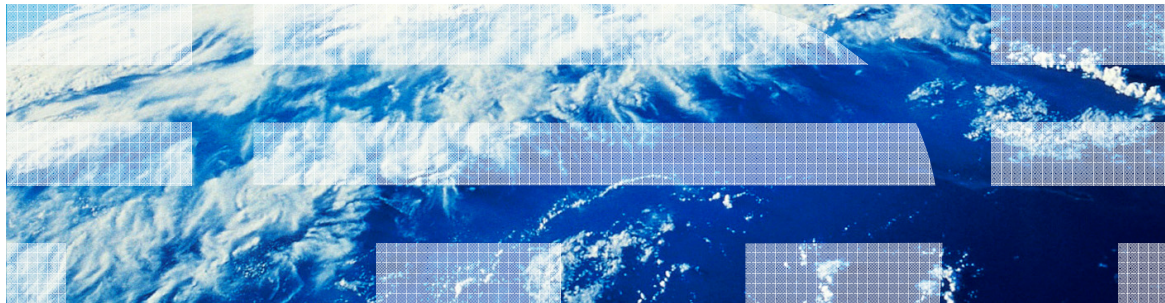


System Administration and Maintenance



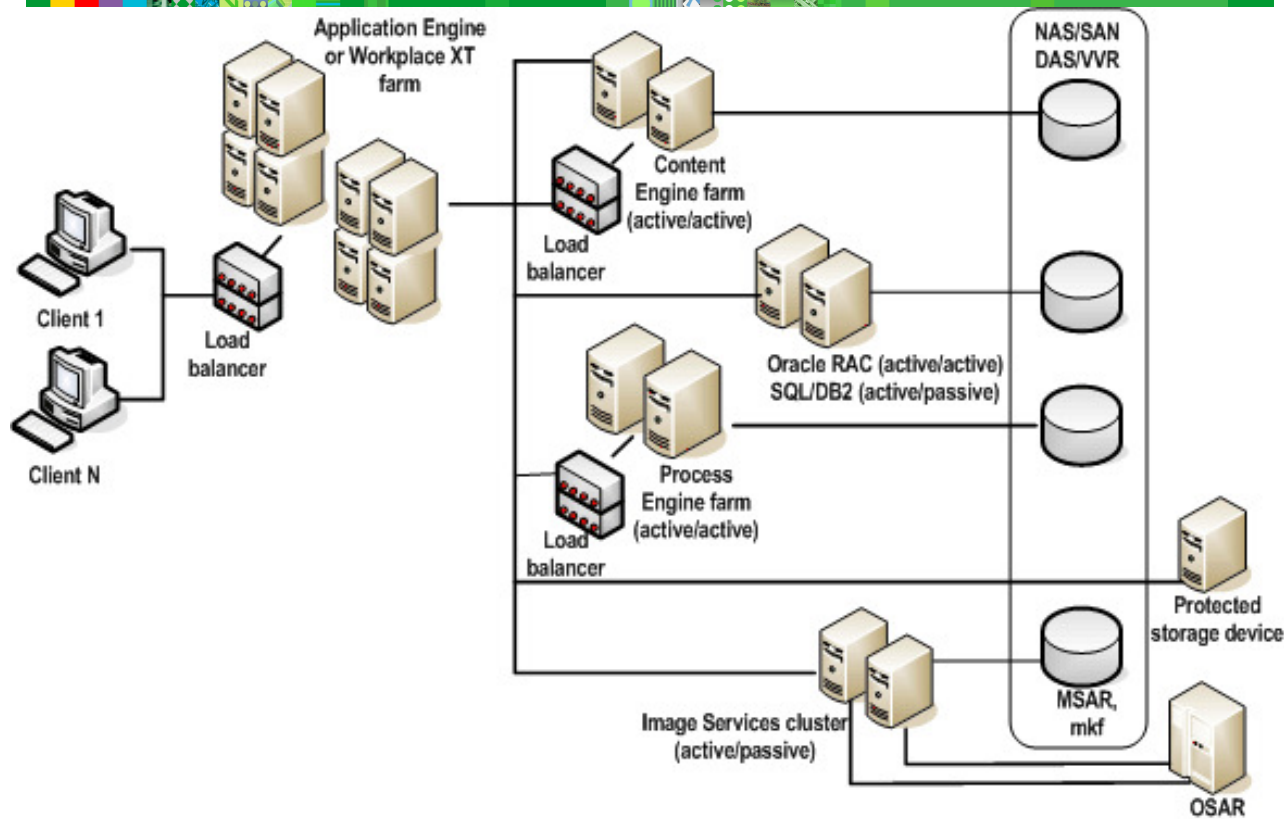
Importance of a routine administration plan



- Ensure system availability to users
- Ensure optimal system performance
 - Especially important if hardware is heavily loaded
- Protect security of resources
- Prevent neglect of key tasks by trained administrators
- Principle: Know what you monitor

Overview of system administration

Know your FileNet P8 system environment



Maintenance and monitoring




- Verify and update site documentation
 - An essential part of a maintenance plan
- Create additional documentation
 - Create a monitoring and maintenance plan.
 - Keep change logs, including patches and configuration changes.
 - Keep problem and resolution logs.
- Monitor and maintain the system
 - Monitor system integrity, security, and performance to prevent system failures.
- Monitor and maintain system logs
 - Monitor the activity of log files to identify system problems.
 - Manage the growth of log files to avoid disk space consumption.
 - Customer support might ask for logs.

What needs to be monitored and maintained



- Underlying infrastructure
- Database
- Disk space
- Log files
- LDAP directory
- Content search system
- System performance
- Backups
- Security
- Custom applications
- Software patches and updates

Tools to help monitor and maintain

- 
- IBM FileNet Enterprise Manager
 - Administrative Console for Content Engine
 - IBM System Dashboard
 - Content Search Engine tools
 - Information Center documentation
 - Operating system tools
 - Database tools
 - Backup tools
 - IBM FileNet Process Engine tools
 - Java EE application server tools

Example administration schedule

- Daily
 - Monitor system, processes, logs
 - Backup databases, file stores, LDAP service
- Weekly
 - Check free space: all file systems and databases
 - Check performance: Content Manager, Process Engine
- Monthly
 - Check IBM Support site for new fix packs.
 - Back up operating systems, application server, installed software.
 - Maintain logs: operating system, Java EE application server, Content Engine, Process Engine, Content Search Engine, database
- Periodically
 - Maintain databases. Monitor table growth and performance bottlenecks.
- Semiannually
 - Apply patches: operating system, Java EE application server, database, LDAP directory, IBM FileNet products
- Annually
 - Perform disaster recovery restore tests at least annually.

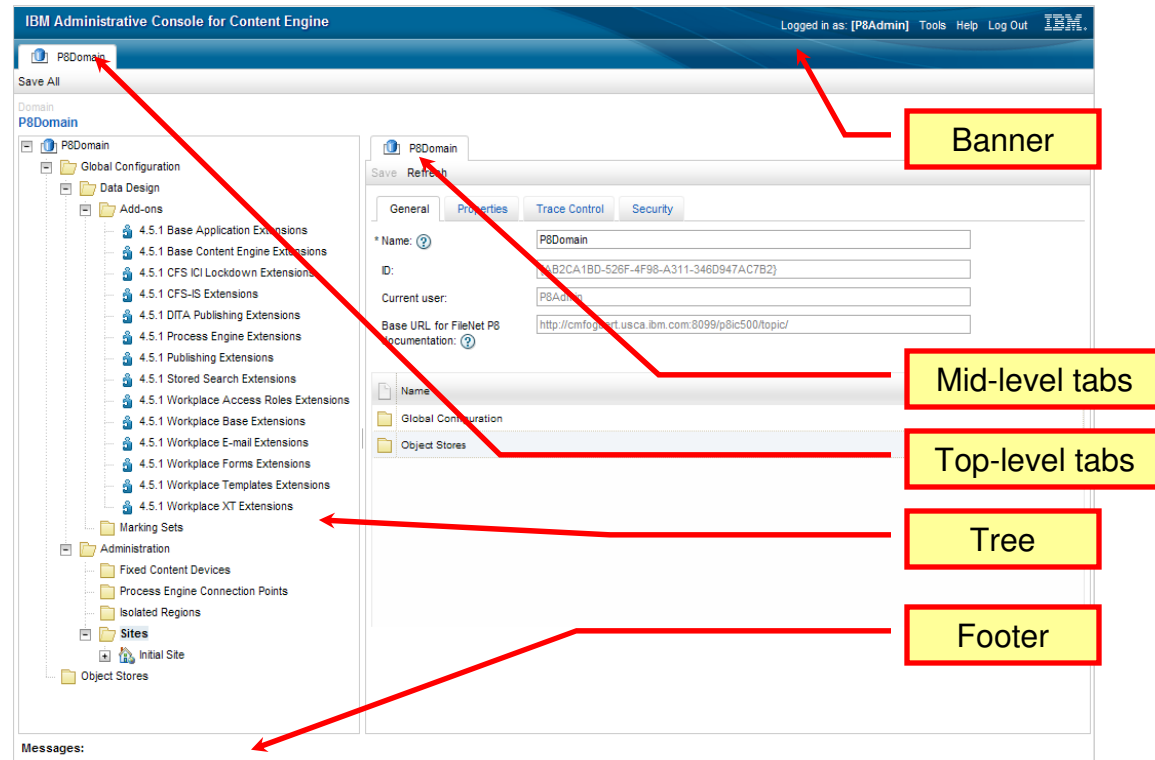
Overview of system administration

Administrative Console for Content Engine

- Web-based application (thin client) packaged with the FileNet P8 Content Engine
 - Available on all platforms supported by FileNet P8
- More accessible than Enterprise Manager
 - Accessed through a Web browser
 - Fully localizable
 - Accessibility options
 - No installation footprint
- Limited functionality for initial release
 - Does not currently replace Enterprise Manager

Overview of system administration

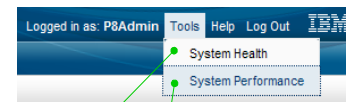
Administrative Console for Content Engine interface



Overview of system administration

System Health and Performance pages

- Accessible from the menu bar in the banner
 - Tools > System Health
 - Tools > System Performance
- Open in a top-level tab

A screenshot of the IBM Administrative Console for Content Engine. The 'System Health' and 'System Performance' tabs are visible. The 'System Health' tab is active, displaying a table of system components and their performance metrics. The table has columns for Component, Counter, Help, Current Count, and Previous Count. The data is organized by component categories like CPU, Content Index, Disk, Event & Subscription, LDAP Integration, Network, Persistence, RPC, and Storage.

Component	Counter	Help	Current Count	Previous Count
CPU	Busy	?	9	4
Content Index	CER Enqueue Dispatch Batch	?	0	0
Content Index	CER Enqueue Dispatch Batch Size	?	0	0
Content Index	CER Verify Index Batch	?	0	0
Content Index	CER Verify Index Batch Items	?	0	0
Disk	Reads	?	3584187	3584187
Disk	Writes	?	4060918	4060971
Event & Subscription	Background processing	?	0	0
LDAP Integration	LDAP Search Operations	?	10	10
LDAP Integration	LDAP User Token Fetch	?	2	2
Network	Collisions	?	0	0
Network	Errors In	?	0	0
Network	Errors Out	?	2	2
Persistence	Database operations	?	158	158
Persistence	Metadata operations	?	23	23
RPC	Execute Changes	?	0	0
RPC	Get Objects	?	40	40
RPC	Execute Search	?	0	0
RPC	Get Search Metadata	?	0	0
RPC	Execute Changes Failed	?	0	0
RPC	Get Objects Failed	?	0	0
RPC	Execute Requests Failed	?	0	0
Storage	Content Requests Resolved	?	0	0

Monitor content storage

Common storage monitoring tasks



- Use common monitoring practices for storage areas.
 - File storage, fixed storage, database storage
 - Use product-specific tools for database and fixed file stores.
- Monitor disk fragmentation on file store servers.
 - On Windows, use Disk Defragmenter or a third-party tool.
- Monitor disk space usage on file store servers.
 - Disk space can be used up faster than expected.
 - Check regularly to recognize the trend.
- Monitor access and status of the file store servers.
 - Use Enterprise Manager and the operating system of the file store.

Monitor content storage

Check storage areas in site or object store

- Use Enterprise Manager to monitor all storage areas for a site or an object store.
 - Sites > site_name or Object Stores > objectstore_name
 - Select the Storage Areas folder and view information
 - View and modify storage area properties or status
- Displayed storage area information
 - Online or offline, object store, type of storage area
 - File count, file bytes, file size limit
 - Located on Properties page
- Actions on storage area
 - Enable
 - Disable
 - Move
 - Refresh data display
 - Delete

Monitor content storage

Check usage and set file store maximums

- Enterprise Manager, Properties page: data for file storage area
 - General tab: file store location and description
 - Statistics tab: file count, file bytes, free bytes
 - Statistics tab: maximum content elements and KB
- System design identifies number of files expected and storage needs over time.
 - Provides values for maximum content elements, size in KB
- Monitor the number of files and their KB against maximums.
 - Compare actual usage with expected and maximum values.
 - If usage exceeds expectations, investigate the cause:
Is the cause user actions, other component actions, or a valid need?
 - If your investigation identifies a problem, fix its cause.
 - If the investigation reveals a valid need, change the maximum values.

Monitor content storage

Metadata and content inconsistencies



- Inconsistencies can develop between the object store database and the file storage area.
- Causes of inconsistency
 - Incomplete backup
 - Incomplete restore of database or of file store
 - Not restoring database and file store concurrently
- Content Consistency Checker
 - Run it to compare file store metadata with metadata in object store database.
 - To run this tool, user must have read permission for all files.
- Run Content Consistency Checker periodically to ensure consistency.
 - Always run it after a restore.
 - Run it when users cannot retrieve document content.

Monitor content storage

Steps to run Content Consistency Checker



1. Start Consistency Checker.
2. First time: Define domain in IBM FileNet Content Manager.
3. Connect to the FileNet P8 domain.
4. Select one or more file storage areas.
5. Set options for checking content consistency.
6. Run the validation.
7. Review the validation status information.
8. Review the validation report and information for each file error.

Monitor content storage

Set options for Consistency Checker



- Check one or multiple file storage areas.
- Specify the maximum number of errors logged.
 - Specify number for each error type.
 - Specify number for the total errors logged.
- Errors found after the maximum number are not logged.
- Set date and time limits on content elements to be checked.
- Two performance options:
 - Number of threads
 - Batch size
 - Use their default values in most cases.

Monitor content storage

Review the validation status



- Content element counts
 - Total number of validated elements
 - Total number of elements in the storage area
 - Elements validated per minute
- Validation error counts
 - Number of files in error for each error type
 - Total number of errors
- Timing data
 - Start time and end time
 - Duration
 - Projected duration
- Progress status
 - Completed

Review the validation report



- Select the storage area, and then select each error listed.
 - For each error, the file GUID, name, and storage location in the file store are provided, and also steps that you can use to fix that error.
- Missing file: has two causes
 - A valid document has no content.
 - A deleted document was restored to database, but not to file store.
- Bad size: file size in file store and database are different.
 - Wrong size in the database
 - Wrong size in the file store
- Other error types
 - Cannot Validate
 - Unreachable Area
 - Access Denied
 - Fixed Storage Area

What is auditing?

- Auditing is the automatic or programmatic logging of actions performed on an object or class.
 - Applications can create custom audit classes.
- Use security auditing to identify access actions.
- Use activity auditing to trace the history of an object.
 - Most objects can be audited.
- Content Engine can automatically log performed operations.
 - You can configure auditing for an object store, class, or operation.
- The audit history shows actions performed on an object.
- You can search for audited events on the following:
 - On the object itself
 - Across objects in the object store

Why audit?

- You configure auditing in order to gain information about Content Engine objects
- For example:
 - How often was this document accessed?
 - When did this property value change?
 - Who made the change?
 - Who deleted that document?
- Additional examples of other data that you can record:
 - Everything that ever changed on this document
 - Every time something was filed in a folder
 - When a user tries to open a document to which he does not have read access
 - Every time a document is opened

Object operations that you can audit



- Change operations
 - Create, update, delete
 - Checkin, checkout, promote and demote versions, cancel checkout, last accessed
 - Change class, classification complete
 - Lifecycle change state
 - File and unfile
 - Update security
 - Property value updates
- Retrieval operations
 - Object retrieved (Get Object)
 - Object content retrieved (Get Content)
 - Queries by class (Get Query)
- Audit configuration operations
 - Auditing enabled or disabled

Audit entries

- Audit entries are stored as objects in object store databases.
 - They can be searched for, exported, and so on.
- Each entry is a subclass of the Event class.
 - Each automatic operation has an Event subclass.
 - CheckinEvent is an Event subclass.
- Each subclass has additional, operation-specific properties.
 - Version Series Id is a property for check in and check out, which are versioning operations.
 - Containment Name is a property for file and unfile, which are folder operations.
- Object state recording level options include the following:
 - None
 - Modified object only
 - Original and modified objects

Audit definition extensions



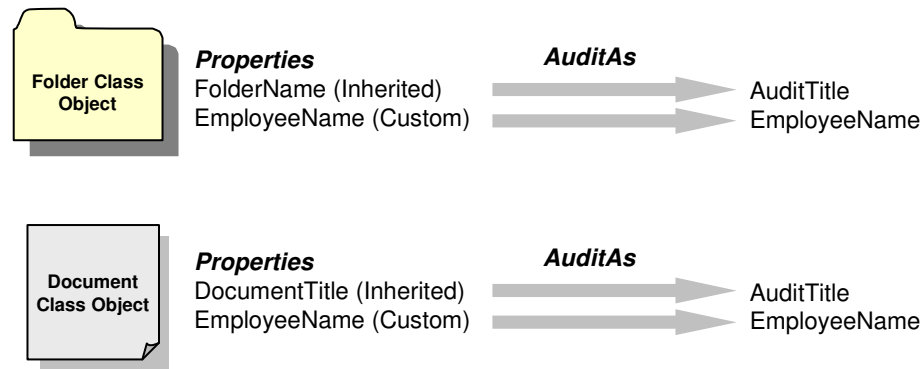
- Filter Expression
 - Audit events conditionally based on specific source object instance data. Functionally equivalent to subscription filtering. For example, Audit update events when AccountBalance < 1000, set Filter Expression = “AccountBalance < 1000.0”
 - Filtered Property Name - points to object-valued property of source object against which filter expression is evaluated
- Named Audit Definitions
 - Enables administrator to identify application-specific audit definitions – purely informational.
- Fine-grained Enablement
 - Enables per-application audit definition usage.
 - Can start or stop auditing for a specific event and class without having to re-create audit definition.

Steps to audit events

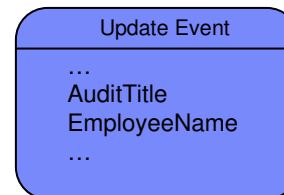


1. Enable auditing for the object store.
 - Use Enterprise Manager.
2. Configure auditing for class.
 - Use Enterprise Manager to set Success or Failure for audit definitions.
3. Generate events.
 - Perform actions on object (for example, create or update).
4. Find audit events.
 - Workplace: object Information > History page
 - Enterprise Manager: Properties > Audit History tab
 - Enterprise Manager: Query Event table

Audit Properties – example



- Use the *AuditAs* object-valued property to map properties as shown for each class.
- Add *AuditTitle* and *EmployeeName* property definitions to *UpdateEvent* Class.
- Configure update event audit definition on each class.
- Trigger update events on objects results in property values captured in Event table (along with default event properties).



Viewing audit history



- You can view the audit information for an object from Workplace XT and from Enterprise Manager.
 - Both provide audit information in the Properties page of the object.
- In Workplace XT, use the History page of the Information pages.
 - Search for history audit events for a document, custom object, or folder.
 - Searches can include all versions and all referenced objects.
- You can view details of an audit log entry.
 - Use the Information page in Workplace XT.
 - View the Properties window in Enterprise Manager.

Audit disposition



- An audit disposition subsystem automates deletion of event records from the audit log.
 - Runs as a background task.
- Audit Disposition Policy
 - Defines *what* gets deleted.
 - Example: Update Events older than 90 days
- Auditing configuration schedule
 - Determines *when* the audit policies are executed.
 - Example: Saturdays at hour 22:00
- Manual audit log disposal options include the following:
 - Predefined search templates
 - Bulk operations

Work with system logs

Monitor system logs

- IBM FileNet P8 Content Manager produces several log files during normal operation.
- You need to monitor these log files in order to do the following:
 - Become familiar with normal log entries.
 - Observe changes in behavior that might indicate a problem.
 - Ensure that log files have enough space for growth.

Guidelines



- Establish a baseline: Know what to expect.
 - Observe normal log activity so that you can identify changes later.
- Monitor logs every day.
 - Watch for new error messages.
 - Watch for any change in error log size.
 - Example: One log file is normally 64KB, and on one day it is 100 KB.
- Increase monitoring after any system changes.
 - Example: Patches applied
- Keep records of normal comparison logs.
 - Keep representative usage time intervals for each month.
 - After a year, keep representative time intervals for each year.

Content Engine logs



- P8_server_error.log
 - Usually the first log requested by customer support
- P8_server_trace.log
 - Customer support might ask you to enable targeted trace logging.
 - Trace log file exists even if trace logging is disabled.
- Trace logging:
 - Enable trace logging only for specific components.
 - Disable trace logging when no longer needed.
 - Remember to check Content Engine audit logs.

Specify trace logging options



- Enable and configure trace logging in Enterprise Manager.
 - Use the Trace Control tab on the Properties page for site or domain.
 - 1. Enable a domain.
 - 2. Enable a site.
 - 3. Specify the subsystems and its flags.
- Each Content Engine subsystem
 - Is a trace logging service or area of functionality within a service.
 - Has a property sheet for viewing and modifying its properties.
 - Has specific trace flags.
 - All subsystems have General and Trace flags.

Work with system logs

Logs from the Web application server



- Each Web application server generates its own logs.
- WebSphere
 - SystemOut.log
 - SystemErr.log
 - startServer.log
 - stopServer.log
 - serverStatus.log
- WebLogic
 - Base_domain.log
 - access.log
 - AdminServer.log

Process Engine server logs

- Process Engine server logs can be found in this location:
 - `/opt/IBM/FileNet/ProcessEngine/data/[pevsname]/logs`
 - Where *pevsname* is the name of the Process Engine virtual server name
 - If there is only one PE server, the virtual server name is `pesvr.default`
 - If multiple virtual servers are installed, the log files for each virtual server are stored in a separate folder.
- Process Engine server log file names can include the following:
 - `PEInit_system.log`
 - `Pesvr_system.log`
 - `PTM_system.log`
 - `VWLog_system.log`
 - `VWool_system.log`

Work with system logs

Additional tools for the Process Engine



- Additional tools to monitor the Process Engine:
 - Command tools, log files, and administrator tools, such as vwtool, vwmsg, vwlog, and vwverify
 - Process Analyzer, an add-on product that collects and presents data used to monitor the Process Engine
- To interpret and use these tools effectively, you need knowledge of the following:
 - Process Engine architecture
 - Component functionality
 - Workflows
- Learn to use these tools in the BPM Administration course.
- Learn to use the IBM FileNet Process Analyzer in the Process Analyzer and Simulator for Administrators course.

Work with system logs

Guidelines: Manage growth of log files

Component	Frequency
Application Engine log4j	Daily
Content Engine trace logs	Daily
Content Engine audit logs	Daily
Content Engine server logs	Weekly
Process Engine logs	Weekly
Database transaction logs	Weekly

Monitor system state with IBM System Dashboard

What is the Dashboard?

- IBM System Dashboard for Enterprise Content Management
 - Also referred to as the *Dashboard*
- A real-time, performance-monitoring tool that tracks the following:
 - IBM FileNet P8 system data
 - Application-specific events
 - System environment data
 - Operating system data
- Use the Dashboard to collect and distribute performance data on FileNet products installed at a site.
 - It comes with many IBM ECM products.
 - Use it to monitor multiple components on an IBM FileNet system.
- Most of its Help topics are available from the Dashboard.
 - It has a few topics in FileNet P8 Documentation.

Monitor system state with IBM System Dashboard

What can you do with the Dashboard?

- View system metrics in real time for the following:
 - Individual components, the system environment, operating systems
- Gather and archive performance data, and run reports to do these tasks:
 - Generate benchmark data.
 - Evaluate workload and its effect on system resources.
 - Observe changes and trends in workloads and resource usage.
 - Test configuration changes or other tuning efforts.
 - Diagnose problems.
 - Target components or processes for optimization.
- Integrate system metrics with external applications.
- Goal: Use the gathered data to identify and resolve potential performance problems before they occur.

Monitor system state with IBM System Dashboard

Dashboard terms (1)

- Cluster
 - A user-defined group of servers that is monitored by the Dashboard
 - Not related to active and passive clusters used for business continuity
 - A cluster must be defined before monitoring components.
- Listener
 - A component that provides performance data from the monitored component to the Dashboard
 - Optionally accumulates and aggregates that data
 - Example: P8 CEMP Listener provides Content Engine information.
- Container
 - It is a node in Dashboard that groups containers, events, and meters.

Dashboard terms (2)

- Event
 - An occurrence that happens in the application that is significant
 - Examples:
 - Documents checked out
 - Database lookup
 - Can have duration
- Meter
 - It is an absolute value of something inside the application software.
- Counter
 - Provides the count of how many events occurred.
- Accumulator
 - Contains the sum of some event-related quantities.
 - Summarizes data from several events (such as averages).
 - Example:
 - Average database lookup duration

Monitor system state with IBM System Dashboard

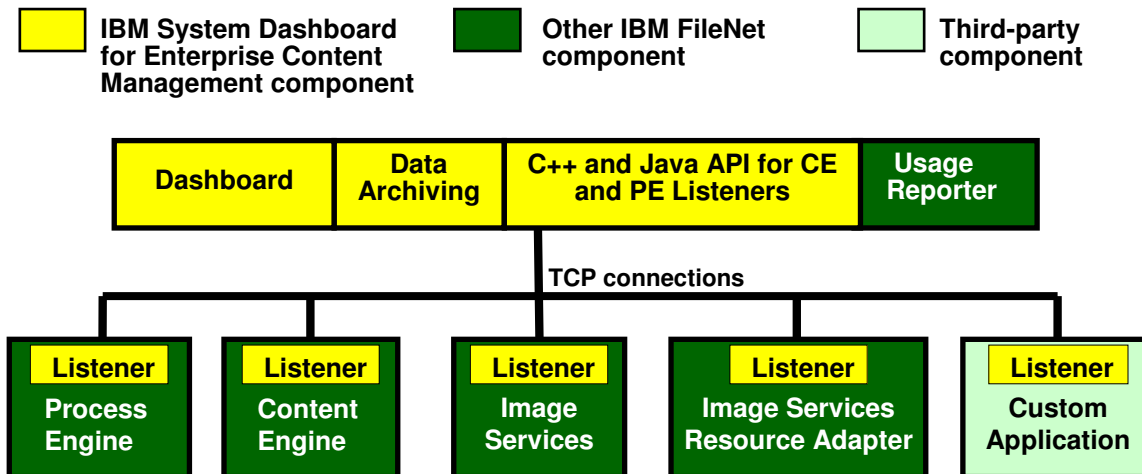
Components of the Dashboard

- Dashboard, used to configure data collection and to view data
 - Configure data collection with clusters and view data for a cluster.
 - Assign servers and a monitoring frequency to each cluster.
- Listener utilities that gather and save component data
 - They send the data to the Dashboard when queried or scheduled.
 - They are built-in for the core IBM FileNet engines.
- Data Archiving options
 - Use Archiving Manager to save data in compressed log files.
 - Archiver.jar stores the data of one Listener to its own log file (1:1).
- You can use Java and C++ APIs to build custom Listeners for custom applications, and to report their performance data.

Monitor system state with IBM System Dashboard

Architecture of the Dashboard

- Dashboard, Data Archiving, and C++ and Java APIs are hosted on any server in the IBM FileNet P8 system.
- The Listener runs on the server that hosts the component that is being monitored by the Listener.



Monitor system state with IBM System Dashboard

Start Dashboard and create clusters to view data

- Use Start menu in Windows, Dashboard shell script in UNIX.
- You must use a cluster in order to view Listener data.
 - A cluster can contain one or more servers.
 - It normally contains all servers related to a particular application.
 - All Listeners on the servers in a cluster are discovered automatically.
- You can define any number of clusters.
- To define a cluster, do the following steps:
 - Name the cluster and add the servers.
 - Specify how often Listener data is accumulated.
- Optional steps
 - Override the time span for summary data collection.
 - Override the number of data points.
 - Save the settings in an XML file to re-use the cluster.

Execute Listener options and view data

- In Details, right-click Listener node and click an option.
 - Query it for the health status (heartbeat) of its application.
 - Query it for the uptime of its application.
 - Save (archive) the data gathered by the Listener.
 - Send a custom message to the Listener.
 - Disconnect a Listener (if its historical data is not needed).
 - Request user list (provides a list of all users signed in by name).
- View accumulator data in tables and charts.
 - Select the accumulator node and view data numerically.
 - Or right-click the accumulator node and click a chart option.
 - Move and size the graph window as you like.
 - Select Chart in the graph window, select other graph option, click OK, and view the data as you selected the view.

Activities

In your Student Exercises

- Unit: System Administration and Maintenance
- Lesson: Monitor system state with IBM System Dashboard
- Activities:
 - Define a cluster.
 - Use Listener options to view data.

Optional lesson

IBM System Dashboard views and reports

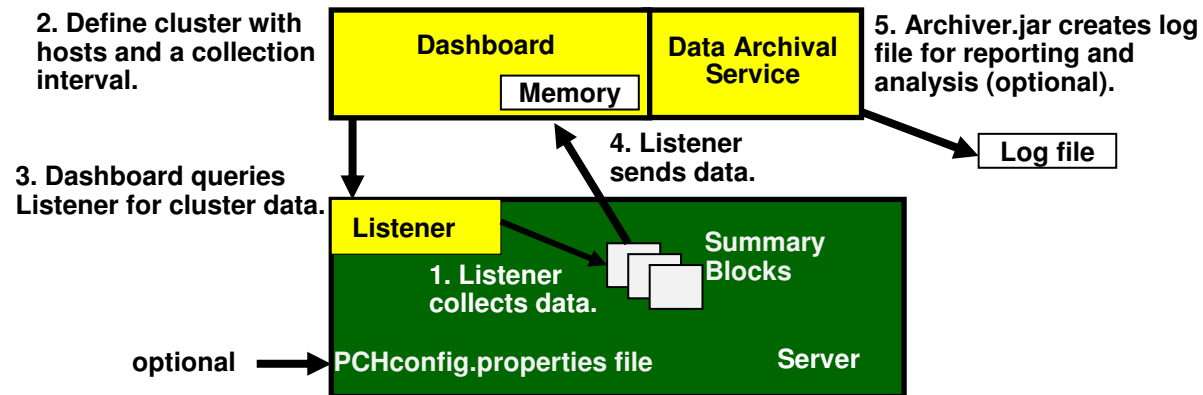
- Why is this lesson important to you?
 - You administer multiple servers. You need to view their activity levels to ensure that they are performing properly.
 - The IBM System Dashboard tool is installed on your IBM FileNet P8 Content Manager system. You need to know how to use the Dashboard to archive the data gathered by all listeners associated with an application so you can create an archive report for later analysis.

Activities that you need to complete

- Monitor components with Dashboard views
- Run Dashboard reports.

Dashboard and Listener data flow

1. The Listener continually gathers data, saving it in summary blocks.
2. Define a cluster to request Listener data and set collection interval.
3. Dashboard sends query to Listener for current and future data.
4. Listener sends current summary blocks to the Dashboard, and uses collection interval to create and send the summary blocks.
5. The summary blocks can be saved to a compressed archive file.



Interpret counter data

- Dashboard exposes the event and meter counters that are generated by the components being monitored.
 - Built-in counters for Content Engine, Dashboard, Image Services, Process Engine
 - In Dashboard Help, topics under Interpret counters and Dashboard counters explain the built-in counters.
- System counters (CPU, DISK, NETWORK)
 - Use these values to understand how a system is functioning and where potential bottlenecks to performance exist.
 - Always examine and report system values, particularly CPU values.
 - Current Named Users, Current Usage: user quantity and RPC load
- Application-specific counters vary with site activity.
 - To identify the counters used at a site, you can run a weekly report that includes all RPC and USER counters.
 - Save the reports and compare them to observe trends over time.

Sample counter definitions

- In the Dashboard Help, the definition tables list counter name, type, and definition of counters for IBM FileNet components.
- Object store counters track event data.
- Details for document creation counter
 - Content Engine node > object store node > Document > Creates
 - Shows Time, Count, Rate per second for each data collection period, and Total Count for running total of all collection intervals to that point.
- Details for Pending Batches counter
 - Content Engine node > object store node > Roll Forward Dispatcher
 - Time, Value (total number pending during collection period), Min, Max (minimum and maximum number of pending batches during period)
- Scroll down to view more current values.
- Some Listeners do not create performance counters until the event occurs the first time.

Use the Dashboard views

- Create and edit clusters in Clusters view.
 - The same cluster is open in all views except Alerts view.
 - Open the cluster from any view, using the File menu.
 - After a cluster is opened, it is available until you exit Dashboard.
- View graphs of heartbeat data in Summary view.
 - View average response time for Remote Procedure Calls.
 - View latest reported average response time and the average CPU utilization of servers within the cluster.
- View data by cluster, server, or Listener type in Details view.
 - View: RPC, DISK, NETWORK, CPU, USER, Environment
- Select, view, and export captured data to a file in Reports view.
 - Run reports against the data available in the Details view.
- View Info, Warning, Critical, Fatal messages in Alerts view.

Run Dashboard reports

- The report template specifies the content of a report.
 - The report template is a named and saved XML file.
 - The report template specifies the metrics recorded in the report.
 - Any number of report templates can be created.
- The report is a comma-separated value (CSV) file.
- To run a report, do the following:
 1. Select the report template.
 2. Name the report file and specify its storage location.
 3. Select a Listener.
 4. Select the report options.
- Each report provides information on one Listener.

Run Dashboard reports on archived data



- Archiving Manager is a utility that you use to do the following:
 - Gather data needed for later analysis.
 - Collect data from a Listener or from the Listeners in a cluster.
 - Save the data in a format recognized by IBM System Dashboard for Enterprise Content Management .
- Run Archiving Manager from any server that can connect to the specified listeners.
- To work with archives, do the following:
 1. Add the archived file to the Archives cluster.
 2. View the archived file from the Details view.
 3. Use a report template to run a report on Listener data in an archived file.