Instructions for installing Autonomic Computing Problem Determination Technology Pack

Introduction:
The BladeCenter Autonomic Computing Problem Determination Technology Pack installed on top of the Autonomic Computing Toolkit aims to provide autonomic capabilities especially in the areas of data collection and problem determination for the BladeCenter equipped with the Cisco IGESM (Intelligent Gigabit Ethernet Switch Module). In this version of the package, components are included to convert native log formats from disparate sources into the Common Base Event format, to archive the collected data in native format for later analysis and to visualize the logs and events side by side in graphical form. Advanced correlation and analysis can be built on top of this layer to perform automated problem mitigation and recovery based on IBM Autonomic Computing's self-healing technologies.

The installed package is highly extensible – it includes the Generic Log Adapter and the Rule Builder (an Eclipse based tool for writing parsing rules), thereby enabling the addition of different log sources for problem determination and root cause analysis. By using this package, you can enable your BladeCenter with current IBM Autonomic Computing technologies and have it ready for new analysis and correlation tools that are part of the Autonomic Computing toolkit.

Prerequisites:
First you need to install some components of the Autonomic Computing toolkit:

1. Generic Log Adapter for Autonomic Computing
2. Log and Trace Analyzer

These can be found as a single download at
http://www-106.ibm.com/developerworks/autonomic/probdet1.html

It is recommended that you familiarize yourself with the configuration and operation of the Generic Log Adapter by reading through the user's guide and *readme* files.

Where to go for help:
If you have any questions or problems associated with the installation of this technology package, please don't hesitate to contact Ed Merenda (merenda@us.ibm.com). If you have problems with the base AC toolkit please follow the links for help of that package directly.

Installing the package:
We recommend that you install the Generic Log Adapter on a management server that has network access to the BladeCenter (specifically the Management Module). Also the Cisco IGESM must be able to send events to this machine. This typically requires that the BladeCenter Cisco IGESM and the management server are in the same network domain.

Assume <*GenericLogAdapter*> indicates the folder where you installed the Generic Log Adapter. Extract the *BladeCenterAC.zip* archive into this folder. This ZIP file contains a *bladecenter_ac.jar* file that will be added to the *lib* folder, configuration files (*.adapter*) that will be added to the *config* folder under a *BladeCenter* subfolder and a few batch files including *mm_realtime.bat, mm_postproc.bat, esm_realtime.bat* and *esm_postproc.bat* that are added to the *bin* folder. More details about each of this are below.

The *bladecenter_ac.jar* contains the custom sensors that are required to collect data from the BladeCenter MM and Cisco IGESM. They will be plugged into the Generic Log Adapter instance at runtime through configuration. The configuration files contain both configuration information and the rules for parsing the native log formats. There are four configuration files 2 each for the BladeCenter's MM (management module) and Cisco IGESM. Of these 2, one is for real-time processing and the other for post-mortem processing.

Edit the *.bat* files that start with *esm* or *mm* in the <*GenericLogAdapter*>*bin* folder and change line 2 to SET GLA_HOME = <*GenericLogAdapter*> (substitute the folder name where you installed the Generic Log Adapter on your machine here)

Table 1: Different configuration files in the package

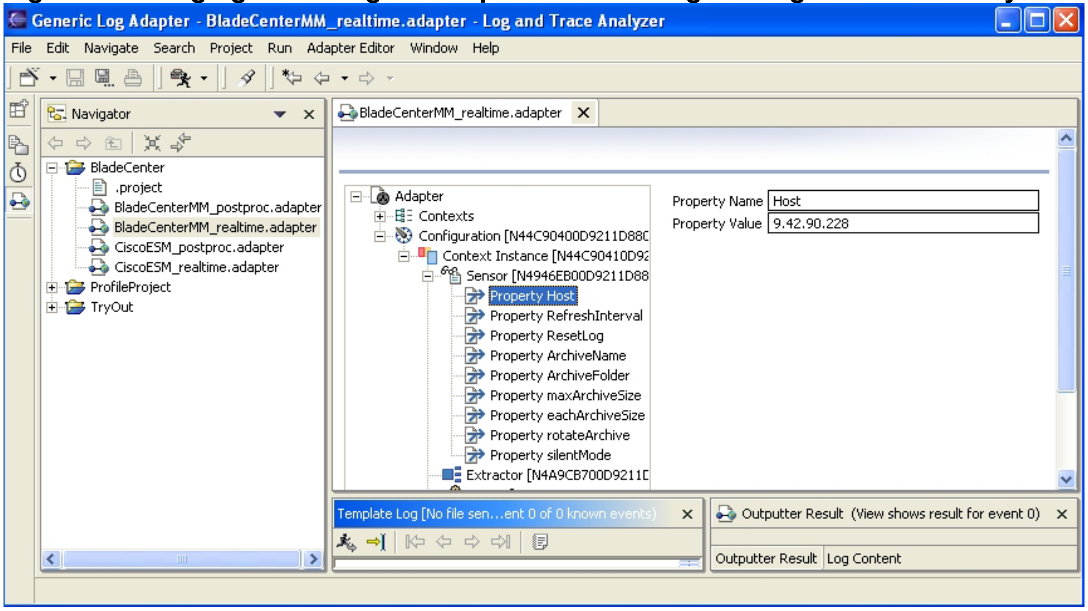
Name of configuration file	Purpose
BladeCenterMM_postproc.adapter	Post mortem processing of a saved / archived management module log file. Files archived by the adapter during a previous real time processing run using the following configuration can be processed with this configuration.
BladeCenterMM_realtime.adapter	Real time processing of a live management module log file from an active BladeCenter's Management Module. This configuration can also archive files during processing and the archived files can be processed later on using the above configuration.
CiscoESM_postproc.adapter	Post mortem processing of an archive of *syslog* formatted entries from the Cisco IGESM. Archives created during a previous real time processing run using the below configuration can be processed with this configuration.
CiscoESM_realtime.adapter	Real time processing of *syslog* events from the Cisco IGESM within an active BladeCenter. This configuration can also archive the events sent to the adapter during processing and the archived files can be processed later on using the above configuration.

Configuration:

The configuration files have different configuration parameters for the two sensors as listed in the tables below. To modify any of the parameters follow the steps below,

1. Open the appropriate file in the Log and Trace Analyzer
2. Expand the tree as shown in the figure below. Different files will show different parameters in this tree.
3. Click on a parameter and use the dialog boxes on the right to enter a new value
4. Save the configuration file with a CTRL-S or using the floppy disk icon on the toolbar

Figure 1: Changing the configuration parameters using the Log and Trace Analyzer



Property Name: Host
Property Value: 9.42.90.228

Generic Log Adapter - BladeCenterMM_realtime.adapter - Log and Trace Analyzer
File
Edit
Navigate
Search
Project
Run
Adapter Editor
Window
Help
Navigator
BladeCenter
.project
BladeCenterMM_postproc.adapter
BladeCenterMM_realtime.adapter
CiscoESM_postproc.adapter
CiscoESM_realtime.adapter
ProfileProject
TryOut
BladeCenterMM_realtime.adapter
Adapter
Contexts
Configuration [N44C90400D9211D88C
Context Instance [N44C90410D92
Sensor [N4946EB00D9211D88
Property Host
Property RefreshInterval
Property ResetLog
Property ArchiveName
Property ArchiveFolder
Property maxArchiveSize
Property eachArchiveSize
Property rotateArchive
Property silentMode
Extractor [N4A9CB700D9211D
Template Log [No file sen....ent 0 of 0 known events)
Outputter Result (View shows result for event 0)
Outputter Result
Log Content

Table 2: Configuration parameters common to both the BladeCenter MM adapter configuration file and the BladeCenter Cisco IGESM adapter configuration file

Parameter Name	Description	Example
ArchiveName	Name of the archive file. Do not provide an extension - *.log* will automatically be added as the extension. Do not specify the path either. If archive rotation is enabled, suffixes will be added to this name automatically. This is a string value.	mm_archive
ArchiveFolder	Complete path to folder where the archive files will be saved. If archive rotation is enabled, all archived files will be saved in this folder. This is a string value.	D:\BCArchives\
maxArchiveSize	This is the maximum size of all archives. If archive rotation is enabled, once the maximum size is reached, the oldest archived file will be removed and replaced with a new one. If archive rotation is not enabled, archiving will not continue once this size is reached. You can set this to 0 to represent a maximum archive size limited only by the amount of disk space available. If you set it to 0, archive rotation will be automatically disabled. This value is in bytes.	10240000
eachArchiveSize	This is the maximum size of each archive. It must be less than the maxArchiveSize if the latter is greater than 0. If archive rotation is enabled, once this size is reached for the current archive file, a new archive file with a different suffix will be created until the maximum size for all archives is reached. This value has no effect if the maximum archive size is set to 0 or if archive rotation is disabled. This value is in bytes. The default setting is 1048576 to represent 1 MB. You should not set this value to 0. Such a setting will automatically default.	2097152
rotateArchive	This Boolean value determines if archive rotation will take place. This may be overridden by a setting of 0 for maxArchiveSize which will disable archive rotation.	false
silentMode	This Boolean value determines if the sensor will show messages on the console or only write them to the adapter's default log file.	true

Note that the above configuration settings apply only in the case of real-time processing of Management Module logs or Cisco IGESM events. For post-processing mode of operation in either case, the sensor has only two configuration parameters – *directory* to specify the directory to read the archived or previously saved MM log / Cisco ESM *syslog* file from and *filename* to specify the name of the archived or previously saved MM log file / Cisco IGESM *syslog* file.

Table 3: Other configuration parameters in the BladeCenter MM adapter configuration file

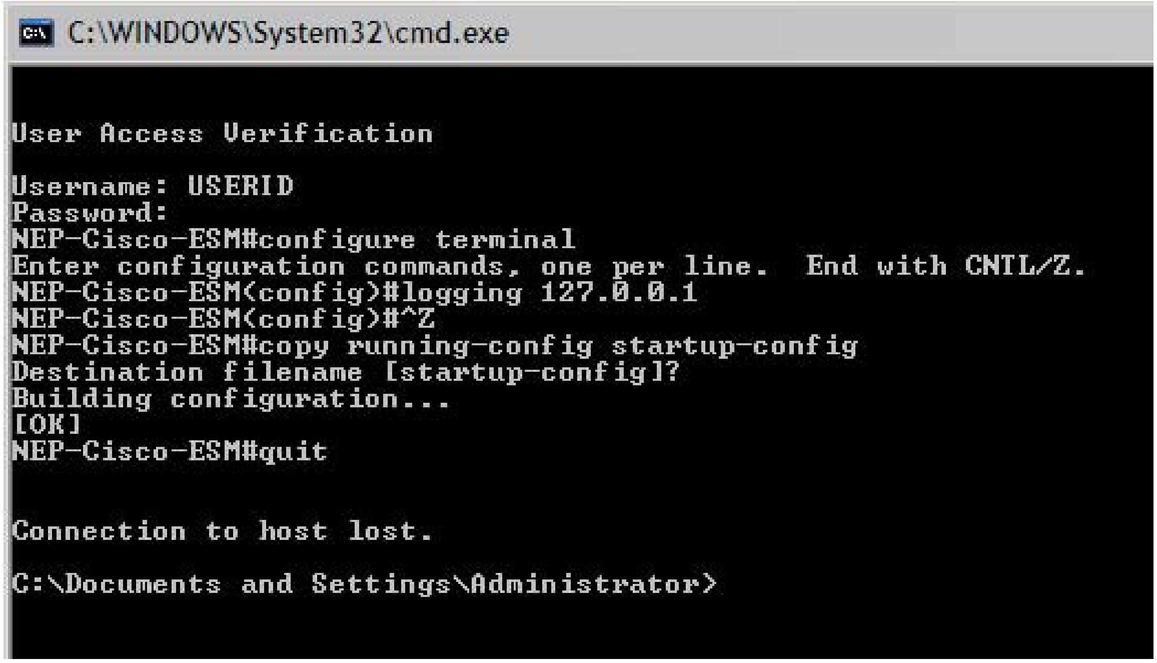
Parameter Name	Description	Example
Host	The IP address / host name of the Management Module from which log messages need to be retrieved. This is of the form x.x.x.x	9.42.90.2
RefreshInterval	Determines how often records will be fetched from the MM log. Since the MM log is of finite size it is possible that records will be lost if this interval is set too high. The lower the value the better – however lower values will cause the adapter to consume a lot of CPU cycles. The refresh interval is specified in milliseconds and can have a maximum value of 9223372036854775807 1 The adapter's context configuration (please see the GLA documentation) has a pause interval setting x milliseconds that determines how often records are read in from the sensor .i.e. how often records are processed. However this setting determines how often the sensor reads from the original source – the sensor will buffer read entries until the adapter asks for them every x milliseconds. Typically this setting will be lower than x.	3000
ResetLog	Set this to true if you want the MM log to be cleared each time it is read. Note that the adapter has capabilities to archive the retrieved log records and we recommend that you reset the log by setting this value to true so that no records are lost because the MM log is full. This is a Boolean value and has *true* or *false* as allowed values	true
Username	This is the username to log on to the Management Module. It is optional. If it is not provided, the adapter will prompt the user for the username when it is started. It is optional because providing username/password in a configuration file may violate security policies. This is a string value.	Admin
Password	This is the password to log on to the Management Module. It is optional. If it is not provided here, the adapter will prompt the user for the password when it is started. It is optional because providing username/password in a configuration file may violate security policies. This is a string value.	Passw0rd

Table 4: Other configuration parameters in the BladeCenter Cisco IGESM adapter configuration file

Parameter Name	Description	Example
Port	This is the port on which the adapter will listen for UDP packets sent by the Cisco Switch. Typically this must be set to 514 which is also the default. The value here must be an integer value.	514
Delimiter	This is the delimiter that the adapter will introduce between fields in the log record before processing them or archiving them for later processing. This must be set to | (pipe) if you plan to use the default rules for the Cisco IGESM log processing that are provided in this package.	|

Changes to BladeCenter Cisco IGESM configuration:
Next, it is necessary to make some minor changes to the Cisco ESM to direct events to be sent to the Generic Log Adapter. Log on to the Cisco IGESM as you normally would (you may have to do an *enable* command with the corresponding password) to get the configuration prompt. In the below visualization, replace 127.0.0.1 with the actual IP address of the machine running the Generic Log Adapter.

Figure 2: Cisco IGESM logging configuration



```
User Access Verification

Username: USERID
Password:
NEP-Cisco-ESM#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
NEP-Cisco-ESM(config)#logging 127.0.0.1
NEP-Cisco-ESM(config)#^Z
NEP-Cisco-ESM#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
NEP-Cisco-ESM#quit


Connection to host lost.

C:\Documents and Settings\Administrator>
```

Data Collection
Next, the adapters must be started depending on the kind of analysis required. As stated earlier, analysis can be either real-time or post-mortem. Refer Table 1 for the appropriate configuration files and edit them if necessary (change file names for post-mortem processing etc.).

To start both adapters for real-time processing, run the *bc_realtime.bat* file from the command prompt. This will start the adapter for Cisco IGESM first and then the one for the Management Module in two separate command windows. If you had not provided the username and password for the Management Module in the configuration file, you will be prompted to enter the same. If silent mode has been enabled in the configuration file, you will not see any messages on the screen. Otherwise you'll see status messages. You may look in the *hgla.log* file in the adapter folders for more runtime logging information.

For post-processing mode, run the *bc_postproc.bat* file from the command prompt. Make sure that you have already edited the appropriate configuration files (*CiscoESM_postproc.adapter* and *BladeCenterMM_postproc.adapter*) to point to the correct archived files and folder of those files to be used for this post processing analysis session.

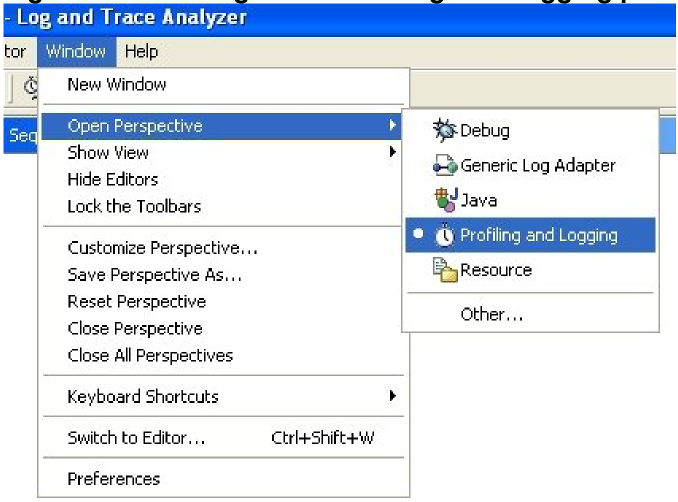
You may edit the batch files that start with *esm* or *mm* to point to different configuration (.adapter) files. Open the appropriate batch files (real-time or post-processing or both) and edit lines 3 and 4 to change the location of the configuration files as necessary.

Connecting to the adapters from the Log and Trace Analyzer

It is necessary to connect from the Log and Trace Analyzer as early as possible to the running adapters to avoid any data loss. We recommend that you keep the Log and Trace Analyzer open before starting any data collection adapters.

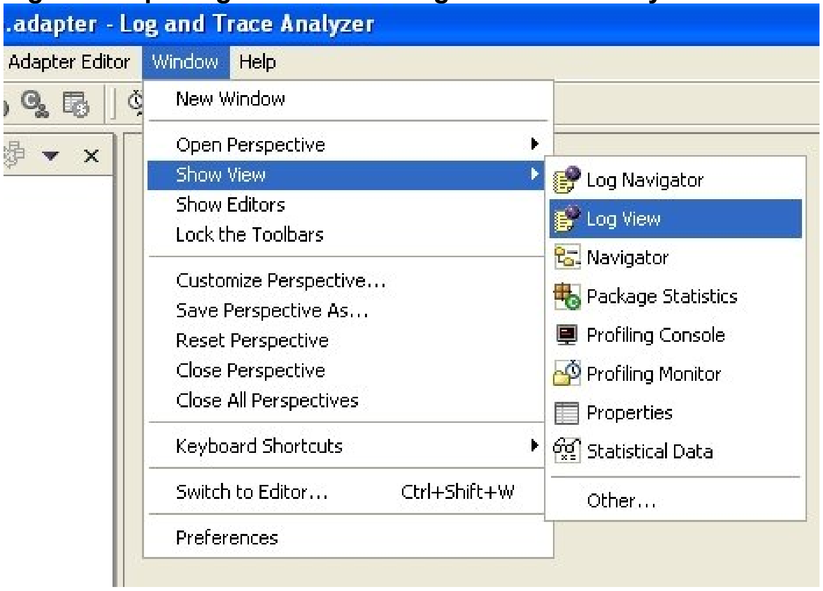
If you haven't already done so, switch to the *Profiling and Logging* perspective in the Log and Trace Analyzer by doing a *Window > Open Perspective > Profiling and Logging*. If this option is not available click on *Other* and choose *Profiling and Logging* from the following dialog box.

Figure 3: Switching to the Profiling and Logging perspective in the Log and Trace Analyzer



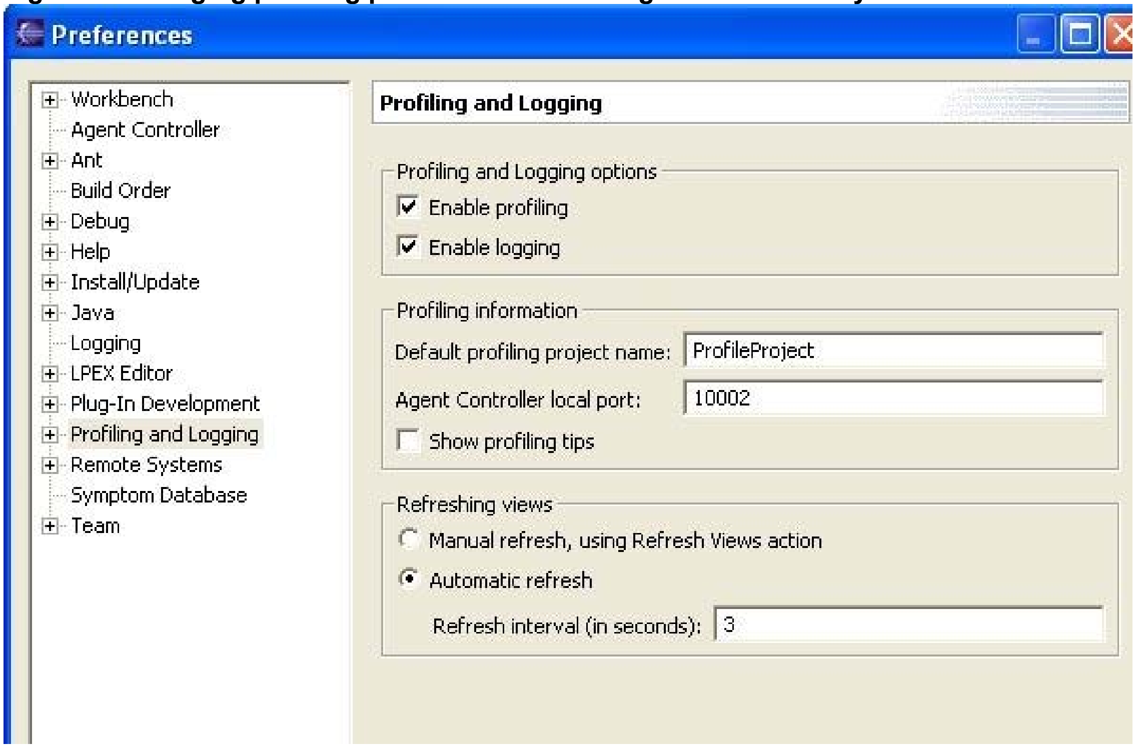
By default the Profiling and Logging perspective will open up with the Profiling Monitor view on the left. If not you should be able to click on the Profiling Monitor tab on the left portion (it may be overlaid by the Navigator view). We also need to enable a couple of other views that will be useful for data correlation and analysis. Click on *Window > Show View > Log View.* Do the same for the *Log Navigator view.*

Figure 4: Opening Views in the Log and Trace Analyzer



It is necessary to change the settings to enable the Log and Trace Analyzer to consume messages from the adapter. Click on *Window > Preferences* and choose *Profiling and Logging* tree node in the following dialog box. Make sure that the *Enable Logging* check box on the right is checked as shown in Figure 4 (by default it is unchecked). Also at the bottom of the dialog under *Refreshing Views* choose *Automatic Refresh* and set a refresh interval at which you'd like the *Log View* to refresh with new Common Base Event representation of native log events sent by the adapters.

Figure 5: Changing profiling preferences in the Log and Trace Analyzer



Profiling and Logging

Profiling and Logging options

☑ Enable profiling

☑ Enable logging

Profiling information

Default profiling project name: ProfileProject

Agent Controller local port: 10002

□ Show profiling tips

Refreshing views

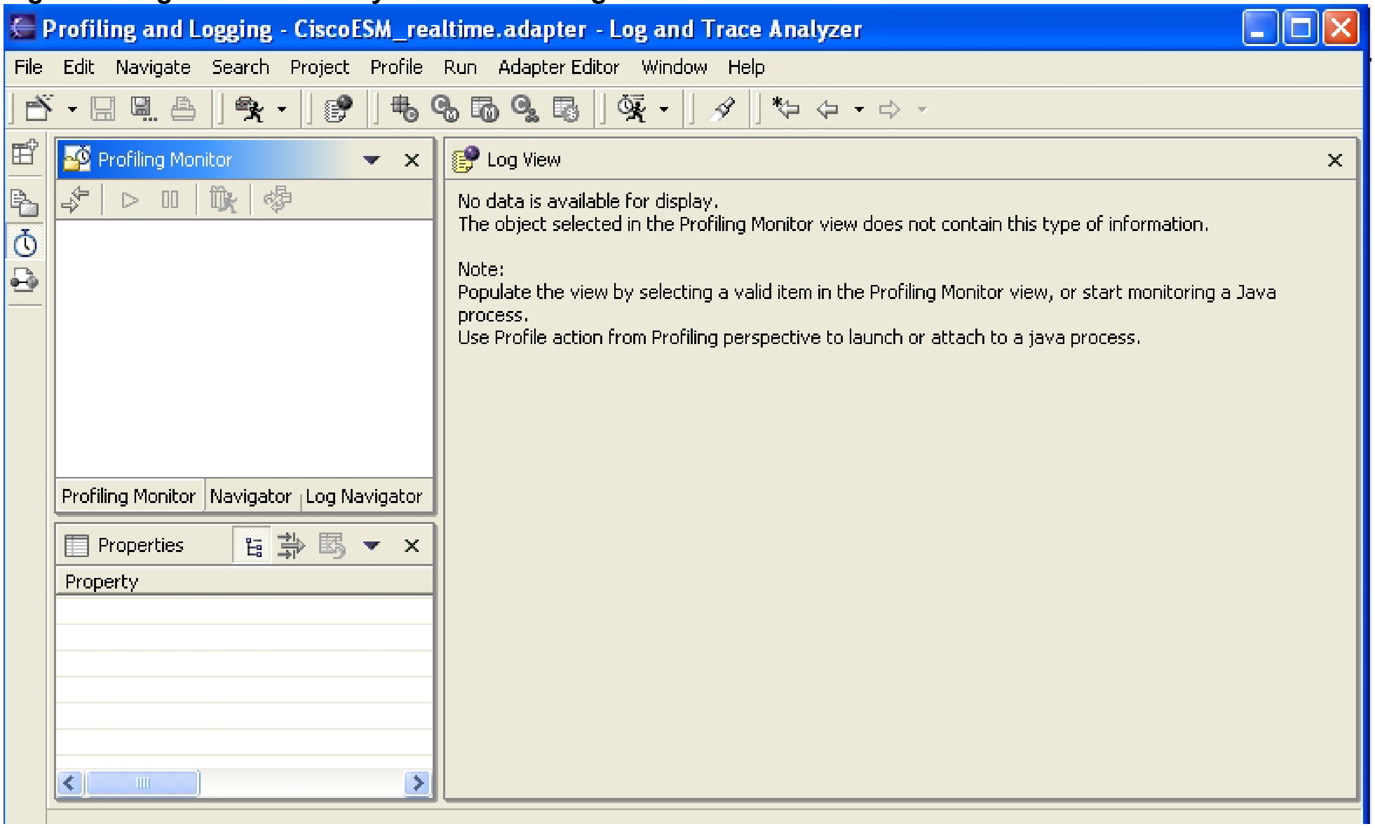
○ Manual refresh, using Refresh Views action

● Automatic refresh

Refresh interval (in seconds): 3

The Log and Trace Analyzer will now resemble Figure 6. Note that the views may be different portions of the screen.

Figure 6: Log and Trace Analyzer after enabling views


Profiling and Logging - CiscoESM_realtime.adapter - Log and Trace Analyzer
File Edit Navigate Search Project Profile Run Adapter Editor Window Help
Profiling Monitor
Log View
Profiling Monitor
Navigator
Log Navigator
Properties
Property

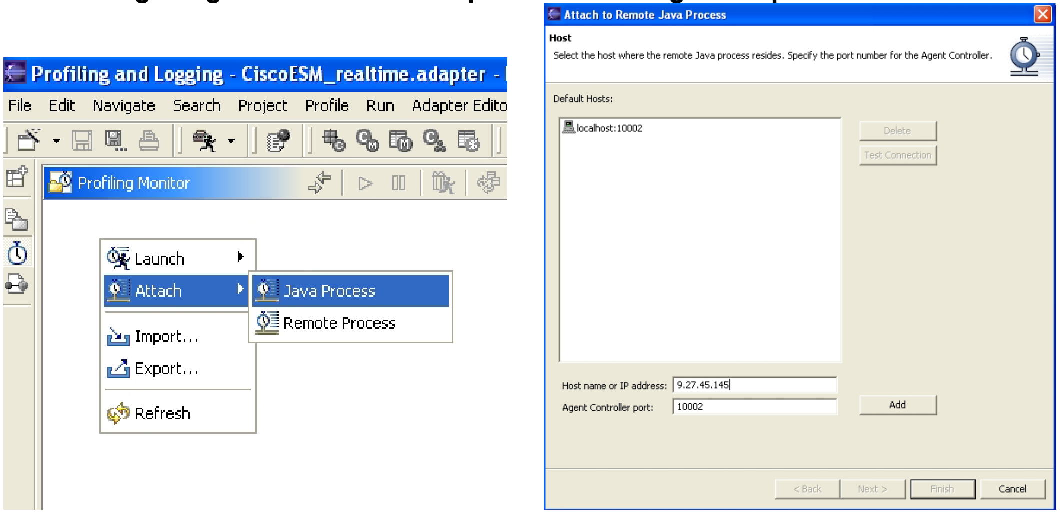
No data is available for display.
The object selected in the Profiling Monitor view does not contain this type of information.

Note:
Populate the view by selecting a valid item in the Profiling Monitor view, or start monitoring a Java process.
Use Profile action from Profiling perspective to launch or attach to a java process.

The log view will be populated with data after we connect to the adapters. The profiling monitor shows all active connections to *agents* that are created by the adapters. Note that the Log and Trace Analyzer can be another machine as long as the machine with the Generic Log Adapters are network accessible to the Log and Trace Analyzer. To connect to the adapters, follow the below steps,

1. Within the *Profiling Monitor* view on the left, right click and choose *Attach* > *Java Process* (If Generic Log Adapter is running on a remote machine choose *Remote Process;* on the following dialog enter IP address of remote machine and click *Add.* You can also do a *Test Connection* after highlighting the added IP in the list. Finally choose the added IP and click *Next* at the bottom)

Figure 7: Attaching to agent & additional step when attaching to adapter on remote machine


Profiling and Logging - CiscoESM_realtime.adapter -
File Edit Navigate Search Project Profile Run Adapter Edito
Profiling Monitor
Launch
Attach
Java Process
Remote Process
Import...
Export...
Refresh
Attach to Remote Java Process
Delete
Test Connection
Add
< Back
Next >
Finish
Cancel

Host

Select the host where the remote Java process resides. Specify the port number for the Agent Controller.

Default Hosts:

localhost:10002

Host name or IP address: 9.27.45.145

Agent Controller port: 10002

You can also initiate this step from the menu by clicking on *Profile > Attach > Java Process / Remote process*

2. On the resulting dialog, expand each of the trees on the left until you find a node that says *BladeCenterMM_Agent.* Choose and add it to the list on the right. Repeat the process for the *CiscoESM_Agent* node. The order in which the agents are added to the list on the right is not important.

3. We will use the defaults for profiling project name and monitor name. Click *Finish* at the bottom of the dialog. If for some reason, you wish to change the profiling project name and/or the monitor name click *Next* and continue the wizard.

4. Once the agents have been added to the *Profiling Monitor* view, right click on them and choose *Start Monitoring*

5. If the *Log View* is not already visible, click on the corresponding tab to bring it up. New records sent by the adapter will populate the log view. Double clicking on the individual agent names in the tree within the *Profiling Monitor* view will change the log view to display either the output of the adapter that is parsing the Management Module log or the adapter that is converting events from the Cisco IGESM.

Correlating log records and events

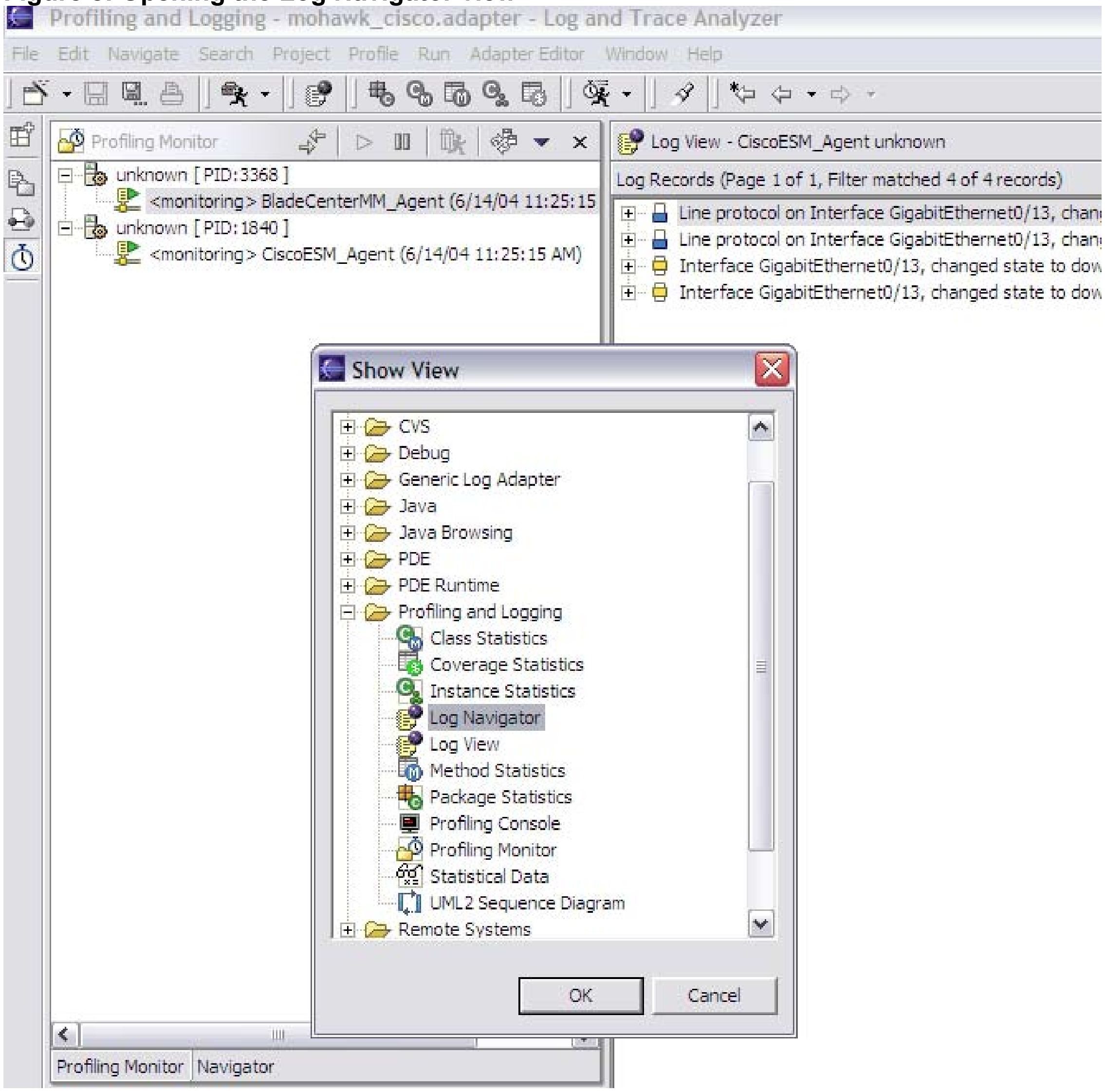
The Log and Trace analyzer can be used to correlate events and records from different sources and create a visual representation of the sequence of events in an UML sequence diagram. While the log views refresh automatically, the correlations have to be performed each time you wish to have a snapshot of all BladeCenter components – correlations are driven by actions on the Log and Trace analyzer and once a correlation has been performed, it will not refresh automatically. Since we have already enabled the Log and Trace analyzer to take input from different adapters we can leverage on that to visually look at correlated events from both the management module and the Cisco ESM through the following steps,

1. Once the views corresponding to either agent (Cisco ESM or BladeCenter MM) have been populated with records, they can be correlated based on time which is the default correlation the Log and Trace analyzer provides. See the following note on time adjustments which describes how time synchronization is achieved between the different sources.

2. To create the new correlation, switch to the Log Navigator view. If the view is not available in your current perspective, you can add it by doing a *Window > Show View > Log Navigator* or if the Log

Navigator view is not available, choose *Window > Show View > Other > Profiling and Logging > Log Navigator*

Figure 8: Opening the Log Navigator view



Log Records (Page 1 of 1, Filter matched 4 of 4 records)

Line protocol on Interface GigabitEthernet0/13, chan

Line protocol on Interface GigabitEthernet0/13, chan

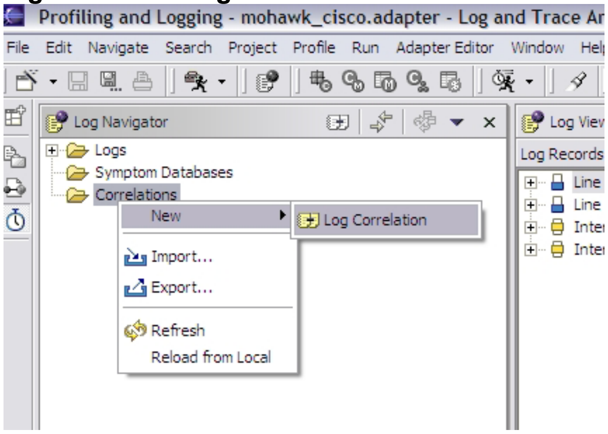
Interface GigabitEthernet0/13, changed state to dow

Interface GigabitEthernet0/13, changed state to dow

Once the Log Navigator view is open, switch to it. It would be helpful to arrange the views in the perspective so that the Log Navigator view and Log View are visible at the same time – typically the Log Navigator view with overlap with the Profiling Monitor view.

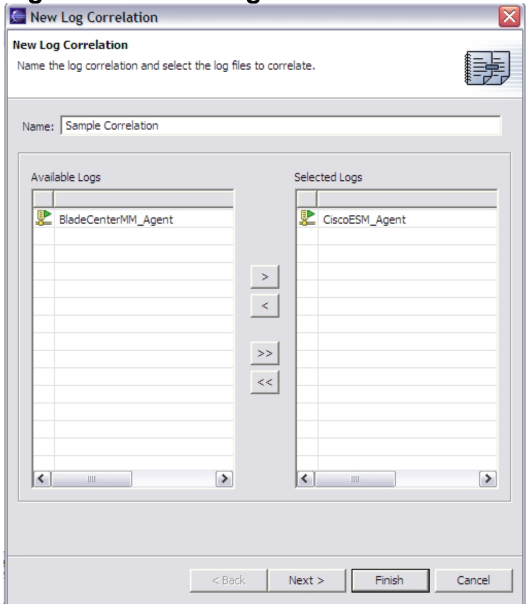
3. In the Log Navigator view, right click on *Correlations* and then select *New > Log Correlation.*

Figure 9: Creating a new correlation



4. In the consecutive dialog, you can provide a name for the correlation if desired. Then you need to choose the data sources that will be used for this correlation. You will find both the agents listed in the table on the right. To add them to the table on the right, you can choose the >> button which will add all the entries in the left table to the table on the right or you can choose each agent individually (if there are more data sources than which you'd want to correlate) and use the > button to add them to the table on the right.

Figure 10: Choosing the data sources to correlate


New Log Correlation

New Log Correlation

Name the log correlation and select the log files to correlate.

Name: Sample Correlation

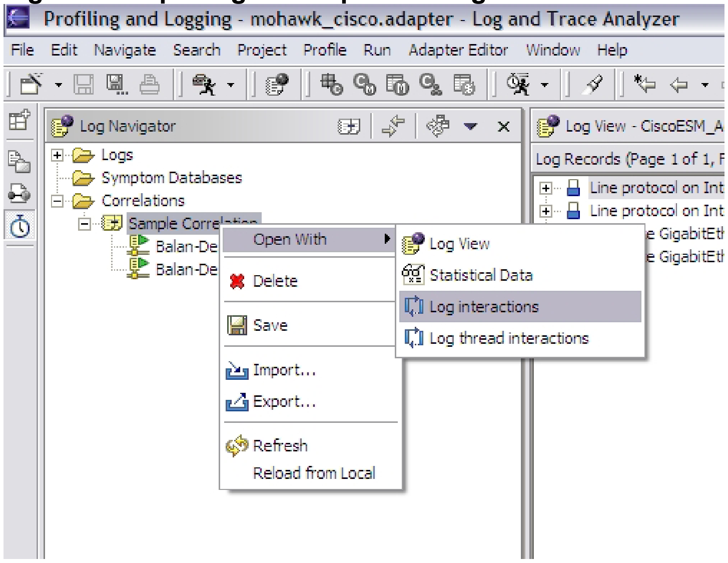
Available Logs: BladeCenterMM_Agent

Selected Logs: CiscoESM_Agent

5. Since we are going to use default time based correlation, you can click finish. If you create your own correlation engines and plug them into the Log and Trace analyzer (details of doing so are included in the Log and Trace Analyzer documentation in the Autonomic Computing toolkit), then you should click *Next* to choose the correlation you want to use.

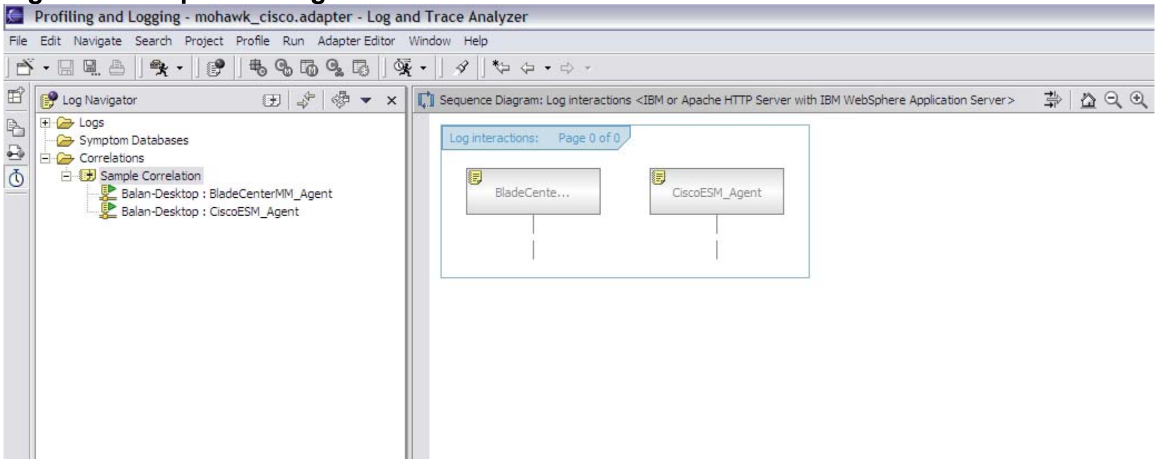
6. A new correlation will be created under the *Correlations* tree node in the Log Navigator view. The data sources (agents) used in the correlation with be listed under it. To view the correlated records in a sequence diagram, right click on the correlation and choose *Open With > Log Interactions.*

Figure 11: Opening the sequence diagram



7. This will open the correlated records in the Sequence Diagram view. A separate timeline will be created for each agent. However it is possible that no records are visible at this time in the time lines.

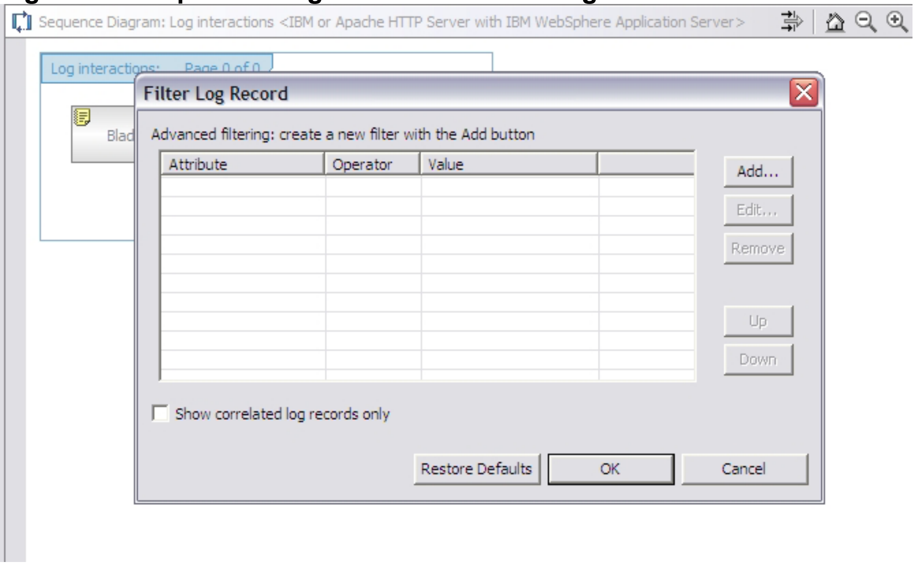
Figure 12: Sequence diagram with individual time lines


Profiling and Logging - mohawk_cisco.adapter - Log and Trace Analyzer
File Edit Navigate Search Project Profile Run Adapter Editor Window Help
Log Navigator
Logs
Symptom Databases
Correlations
Sample Correlation
Balan-Desktop : BladeCenterMM_Agent
Balan-Desktop : CiscoESM_Agent
Sequence Diagram: Log interactions <IBM or Apache HTTP Server with IBM WebSphere Application Server>
Log interactions: Page 0 of 0
BladeCente...
CiscoESM_Agent

8. Click on the *Filter* icon in the Sequence Diagram view. The *Filter* icon is the icon with the arrows immediately next to the title bar of the Sequence Diagram view. It is the icon to the left of the home and zoom in/out icons.

   In the resulting dialog box, make sure the *Show correlated log records only* check box is **unchecked.** Click OK.

Figure 13: Sequence diagram view filter settings



Sequence Diagram: Log interactions <IBM or Apache HTTP Server with IBM WebSphere Application Server>

Log interactions: Page 0 of 0

Filter Log Record

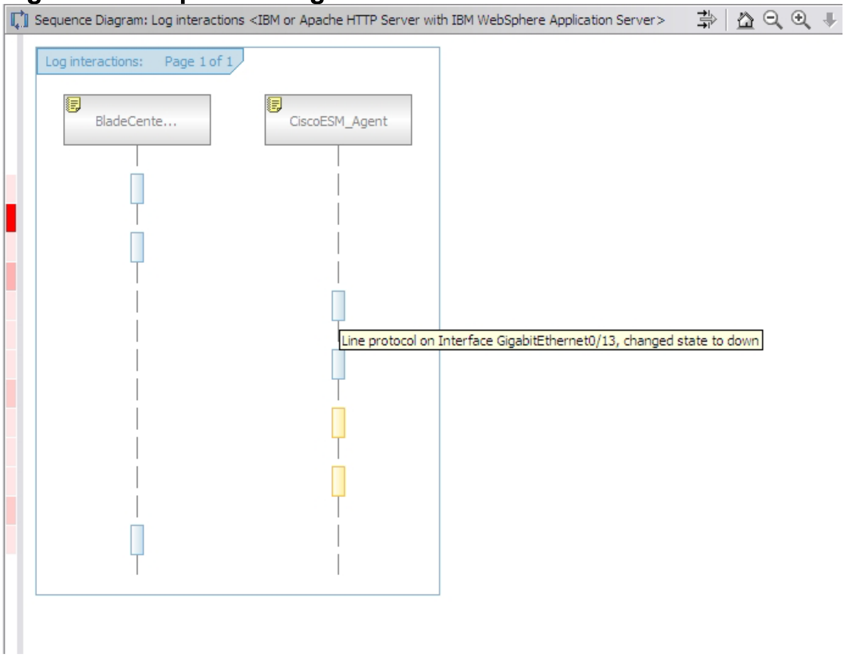
Advanced filtering: create a new filter with the Add button

Attribute	Operator	Value	

□ Show correlated log records only

9. Now all the records will be visible in the time lines. You can move the mouse over individual blocks representing the log records to see the records as tool tips.

Figure 14: Sequence diagram view with correlated records



Sequence Diagram: Log interactions <IBM or Apache HTTP Server with IBM WebSphere Application Server>

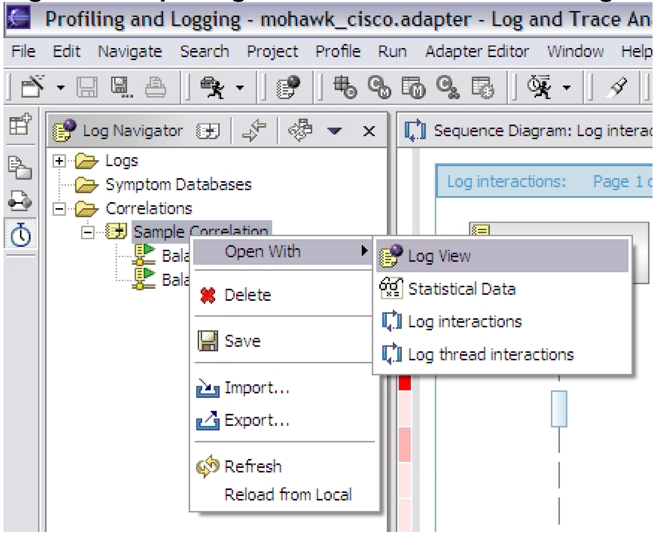
Log interactions: Page 1 of 1

Line protocol on Interface GigabitEthernet0/13, changed state to down

10. The correlated diagram shows the relative times at which events happened in the different BladeCenter components. You can setup additional adapters for monitoring other BladeCenter components (like the Operating Systems and software components running on the blades) using the rule sets packaged with the Generic Log Adapter in the Autonomic Computing toolkit. These will show up as separate time lines with the proper arrangement of records in a relative time basis allowing you to obtain a complete snapshot of the BladeCenter operation at any point in time.

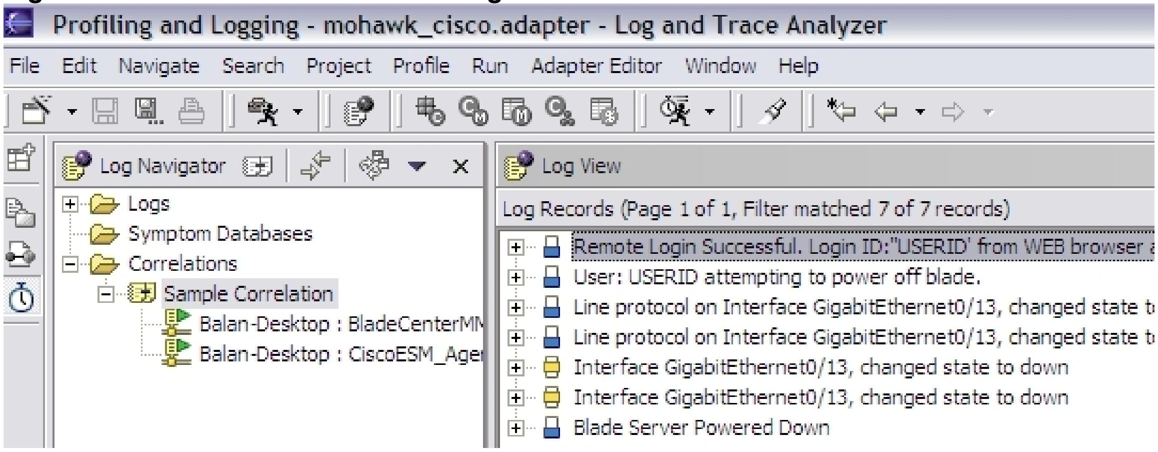
11. You can also right click on the log correlation created under the *Correlations* tree node in the Log Navigator view as in step 7 and open the correlated records in the log view.

Figure 15: Opening correlated records in the log view



12. This will bring up the correlated records in the log view – this represents a consolidation of all records in a single view sorted by time and shows the interleaving of messages from different BladeCenter components. In the below screenshot, messages from the BladeCenter MM and ESM are interleaved.

Figure 16: Correlated records in the log view


Profiling and Logging - mohawk_cisco.adapter - Log and Trace Analyzer
File Edit Navigate Search Project Profile Run Adapter Editor Window Help
Log Navigator
Logs
Symptom Databases
Correlations
Sample Correlation
Balan-Desktop : BladeCenterMM
Balan-Desktop : CiscoESM_Ager
Log View

Log Records (Page 1 of 1, Filter matched 7 of 7 records)

```
Remote Login Successful. Login ID:'USERID' from WEB browser a
User: USERID attempting to power off blade.
Line protocol on Interface GigabitEthernet0/13, changed state t
Line protocol on Interface GigabitEthernet0/13, changed state t
Interface GigabitEthernet0/13, changed state to down
Interface GigabitEthernet0/13, changed state to down
Blade Server Powered Down
```

Time synchronization between data sources

Since different BladeCenter components are being monitored and it is possible that these sources have different time stamps it is important that the time stamps are standardized before time based correlations can be performed. Since the Generic Log Adapter is used to monitor all the different BladeCenter components, the Generic Log Adapter performs the required time synchronization.

The Generic Log Adapter adjusts the time stamps from the different sources to match the time on the machine where it is running by calculating the differences in time on the BladeCenter components and the local machine. This is performed only in the case of real-time processing; since the messages are processed almost immediately after they are generated the time standardization does not hurt accuracy or ordering of events from different sources.

It is recommended that you set the context refresh interval (found under the *Context* section/tag in the configuration file when opened in the rule builder) for the Cisco ESM adapter and the BladeCenter MM adapter to similar values. This will further guarantee the accuracy of the time ordering between the various sources and consistent refreshes in the individual log views.

Known Issues

1. Adapter for BladeCenter Management Module cannot log on to the Management Module to collect data (startup unsuccessful message)
   Description: This may happen if too many connections to the Management Module are attempted. Typically this happens if you start and stop the adapter multiple times and hence will surface even under normal operation after some time.
   Workaround: Stop the adapter. Log on to the Management Module through a web browser and restart the Management Module. Start the adapter again.
2. Management module restarts will disable data collection activity of currently executing adapter instance
   Description: If the management module is restarted (or BladeCenter is shutdown and restarted), a currently running instance of the BladeCenter management module adapter will no longer be able to retrieve new log messages. However it will not throw any exceptions either or terminate.
   Workaround: Restart the adapter whenever the management module / BladeCenter is restarted