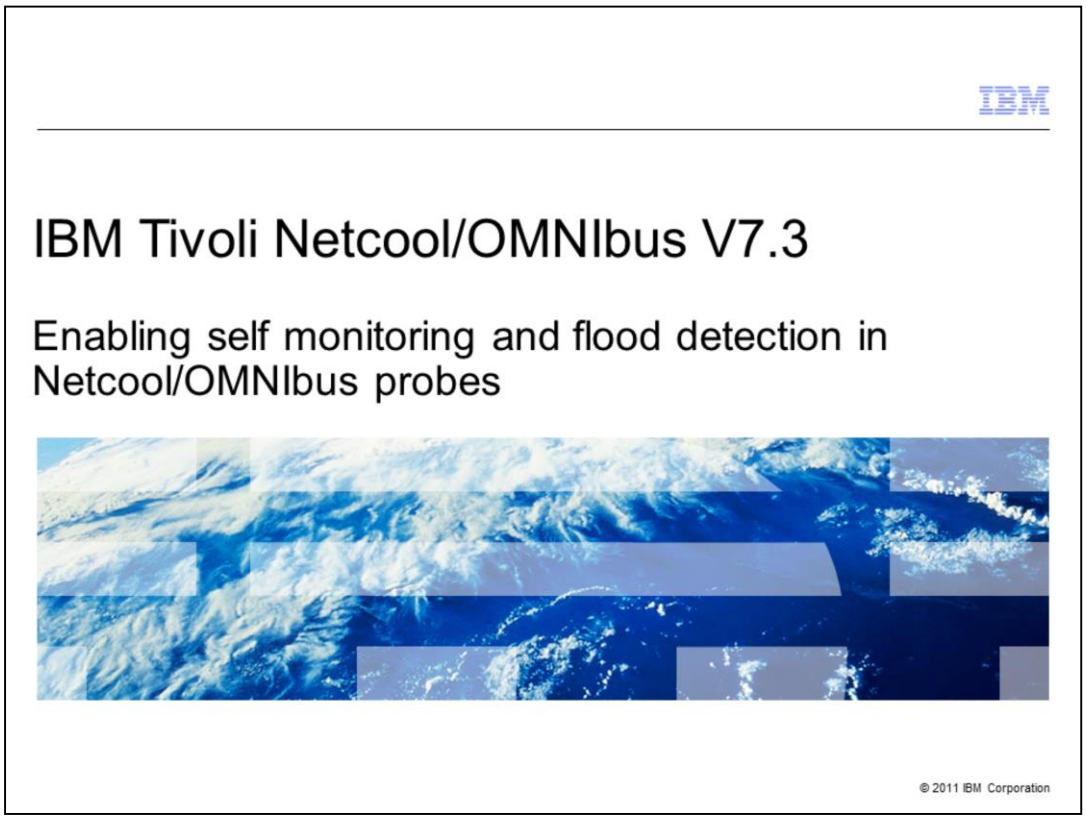


IBM Tivoli® Netcool® OMNIbus 7.3: Enabling self monitoring and flood detection in Netcool/OMNIbus probes.

In this training module, you learn about enabling self monitoring and flood detection in Tivoli Netcool/OMNIbus probes.

Assumptions.

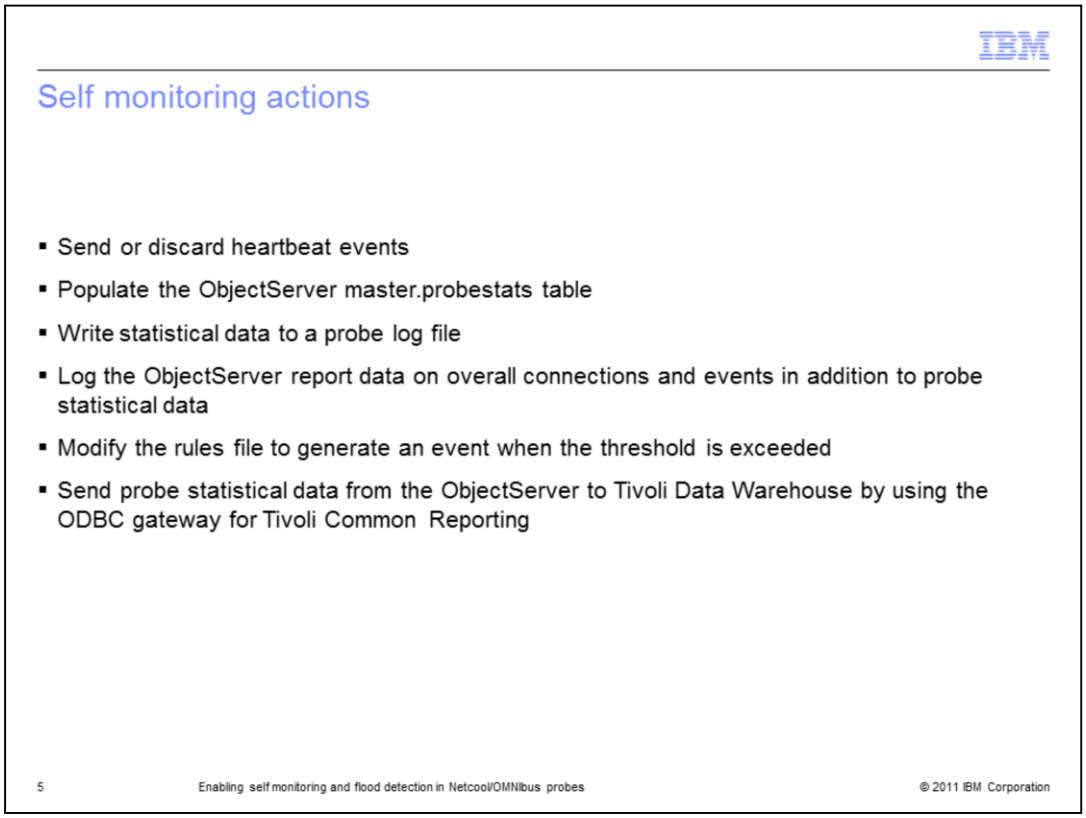
Before you begin this module, you must have a general knowledge of Netcool/OMNIbus.

Objectives.

After you complete this module, you can enable self monitoring and flood detections in Netcool/OMNIbus probes.

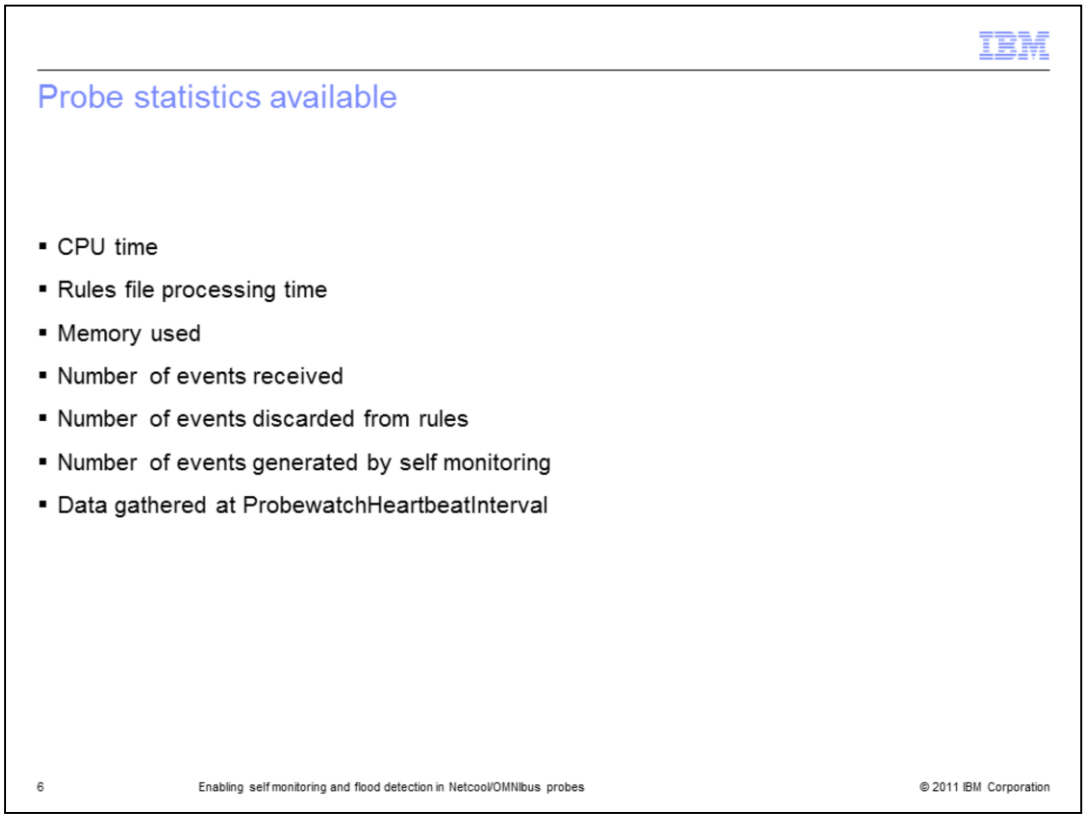
Self monitoring overview.

You can configure probes to send a ProbeWatch Heartbeat if events are not sent to the ObjectServer at a designated interval. This self-monitoring mechanism provides probe statistical data that you can use to assess the condition of the probe.



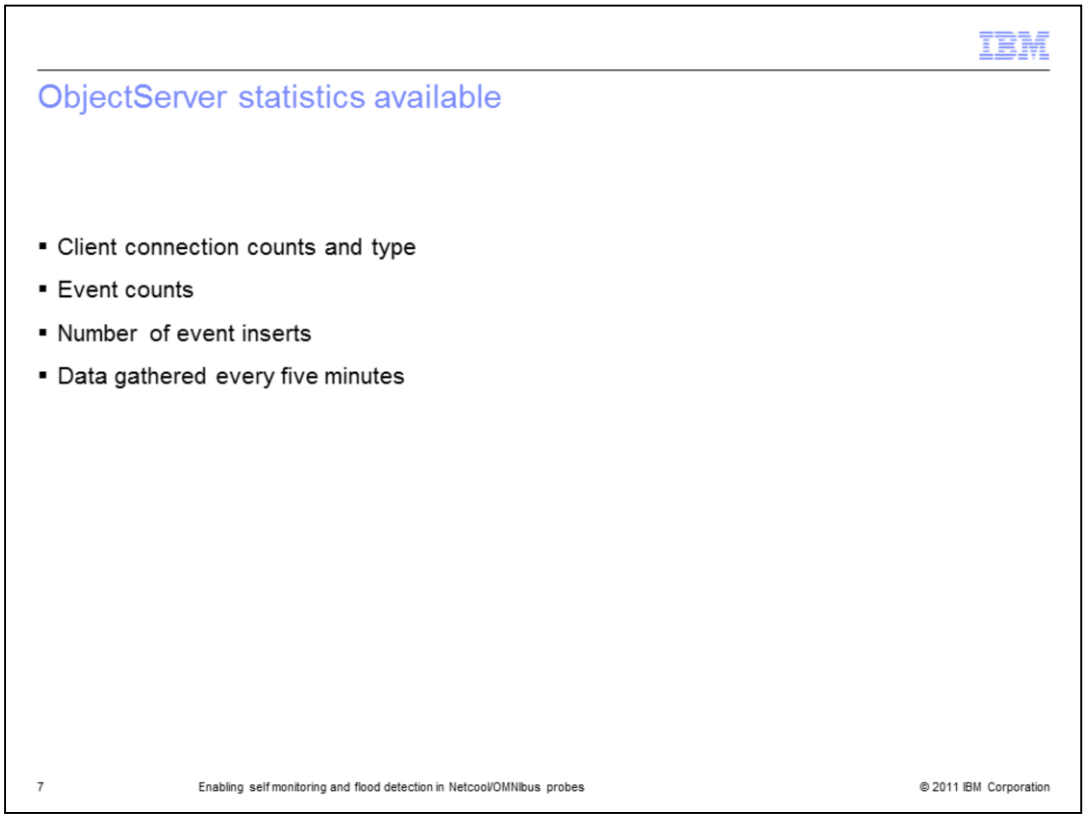
Self monitoring actions.

Self monitoring actions include sending or discarding heartbeat events, populating the ObjectServer master.probestats table, and writing statistical data to a probe log file. The ObjectServer reports include statistical data about overall connection and events in addition to probe statistical data. Optionally, you can modify rules files to generate an event. For example, you might modify these files when the threshold is exceeded. Probe statistical data can be sent from the ObjectServer to Tivoli Data Warehouse by using the ODBC gateway for Tivoli Common Reporting.



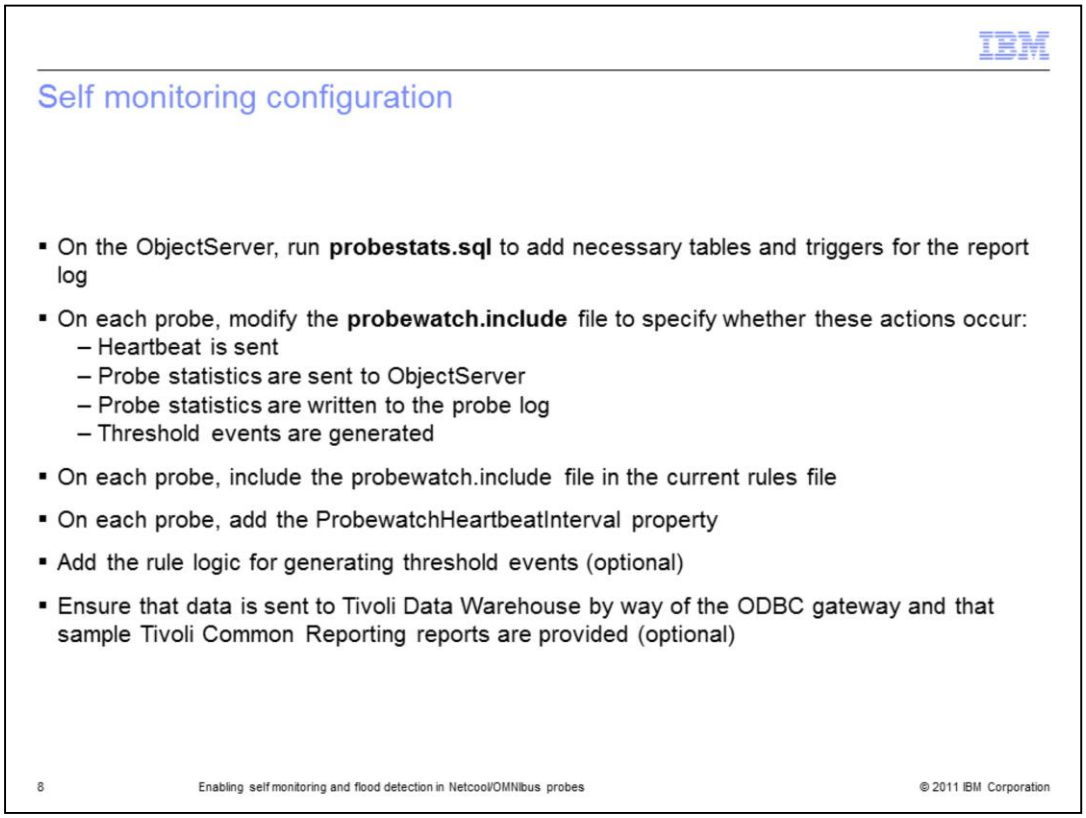
Probe statistics available.

The probes statistics that are available are listed on the slide. They include CPU time, rules file processing time, memory used, number of events received, number of events discarded from rules, number of events generated by self monitoring, and data gathered at ProbewatchHeartbeatInterval.



ObjectServer statistics available.

The ObjectServer statistics that are available are client connection counts and type, event counts, number of event inserts, and data that is gathered every five minutes.

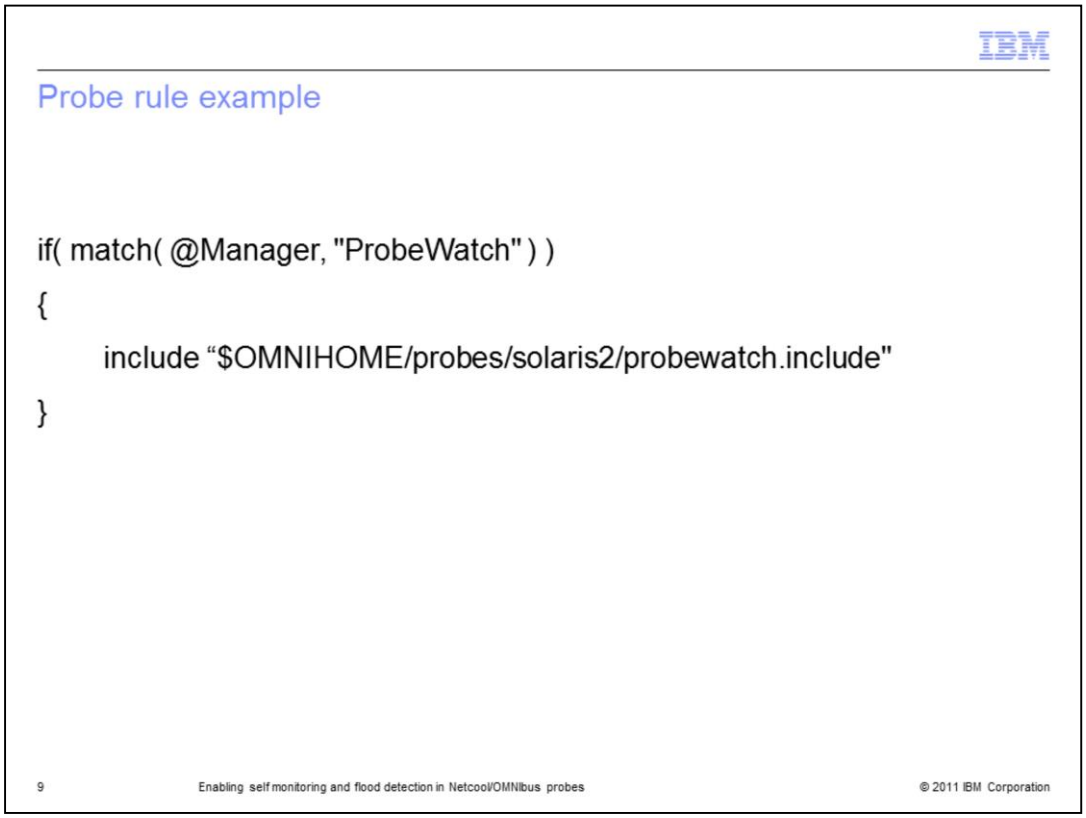


Self monitoring configuration.

When you configure the probes for self monitoring and flood detection, you perform several tasks. On the ObjectServer, you run **probestats.sql** to add the necessary tables and triggers for the report log.

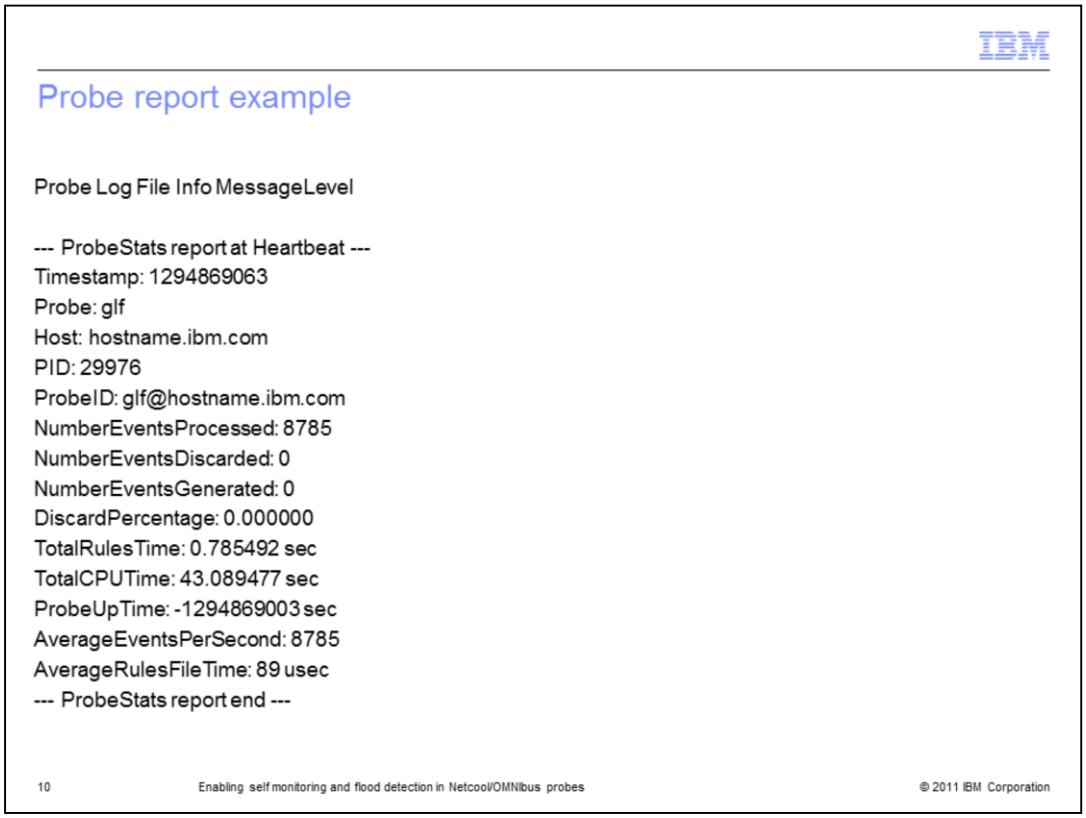
On each probe, you modify the **probewatch.include** file to specify whether the heartbeat is sent and whether the probe statistics are sent to the ObjectServer. You also specify whether the probe statistics are written to the probe log and whether threshold events are generated on each probe.

You include the probewatch.include file in the current rules file and add the **ProbewatchHeartbeatInterval** property on each probe. Optionally, you can add rule logic for generating threshold events. If data is sent to Tivoli Data Warehouse by way of the ODBC gateway, the sample Tivoli Common Reporting reports are provided.



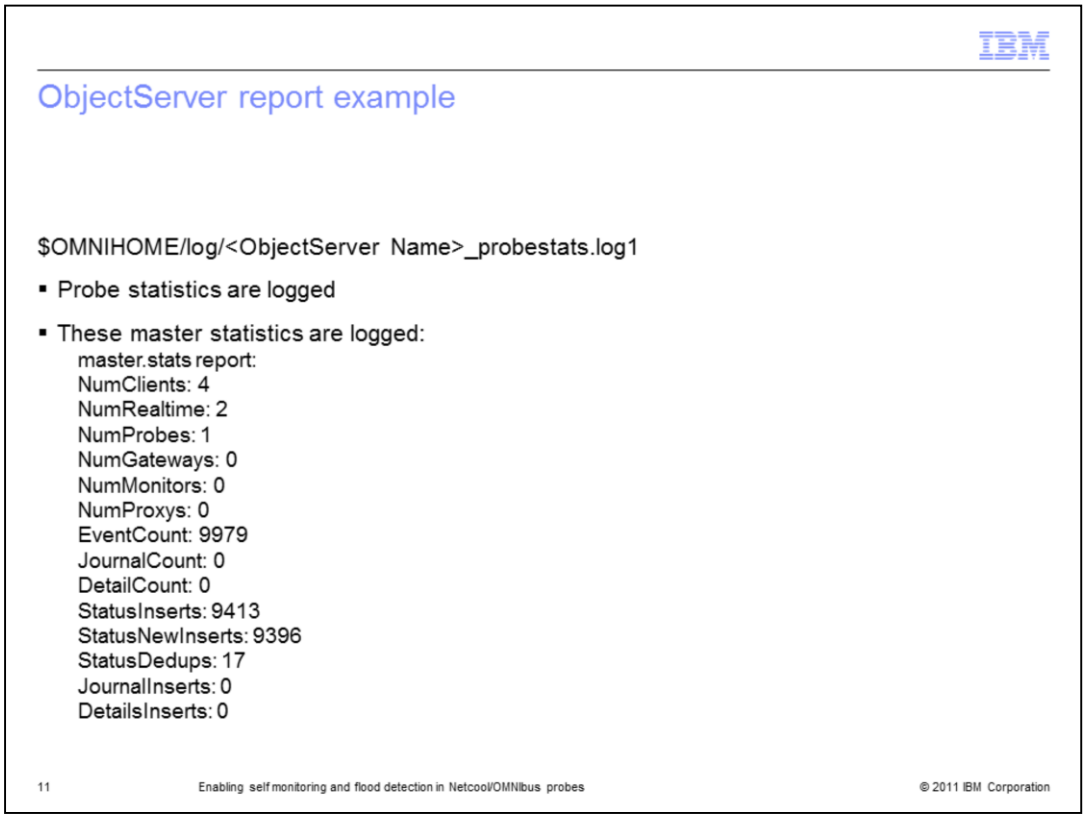
Probe rule example.

In this example, you replace the ProbeWatch section at the beginning of the rules file with an include statement for the **probewatch.include** file.



Probe report example.

In this example, the probe statistics are logged by using the MessageLevel property to specify the message logging level. In this case, the level is **Info**.

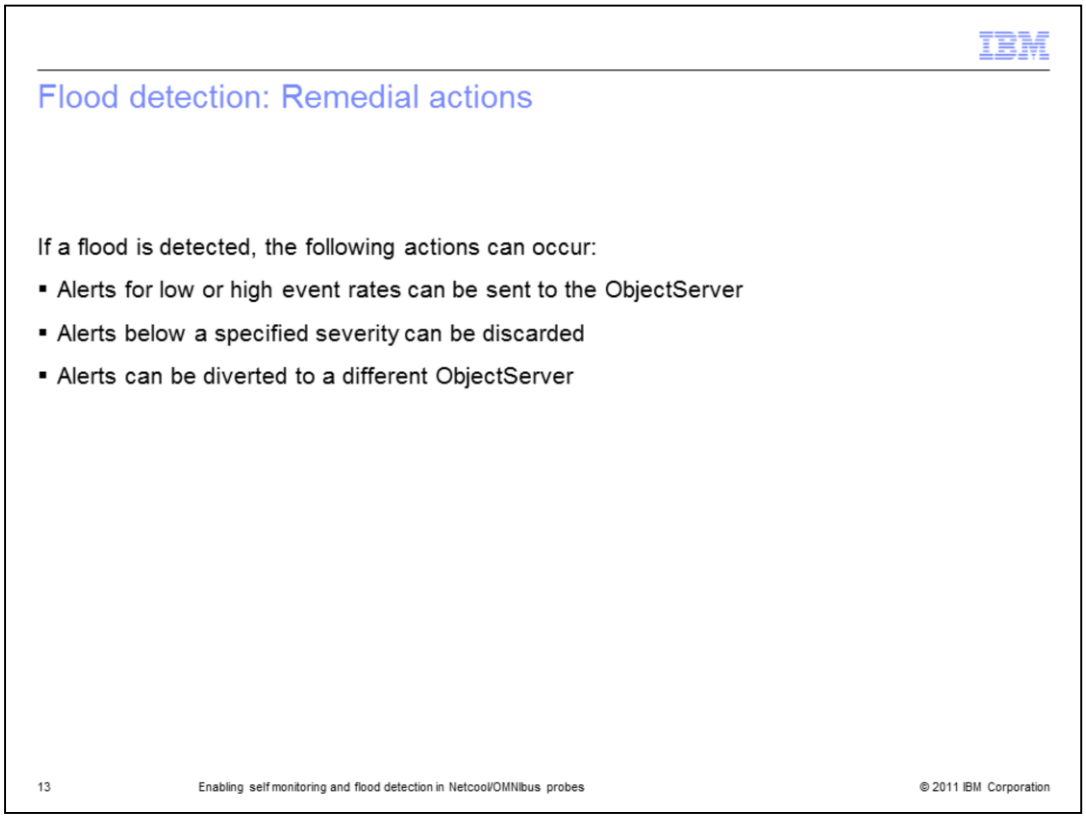


ObjectServer report example.

In this example, the probe statistics and the master statistics are logged in the ObjectServer report.

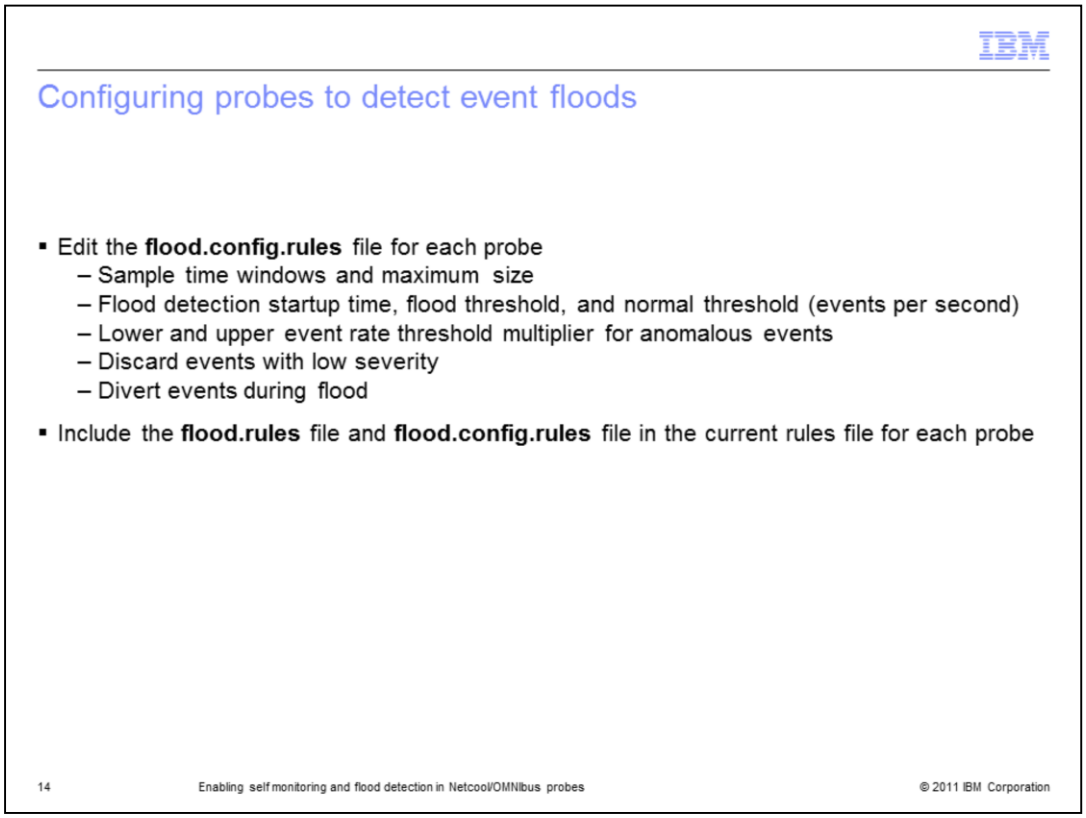
Flood detection overview.

You can configure a probe rule, based on a flood rate threshold. You can also configure a rule for an anomalous event rate. When an event rate is detected, the ObjectServer receives an informational alert that describes the event rate, which might be higher or lower than an average rate.



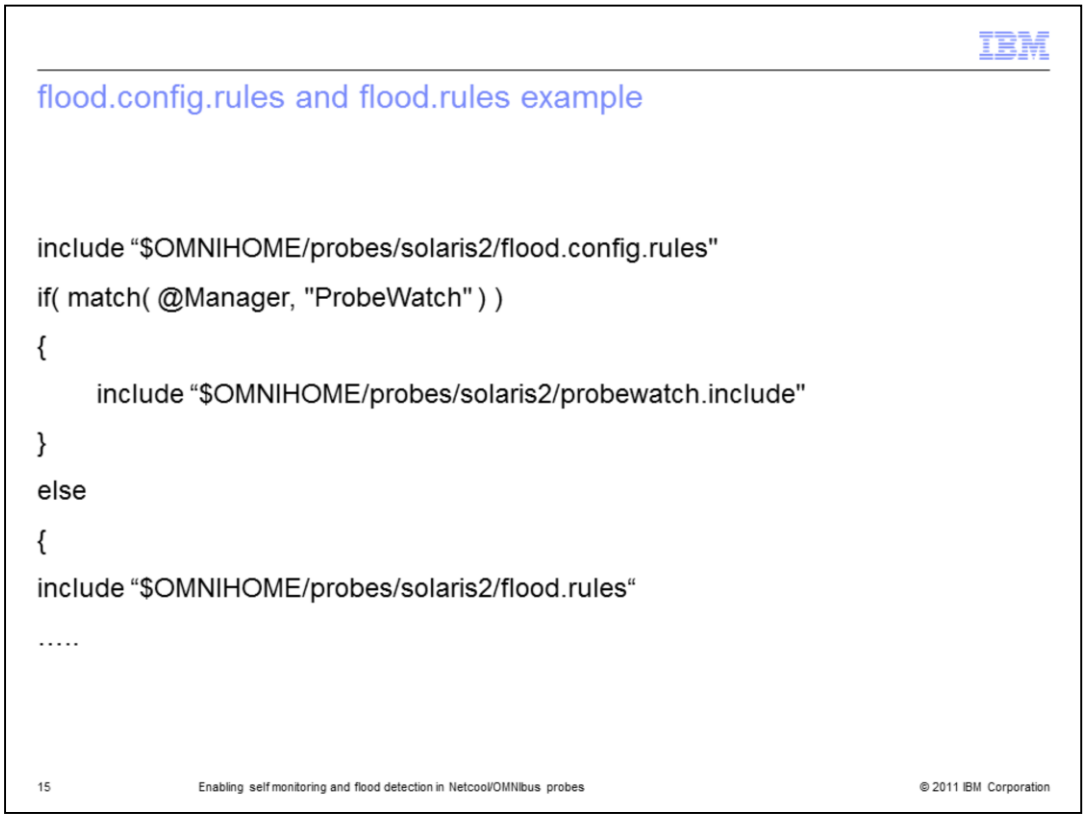
Flood detection remedial actions.

If a flood is detected, alerts for a low or high event rate can be sent to the ObjectServer. Alerts that are below a specified severity can be discarded. Alerts can also be diverted to a different ObjectServer.



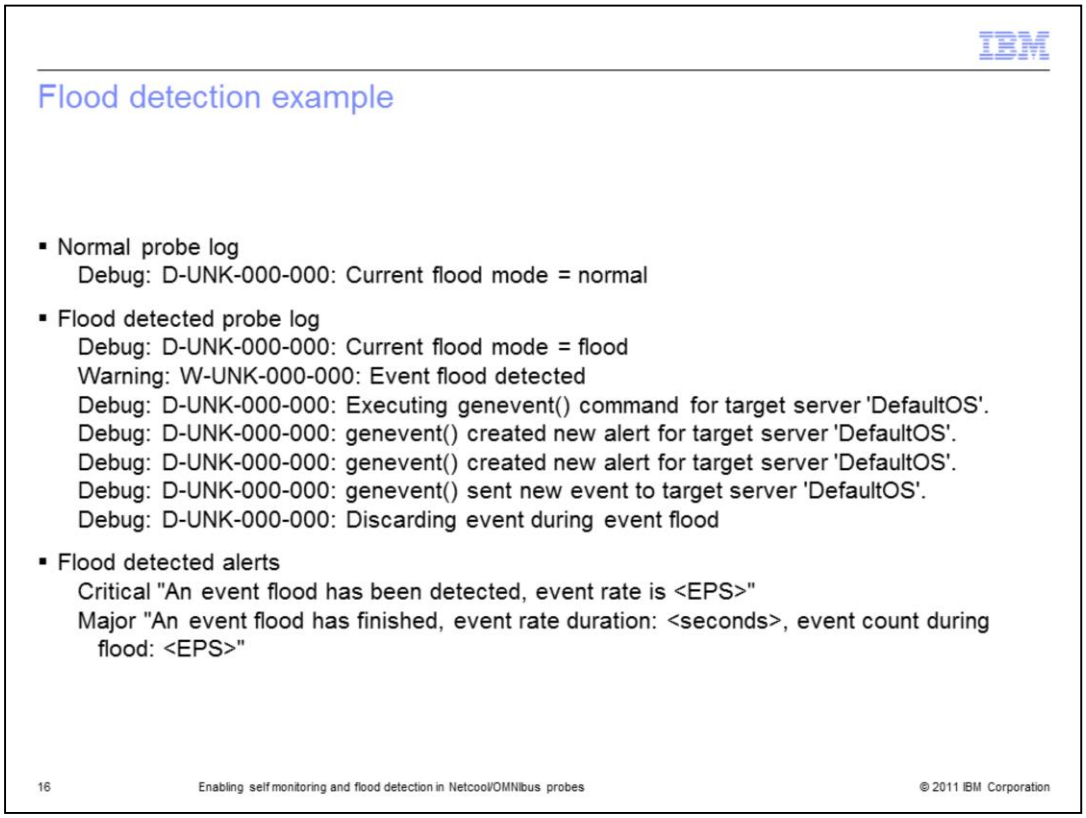
Configuring probes to detect event floods.

When you configure the probes to detect event floods, you edit the **flood.config.rules** file for each probe. These edits include the sample time windows and maximum size, the flood detection startup time, the flood threshold, and normal threshold in events per second. The edits also include a lower and upper event rate threshold multiplier for anomalous events, discard events with low severity, and divert events during flood. You must include the flood.rules file and the flood.config.rules file in the current rules file on each probe.



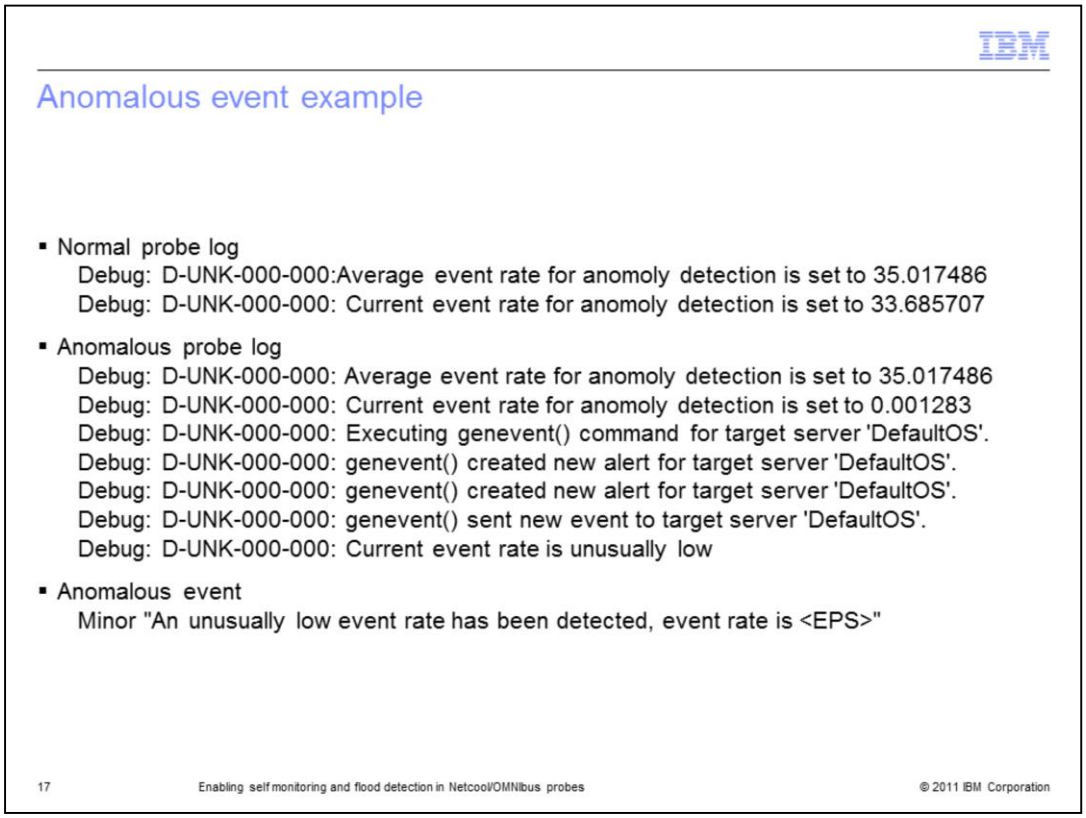
flood.config.rules and flood.rules example.

At the beginning of the rule file, include the **flood.config.rules** file. In the section before normal processing of flood events, include the **flood.rules** file.



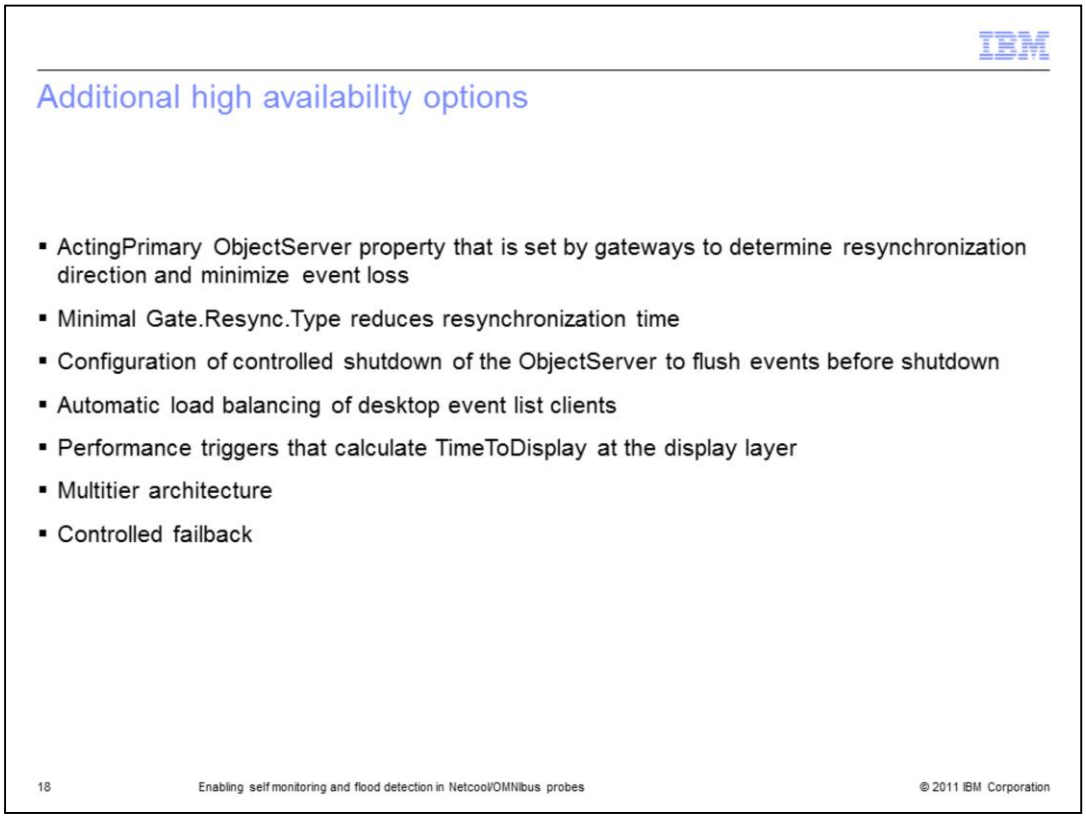
Flood detection example.

In this example, you see a normal probe log, a flood detected probe log, and flood detected alerts. In the flood detected probe log, you see that an event is sent to the ObjectServer for the detected flood. The event is discarded because of severity. An informational alert is sent to the ObjectServer when the event flood is detected and when it is resolved.



Anomalous event example.

In the anomalous probe log, the current event rate is much lower than normal. An alert about the low event rate is sent to the ObjectServer.

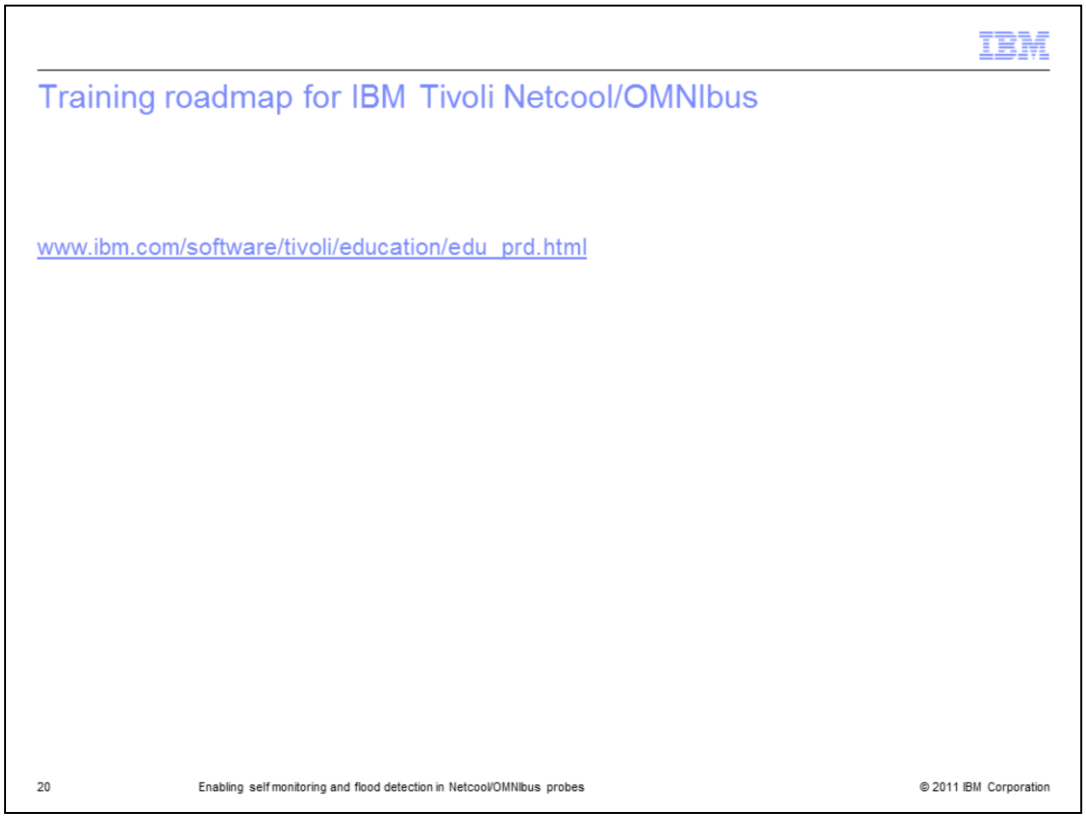


Additional high availability options with Netcool/OMNIbus 7.3.

Additional high availability options are available in Netcool/OMNIbus 7.3. You can use the ActingPrimary ObjectServer property to determine resynchronization direction and minimize event loss. You can use the Gate.Resync.Type property to specify the type of resynchronization that is required and reduce synchronization time. You can configure a controlled shutdown of any ObjectServer to flush the events before shutdown. You can set up automatic load balancing of desktop event list clients. You can use performance triggers to calculate the TimeToDisplay value at the display layer. You can use multitiered architecture and controlled failback. See the *IBM Tivoli Netcool/OMNIbus Administration Guide* for more information about these options.

Summary.

Now that you have completed this module, you can enable self monitoring and flood detection in Netcool/OMNIbus probes.



Training roadmap for IBM Tivoli Netcool/OMNIbus.

You can see the training roadmap for IBM Tivoli Netcool/OMNIbus by going to the web site that is shown on the slide.

Trademarks, disclaimer, and copyright information