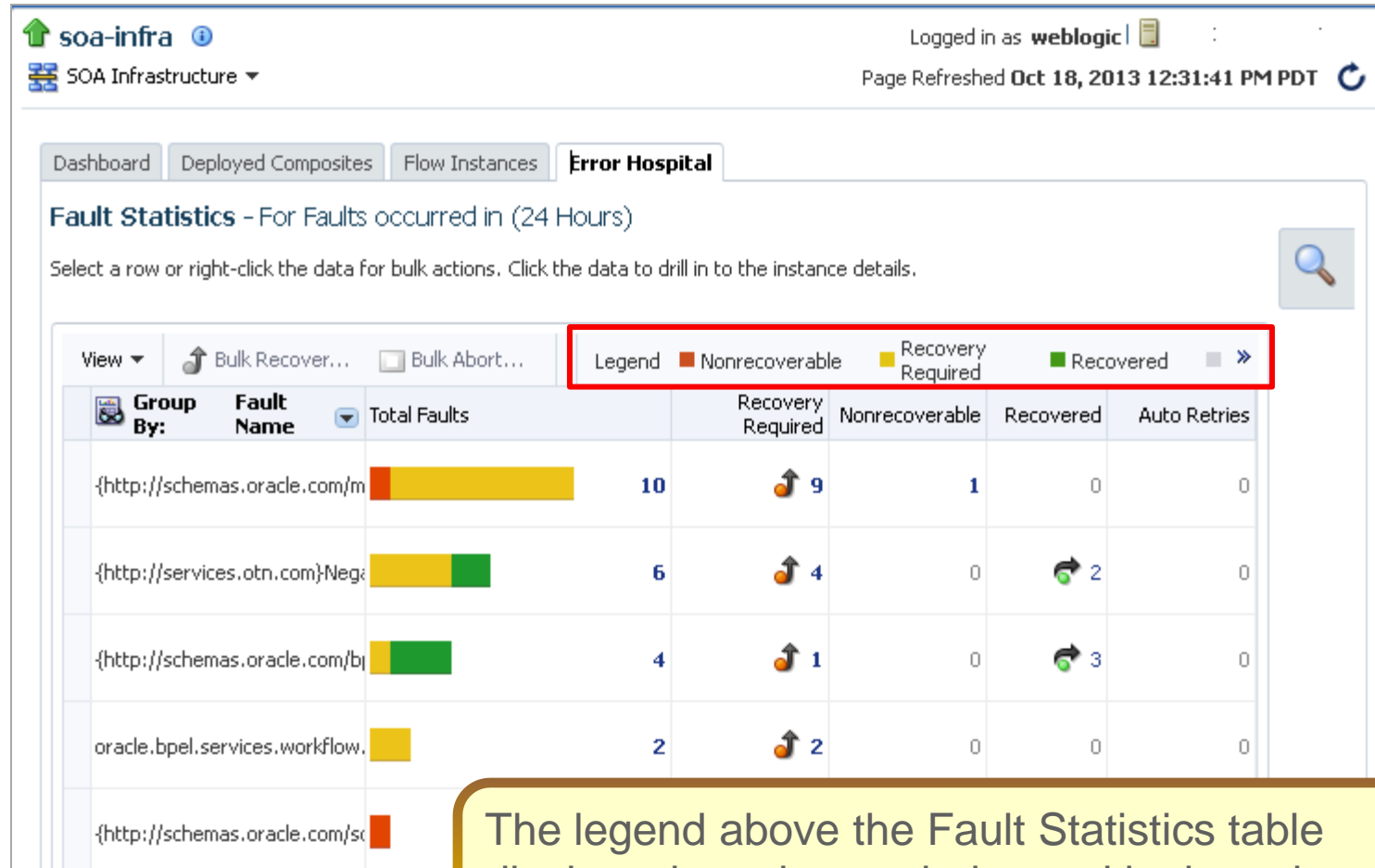
Managing Faults in the Error Hospital



Specifying and Saving Fault Search Criteria



Viewing Aggregated Fault Statistics















The legend above the Fault Statistics table displays the color symbols used in the columns of the table to identify the state of the faults.

Performing Bulk Fault Recoveries and Terminations

Fault Statistics - For Faults occurred in (24 Hours)

Select a row or right-click the data for bulk actions. Click the data to drill in to the instance details.

| | | | | | | | |
|--|---|---|---|--|---|---|---------------------------|
| View ▾ |  Bulk Recover... |  Bulk Abort... | Legend |  Nonrecoverable |  Recovery Required |  Recovered | System Auto Retries |
|  Group By: Fault Name ▾ | Total Faults | | Recovery Required | | | | |
| {http://schemas.oracle.com/mediator/faults}mediatorFault |  3 | |  3 | | | | |
| {http://services.otn.com}NegativeCredit |  2 | |  2 | | | | |
| oracle.bpel.services.workflow.WorkflowException |  1 | |  1 | | | | |

Quiz



Using the error hospital, at which level can you view and manage fault data?

- a. SOA Infrastructure level
- b. Individual partition level
- c. Composite level
- d. Service component level
- e. All of the above
- f. Only a and b

Summary

In this lesson, you should have learned how to:

- Configure logging, audit levels, and sensors
- Manage faults in the error hospital

Practice 10: Overview

This practice covers the following topics:

- Practice 10-1: Deploying the Composite Applications
 - In this practice, you use an ant script to deploy a pair of composite applications to the SOA server. A second script generates a series of data files that provide input to the applications. You use the Enterprise Manager web application to monitor the sensors, events, analytics, faults and more.
- Practice 10-2: Exploring the Features of the Error Hospital
 - In this practice, you cause an application to generate a large number of faults, and then use the bulk recovery feature of the error hospital to recover them.