IBM Tivoli Access Manager for e-business 6.0

Logging

Tivoli. software

Objectives

- Upon completion of this module, you should be able to:
  - Find the locations for log files
  - Enable logging
  - Describe the LogViewer
  - Describe Tivoli Common Logging

Logging

- To enable logging, you define which types of events to capture.

- When events are captured, they can be written to
  - log files,
  - to the standard output (STDOUT) device,
  - to the standard error (STDERR) device,
  - or to a combination of these destinations.

- Can also redirect to a remote server or to an application for processing using log agents.

Before you enable logging you should decided which types of events you would like to capture. Captured events are written to: log files which can be in XML format or plain text. They can be written to standard out or standard error or any combination depending on the type of event. They can also redirect to a remote server or to an application for processing using log agents.

IBM

Tivoli XML LogViewer

- The Tivoli XML log format and is used by a number of Tivoli applications.

- Displays trace information in a common XML format.

- Java-based log viewer:
  - Allows message and trace information to be filtered by time, severity, thread ID, and component.
  - Allows conversion into ASCII or HTML

- Not installed as part of any Tivoli Access Manager installation.

- The XMLFILE, XMLSTDERR, and XMLSTDOUT format in the routing file are used to produce XML message logs and XML trace logs.

The Tivoli XML LogViewer comes with Tivoli Access Manager. It is not installed by default. The Tivoli XML log format is used by a number of Tivoli applications. It displays trace information in common XML format. The XML LogViewer is a Java-based application that allows you to filter by time, severity, thread ID, and component. It allows the log to be converted into ACSII or HTML. The XMLFILE, XMLSTDERR, and XMLSTDOUT format in the routing file are used to produce XML message logs and XML trace logs.

Routing files

- Customize logging of message and trace events to control:
  - Whether to enable logging for specific event classes
  - Where to direct the output for each event class
  - How many log files to use for each event class
  - How large each log file can be for each event class

Once you have decided to enable logging, whether to enable logging for specific events, where to direct the output, how many log files to use for each event and how large each log file can be for each event.

loggingtrace.ppt

Location of routing files

- %PD_HOME%\etc or /opt/PolicyDirector/etc
- Routing file for each component: routing (runtime), pdmgrd_routing, pdacld_routing, pdmgrproxyd_routing
- For WebSEAL
  - %PD_WEB%\etc\routing
  - /opt/pdweb/etc/routing
- PD_SVC_ROUTING_FILE environment variable for alternative routing file

The location for the log file is in the %PD_HOME% directory for Windows and /opt/PolicyDirector/etc for Linux and UNIX. There is a different routing file for each component: routing is for the runtime, the pdmgrd_routing is for the policy server, the pdacld_routing is for the authorization server, and for the pdmgrpoxyd_routing is for the policy proxy server. You can change the location of the routing file by changing by PD_SVC_ROUTING_FILE.

Routing file entries

- File contains entries that control the logging of message events and trace events

- Format differs by type
  - Message events
    - severity:destination:location [[;destination:location]...] [;GOESTO:{other_severity | other_component}]
  - Trace events
    - component:subcomponent.level[[,subcomponent.level]...] :destination:location [[;destination:location]...] [;GOESTO:{other_severity | other_component}]
  - Where
    - Severity will be one of FATAL, ERROR, WARNING, NOTICE, NOTICE_VERBOSE or * (all).
    - Destination will be DISCARD, FILE/TEXTFILE, STDERR, STDOUT, UTF8FILE, XMLFILE, XMLSTDERR, XMLSTDOUT
    - Location specifies the name and location of the log file.

- Files also contain instructions and examples

Routing file entries vary depending on the type (message or trace events), both will need to have severity of FATAL, ERROR, WARNING, NOTICE, NOTICE_VERBOSE or * (all). All is designated by the asterisks (*). The designation for each will also need to specified. It can be DISCARD, FILE/TEXTFILE, STDERR, STDOUT, UTF8FILE, XMLFILE, XMLSTDERR, XMLSTDOUT. XMLFILE, XMLSTDERR, XMLSTDOUT are for use with the LogViewer. You will also need to specific the location and name of each log file. Each routing file contains instructions and examples.

Tivoli common directory

- Tivoli Access Manager has the ability to use Tivoli Common Directory logging; a single location for all Tivoli Product log files

- Not enabled by default

- Products that support Tivoli Common Directory store:
  - Logs files
  - First-failure data capture (FFDC) files
  - Serviceability scripts

The Tivoli common directory is a single directory for all Tivoli products to store their log files. It is not enabled by default. The products that support Tivoli Common Logging store log files, FFDC files and serviceability scripts. To enable Tivoli Common Logging you are presented with the option as a checkbox during installation of each component.

IBM

Location of the Tivoli common directory

- If any product on the system uses Tivoli Common Directory, the parent directory is defined in the log.properties file:
  - Linux and UNIX operating systems /etc/ibm/tivoli/common/cfg/log.properties
  - Windows operating systems c:\program files\ibm\tivoli\common\cfg\log.properties
- On a Linux or UNIX operating system, this file should have the 664 permission and should be owned by group tivoli.

The location of each Tivoli Common Directory varies by platform. Remember to on Linux and UNIX to set permissions 664 and make the group owned by Tivoli.

Common directories used by TAM

- Tivoli Access Manager uses /logs subdirectory to store message and trace logs.

- Tivoli Access Manager does not use the /ffdc or /scripts subdirectories.

- The logs files can be found at: common_directory/xxx/logs/

- Where…

  - Common_directory is
    - Linux and UNIX operating systems /var/ibm/tivoli/common
    - Windows operating systems c:\program files\ibm\tivoli\common\
      - HPD – Tivoli Access Manager
      - DPW – Tivoli Access Manager WebSEAL
      - AMZ – Tivoli Access Manager Plug-in for Web Servers
      - AWL – Tivoli Access Manager for WebLogic Server
      - AWD – Tivoli Access Manager Plug-in for Edge Server
      - AOS – Tivoli Access Manager for Operating Systems
      - DRQ – Tivoli Access Manager for Business Integration

The common directory used by Tivoli Access Manager is /logs. It stores both message and trace logs. Tivoli Access Manager does not use /ffdc or /scripts. Those are used by Tivoli Common Logging.The log files are located in the common directory under the three letter code for the product. WebSEAL, for example, is DPW. The exact directory varies by platform.

IBM

Training roadmap for *IBM Tivoli Access Manager for e-business 6.0*

- **http://www.ibm.com/software/tivoli/education/edu_prd.html**

IBM Tivoli Training   Logging   © 2007 IBM Corporation

For more information about logging please see the Tivoli Access Manager Problem Determination Guide. For more information see the IBM Tivoli Access Manager for e-business 6.0 training roadmap.

Summary

- Key terms to remember:
  - Logviewer
  - Tracing
  - Routing files

The logview is an XML Log Viewer that allows you to filter by time, component, thread ID and severity. Tracing and messaging are both configured in the routing files. The routine files are in designations based on platform and component.

loggingtrace.ppt

Copyright and trademark information

IBM trademarks

http://www.ibm.com/legal/copytrade.shtml#ibm

Fair use guidelines for use and reference of IBM trademarks

http://www.ibm.com/legal/copytrade.shtml#fairuse

General rules for proper reference to IBM product names

http://www.ibm.com/legal/copytrade.shtml#general

Special attributions

http://www.ibm.com/legal/copytrade.shtml#section-special