Sterling Control Center

System Administration Guide

Version 54.1

Sterling Control Center

System Administration Guide

Version 54.1

Note
Before using this information and the product it supports, read the information in "Notices" on page 267.

This edition applies to version 5.4.1 of IBM Sterling Control Center and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Manage Objects 1

Overview of managing Sterling Control Center objects 1
Common buttons 1
Filtering objects 2
Adding objects 3
Duplicating objects 4
Checking object properties 4
Obtaining an object's audit log 5
Printing listings of objects 6
Saving listings of objects 7
Cross-referencing objects 8
Removing objects 8
Create multiple objects 9
Creating multiple objects by using the sample script 10
Template contents 13
Creating your own templates 16
Create and maintain objects with the CCAPI . . 17
Installing the Sterling Control Center API . . 18
Copying configuration objects between installations 19
Copying configuration objects between UNIX installations 20
Copying configuration objects between Microsoft Windows installations 21

Chapter 2. Manage Data Visibility Groups 25

Creating a data visibility group 25
Displaying the data visibility group listing . . . 26
Viewing or changing a data visibility group . . 26
Data visibility group field descriptions 26

Chapter 3. Manage Roles and Users . . 31

Manage roles 31
Permissions 31
Creating a role 34
Displaying the roles listing 35
Viewing or changing a role 35
Role field descriptions 35
Manually restoring the superuser role . . . 36
Manage users. 37
Adding users 37
Viewing and changing user information . . . 38
User field descriptions. 38
Configuring account lockout for failed login attempts 39
Set password policy 40
Modifying the password policy file 40
Sample passwordPolicy.xml files 41

Chapter 4. Manage Servers 45

Adding a server 45
Viewing or changing server properties . . . 47
Setting up a server to monitor a Sterling B2B Integrator cluster via individual connections . . 47
Setting up a server to monitor a Sterling B2B Integrator cluster through a load balancer . . 48
Monitoring File Agents 49
Server field descriptions 49
Resetting the maximum concurrent session count for a server 58
Removing a server from Sterling Control Center 59
Manage server groups 59
Creating a server group 59
Viewing or changing a server group definition . 60
Removing a server group. 60
Resolving system server group naming conflicts 61
Managing licenses 61
Manually importing licenses. 62
Viewing and comparing licenses 63
Deleting licenses. 63
License import field definitions. 63
Pushing licenses to servers 64
License push field definitions 64
Automatically importing licenses 65

Chapter 5. Manage Rules and Actions 67

Manage rules. 67
Creating a rule 67
Displaying the Rules listing 69
Using data visibility groups to view rule sets . . 69
Viewing or modifying rule properties. 70
Rules field descriptions 70
Changing the order of rules 71
Enabling or disabling a rule 72
About actions. 72
Creating an action 74
Displaying the Actions listing 76
Viewing or modifying actions 76
Actions field descriptions. 77
Use predefined actions and rules 79

Chapter 6. Manage Service Level Criteria. 81

SLCs and QuickFile 81
About creating SLCs 82
Displaying an SLC group listing 82
Using data visibility groups to view SLC groups . . 83
Viewing or modifying properties of an SLC group 84
Adding or removing schedules from an SLC group 84
Enabling or disabling an SLC 84
Using predefined actions and rules in SLCs . . 85
Creating multiple SLCs 85
Creating a standard SLC group. 85
Standard and wildcard SLC field descriptions . . 87
Importing information into a standard SLC group 88
Exporting information from a standard SLC Group 89

Creating a wildcard SLC group 90
Testing expressions 91
Creating a workflow SLC Group 91
Workflow SLC field definitions 92
Maintain message lists. 94
Maintain Milestones 96
About simple SLCs 98
Using the Create Simple SLC Group Wizard . . 99
Creating a simple SLC group 99
Viewing or modifying properties of a simple SLC group 100
Enabling or disabling a simple SLC group. . . 100

Chapter 7. Schedules overview. . . . 103
Creating an SLC calendar schedule 103
Creating a rule calendar schedule 104
Creating a metadata calendar schedule 105
Creating an SLC duration schedule 105
Displaying a schedules listing 106
Viewing or modifying schedule properties. . . 106
Schedule field descriptions 106
Enabling or disabling a schedule 108
About calendars 108
Creating a calendar 108
Recurrence patterns 109
Viewing or modifying a calendar 110
Calendar field descriptions 110
Calendar example - Monday through Friday processing 111

Chapter 8. Manage email lists 113
Creating an email list. 113
Exporting information from an email list . . . 113
Exporting email information from an action . . 114
Displaying a listing of email lists 114
Viewing or modifying email lists 114
Email list field descriptions. 115

Chapter 9. Metadata rules overview 117
Creating a metadata rule 117
Displaying the metadata rules listing 118
Viewing or modifying a metadata rule 118
Reordering metadata rules 119
Enabling metadata rules. 119
Metadata rules field definitions 120
Managing metadata type mapping 120
About metadata actions 121
Creating metadata actions 121
Displaying metadata actions 121
Viewing and modifying metadata actions . . . 122

Chapter 10. Perform guided node discovery 123
Identify servers for node discovery 123
Adding a managed server to the Explorer List 123
Adding an unmanaged server to the Explorer List. 124
Manage the Explorer List 125
Viewing or modifying a server definition after node discovery 125
Enabling a server for discovery 125
Disabling a server for discovery 125
Removing a server from the Explorer List . . 126
Running node discovery. 126
Identify the status of servers in the node discovery list 127
Manage the Discovery List and My List 127
Moving a server to My List. 127
Moving a server to the Discovery List 127
Moving a server to the Explorer List 128
Showing partners 129
Adding discovered node comments 129
Removing a server from the Discovery List or My List 130

Chapter 11. About Sterling Control Center reports 131

Chapter 12. Sterling Control Center settings 133
Changing system settings 134
Database settings 135
Database settings field definitions 135
Email settings 138
SNMP host settings 138
Adding an SNMP host 138
Editing an SNMP host 139
Removing an SNMP host 139
SNMP host settings field definitions 139
Application log field description 140
Services field descriptions 140
Engine connection field descriptions. 141
Console settings field descriptions 141
License management field descriptions 144
File Agent field descriptions 144

Chapter 13. Administering Other systems. 145
Accessing the Sterling Connect:Direct Browser User Interface 145
Accessing Sterling B2B Integrator. 145
Accessing Sterling File Gateway 146

Chapter 14. Database administration 147

Chapter 15. Tune Sterling Control Center 149
Tune the Sterling Control Center engine 149
Use the Sterling Control Center console wisely 152
Tune the database server 153
Additional reference information 156

Chapter 16. Event type descriptions 157
Event type: Sterling Connect:Direct statistic record ID cross-reference 160

Chapter 17. Administrative troubleshooting 165

Chapter 18. Predefined actions and rules 169

Chapter 19. Message IDs for rules . . 173
Messages IDs specific to Sterling Connect:Direct 173
Message IDs specific to Sterling Connect:Enterprise 173
Messages IDs specific to QuickFile 176
Messages IDs specific to Sterling Connect:Express 176
Message IDs specific to Sterling B2B Integrator . . 178
Message IDs (Event Codes) specific to Sterling File Gateway 178
Message IDs for Sterling Control Center 179
Message IDs specific to configuration management 184

Chapter 20. Regular expressions . . . 193

Chapter 21. Sterling Control Center variables 195
Variables by event type 212

Chapter 22. Modify log4j to retain log fies 225
Sample CCEngine.log4j file 225
Sample CCClient.log4j file 227
Parameters modified in the sample log4j files. . . 228

Chapter 23. Failover configuration 229
Handling failures when the engine is installed on a SAN 230
SAN scenario 1—the server on which the Sterling Control Center engine is executing fails . 231
SAN scenario 2—the computer where the database server is executing fails 232
SAN Scenario 3—The Computer Where the Engine Is Executing and the Computer Where the Database Server Is Executing Both Fail . . 233
Handling failures when the engine is not installed on a SAN 234
Safeguarding the managed server's checkpoint data 234
Testing the standby Sterling Control Center engine. 235
Scenario 1—The computer where the Sterling Control Center engine is executing fails . . 235
Scenario 2—the computer where the primary database is executing fails 236
Scenario 3—The Computer Where the Engine Is Executing and the Computer Where the Database Server Is Executing Both Fail . . . 237

Chapter 24. Keys and fields 239

Chapter 25. Monitor a Sterling B2B Integrator server 255
Collecting Sterling B2B Integrator process data . . 256
Using collected Sterling B2B Integrator process data 256

Chapter 26. Monitor file transfers performed by Sterling File Gateway . . 259
Viewing Sterling File Gateway activities 259
Statistics Viewer 260
Sterling File Gateway terms 260

Chapter 27. Monitor file transfers performed by QuickFile 261

Chapter 28. Monitor MQ MFT file transfers 265

Notices 267

Index 271

Chapter 1. Manage Objects

Overview of managing Sterling Control Center objects

For greater ease of use, the Sterling Control Center console handles many components (referred to here as objects) in standard ways. So if you duplicate a role in the Roles listing, for example, you know how to begin duplicating a calendar schedule in the Schedules listing.

Sterling Control Center provides standard ways of handling objects which pertain to filtering, creating, duplicating, cross-referencing, and removing objects. In addition, you can easily check the properties of objects, print object lists, and obtain the audit log files.

Common buttons

When you are working with objects in Sterling Control Center, you might see certain buttons. Click a button to perform the action listed in the Description column of the following table.

Button	Name	Description
	Filter button	This button displays the Filter Listing window.
	Clear Filter button	This button clears the filter criteria and the contents of the current window are displayed as originally shown. The filter criteria is shown as NONE in the window title bar.
	Export list to PDF button	This button allows you to export the contents of the current window to a PDF file.
	Refresh Now button	This button allows you to manually refresh the current contents of the screen.
	Properties button	This button displays a dialog box that shows the properties of the object.
	Create button	This button allows you to add an object, such as a rule, calendar, or action.
	Remove button	This button allows you to delete an object, such as a rule, calendar, or action.
	Duplicate button	This button allows you to quickly create a new object from a similar existing one without having to input every data field.

Button	Name	Description
	Elliptical button	This button allows you to see more information about the field it follows.
	Right Arrow button	This button moves a selected item to the right to another column or list. In Calendar functions, moves forward through a calendar.
	Left Arrow button	This button moves a selected item to the left to another column or list. In Calendar functions, moves backwards through a calendar.
	Help button	This button opens the Sterling Control Center Information Center.

Filtering objects

You can limit the number of items that display in many Sterling Control Center listings by specifying filter criteria. Filtering a listing can make it more manageable to work with.

About this task

You can limit the number of items that display in many Sterling Control Center listings by specifying filter criteria. Filtering a listing can make it more manageable to work with. You can filter listings of the following Sterling Control Center objects:

- Actions
- Netmap Node Entries
- Activity Monitor
- On-Demand Reports
- Adapters
- Reports Schedules
- Alerts Monitor
- Roles
- Automated Reports
- Report Schedules
- Calendars
- Rules
- Daemons
- Rules Schedules
- Data Visibility Groups
- Secure+ Cipher Suites
- Email Lists
- Secure+ Key Certificates
- Functional Authorities

- Secure+ Nodes
- Initialization Parameters
- Secure+ Trusted Certificates
- Metadata Actions
- Servers
- Metadata Rules
- SLC Groups
- Netmap Communication Paths
- User Proxies
- Netmap Modes
- Users

Procedure

1. In the listing, click the **Filter button**. The Filter Listing window displays.
2. Select a **Key**. Available keys depend upon the object.
3. Select an **Operator**. Available operators depend on the key's data type (numeric or character).

Adding objects

Adding an object to many Sterling Control Center lists is easy and involves using a common button.

About this task

The kinds of objects you can add in this way include:

- Actions
- Report Schedules
- Calendars
- Roles
- Column Layout Views
- Rules
- Data Visibility Groups
- Rules Schedules
- Metadata Actions
- SLC Groups
- Metadata Rules
- Users

Procedure

1. In the listing for the object (for example, the Rules listing or the Workflow SLCs listing), click the Create button. A Create wizard displays.
2. Complete the Create wizard. For more information about the fields that make up the wizard, see *System Administration*. On the Finish page, click **Finish** to create the new item.

Duplicating objects

Duplicating objects in Sterling Control Center is easy and involves using a common button. Duplicating is a quick way of creating a new object from a similar existing one while avoiding having to input every data field.

About this task

The kinds of objects you can duplicate include the following:

- Actions
- On-Demand Reports
- CalendarsColumn
- Layout Views
- Roles
- Data Visibility Groups
- Email Lists
- Rules Schedules
- Metadata Actions
- SLC Groups
- Metadata Rules
- Users

Procedure

To duplicate an object:

1. In the listing for this object (such as the Rules listing or the Workflow SLCs listing), select the item you want to duplicate and click the Duplicate button. A Create wizard displays, with all fields filled in.
2. Supply a unique **Name** for the new object.
3. Make changes to any other fields as necessary, clicking **Next** to page through the wizard.
4. On the Finish page, click **Finish** to create the new item.

Checking object properties

Checking the properties of Sterling Control Center objects is easy and standardized.

About this task

You can check the properties of the following types of objects:

- Actions
- Roles
- Calendars
- Rules
- Column Layout Views
- Rules Schedules
- Data Visibility Groups
- SLC Groups
- Metadata Actions

- Server Groups
- Metadata Rules

To check properties for an object:

Procedure

1. In the listing for the object (such as the Rules listing or the Workflow SLCs listing), do one of the following:
   - Select the item and click the Properties button.
   - Double-click the item.

   The Properties dialog displays the object's properties.
2. Click **OK** to return to the listing.

Obtaining an object's audit log

You can get an audit log for any object contained in a listing.

About this task

You can get audit logs for the following types of objects:

- Actions
- Report Schedules
- Calendars
- Roles
- Daemons
- Rules
- Data Visibility Groups
- Rules Schedules
- Email Lists
- Secure+ Cipher Suites
- Functional Authorities
- Secure+ Key Certificates
- Initialization Parameters
- Secure+ Nodes
- Metadata Actions
- Secure+ Trusted Certificates
- Metadata Rules
- SLCs
- Netmap Communication Paths
- User Proxies
- Netmap Node Entries
- Users
- Netmap Modes

To get an object's audit log:

Procedure

1. Display the listing. For example, to display the listing of rules, click **Manage** > **Rules and Actions** > **Rules**.
2. Right-click the listing and select **Audit Log**.

Printing listings of objects

You can easily print listings of objects by using the Export List to PDF function in Sterling Control Center.

About this task

You can print the following kinds of object listings:

- Actions
- Netmap Modes
- Automated Reports
- On-Demand Reports
- Calendars
- Report Schedules
- Daemons
- Data Visibility Groups
- Rules
- Email Lists
- Rules Schedules
- Functional Authorities
- Secure+ Key Certificates
- Metadata Actions
- Secure+ Nodes
- Metadata Rules
- Secure+ Trusted Certificates
- Netmap Communication Paths
- SLC Groups
- Netmap Node Entries
- User Proxies
- Roles
- Users

Procedure

1. When the listing you want to print is displayed, take one of the following actions:
   - Right-click the listing, and select the **Export List to PDF** option.
   - Click the **Export List to PDF** button.

   The Export window is displayed with the **My Documents** folder open.
2. Type a filename and click **Export**. The file is saved in the **My Documents** folder and the Export window is closed.
3. Open the **My Documents** folder, select your newly-created file, and use the Adobe Reader print function.

Saving listings of objects

You can save any Sterling Control Center listing if the Export list to PDF button is visible.

About this task

You can save the following types of object listings to PDF:

- Actions
- Automated Reports
- On-Demand Reports
- Report Schedules
- Calendars
- Roles
- Daemons
- Rules
- Rules Schedules
- Data Visibility Groups
- Email Lists
- Functional Authorities
- Secure+ Cipher Suites
- Secure+ Key Certificates
- Secure+ Trusted Certificates
- Secure+ Nodes
- Initialization Parameters
- Metadata Actions
- Metadata Rules
- SLC Groups
- Netmap Communication Paths
- Netmap Modes
- Netmap Node Entries
- User Proxies
- Users

Procedure

1. When the listing you want to save is displayed, take one of the following actions:
   - Right-click the listing, and select the **Export List to PDF** option.
   - Click the **Export List to PDF** button.

   The Export window is displayed with the **My Documents** folder open.
2. Type a filename and click **Export**. The file is saved in the **My Documents** folder and the Export window is closed.

Cross-referencing objects

When making decisions about changing or deleting Sterling Control Center objects, you can determine whether other objects reference them. Showing any related objects can help you avoid making changes that would adversely affect other parts of the system.

About this task

Sterling Control Center objects you can cross-reference with other objects include:

- Actions
- Automated Reports
- On-Demand Reports
- Report Schedules
- Calendars
- Roles
- Email Lists
- Rules
- Rules Schedules
- Metadata Rules
- Metadata Actions
- SLC Groups
- Message Lists
- Users

To cross-reference an object:

Procedure

1. In the listing (for example, the Users listing or the Rules listing), right-click the item to cross-reference.
2. From the contextual menu that displays, select **Cross-reference**, and then one of the object types listed. The choices depend upon what other objects the object being cross-referenced might be interrelated with. For example, a message list is potentially interrelated with workflow SLC groups and roles. You can also specify All Objects.

Results

A list is displayed of objects (of the type specified) that reference the object in question.

Removing objects

You can easily removing objects in Sterling Control Center by using a common button.

About this task

The kinds of objects you can remove from listings in this way include:

- Actions
- Report Schedules

- Automated Reports
- On-Demand Reports
- Roles
- Calendars
- Rules
- Rules Schedules
- Metadata Rules
- Metadata Actions
- Column Layout Views
- Data Visibility Groups
- Servers
- Server Groups
- Email Lists
- SLC Groups
- Users

To remove an object:

Procedure

1. In the listing, select the item you want to remove and click the Remove button.
2. Click **OK** to remove the item.

Create multiple objects

Sterling Control Center provides a batch creation utility (RUNBATCH), sample script, and sample templates to create multiple Sterling Control Center objects. You can use these tools to create objects, such as actions, rules, schedules, email addresses, and SLCs, without manually creating each one through the console. You can use the same program to add or update server definitions.

Restriction: Server group-restricted users cannot use the RUNBATCH utility to create servers.

The templates are in the `ControlCenterInstallDir\conf\templates` folder. The sample script (script.txt) is in the `..\conf` directory.

Each template is a text file that contains a list of XML tags and variables corresponding to dialog field names. Each variable uses the format *&name;* where name is the variable name. Each variable name ends with a semicolon.

To run the procedures detailed here, you need to know how to edit XML tags and run batch scripts.

For more information, see the following topics in *How-to*:

- *How can I use RUNBATCH to create schedules for an hourly process?*
- *How can I do a bulk update of the passwords used by Sterling Control Center for monitored servers?*

Be sure to review the information in this documentation before attempting to implement those examples in your system to understand how templates and scripts are used with the RUNBATCH program to create and update multiple objects.

Creating multiple objects by using the sample script

You can create multiple objects by using a script.

About this task

Each section in a script corresponds to one object (such as one SLC duration schedule). Each script is used to create multiples of only one type of object. For example, create one script to create multiple standard SLCs, one script to create multiple wildcard SLCs, and one script to create multiple rules. Each section of a script contains the following information:

- A copy command that specifies the template name to be copied.
- The variables and values you want to substitute. See *Template contents* for a list of variable fields. Provide values for all fields.
- A final statement that defines the object you are adding to Sterling Control Center.

If the final statement for each section has the text "UPDATE" appended to it, for example, RULEUPDATE , then instead of creating an object, the object is assumed to exist. An update to that object is attempted.

To create multiple objects by using the sample script:

Procedure

1. Use a text editor such as WordPad to open the provided sample script file.

```
# Sample script to build SLCs, schedules, rules, actions, servers, etc. quickly.
#
# To build your own templates, do the following:
#
# Use Control Center GUI to build the SLC Group, SLC WC Group, schedule,
# time-schedule, rule, action, server,etc., like you want it.
#
# Copy the new rule, etc, into the conf/templates subdirectory and change
# the extension to .tmp from .xml

# SLC Groups are found in conf/slcs/groups and conf/slcs/groups/
# visibilityGroups
# SLC Schedules are found in conf/slcs/schedules
# Rules are found in conf/rules and conf/rules/visibilityGroups
# Actions are found in conf/actions
# Servers are found on conf/services/nodes
# Metadata rules are found on conf/metadataRules
# Metadata actions are found on conf/metadataActions
# Rule and Metadata rule schedules are found on conf/ruleSchedules
# Data Visibility Groups are found on conf/dataVisibilityGroups
# Calendars are found on conf/calendars
# Roles are found on conf/roles
# Users are found on conf/users
# Message Lists are found on conf/slcs/messageLists
#
# Edit the template and substitute variable names where appropriate.  Be sure
# to end each variable name with a semicolon (eg.  &name;).
#
# Write a script (such as this one) to copy your template and substitute
# the appropriate variables (see the following script for examples).
```

```
#
# The final statement for each section indicates what kind of SLC group, rule,
# etc, you are adding to Control Center:

# SLCGROUP             - SLC Group
# SLCWCGROUP           - Wildcard SLC Group
# SLCWFGROUP           - Workflow SLC Group
# SLCSCHEDULE          - SLC Time Schedule
# RULE                 - Control Center Rule
# RULESCHEDULE         - Control Center Rule/Metadata Rule Schedule
# REPORTSCHEDULE       - Control Center Report Schedule
# CALENDAR             - Control Center Calendar
# AUTOMATEDREPORTGROUP - Control Center Automated Report Group
# EMAILLIST            - Control Center EMail List
# ACTION               - Control Center Action
# SERVER               - Create a new Server/Node definition
# SERVERGROUP          - Create a new Server/Node definition
# METADATARULE         - Create a new Metadata Rule
# METADATAACTION       - Create a new Metadata Rule Action

&servergroup;  = ServerGroup
&node;         = Node1
&missingevent;  = true
&monitortolerance; = 6
SLCWCGROUP
#

copy slc_group
&id;           = WCSLC_6
&enabled;      = true
&desc;         = description
&filename;     = dest
&node;         = SERVER
&process;      = PROCESS
&remotenode;   = SERVER
&schedule;     = schedule
&submitter;    = submitter
&duplicatefilenames; = false
&duplicateprocesses; = false
&missingevent; = true
&monitortolerance; = 6
&servergroup;  = ServerGroup
SLCGROUP
#

copy duration
&id;           = duration_schedule
&enabled;      = true
&dmax;         = 0:30
&dmin;         = 0:25
&desc;         = description
SLCSCHEDULE
#

copy email
&desc;         = description
&email;        = name@address
&id;           = email_action
ACTION
#

copy opSys
&desc;         = description
&id;           = opsys_action
&operation;    = c:\\doit.batACTION#copy rule
&id;           = sample_rule
&desc;         = description
```

```
&enabled;      = true
&messageid;        = MSGID01I
&actionid;     = alert0
&eventtype;    = 6RULE
#
```

2. Choose from among the following final statements:

Statement	Object
ACTION	Sterling Control Center action
AUTOMATEDREPORTGROUP	Sterling Control Center automated report group
CALENDAR	Sterling Control Center calendar
DVG	Sterling Control Center Data Visibility Group
EMAILLIST	Sterling Control Center email list
MESSAGELIST	Sterling Control Center data message list
METADATAACTION	Sterling Control Center metadata action
METADATARULE	Sterling Control Center metadata rule
REPORTSCHEDULE	Sterling Control Center rule/metadata rule schedule
ROLE	Sterling Control Center role
RULE	Sterling Control Center rule
RULESCHEDULE	Sterling Control Center rule schedule
SERVER	Create a new server/node definition
SERVERGROUP	Create a new server/node definition
SLCGROUP	Sterling Control Center SLC group
SLCSCHEDULE	Sterling Control Center SLC schedule
SLCWCGROUP	Sterling Control Center wildcard SLC group
SLCWFGROUP	Sterling Control Center workflow SLC group
USER	Sterling Control Center user

3. Name and save the file.
4. When the Sterling Control Center engine is running and is initialized, open a command window and change your working directory to `ControlCenter\bin`.
5. Type one of the following commands:
   - In Microsoft Windows:

     `runBatch` *`hostname port userid password scriptname`*
   - In UNIX:

     `runBatch.sh` *`hostname port userid password scriptname`*

   The following table shows the parameter values:

Tag	Description
hostname	The IP address or DNS host name where Sterling Control Center is installed.
port	The HTTP port number that the Sterling Control Center engine monitors.
userid	The user name to access the Sterling Control Center. This value is case-sensitive.
password	The password to access the Sterling Control Center. This value is case-sensitive.
scriptname	The path and name of the script created in step 1 .

For example, in Microsoft Windows, type:

```
runBatch 127.0.0.1 58080 admin admin ..\conf\slcscript.txt
```

In UNIX, type:

```
runBatch.sh 127.0.0.1 58080 admin admin ../conf/slcscript.txt
```

The script executes and creates the objects.

6. If any script errors occur:
   a. Type one of the following to delete all defined objects:
      - In Microsoft Windows, type:
        `runBatch hostname port userid password scriptname delete`
      - In UNIX, type
        `runBatch.sh hostname port userid password scriptname delete`
   b. Review the template and scripts to determine where the error occurred.
   c. Make the necessary corrections and issue the **runBatch** command again.

Template contents

You can use several different types of templates to quickly implement Sterling Control Center.

Sterling Control Center contains the following types of templates:

- Duration Schedule Template
- E-mail Template
- Operating System Commands Template
- Rules Template
- Calendar Schedule Template
- Standard SLC Groups Template
- Wildcard SLC Groups Template

Duration schedule template

The duration.tmp file is used for SLC duration schedules. It contains the following fields:

Tag	Description
<dMax>&dmax;</dMax>	Maximum duration
<dMin>&dmin;</dMin>	Minimum duration
<desc>&desc;</desc>	Schedule description
<enabled>&enabled;</enabled>	Enabled (true or false)
<id>&id;</id>	Schedule Name
<name>&id;</name>	Schedule Name

Email template

The email.tmp file is used for email address in actions. It contains the following fields:

Tag	Description
<desc>&desc;</desc>	Action description
<email>&email;</email>	Email address

Tag	Description
<id>&id;</id	Action name

Note: The final statement for the e-mail template must be ACTION.

Operating system command template

The opSys.tmp file is used for operating system commands in actions. It contains the following fields:

Tag	Description
<desc>&desc;</desc>	Action description
<id>&id;</id>	Action name
<operation>&operation;</ operation>	Operating system command

Note: The final statement for the operating system command template must be ACTION.

Rules template

The rule.tmp file is used for creating rules. It contains the following fields:

Tag	Description
<actionId>&actionid;</actionId>	Action name associated with the rule
<desc>&desc;</desc>	Rule description
<enabled>&enabled;</enabled>	Enabled (true or false)
<eventType>&eventtype;</eventType>	The event type that generates the rules.
<id>&id;</id>	Rule name
<match>"/event[eventType = '&eventtype;' and messageId = '&messageid;'] "</match>	The event type and message ID to match. • &eventtype; is the event type code • &messageID; is the message ID

Calendar schedule template

The schedule.tmp file is used for creating calendar schedules. It contains the following fields:

Tag	Description
<calendarId>&calendar;</ calendarId>	Calendar name associated with the schedule
<desc>&desc;</desc>	Schedule description
<enabled>&enabled;</enabled>	Enabled (true or false)
<id>&id;</id>	Schedule ID
<name>&id;</name>	Schedule ID
<day>&day;</day>	Normal End Range day. 0 = NSR start day, 1 = NSR start day + 1, and so on.

Tag	Description
<end>&nerend;</end>	Normal End Range end time. Format hh:mm:ss.
<start>&nerstart;</start>	Normal End Range start time. Format hh:mm:ss.
<end>&nsrend;</end>	Normal Start Range end time. Format hh:mm:ss.
<start>&nsrstart;</start>	Normal Start Range start time. Format hh:mm:ss.
<timeZone>&timezone;</ timeZone>	The time zone.

Standard SLC groups template

The slc_group.tmp file is used for creating standard SLC groups. It contains the following fields:

Tag	Description
<desc>&desc;</desc>	Schedule description
<duplicateFileNames>&duplicatefilenames; </duplicateFileNames>	Allow duplicate file names (true or false)
<duplicateProcesses>&duplicateprocesses; </duplicateProcesses>	Allow duplicate Process names or Batch IDs (true or false)
<enabled>&enabled;</enabled>	Enabled (true or false)
<fileName>&filename;</fileName>	File Name
<id>&id;</id>	SLC ID
<missingEvent>&missingevent; </missingEvent>	Generate notification if event has not occurred (true or false)
<monitorTolerance>&monitortolerance; </monitorTolerance>	The monitor tolerance windows in hours
<name>&id;</name>	SLC ID
<node>&node;</node>	The servers selected for the SLC
<process>&process;</process>	The Process name. or Batch ID
<remoteNode>&remotenode; </remoteNode>	The remote node name
<schedule>&schedule;</schedule>	The associated schedule
<serverGroup>&servergroup; </serverGroup>	The server groups selected for the SLC
<submitter>&submitter;</submitter>	The submitter ID

Wildcard SLC groups template

The slc_regex.tmp file is used for creating wildcard SLC groups. It contains the following fields:

Tag	Description
<desc>&desc;</desc>	Schedule description
<enabled>&enabled;</enabled>	Enabled (true or false)
<fileName>&filename;</fileName>	The file name expression
<fileNameRegex>&filenameregex; </fileNameRegex>	Matches the file name using a Regex expression (true or false)
<id>&id;</id>	SLC ID

Tag	Description
<missingEvent>&missingevent; </missingEvent>	Generate notification if event has not occurred (true or false)
<monitorTolerance>&monitortolerance; </monitorTolerance>	The monitor tolerance windows in hours
<name>&id;</name>	SLC ID
<node>&node;</node>	The servers expression
<nodeRegex>&noderegex;</ nodeRegex>	Matches the servers using a Regex expression (true or false)
<process>&process;</process>	The Process name or Batch ID expression
<processRegex>&processregex; </processRegex>	Matches the Process name or Batch ID using a Regex expression (true or false)
<remoteNode>&remotenode; </remoteNode>	The remote node name expression
<remoteNodeRegex> &remotenoderegex; </remoteNodeRegex>	Matches the remote node name using a Regex expression (true or false)
<schedule>&schedule;</schedule>	The associated schedule
<serverGroup>&servergroup; </serverGroup>	The server groups selected for the SLC
<submitter>&submitter;</submitter>	The submitter ID expression
<submitterRegex>&submitterregex; </submitterRegex>	Matches the submitter ID using a Regex expression (true or false)

Creating your own templates

You can create your own templates using the Sterling Control Center console.

About this task

To use the Sterling Control Center console to create your own templates:

Tip: No template is provided to create servers or workflow SLCs in batch. You must create your own template for these.

Procedure

1. Create an object of the type for which you want to create a template using the Sterling Control Center console. Sterling Control Center creates an .xml file for the object in the `ControlCenter\conf\objecttype` directory. For example, rule .xml files are located in the `ControlCenter\conf\rules` directory.
2. Copy the .xml file for the object to the `ControlCenter\conf\templates` directory.
3. Rename the .xml file in the `ControlCenter\conf\templates` directory as a .tmp file.
4. Open the .tmp file with a text editor such as WordPad.
5. Replace the values between the XML tags with variables. The following is an example of a roles template before and after editing:

Before Editing	After Editing
<role>	<role>
<id>superuser</id>	<id>&role;</id>
<ver>1</ver>	<ver>1</ver>
<desc>Administrator role definition</desc>	<desc>&desc;</desc>
<!-- auths -->	<!-- auths -->
<rules>manage</rules>	<rules>&rulespermiss;</rules>
<actions>manage</actions>	<actions>&actionpermiss;</actions>
<alerts>manage</alerts>	<alerts>&alertpermiss;</alerts>
<processes>manage</processes>	<processes>&procpermiss;</processes>
<users>manage</users>	<users>&userpermiss;</users>
<roles>manage</roles>	<roles>&rolespermiss;</roles>
<servers>manage</servers>	<servers>&serverpermiss;</servers>
<slcs>manage</slcs>	<slcs>&SLCpermiss;</slcs>
<systemSettings>manage</systemSettings>	<systemSettings>&syspermiss;</systemSettings>
<reports>manage</reports>	<reports>&reportpermiss;</reports>
</role>	</role>

6. Save the .tmp file.
7. Continue with step 1 of *Creating multiple objects by using the sample script* to build and run a script file.

Create and maintain objects with the CCAPI

The IBM® Sterling Control Center API (CCAPI) enables a Java application to connect with a Sterling Control Center engine to perform operations such as getting, creating, updating, and deleting Sterling Control Center objects. With the CCAPI, you can programmatically create and maintain objects, such as users, roles, data visibility groups (DVGs), servers, and server groups for large scale efficiency.

In addition, you can perform the following node object configuration operations:

- Construct new node configuration objects
- Delete existing node configuration objects
- Update existing node configuration objects
- Perform a rekey of a server's Sterling Connect:Direct® Secure Plus parameter file using a provided seed value
- Perform a Sterling Connect:Direct Secure Plus parameter file validation for a server

The Sterling Control Center *InstallDirectory*\sdk directory includes the compressed distribution file containing the CCAPI. For more information about installing the CCAPI, see *Installing the Sterling Control Center API*.

For more information about the using the CCAPI, see the readme file in the `CCAPI\` folder and Javadoc in the `CCAPI\doc\` folder.

The CCAPI can connect to the engine with either secure or nonsecure connections. Secure connections require configuration of a secure connection on the Sterling Control Center engine and your CCAPI program. For more information, see *Getting Started*.

Installing the Sterling Control Center API

The IBM Sterling Control Center Application Programming Interface for Java (CCAPI) enables a Java application to connect to Sterling Control Center and initiate node configuration-related tasks and create, update, and obtain, Sterling Control Center role, user, server, server group, and data visibility group (DVG) objects.

Before you begin

Knowledge of the Java programming language and basic Sterling Control Center operations is necessary to use this application programming interface (API). If you plan to use a secure connection to a Sterling Control Center engine, you also need knowledge of the JSSE (Java Secure Sockets Extension).

About this task

To install the CCAPI:

Procedure

1. Create a directory and copy the CCAPIxxxx.zip distribution file into this directory.
2. Extract the files from the compressed CCAPIxxxx.zip distribution file by typing a command similar to the following command: `jar -xvf CCAPIxxxx.zip`

   Note: If you use an archive utility to extract the files, be sure to select the **Use folder names** check box.

Results

The following files and folders are extracted:

- Readme.txt
- Sample.java - a sample Java application that uses the CCAPI
- `conf` - a folder that contains CCAPI.log4j, the logging configuration file
- `doc` - a folder that contains the Javadoc based documentation of the CCAPI. To view this file, open index.html.
- `lib` - a folder to hold the JAR files necessary for using the CCAPI. You must copy the JAR files to this folder. For a list of the JAR files that must be copied, see the Readme.txt file.

  Note: The JAR files used with the CCAPI must be at the same level as the Sterling Control Center engine. This structure is checked when the CCAPI attempts to sign on to the Sterling Control Center engine. Each time you apply maintenance to Sterling Control Center or upgrade to a new release, you must copy these JAR files into your CCAPI folder again.

- `log` - a folder that contains the log file, CCAPI.log, which is generated when running CCAPI-based applications.

What to do next

For information about getting started with the CCAPI, see the Javadoc in the `\doc` directory.

Copying configuration objects between installations

You can copy all Sterling Control Center configuration objects from a source Sterling Control Center installation to a target Sterling Control Center installation. After these steps are performed, any existing configuration objects at the target installation are not used by the Sterling Control Center engine because you either delete or rename the old \conf folder on the target installation.

You may want to perform this copy procedure for a variety of reasons including:

- To prepare for disaster recovery.
- To copy a test instance of Sterling Control Center to a production instance

The source installation and target installation must be the same version level, including the minor version. For example, if the source Sterling Control Center installation is 5.0.02, then the target installation must be 5.0.02.

You must copy the entire configuration objects directory as a whole. Do not copy configuration objects selectively. You must not attempt to merge the source configuration data with any existing target configuration data. The source configuration is a complete replacement of all the target configuration's objects.

The following Sterling Control Center configuration objects are stored in the *SCCInstallDirectory*`\IBM\ControlCenter\conf` directory, where *SCCInstallDirectory* is the directory where you installed Sterling Control Center:

- Definitions and checkpoint files for all managed servers
- Rules and Actions
- Rule Schedules, SLC Schedules and Automated Report Schedules
- Calendars
- Email Lists
- Metadata Rules and Actions
- Report definitions
- Automated Report Definitions
- Users, Roles, and User Profiles
- Server Groups
- Templates for Batch creation utility
- Password Policy file
- Welcome Message file
- Various engine connector service definitions
- Various System Service files such as JDBC Service

The configuration objects include the JDBC Configuration (Database connection) details. After you copy the configuration objects to another installation, you must run configCC.bat (for Microsoft Microsoft Windows) or configCC.sh (for UNIX) to change the database connection details so the target installation uses the

appropriate database. For more information, see *Copying configuration objects between Microsoft Windows installations* or *Copying configuration objects between UNIX installations*.

The checkpoint files for managed servers are also included in the configuration objects. Therefore, when the configuration objects are copied to another installation, the target engine will use those checkpoint files and start collecting the statistics onwards from the date and time found in those files. If you do not want this to be the case, use runEngineCold.bat (for Microsoft Windows) or runEngineCold.sh (for UNIX).

Copying configuration objects between UNIX installations

You can copy configuration objects from one Sterling Control Center installation on UNIX to another.

About this task

To copy the configuration objects from one Sterling Control Center installation on UNIX to another:

Procedure

1. Stop the engine from where you are planning to copy the Sterling Control Center configuration objects.
2. Archive the entire conf folder located under the SCCInstallDirectory folder using tar. For example, you could use the following command:

   ```
   tar -cvf conf.tar conf
   ```
3. Transfer the archived file to the target installation host.
4. Restart the engine if desired.
5. Stop the SCC engine running on the target installation.
6. Make a backup of the conf folder on the target installation.
7. Rename (or delete) the existing conf folder on the target installation. For example, you could use the following command:

   ```
   mv conf conf_old
   ```

   CAUTION:
   Do not attempt to merge the source configuration data with any existing target configuration data.
8. From the target SCC engine installation location, extract the archive file that was transferred from the source installation. For example, you could use the following command:

   ```
   tar -xvf conf.tar
   ```

   After the extraction, you should see the conf folder under the `SCCInstallDirectory` folder.
9. Run configCC.sh to change the database connection details. If you do not, the Database connection used by the target installation will be the same as the source SCC installation. When you run configCC, you will get a message that all the steps have been already configured, but you must still go through the following steps and specify different values wherever required:
   - Engine Name configuration step: You may need to specify a different name.

- Time Zone configuration step: You may need to specify different value if the source installation and target installation were not in the same time zone.
- JDBC Driver configuration step: You must select the appropriate database type and specify the JDBC Driver for that database type even though this has been already configured.
- Production Database connection parameters configuration step: You must specify different connection details. If you do not specify different database connection details, two different engines could be using the same database.
- Production Database initialization step: Answer "No" to initialize the step. If you answer "Yes," all existing data in the database will be lost.
- Staging Database connection parameters configuration step: You must specify different connection details. If you do not specify different database connection details, two different engines could be using the same database.
- Staging Database initialization step: Answer "No" to initialize the step. If you answer "Yes," all existing data in the database will be lost.
- Key Store/Trust Store configuration step: If you specified a valid key store and trust store previously, you must specify them again.
- Http Connector Configuration: Reconfigure this with the appropriate port number.
- Secure Http Connector Configuration: Reconfigure this if you need a secure connection between the engine and console.
- Servlet Container Configuration step: Reconfigure this with the appropriate port number and host name.

10. Start the engine taking one of the following actions:
    - To collect the statistics that were generated when the engine was down, use runEngine.sh.
    - To start collecting statistics now, use runEngineCold.sh.
11. Using the Sterling Control Center console, update the following system settings if required (through the option, **Control Center** > **System Settings**):
    - E-mail server connection (on the E-mail tab)

      Note: You cannot update email settings through the console; you must run configCC. For more information, see *Changing engine settings after installation* in *Getting Started*.
    - Host computers where SNMP traps are sent (on the SNMP Hosts tab)
    - Simultaneous pollers (on the Services tab)
    - Settings effecting the monitor performance (on the Console Settings tab)
    - Settings related to moving data from the Production to the Staging databases (on the Database tab)

Copying configuration objects between Microsoft Windows installations

You can copy configuration objects from one Sterling Control Center installation on Microsoft Windows to another.

About this task

To copy the configuration objects:

Procedure

1. Stop the engine from which you are planning to copy the Sterling Control Center configuration objects.
2. Archive the entire conf folder located under the `SCCInstallDirectory` folder using WinZip or a similar tool.
3. Transfer the archived file to the target installation host.
4. Restart the engine if desired.
5. Stop the Sterling Control Center engine running on the target installation.
6. Make a backup of the conf folder on the target installation.
7. Rename (or delete) the existing conf folder on the target installation.

   CAUTION:
   Do not attempt to merge the source configuration data with any existing target configuration data.
8. From the target Sterling Control Center engine installation location, extract the archive file that was transferred from the source installation. After the extraction, you should see the conf folder under the `SCCInstallDirectory` folder.
9. Run configCC.bat to change the database connection details. If you do not, the Database connection used by the target installation will be the same as the source Sterling Control Center installation.

   When you run configCC, you will get a message that all the steps have been already configured, but you must still go through the following substeps and specify different values where required:

   a. Engine Name configuration step: You may need to specify a different name.
   b. Time Zone configuration step: You may need to specify different value if the source installation and target installation were not in the same time zone.
   c. JDBC Driver configuration step: You must select the appropriate database type and specify the JDBC Driver for that database type even though this has been already configured.
   d. Production Database connection parameters configuration step: You must specify different connection details. If you do not specify different database connection details, two different engines could be using the same database.
   e. Production Database initialization step: Answer “No” to initialize the step. If you answer “Yes,” all existing data in the database will be lost.
   f. Staging Database connection parameters configuration step: You must specify different connection details. If you do not specify different database connection details, two different engines could be using the same database.
   g. Staging Database initialization step: Answer “No” to initialize the step. If you answer “Yes,” all existing data in the database will be lost.
   h. Key Store/Trust Store configuration step: If you specified a valid key store and trust store previously, you must specify them again.
   i. Http Connector Configuration: Reconfigure this with the appropriate port number.
   j. Secure Http Connector Configuration: Reconfigure this if you need a secure connection between the engine and console.
   k. Servlet Container Configuration step: Reconfigure this with the appropriate port number and host name.
10. Start the engine taking one of the following actions:

- To collect the statistics that were generated when the engine was down, use runEngine.bat.
- To start collecting statistics now, use runEngineCold.bat.

11. Using the Sterling Control Center console, update the following system settings if required (through the option, **Control Center** > **System Settings**):
    - E-mail server connection (on the E-mail tab)

      Note: You cannot update email settings through the console; you must run configCC. For more information, see *Changing engine settings after installation* in *Getting Started*.
    - Host computers where SNMP traps are sent (on the SNMP Hosts tab)
    - Simultaneous pollers (on the Services tab)
    - Settings effecting the monitor performance (on the Console Settings tab)
    - Settings related to moving data from the Production to the Staging databases (on the Database tab)

Chapter 2. Manage Data Visibility Groups

Data visibility groups (DVGs) limit what events (data) a specific user can monitor. For example, when multiple users have access to a single server, a data visibility group (together with a server group) provides a way to segment the data a user can view and act upon for that server.

The high-level process for setting up data visibility groups is as follow:

1. Specify criteria for segmenting data as needed for your organization.

   For example, you can segment data into different lines of business (LOBs) or different functional areas, such as accounting or payroll. When events match on any criteria for a data visibility group, that data visibility group name is put into the DVG attribute of the event.
2. After you define data visibility groups, you assign them to roles, thus restricting the roles.

   A role can have a server group restriction or data visibility group restriction or both server group and data visibility group restrictions. When restricted roles are assigned to objects, you can elect to either make the object visible to all users or only restricted users in the selected roles.
3. The roles are then assigned to users, making the users data visibility restricted.

Creating a data visibility group

Create data visibility groups to limit what events (data) a specific user can monitor.

Before you begin

Before you create data visibility groups, see *Implementation*.

Procedure

To create a data visibility group:

1. Select **Manage** > **Data Visibility Group** from the Sterling Control Center window to display the **Data Visibility Group** listing.
2. Click the Create button to display the **Create Data Visibility Group** wizard.
3. Define a name for the group and provide a description. Click **Next**. For more information, see *Data visibility group field descriptions*.
4. Click the Create button to display the **Create Data Visibility Group Criteria** wizard. You must specify at least one criterion that defines what events (data) a user has access to.
5. Define a name for the criterion and provide a description. Click **Next**.
6. Specify one or more parameters to define the criterion by choosing a **Key** and **Operator** and entering a **Value**. For more information about the keys you can use in parameters, see *Data visibility group field descriptions* and *Keys and Fields*. Click **Next**.
7. Confirm your selections and click **Finish**. The criterion you defined is listed in the **Data Visibility Group - Criteria list**.
8. Click the Create button to create another criterion. After you add all criteria for the data visibility group, click **Next**.

9. Confirm your selections and click **Finish**. Click **Close** to exit the wizard. The data visibility group is displayed in the **Data Visibility Groups** listing.

Displaying the data visibility group listing

You can display a listing of data visibility groups.

About this task

To display the Data Visibility Groups listing:

Procedure

- From the Sterling Control Center window, select **Manage** > **Data Visibility Group**.
- To sort a column, click its heading.

Viewing or changing a data visibility group

If you have the requisite permissions, you can view the information that defines a data visibility group or changes its information.

About this task

To view or change a data visibility group:

Procedure

1. Select **Manage** > **Data Visibility Group** from the Sterling Control Center window to display the Data Visibility Groups listing.
2. Do one of the following to display the Data Visibility Groups Properties window:
   - Select a data visibility group and click the Properties button.
   - Double-click a data visibility group
3. Click the **General**, **Criteria**, and **Summary** tabs to view and change the data visibility group property information as needed. See *Data visibility group field descriptions* for definitions of the fields.
4. Click **Update**. The data visibility group property information is updated.

Data visibility group field descriptions

You can use many fields to specify a data visibility group.

Field	Description
Description	A description of the data visibility group.
Name	The name for the data visibility group. A data visibility group defines events (data) that users will be able to view and act upon.

Field	Description
Parameters	Parameters that specify the data users can monitor. Parameters are specified as keys, operators, values. The following keys are available for use in data visibility groups. See *Keys and Fields* for parameter descriptions. CX.Event Type CX.File Bytes Transferred CX.File Label CX.File Transfer Protocol CX.Local File Name CX.Local Node Name CX.Network Bytes Transferred CX.Network Return Code CX.Number of Records Transferred CX.Operating System CX.Other Node Name CX.Process Originator CX.Protocol Return Code CX.Receiver of File CX.Request Type CX.Return Code CX.Sender of File CX.Server Name CX.System Return Code CX.Transfer Destination CX.Transfer Direction CX.Transfer Identified CX.Transfer Origin CX.Type of Link CX.User Data Received CX.User Data Sent Destination File Direction (inBound or outBound) FG.Activity (A or R or D) FG.Arrived File Name FG.Business Process Name FG.Consumer FG.Consumer ContentType FG.Consumer Mailbox Path FG.ConsumerType FG.Layer Count FG.Layer Description FG.Layer Filename FG.Layer Type FG.PayloadName FG.Producer FG.Producer File Structure FG.Producer Payload FG.Route Count FG.Routing Channel Template Name File Agent Name File Agent Rule File Agent Trigger File From Server Local Node (P or S)

Field	Description
	MQMFT.The MQ MFT message id MQMFT.The MQ MFT action type MQMFT.The action time MQMFT.-call's outcome MQMFT.-call result's error MQMFT.-call result's outcome MQMFT.-call result's return code MQMFT.-call result's stderr output MQMFT.-call result's stdout output MQMFT.-call result's time MQMFT.-call result's retries MQMFT.-call command arguments MQMFT.-call command name MQMFT.-call command retry count MQMFT.-call command retry wait MQMFT.-call command successful return code MQMFT.-call command type MQMFT.Destination queue manager MQMFT.Destination agent MQMFT.Destination bridge URL MQMFT.Destination's OS arch MQMFT.Destination's OS name MQMFT.Destination's OS version MQMFT.MQ MFT identifier for the transfer MQMFT.Job name (if provided). Otherwise, "MQMFT_transfer". MQMFT.User provided metadata MQMFT.Hostname of the originator MQMFT.The originator's MQMD userid MQMFT.The originator's userid MQMFT.-postdest call's outcome MQMFT.-postdest call's error MQMFT.-postdest call result's outcome MQMFT.-postdest call result's return code MQMFT.-postdest call result's stderr output MQMFT.-postdest call result's stdout output MQMFT.-postdest call result's time MQMFT.-postdest call result's retries MQMFT.-postdest command arguments MQMFT.-postdest command name MQMFT.-postdest command retry count MQMFT.-postdest command retry wait MQMFT.-postdest command successful return code MQMFT.-postdest command type MQMFT.-postsrc call's outcome MQMFT.-postsrc call's error MQMFT.-postsrc call result's outcome MQMFT.-postsrc call result's return code MQMFT.-postsrc call result's stderr output MQMFT.-postsrc call result's stdout output MQMFT.-postsrc call result's time MQMFT.-postsrc call result's retries MQMFT.-postsrc command arguments MQMFT.-postsrc command name

Field	Description
	MQMFT.-postsrc command retry count MQMFT.-postsrc command retry wait MQMFT.-postsrc command successful return code MQMFT.-postsrc command type MQMFT.-predest call's outcome MQMFT.-predest call result's error MQMFT.-predest call result's outcome MQMFT.-predest call result's return code MQMFT.-predest call result's stderr output MQMFT.-predest call result's stdout output MQMFT.-predest call result's time MQMFT.-predest call result's retries MQMFT.-predest command name MQMFT.-predest command retry count MQMFT.-predest command retries MQMFT.-predest command successful return code MQMFT.-predest command type MQMFT.-presrc call's outcome MQMFT.-presrc call result's error MQMFT.-presrc call result's outcome MQMFT.-presrc call result's return code MQMFT.-presrc call result's stderr output MQMFT.-presrc call result's stdout output MQMFT.-presrc call result's time MQMFT.-presrc call result's retries MQMFT.-presrc command arguments MQMFT.-presrc command name MQMFT.-presrc command retry count MQMFT.-presrc command retry wait MQMFT.-presrc command successful return code MQMFT.-presrc command type MQMFT.Source agent queue manager MQMFT.Source agent name MQMFT.Source agent bridge URL MQMFT.Source agent's OS arch MQMFT.Source agent's OS name MQMFT.Source agent's OS version MQMFT.Statistics actual start time MQMFT.Statistics number of file failures MQMFT.Statistics number of file warnings MQMFT.Statistics retry count MQMFT.rslt code MQMFT.MQ MFT msg MQMFT.Destination checksum MQMFT.Destination checksum method MQMFT.Destination exists MQMFT.Destination last modification date/time MQMFT.Destination queue group id MQMFT.Destination queue message count MQMFT.Destination queue message id MQMFT.Destination queue message length MQMFT.Destination file size MQMFT.Transfer mode

Field	Description
	MQMFT.Srouce checksum MQMFT.Source checksum method MQMFT.Source disposition MQMFT.Source last modified date/time MQMFT.Source queue group id MQMFT.Source queue message count MQMFT.Source queue message id MQMFT.Source queue message length MQMFT.Source file size MQMFT.Transfer result code MQMFT.Transfer message MQMFT.Transfer start timeOrig Node Pnode Account Info Process Name QuickFile Event Type QuickFile Operation QuickFile Recipient Email Addr QuickFile Recipient User ID QuickFile User Email Addr QuickFile User ID QuickFile User Registered Remote Node Server Id Servers and Server Groups Server Type Source File Step Name Submitter

Chapter 3. Manage Roles and Users

Manage roles

Roles are sets of permissions that specify the Sterling Control Center actions users can take and the servers and server groups they can act upon. You set up roles based on the needs of your organization.

Sterling Control Center is distributed with two roles: superuser and user. The superuser role can perform all Sterling Control Center functions on all managed servers. The superuser can create additional roles or modify existing ones to serve business requirements. By default, the user role can view Sterling Control Center activity but cannot perform management functions such as adding servers or creating SLCs or rules.

Note: Because the predefined user and superuser roles that ship with Sterling Control Center are replaced with maintenance releases or upgrades, refrain from changing those roles. Instead, make copies of those roles and manipulate and use the copies.

For more information about roles, see *Define Roles* in *Implementation*.

Permissions

Permissions define the actions that Sterling Control Center users can perform. There are three permission levels: Manage, View Only, and None.

If a role does not have permission to access a function, that function is dimmed on the affected user's console and cannot be selected. After you define a role with restricted access, you can restrict access to actions, rule schedules, SLC schedules, and calendars. You can restrict access by associating the restricted role with the item you create.

The following table summarizes Sterling Control Center permissions:

Function	Manage Permission	View Only Permission	None
Servers/Groups	Allows a user to add any server type that is supported by Sterling Control Center in your network regardless of server-level restrictions. Manage permission allows the user to do the following functions: • Add, update, view, and remove servers and server groups • Stop Sterling Connect:Direct servers	View server and server group properties and status	Cannot view server/server group status or properties or manage servers

Function	Manage Permission	View Only Permission	None
Data Visibility Groups	Allows a user to add, update, view, and delete data visibility groups. Only Sterling Control Center administrators can manage data visibility groups. To qualify as an administrator, the role must not be server or data visibility group-restricted and must have "manage" authority to required elements. If a role qualifies as an administrator, the "manage" permission is allowed; otherwise, only "view" or "none" are allowed.	View data visibility groups	Cannot view data visibility groups
Processes	Delete, suspend, or release processes. View process statistics and properties	View process statistics and properties	Cannot view process statistics and properties or manage processes
Alerts	Delete and view Sterling Control Center alerts	View Sterling Control Center alerts.	Cannot view Sterling Control Center alerts or manage alerts
Calendars	Create, change, delete, and view calendars	View calendars	Cannot view or manage calendar functions
SLCs/Schedules	Create, change, delete, and view SLCs and SLC schedules	View SLCs and SLC schedules	Cannot view or manage SLC schedules
Rules/Schedules	Create, change, delete, and view rules and rule schedules	View rules and rule schedules	Cannot view rules or manage rules schedules
Actions	Create, change, delete, and view actions	View actions	Cannot view actions or manage actions
Email Lists	Create, change, delete, and view email lists for automated reports	View email list information	Cannot view email list information or manage email lists
Users	Add, change, delete, and view user information	View user information	Cannot view user information or manage users
Roles	Add, change, delete, and view subordinate roles	View role information	Cannot view role information or manage roles
Reports/ Schedules	Generate and view standard Sterling Control Center reports	Cannot access the Sterling Control Center reports function	Cannot access the Sterling Control Center reports function
Automated Reports	Add, change, delete, and view automated report setup information	Cannot access Sterling Control Center automated reports	Cannot access Sterling Control Center automated reports
System Settings	Create, change, and view Sterling Control Center system settings	View Sterling Control Center system settings	Cannot view or change Sterling Control Center system settings
Mobile Device	Can access Sterling Control Center from a mobile device to: • View and handle alerts • View properties of objects that are associated with alerts • monitor server, adapter, and daemon status	N/A	Cannot access Sterling Control Center from a mobile device

Function	Manage Permission	View Only Permission	None
Web Access	Auto Login: Allow the user to automatically log in to IBM Sterling Connect:Direct Browser User Interface from the Sterling Control Center console without requiring password authorization	Prompt: Allow the user to log in to IBM Sterling Connect:Direct Browser User Interface from the Sterling Control Center console after requiring password authorization	N/A
Console Auto Refresh	Allow the role to set the **Console Auto Refresh** value in **System Settings** (**Console Settings** tab) and to set their own refresh setting in **Tools** > **Console Preferences**.	Use system setting. Does not allow the role to set Auto Refresh setting or set their own Console Preferences setting.	Require the role to refresh a monitor through one of the following methods: • Clicking the monitor **Refresh** button • Selecting the **Server** > **Manual Refresh** menu item • Pressing the **F5** key
Console Timeout	Allow the role to set the **Time out after *n* minute(s) of inactivity** and the **Display warning message *n* minute(s) before timing out** values in **System Settings** (**Console Settings** tab) and to set their own timeout setting in **Tools** > **Console Preferences**.	Use system setting. Does not allow the role to set Console Timeout settings or set their own Console Preferences setting.	Console Timeout feature is not used. User will not be logged out due to inactivity.

For Web Access permissions, select **Auto Login** to allow a role to automatically log in to one of the following selected server types:

- Sterling Connect:Direct server with the IBM Sterling Connect:Direct Browser User Interface
- Sterling B2B Integrator server with the Sterling B2B Integrator Dashboard
- Sterling File Gateway server with myFileGateway

Attention: Even if you select **Auto Login** for a role, if a Connection Dashboard Port value is not specified for a Sterling B2B Integrator managed server, automated login is not functional. As a result, the Sterling B2B Integrator Dashboard option on the **Manage** menu is dimmed and cannot be selected.

Select **Prompt** to require the role to provide a user ID and password to log in.

Node configuration permissions

In addition to permissions pertaining to general use of Sterling Control Center, a role can be assigned permissions with respect to configuration management capabilities.

These permissions are described in the following table:

Function	Manage Permission	View Only Permission	None
Templates	Create, update, and delete templates used in creating Sterling Connect:Direct server configuration objects.	View and use templates to create server configuration objects.	N/A

Function	Manage Permission	View Only Permission	None
Netmap Entries	Create, update, delete entries for the netmaps of Sterling Connect:Direct servers.	View netmap of Sterling Connect:Direct servers.	No netmap permissions.
Initialization Parameters	Create, update, delete initialization parameters for a Sterling Connect:Direct server.	View Initialization parameters for a Sterling Connect:Direct server.	No Sterling Connect:Direct server initialization parameter permissions.
User Proxies	Create, update, delete user proxies.	View user proxies for Sterling Connect:Direct servers.	No user proxies permissions.
Functional Authorities	Create, update, delete functional authorities.	View user and group functional authorities for Sterling Connect:Direct servers.	No functional authorities permissions.
Secure+ Entries	Create, update, and delete entries for Sterling Connect:Direct Secure Plus objects.	View Sterling Connect:Direct Secure Plus objects objects.	No permissions for Sterling Connect:Direct Secure Plus objects objects.

Creating a role

Create roles to specify the Sterling Control Center actions users can perform and the servers and server groups they can perform these actions on.

About this task

CAUTION:
If you change permissions or restrictions for the superuser role, you cannot reverse them without reinstalling Sterling Control Center or manually restoring the superuser role. For information about manually restoring this role, see *Manually restoring the superuser role***.**

To create a role:

Procedure

1. Select **Control Center** > **Roles** from the Sterling Control Center window to display the **Roles** listing.
2. Click the Create button to display the **Create Role** wizard.
3. Define a name for the role and provide a description and click **Next**. See *Role field descriptions* for definitions of all role fields.
4. For restricted roles, select the server groups and/or data visibility groups to which this role should have access and click **Next**.
5. Define the permissions to associate with the role and click **Next**. Refer to *Permissions* for a description of the permissions.
6. Define the node configuration permissions to associate with the role. Refer to *Node configuration permissions* for a description of the node configuration permissions. Click **Next**.
7. Confirm your selections and click **Finish**. Click **Close** to exit the wizard.

Results

The role is displayed in the **Roles** listing.

Displaying the roles listing

You can display a listing of the roles defined for Sterling Control Center.

About this task

To display the roles listing:

Procedure

1. From the Sterling Control Center window, select **Control Center** > **Roles**.
2. To sort a column, click its heading.

Viewing or changing a role

If you have the requisite permissions, you can view the information that defines a role or change its information.

Before you begin

Attention: If you change permissions or restrictions for the superuser role, you cannot reverse them without reinstalling Sterling Control Center or manually restoring the superuser role. For information about manually restoring this role, see *Manually restoring the superuser role*.

To view or change a role:

Procedure

1. Select **Control Center** > **Roles** from the Sterling Control Center window to display the **Roles** listing.
2. Do one of the following to display the **Role Properties** window:
   - Select a role and click the **Properties button**.
   - Double-click a role
3. Click the **General**, **Restrictions, Permissions**, **Node Configuration Permissions**, and **Summary** tabs to view and change the role property information as needed. See *Role field descriptions* for definitions of the fields.
4. Click **Update**. The role property information is updated.

   If you change role information for a user who is currently signed on to Sterling Control Center, the user's permissions are immediately affected. For example, if a role change removes access to certain functions, those functions are immediately unavailable to the user.

Role field descriptions

You can use the following fields to define a role.

Note: If you modify a role that has Server Group or Data Visibility Group restrictions by removing both the Server Group and Data Visibility Group restrictions, the role is changed from restricted to unrestricted. Any previously created object that has this role in its list of permissible roles will have this role removed.

Field	Description
Data Visibility Groups	The data visibility groups to associate with the role. To add a data visibility group, highlight a data visibility group in **Data Visibility Groups** and click the Right Arrow button. To remove a data visibility group from Selected Data Visibility Groups, highlight it and click the Left Arrow button.
Description	A description of the role.
Node Configuration Permissions	The set of configuration management actions the role can perform. See *Node configuration permissions* for a detailed description of each particular permission.
Permissions	The set of Sterling Control Center actions the role can perform. See *Permissions* for a detailed description of each particular permission.
Role Name	The name for the role. A role defines a set of permissions that specify what Control Center actions a user can perform and what managed servers he or she can perform these actions upon.
Server Groups	The server groups to associate with the role. To add a server group, highlight a server group in **Server Groups** and click the Right Arrow button. To remove a server group from **Selected Server Groups**, highlight it and click the Left Arrow button.

Manually restoring the superuser role

If you have deleted the superuser role or modified it and need to restore it, you can manually restore the superuser role.

About this task

To manually restore the superuser role:

Procedure

1. Stop the Sterling Control Center engine.
2. Open the superuser.xml file located in conf\roles.
3. Replace the file's contents with the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<role>
        <actions>manage</actions>
        <alerts>manage</alerts>
        <autorefresh>arman</autorefresh>
        <calendars>manage</calendars>
        <desc>Administrator role definition</desc>
        <dvgs>manage</dvgs>
        <emailLists>manage</emailLists>
        <functionalauth>manage</functionalauth>
        <id>superuser</id>
        <initparms>manage</initparms>
        <mobileDevice>manage</mobileDevice>
        <netmap>manage</netmap>
```

```
        <processes>manage</processes>
        <reports>manage</reports>
        <roles>manage</roles>
        <rules>manage</rules>
        <scheduledReportGroup>manage
</scheduledReportGroup>
        <secureplus>manage</secureplus>
        <serverConfigTemplates>manage
</serverConfigTemplates>
        <servers>manage</servers>
        <slcs>manage</slcs>
        <systemSettings>manage</systemSettings>
        <templates>manage</templates>
        <userproxy>manage</userproxy>
        <users>manage</users>
        <ver>1</ver>
        <viewEngineLogs>view</viewEngineLogs>
        <webAccess>manage</webAccess>
</role>
```

4. Save the file.
5. Restart the Sterling Control Center engine.

Manage users

Before a user can log in to Sterling Control Center, the user must be defined. Use the Users listing to add users, modify user definitions, and remove users.

For each user you define, you must identify one or more of the following criteria by which to authenticate the user:

- Password
- Host Name
- Microsoft Windows Domain
- TCP/IP Address

Note: If you are using IBM Sterling External Authentication Server, you do not need this authentication criteria.

Information is required in one of these four fields. If the user fails to provide the authentication information, an error message warns the user that the information is required.

Additionally, you must define the role each user is authorized to perform when you define the user.

Sterling Control Center ships with a default admin user ID named “admin.” Keep in mind the following when dealing with this user ID:

- You cannot delete it.
- It is assigned the superuser role.
- You can change this user's role to something other than superuser.

Adding users

You can add users to Sterling Control Center.

About this task

To add a user to Sterling Control Center:

Procedure

1. Select **Control Center** > **Users** from the Sterling Control Center window to display the Users listing.
2. Click the Create button to display the Add User window. See *User field descriptions* for detailed definitions of the fields that comprise user information.
3. Type the User ID for the user you are defining.
4. Provide information in at least one of the following fields to authenticate the user during sign-on:
   - Password and Retype Password
   - Host Name
   - Windows Domain (except Web console)
   - TCP/IP Address

   Note: If you are using IBM Sterling External Authentication Server, you can skip this step.

   Note: Information is required in at least one of these four fields to authenticate the user. If the user fails to provide authentication information, an error message warns the user that the information is required.
5. Supply an optional description.
6. Select a **Role** to assign to the user.

   Note: You can create a role by clicking the Create button next to **Role**. You can duplicate an existing role and modify the duplicate by clicking the Duplicate button. View role properties by selecting the role and clicking the Properties button.
7. Click **OK**. The user is added to the **Users** listing.

Viewing and changing user information

You can view and change user information if you have "manage" permission to do so.

About this task

To view and change user information:

Procedure

1. Select **Control Center** > **Users** from the Sterling Control Center window to display the **Users** listing.
2. Do one of the following to display the **User Properties** window:
   - Select a user and click the Properties button
   - Double-click a user
3. Change the information as required and click **Update**. (See *User field descriptions* for descriptions of the **Users** listing fields.)

User field descriptions

You can use many fields to describe the fields that define Sterling Control Center users.

Field	Description
User ID	User identification. A code used to identify and authenticate a user who wants to access Sterling Control Center.
Password	A code the user enters to gain access to Sterling Control Center.
Host Name	The host computer through which the user accesses Sterling Control Center and IBM Sterling External Authentication Server.
Windows Domain	The Microsoft Windows domain from which the user signs in.
TCP/IP Address	The IP address from which the user can sign in.
Description	Descriptive information about the user.
Role	The role, with its attendant permissions, that is assigned to the user.

Configuring account lockout for failed login attempts

You can configure account lockout for an excessive number of failed user login attempts.

Before you begin

Setting account lockout requires knowledge of XML file editing.

About this task

Account lockout is configured in the `conf/security/loginPolicy.xml` file. You can set the maximum number of failed attempts before a user account is locked out for a specified number of minutes. For example, based on the default values, a user is locked out if they enter an incorrect password 3 times. The user remains locked out for 15 minutes. To configure account lockout for failed login attempts:

Procedure

1. Open the *Sterling Control Center installation*`/conf/security/loginPolicy.xml` file with a text editor such as Microsoft NotePad. The following example shows the default loginPolicy.xml file.

```
<?xml version="1.0" encoding="UTF-8"?>
<loginPolicy>
<enabled>true</enabled>
<maxFailedLogins>3</maxFailedLogins>
<lockoutDuration>15</lockoutDuration>
</loginPolicy>
```

2. To set the number of maximum failed login attempts before an account is locked out, type a value between the <maxFailedLogins> and </maxFailedLogins> tags. The default is 3.
3. To set the amount of time (in minutes) that an account is locked out, type a value between the <maxLength> and </maxLength> tags. The default is 15 minutes.
4. Save the loginPolicy.xml file.
5. Restart Sterling Control Center.

Set password policy

If you require a password to authenticate users, you can configure Sterling Control Center to accept only passwords that conform to the password policy of your organization.

The following settings can be used in your password policy:

- Minimum and maximum password lengths
- Requiring lowercase, uppercase, and special (non-alphanumeric) characters in the password

Note: The ampersand (&), greater than (>), and less than (<) symbols might not be used for special character exclusion in the passwordPolicy.xml file.

- Excluding lowercase, uppercase, and special characters in the password
- Using regular expressions (regex) to define specific password patterns
- Using regular expressions (regex) to define specific patterns to exclude

To configure Sterling Control Center to accept only passwords that conform to your password policy, modify the passwordPolicy.xml file. Any modifications you make affect only new or modified passwords. Existing passwords continue to work.

Attention: Setting password policy is an advanced procedure that requires knowledge of XML file editing. Back up the passwordPolicy.xml file before performing this procedure. If you make an XML syntax error when editing the passwordPolicy.xml file, Sterling Control Center might not start. If this occurs, either correct the passwordPolicy.xml file, or replace the edited passwordPolicy.xml file with the backup file, and then restart Sterling Control Center.

Modifying the password policy file

You can change the password policy file.

About this task

To modify the passwordPolicy.xml file:

Procedure

1. Make a copy of the passwordPolicy.xml file in *Sterling Control Center installation*\conf\security. Name it passwordPolicy.bak.
2. Open passwordPolicy.xml file with a text editor such as Microsoft NotePad. The following example shows the default passwordPolicy.xml file.

```
<!-- all nested elements are optional, so an empty password policy is valid -->
<passwordPolicy>
 <!-- available for Release 2 -->
 <matchingPatterns>
  <minLength>0</minLength>  <!-- Omission means that there is no limit -->
  <maxLength>64</maxLength>  <!-- Omission means that there is no limit -->
  <!-- <required>3</required> -->  <!-- this number must be less than or equal
   to the # patterns listed below -->
  <!-- <patterns> -->
  <!-- <pattern>[a-z]</pattern> --> <!-- patterns are Java regex patterns that
    must match -->
  <!-- <pattern>[A-Z]</pattern> -->
  <!-- <pattern>[0-9]</pattern> -->
  <!-- <pattern>\W</pattern> -->  <!-- a regex which means special characters -->
 <!-- </patterns> -->
```

```
 </matchingPatterns>
 <nonMatchingPatterns>    <!-- password patterns to exclude -->
 <!-- <patterns> -->
  <!-- <pattern></pattern> -->  <!-- passwords which match these
    patterns are not allowed -->
 <!-- </patterns> -->
 </nonMatchingPatterns>
</passwordPolicy>
```

3. To set a minimum password length, type a value between the <minLength> and </minLength> tags. For example, to set the minimum password length at six characters, type:

   ```
   <minLength>6</minLength>
   ```

4. To set a maximum password length, type a value between the <maxLength> and </maxLength> tags. For example, to set the maximum password length at 72 characters, type:

   ```
   <maxLength>72</maxLength>
   ```

5. To specify the number of patterns that a password must match:
   - Delete the comment marks (<!-- and -->) preceding and following the <!-- <required>3</required> --> tags under the <matchingPatterns> tag.
   - Type the minimum number of patterns that a password must match between the <required> </required> tags. For example, if you want a password to match at least two password patterns, type:

     ```
     <maxLength>72</maxLength>
     ```

6. To require certain characters in the password:
   - Delete the comment marks (<!-- and -->) preceding and following the <patterns> and </patterns> --> tags.
   - Delete the comment marks (<!-- and -->) preceding and following the <pattern></pattern> tags you want to require. You can use regex to define more specific password patterns. See *Regular expressions*, for more information.
7. To exclude certain characters or combinations in the password:
   - Delete the comment marks (<!-- and -->) preceding and following the <patterns> and </patterns> --> tags following the <nonMatchingPatterns> tag.
   - Delete the comment marks (<!-- and -->) preceding and following the <pattern></pattern> tags.
   - Type the pattern to exclude between the <pattern> and </pattern> tags. For example, if you want to exclude passwords with three consecutive identical characters, type:

     ```
     <pattern>(.)\1\1</pattern>
     ```

8. Save the passwordPolicy.xml file.
9. Restart Sterling Control Center.

   Note: The changed password policy takes effect when an existing user tries to change his password or a new user is created that requires a password.

Sample passwordPolicy.xml files

You can use the following sample password policy files when creating your own passwordPolicy.xml file.

The following example requires that passwords contain uppercase letters, numbers, and special characters.

```
<!-- all nested elements are optional, so an empty password policy is valid -->
<passwordPolicy>
 <!-- available for Release 2 -->
 <matchingPatterns>
  <minLength>0</minLength>  <!-- Omission means that there is no limit -->
  <maxLength>64</maxLength>  <!-- Omission means that there is no limit -->
  <required>3</required>    <!-- this number must be less than or equal to the
  # patterns listed below -->
  <patterns>
   <!-- <pattern>[a-z]</pattern> --> <!-- patterns are Java regex patterns that
   must match -->
   <pattern>[A-Z]</pattern>
   <pattern>[0-9]</pattern>
   <pattern>\W</pattern>   <!-- a regex which means special characters -->
  </patterns>
 </matchingPatterns>
 <nonMatchingPatterns>  <!-- password patterns to exclude -->
  <!-- <patterns> -->
  <!-- <pattern></pattern> -->
  <!-- passwords which match these patterns are not allowed -->
  <!-- </patterns> -->
 </nonMatchingPatterns>
</passwordPolicy>
```

The following example requires that passwords contain lowercase and uppercase letters, numbers, and exclude special characters.

```
<passwordPolicy>
  <matchingPatterns>
    <minLength>3</minLength>
    <maxLength>64</maxLength>
    <required>3</required>
    <patterns>
       <pattern>[a-z]</pattern>
       <pattern>[A-Z]</pattern>
       <pattern>[0-9]</pattern>
       <!--   <pattern>\W</pattern> -->
    </patterns>
  </matchingPatterns>
  <nonMatchingPatterns>
    <patterns>
       <pattern>\W</pattern>
    </patterns>
  </nonMatchingPatterns>
</passwordPolicy>
```

The following example requires that passwords be a minimum of 8 characters, a maximum of 64 characters, and contain at least 3 of the following patterns:

- lowercase letters
- uppercase letters
- numbers
- special characters

Also, this example does not allow three consecutive characters in the password.

```
<passwordPolicy>
  <matchingPatterns>
    <minLength>8</minLength>
    <maxLength>64</maxLength>
    <required>3</required>
    <patterns>
      <pattern>[a-z]</pattern>
      <pattern>[A-Z]</pattern>
      <pattern>[0-9]</pattern>
      <pattern>\W</pattern>
```

```
     </patterns>
</matchingPatterns>
<nonMatchingPatterns>
     <patterns>
      <pattern>(.)\1\1</pattern>
    </patterns>
  </nonMatchingPatterns>
</passwordPolicy>
```

Chapter 4. Manage Servers

Adding a server

To manage a server with Sterling Control Center, you begin by adding the server.

About this task

To add a server to Sterling Control Center:

Procedure

1. Select **Manage** > **Add Server**. The **Add Server** wizard displays.
2. Type the server name or alias and an optional description. Click **Next**.
3. Select the server type:
   - Sterling Connect:Direct with TCP/IP API:
     - Sterling Connect:Direct for HP NonStop
     - Sterling Connect:Direct for UNIX
     - Sterling Connect:Direct for Microsoft Windows
     - Sterling Connect:Direct for z/OS®
   - Sterling Connect:Direct for i5/OS™
   - Sterling Connect:Enterprise® for z/OS
   - Sterling Connect:Enterprise for UNIX
   - Sterling B2B Integrator (SI)
   - Sterling Connect:Express for z/OS
   - Sterling Connect:Express for UNIX or Microsoft Windows
   - MQ MFT
   - IBM QuickFile
   - File Transfer Protocol (FTP) Server – z/OS or WS_FTP
   - File Transfer Protocol (FTP) Server – xferlog
   - File Transfer Protocol (FTP) Server – IIS
   - File Transfer Protocol (FTP) Server – W3C
4. Use the information that you collected in *Adding a server* to complete either the **Connection** page or the **OS Type** and **SNMP Connection** pages of the **Add Server** wizard, depending on the server type.
5. For FTP servers that use an xferlog or IIS log format, click **Advanced** on the **Connection** page and verify the log file format. For more information, see the *Server field descriptions*. After you are finished, click **Update** to continue.
6. For Sterling Connect:Direct with TCP/IP API servers, click **Test Connection** to validate the connection information.

   Important: For QuickFile and Sterling Connect:Express for z/OS servers, the **Test Connection** button tests the ability of the Sterling Control Center engine to establish a connection to the message queue. Until Sterling Control Center receives a message on that message queue from the server that is being monitored, the server icon indicates that it is an uncontacted server.
7. Optionally, modify the following information when requested:

- Heartbeat Interval (Sterling Connect:Enterprise for z/OS, Sterling Connect:Express for z/OS, MQ MFT, and QuickFile only)
- Source Port Numbers (Sterling Connect:Direct with TCP/IP API, FTP Server, QuickFile, and Sterling Connect:Enterprise for UNIX)
- Monitor Rest Time
- Time Zone
- Use above Time Zone and ignore server-provided UTC Offset
- Start License Notification nn days prior to expiration

8. To specify advanced server settings, click **Advanced** and specify values for the following fields, clicking **Update** to return to the Settings wizard panel:
   - Graphical Activity Monitor expected maximum processes
   - Metadata Rule Handling
   - Max Completed Processes
   - Whether Business Processes are to be monitored (Sterling B2B Integrator only)
   - Whether Sterling File Gateway activity is to be monitored (Sterling B2B Integrator only)
   - Connection Timeout
   - Tracing

     Attention: Do not select **Tracing Enabled** unless instructed by IBM customer support personnel. Tracing significantly impacts performance.
   - Check for Configuration Changes (Sterling Connect:Direct with TCP/IP API servers)
   - Minimum Number of Versions (Sterling Connect:Direct with TCP/IP API servers)
   - Minimum Age of Versions (Sterling Connect:Direct with TCP/IP API servers)
9. Optionally, add this server to a server group by selecting a group name in Groups and moving it to Selected Groups by clicking >.
10. Optionally, specify server metadata in any of the 10 Server Metadata fields; then, click **Next**. The metadata fields are freeform and can be defined in whatever way makes sense for your operation. You can use the metadata fields in reporting and filtering.
11. Supply contact information for this server:
    - Name
    - Phone
    - E-mail
    - Comments
12. When you complete the wizard, click **Finish**. The server is added to Sterling Control Center. An icon for the server appears in the node tree pane of the Sterling Control Center window.

Results

- If the server icon is overlaid with a question mark (?), one of the following might apply:
  - The server is not available and Sterling Control Center does not allow it to be managed
  - You made a data entry error (such as typing an incorrect IP address) in the **Add Server** wizard.

- If the server icon is overlaid with a universal no symbol, check your login information.
- If the server name is printed in red or the server down icon is displayed before the server name, the server is down. Review the CCEngine log to investigate the problem. Use Server Properties to correct any errors. For more information, see *Viewing or changing server properties*.

What to do next

You can group servers together to meet the needs of your organization. See *Creating a server group*.

Viewing or changing server properties

After you define servers, you can view and change server properties.

About this task

To view or change server properties:

Procedure

1. In the Sterling Control Center window, double-click the server you want to view or change. The **Server Properties** window displays.
2. Click a tab to view server properties under that heading. See *Server field descriptions* for a description of each field.
3. Change the information as required and click **Update**. The server information is updated.

   Note: When you change server information, the server icon can indicate that the server is uncontacted until Sterling Control Center contacts the server again. For QuickFile servers, the **Test Connection** button tests the ability of the Sterling Control Center engine to establish a connection to the message queue. Until Sterling Control Center receives a message on that message queue from the server that is being monitored, the server icon indicates that it is an unconnected server.

   If the same user ID and password are used to log on to multiple servers, you can change the passwords for all servers at one time. For more information, see *Parameters modified in the sample log4 files* and *How can I do a bulk update of the passwords used by Sterling Control Center for monitored servers?* in *How-To*.

Setting up a server to monitor a Sterling B2B Integrator cluster via individual connections

You can monitor a Sterling B2B Integrator clustered instance whether Sterling Control Center is individually connected to each node in the Sterling B2B Integrator cluster instance, or connected to the cluster instance through a load balancer. In either case, Sterling Control Center ensures continuous monitoring of business process activities in case of a node failure and generates events if a cluster node goes down. In addition, you can see the adapter status of all cluster nodes in a single view.

About this task

Note: If nodes are dynamically added or removed from a Sterling B2B Integrator cluster monitored by Sterling Control Center, Sterling Control Center will not

automatically recognize the change. As a result, any adapters on added nodes will not be monitored until Sterling Control Center knows about those nodes. For Sterling Control Center to recognize when a node has been added or removed, you will either have to stop and start Sterling Control Center or pause and resume monitoring of the node.

To set up Sterling Control Center to monitor a Sterling B2B Integrator cluster when it is connected to each node individually:

Procedure

1. On the Sterling B2B Integrator side, create a Web Service called **SCCInteropService** on one of the nodes in the Sterling B2B Integrator cluster. When you create the web service on one of the cluster nodes, it appears on all other cluster nodes, too. This step ensures that Sterling B2B Integrator and Sterling Control Center have access to the appropriate process and file transfer data. For detailed instructions, refer to the Sterling B2B Integrator documentation.
2. On the Sterling Control Center side, add a server for the Sterling B2B Integrator cluster and for Node Type, select Sterling B2B Integrator Cluster not through a load balancer. Specify the host name and ports for each server, and put them in priority order.

Setting up a server to monitor a Sterling B2B Integrator cluster through a load balancer

You can monitor a Sterling B2B Integrator clustered instance whether Sterling Control Center is individually connected to each node in the Sterling B2B Integrator cluster instance, or when it is connected to the cluster instance through a load balancer. In either case, Sterling Control Center ensures continuous monitoring of business process activities in case of a node failure and generates events if a cluster node goes down. In addition, you can see the adapter status of all cluster nodes in a single view.

About this task

Note: If nodes are dynamically added or removed from a Sterling B2B Integrator cluster monitored by Sterling Control Center, Sterling Control Center will not automatically recognize the change. As a result, any adapters on added nodes will not be monitored until Sterling Control Center knows about those nodes. For Sterling Control Center to recognize when a node has been added or removed, you will either have to stop and start Sterling Control Center or pause and resume monitoring of the node.

To set up Sterling Control Center to monitor a Sterling B2B Integrator cluster through a load balancer:

Procedure

1. On the Sterling B2B Integrator side, create a Web Service called **SCCInteropService** in each node of the Sterling B2B Integrator cluster. For detailed instructions, refer to the Sterling B2B Integrator documentation. This step ensures that Sterling B2B Integrator and Sterling Control Center have access to the appropriate process and file transfer data.
2. Configure the load balancer in front of Sterling B2B Integrator to include the host addresses of all nodes in the cluster. The load balancer ensures continuous monitoring of business process activities in case of any node failure.

3. On the Sterling Control Center side, add one server to define the overall cluster server (load balancer) and for Node Type, select Single Sterling B2B Integrator instance or Sterling B2B Integrator through a load balancer. The host name and ports point to the load balancer, which then gets the data from the individual nodes.

Monitoring File Agents

You can configure Sterling Control Center to monitor Sterling Connect:Direct File Agents associated with Sterling Connect:Direct servers. While you do not add File Agents like a server, you do need to configure Sterling Control Center to monitor them by specifying the address and port the File Agent nodes have been configured to send their traps to.

For more information on configuring Sterling Control Center to monitor Sterling Connect:Direct File Agents, see *File Agent field descriptions* and in *Setting up Sterling Control Center to monitor Sterling Connect:Direct File Agent* in *Getting Started*.

Note: File agent name must be unique for the Sterling Connect:Direct server to which it is submitting processes. If two file agents with the same name are submitting to the same Sterling Connect:Direct server, they will be treated as the same file agent.

Server field descriptions

Server fields are used to specify information about individual servers when you are creating and updating server definitions. Fields displayed depend on the server type you are configuring.

Field	Description
API Port	The API port number used to access a Sterling Connect:Direct, Sterling Connect:Enterprise for UNIX, Sterling Connect:Express for Microsoft Windows, Sterling Connect:Express for UNIX or FTP server. For Sterling Connect:Enterprise, API Port is the listening port for cmusvid. Sterling Connect:Direct default is 1363; must be 1024-65535. FTP default is 21; must be 1-65535.
Account List	The accounts on which to retrieve information. If this field is left blank, information for all accounts is retrieved. Separate accounts with commas.
Adapter Status Monitor Rest Time	The amount of time Sterling Control Center waits between polls of adapter status from Sterling B2B Integrator servers. Values are 1-60 minutes. The default is 1 minute.
Agent Address	The server address of the FTP agent.
Agent Port Number	The port number for the FTP agent.
Alerts	The number of alerts issued for this server, broken into high, medium, and low severity. Display only.
Available Fields	Fields that can be used to describe your IIS or xferlog record layout. If your FTP server log contains these fields, move them to Selected Fields. Use the Move Up and Move Down buttons to position a particular field in its proper position. Use the **<ignored-placeholder>** field if your FTP log contains a field that is not listed in Available or Selected Fields.

Field	Description
BP List	Click **BP List** to display a list of all available Sterling B2B Integrator business processes. You can select from this list the business processes that you want to monitor. **Note:** Complete the entire procedure to create the server. Then, return to the **Settings** tab in the Server Properties window to see this button.
Business Process	A list of all available Sterling B2B Integrator business processes. Click **Find** to type a string of characters to quickly look up a particular business process. Then, click the down and up arrows to move from instance to instance. Click **Refresh** to ensure that the list is up-to-date.
Channel Name	The name of the JMS channel that Sterling Control Center communicates with to receive messages.
Check for configuration changes	When to check for configuration changes in servers centrally managed by Sterling Control Center. You can choose to use the system settings, never check for changes, or check daily at a specific time.
Comments	Optional contact information for the server. Up to 255 characters. To include a link you can click, use one of the following prefixes, and then type the remaining information: http:// ftp:// mailto:// file://
Component Licenses	This display-only listing shows license information for each component licensed in Sterling B2B Integrator. The components include the following: Sequence #, Product Version, Component, Product ID, IP, Start Date, and Expiration Date.
Connection	The protocol (TCP/IP, SSL, or TLS) used for communication with a Sterling Connect:Direct TCP/IP API server.
Connection Timeout	The amount of time the Sterling Control Center engine waits for a response from a server it has attempted to contact. Do not change this value unless you are receiving timeout errors in the engine log for the server in question. The default and minimum is 30 seconds; 120 seconds for Sterling B2B Integrator servers. Maximum value is 600 seconds.
Customer Name	The name of the customer to whom the license was issued. Display only.
Dashboard Port	The port for accessing the Sterling B2B Integrator dashboard.
Date/Time in Last Record Retrieved	Date and time the last record was retrieved from the server.

Field	Description
Description	A description of the server. To include a link you can click, use one of the following prefixes, and then type the remaining information: http:// ftp:// mailto:// file://
Details	Click to view license details for this server. Display only.
Do not allow configuration management on this server	Check to prevent configuration management from being performed on this server. Optional.
Do not collect process step statistics	Check this box to prevent server management from collecting statistics generated by a Process step. Optional.
Do not monitor this server	Check to prevent server management from monitoring the server. Optional.
E-mail	Server contact email address. Optional. Special characters allowed. Spaces are not allowed.
Expiration Date	Date that the managed servers license expires. Display only.
Field	This column contains the names of variables that pertain to the Sterling B2B Integrator environment.
Graphical Activity Monitor expected maximum processes: Use High Water Mark	Use High Water Mark as the maximum number of processes this server is expected to have active at one time. High Water Mark is a system-generated statistic that indicates the maximum processes active on a server since the value was last reset. Used in graphical depictions of server activity.
Graphical Activity Monitor expected maximum processes: Use other value	Click to use a value other than the High Water Mark or System Settings-Visualization. Enter a value to set the maximum number of processes the server is likely to have active at one time. The range is 0-2,147,483,647. Used in graphical depictions of server activity.
Graphical Activity Monitor expected maximum processes: Use System Settings	Click to set the maximum number of processes that the server is likely to have active at one time to the default value on the System Settings panel, **Visualization** tab. Used in graphical depictions of server activity.
Groups	The server groups to choose from. Move by selecting a server group and clicking the Right Arrow button. Optional.

Field	Description
Heartbeat Interval	For Sterling Connect:Enterprise for z/OS and Sterling Connect:Express for z/OS, the amount of time Sterling Control Center waits for an SNMP trap. For QuickFile, the amount of time Sterling Control Center waits for messages. Values are: • Sterling Connect:Enterprise for z/OS and Sterling Connect:Express for z/OS - 60-3600 seconds. The default is 900 seconds. • QuickFile - 30-3600 seconds. The default is 900 seconds. • MQ MFT - Interval in seconds within which an agent properties message must be received for the server to be considered up. The range is 30-3600 seconds. The default is 900 seconds. Set this value to twice the heartbeat interval set for the MQ MFT agents.
Hostname	The host address the JMS provider listens on.
i5/OS Host Name	The host name for the Sterling Connect:Direct for i5/OS server.
JMS Provider	The type of JMS provider: IBM WebSphere® MQ.
Last Contact At	Date and time of last contact with the server.
Last Retrieved	The date and time that the license was last retrieved and validated. Display only.
Last System Message	Last status message or messages received from the node service monitoring the server. Display only.
Library Name	The host name for the Sterling Connect:Direct for i5/OS server.
License Key	Server license key. Display only.
License Push Supported/Not Supported	The IBM product specified in the license key. Display only.
License Type	Type of license in place for the server. Display only.
Limit	The maximum number of queued processes allowed for this server before Sterling Control Center generates an event. If the limit is exceeded, Sterling Control Center generates an event of type Server Status with a message ID of CCNS020E. When the actual number of processes (depth) falls at or below the limit, Sterling Control Center generates a Server Status event with a message ID of CCNS030I. You can write a rule to trigger an alert on either of these server status events. For more information, see *Creating a rule*.
Location	Location of Sterling B2B Integrator installation files.

Field	Description
Log File Name/Directory	Name of the FTP log file and its directory path or both. If the FTP server log has a static name, specify the directory and file name, for example, `C:\FtpServer\Logs\server.txt`. If the FTP server log is dynamic, such that it changes every day or hour, specify only the directory without a file name, for example, `C:\FtpServer\Logs`. If the directory contains files other than the managed FTP server log files, qualify what you enter. When you do this, Sterling Control Center monitors only information from the appropriate log files. Otherwise, errors occur. For example, if all your log files start with ABC, you could enter ABC*.txt as a wildcard log name template. Or if your log files have a naming standard, such as, serverYYYY-MM-DD.log for a daily rotating log, set **Log File Name** to `C:\FtpServer\Logs\server*.log`. With this option, you can select the changing daily log name and ensure that only the FTP Server logs are processed.
Max Completed Processes	The maximum number of completed events that the engine keeps in memory and displays in the Completed Activity Monitor. Range is 1-200. Default is 100. For the server, the Completed Activity Monitor never shows more rows than this number (1 cache per server) unless data visibility groups (DVGs) are in effect. When DVGs are used, the formula is 1 cache per server for the global data visibility group + 1 cache for each specific DVG activity) resulting in: Configured number of max completed processes * # of caches For example: Server CDServer with max completed processes set at 50 CDServer with no data visibility-specific activity 50 max completed processes * 1 (cache) = 50, resulting in 50 rows displayed CDServer with activity from 1 data visibility group 50 max completed processes * 2 (caches) = 100, resulting in 100 rows displayed CDServer with activity from 2 data visibility groups 50 max completed processes * 3 (caches) = 150, resulting in 150 rows displayed
Max Concurrent Processes	The maximum number of concurrent sessions that have occurred on the server, the number of times that this maximum was reached, and the last date and time that the maximum was reached. This information is display only, although it can be reset to zero. See *Resetting the maximum concurrent session count for a server.*
Metadata Rule handling: Apply Metadata Rules to statistics	Select to apply metadata rules to statistics for this server. For more information, see *Metadata rules overview*.

Field	Description
Minimum age of version	The minimum number of days that Sterling Control Center retains a configuration object version. You can specify that this value default to the one in System Settings or override it with a different value.
Minimum number of versions	The minimum number of versions retained by Sterling Control Center for each configuration object type. You can specify that this value default to the one in System Settings or override it with a different value.
Monitor	Check to monitor the queue.
Monitor Business Processes	Check to monitor Sterling B2B Integrator business processes.
Monitored	Business processes being monitored by Sterling Control Center. Clear to exclude.
Monitor File Gateway Activity	Check to monitor Sterling B2B Integrator events and activities.
Monitor Rest Time	The amount of time Sterling Control Center waits before polling the server to check status and collect statistics. Values are: • Sterling Connect:Direct - 5-86400 seconds. The default is 60 seconds. • Sterling Connect:Direct for i5/OS - 1-86400 seconds. The default is 60 seconds. • Sterling B2B Integrator - 5-86400 seconds. The default is 60 seconds. • Sterling Connect:Enterprise for UNIX - 1-1440 minutes. The default is 1 minute. • Sterling Connect:Express for Microsoft Windows and Sterling Connect:Express for UNIX - 1-86400 seconds. The default is 60 seconds. • MQ MFT - 1-86400 seconds. The default is 60 seconds. • FTP servers - 1-86400 seconds. The default is 30 seconds.
Name	A contact name for the server. Optional. Up to 50 characters.
Name or Alias	The name or alias that identifies a server in the Sterling Control Center window, up to 25 characters. The name/alias must be unique within Sterling Control Center. Typically, the name or alias is the Sterling Connect:Enterprise, Sterling Connect:Direct, Sterling B2B Integrator, or FTP server name.
Node Type	Type of Sterling B2B Integrator or MQ MFT node. For Sterling B2B Integrator, possible values include a single instance or cluster not through a load balancer. For MQ MFT, possible values include a single Queue Manager instance or through a load balance, or a multi-instance Queue Manager.
Operating System	The server operating system. Display only.
Password	The 1–64-character password (1–8 characters for z/OS) associated with the user ID. This field is required and is case sensitive. For QuickFile, this is the password to access the message queue in QuickFile. The default userid/password for QuickFile is eventmon/password.

Field	Description
Phone	Server contact phone number. Optional. Up to 50 characters. Optional contact information for the server. Up to 255 characters. To include a link you can click, use one of the following prefixes, and then type the remaining information: http:// ftp:// mailto:// file://
Port	The port the JMS provider listens on.
Process Data XPath	A path used to access information in a process data XML document. Must begin with the prefix, `/ProcessData`, for example, `/Process Data/ FTPClientBeginSessionServiceResults/ServerRepose/ Text.`
Processes	The number of executing and nonexecuting processes found for the server. Display only.
Product	The IBM product specified in the license key. Display only.
Protocol	The web protocol (HTTP or HTTPS) for Sterling B2B Integrator.
Protocols to Monitor	Protocols you want to monitor with Sterling Control Center: AS2, Connect:Direct, FTP, HTTP, MailboxService, MBI, OFTP, SAP, SFTP, SWIFTNet, webDAV, WMQFTE.
Queue	ID of the queue to monitor. For Sterling Connect:Direct servers, you can choose to monitor the EXEC, HOLD, TIMER, or WAIT queues. For Sterling B2B Integrator servers, you can choose to monitor Queues 0 through 9.
Queue Manager Name	The name of the JMS Queue Manager that holds the messages Sterling Control Center receives.
Reset Watermark	Click to reset the values in Max Concurrent Processes to zero. The watermarks that are reset include the maximum number of concurrent sessions, number of times that this maximum was reached, and last date and time the maximum was reached.
Retrieve	Click this button to retrieve a new version of the license for this server.
SCI Extensions	Sterling B2B Integrator system-related license and version information.
SNMP Listener Address	If your Sterling Control Center engine has a dual-homed IP stack (for example, multiple adapters), specify the IP address (up to 255 characters) to which to bind. Otherwise, Sterling Control Center binds to any available address.
SNMP Listener Port Number	The port number (1–65535) on which Sterling Control Center is to listen to receive traps from the server.

Field	Description
Selected Fields	Fields included in the FTP xferlog or IIS log file record to be monitored. **Important:** Some fields listed in the Selected Fields list are required. You cannot move required fields to the Available Fields list. They must remain in the Selected Fields list.
Selected Groups	The server groups to which the server belongs. Move a server out of Selected Groups by selecting it and clicking the Left Arrow button. Optional.
Server Address	The API address used to establish a session with the Sterling Connect:Direct, Sterling Connect:Enterprise, Sterling Connect:Express for Microsoft Windows, or Sterling Connect:Express for UNIX server.
SERVER_DATA_1	Server Metadata 1. The server metadata fields are user-definable fields for writing metadata rules and actions, and for reporting purposes Optional. For more information, see *Metadata rules overview*.
SERVER_DATA_2	Server Metadata 2. Optional.
SERVER_DATA_3	Server Metadata 3. Optional.
SERVER_DATA_4	Server Metadata 4. Optional.
SERVER_DATA_5	Server Metadata 5. Optional.
SERVER_DATA_6	Server Metadata 6. Optional.
SERVER_DATA_7	Server Metadata 7. Optional.
SERVER_DATA_8	Server Metadata 8. Optional.
SERVER_DATA_9	Server Metadata 9. Optional.
SERVER_DATA_10	Server Metadata 10. Optional.
Server is Being Monitored/Server is Paused	Allows authorized user to pause monitoring of the selected server. If the button displays “Pause,” click it to stop monitoring. If the button displays “Resume,” click it to resume monitoring.
Server Type	The type of server: • Sterling Connect:Direct with TCP/IP API • Sterling Connect:Direct for i5/OS • Sterling Connect:Enterprise for z/OS • Sterling Connect:Enterprise for UNIX • Sterling B2B Integrator • Sterling Connect:Express for UNIX or Microsoft Windows • Sterling Connect:Express for z/OS • QuickFile • MQ MFT • File Transfer Protocol Server – z/OS or WS_FTP • File Transfer Protocol Server – xferlog • File Transfer Protocol Server – IIS • File Transfer Protocol Server – W3C
Server Version	The version of the managed server. Display only.

Field	Description
Source Port Numbers	The optional port numbers used to traverse a firewall, if the managed server is behind a firewall. Each port number is 1-5 digits. Acceptable formats are nnnnn-nnnnn, or nnnnn, nnnnn, nnnnn-nnnnn. Example entries are 5555-5580, 48888-48890, and 5888, 5900-5920. The Sterling Control Center engine uses the first available source port specified when connecting to the server. If none is available, a connection cannot be made. If source ports are used, give each server at least two unique ports to choose from.
Start Certificate Expiry Notification	Select an option for the number of days before expiry of trusted or key certificates when Sterling Control Center begins generating events: 1) use the current Sterling Control Center system setting for the number of days or 2) specify the number of days for this server. **Important:** This option can be set only for servers that allow configuration management. Certificate expiry checking works only for certificates in the Sterling Control Center object repository. To ensure that your certificates are in the repository, you can manually check and add them using **Configure Servers** > **Secure+** > **Secure+ Key Certificates** or **Configure Servers** > **Secure+** > **Secure+ Trusted Certificates**. Or, you can automatically check for configuration changes on a daily basis by using the **Check for configuration changes on servers** system setting on the **Services** tab . When a certificate reaches the point when expiry notifications are to be generated, notifications are generated once a day until the certificates expiration time changes. To act upon certificate expiry events, or notifications, use the Certificate Expiry Warning predefined rule. You can use this rule to define the number of days before expiry that action is taken. To act upon certificate expiry events, or notifications, you can use the Certificate Expiry Warning predefined rule to define the number of days before expiry that action will be taken. For more information, see *How can I know when my Sterling Connect:Direct Secure Plus certificates are about to expire?* in *How-To*.
Start License Notification	The number of days before a server license expiration date to begin generating license expiration events. The range is 1-30 days. The license status is checked daily at midnight engine time. A license expiration event (event type of Server License, message ID of CCNS004E) is generated if the license expires within the specified number of days. Set this value high enough to allow time to obtain and install a new license key.

Field	Description
Subscriber Name	Unique name of the client that receives messages. Subscribers receive all messages published on a topic. For QuickFile and MQ MFT, this is a user-defined name and must be a syntactically valid JMS Client ID. **Attention:** For QuickFile and MQ MFT users: If more than one client is subscribing to the same topic on a message queue, they must use unique Subscriber Names to prevent conflicts.
System Version	The Sterling Connect:Direct, Sterling Connect:Enterprise, Sterling Connect:Express,Sterling B2B Integrator, QuickFile, MQ MFT, or FTP software version. Display only.
Time Zone	The time zone where the managed server is located. Use this option when the server's date and time settings are wrong, or a region's changeover to daylight saving time differs from the national norm. This field also shows the difference between the time zone and Coordinated Universal Time (UTC).
Topic Name	Name of the JMS topic to subscribe to where messages are published. For MQ MFT, the value is set as SYSTEM.FTE/# and cannot be changed.
Tracing	Enable or disable tracing for this server. Enabling tracing sends additional debug logging to the CCEngine log for the server. Due to the amount of data sent to the engine log, use tracing only when requested by IBM Customer Support.
User ID	The user ID used to log on to the server or message provider.
Use the above Time Zone and ignore server-provided UTC Offset	Select this option when the time zone is not provided by the server, or when it is incorrect.
UTC Offset	Difference between Time Zone and Coordinated Universal Time (UTC). Display only.
(Value)	The data values for Sterling B2B Integrator environment variables.
View License Key	Click this button to view the raw Sterling B2B Integrator license key data. Display only.
Web Service Address	Address of the Sterling B2B Integrator web service. **Restriction:** Sterling Control Center cannot monitor Sterling B2B Integrator servers using IPv6. You must specify an IPv4 address or a DNS name for the connection.
Web Service Port	The port for the Sterling B2B Integrator web service.
Welcome Message	An informational message set by the FTP administrator for users of an FTP server. The message might contain directory information, usage guidelines, unauthorized access warnings, server news, or other information.

Resetting the maximum concurrent session count for a server

After you define a server, information about it is displayed in the Server Status Monitor, including the maximum number of concurrent sessions that have

occurred, the number of times this maximum number of concurrent sessions was reached, and the last date and time when that occurred. You can reset these values to zero.

About this task

To reset the maximum concurrent session count to zero for a server:

Procedure

1. In the server list, right-click the server in question and select **Properties**.
2. In the **Server Properties** window, click the **Server Status** tab. The current value is displayed in **Max Concurrent Processes**.
3. To reset this value, click **Reset** under **Reset Watermark**.
4. Click **Update**. The watermark is reset.

Removing a server from Sterling Control Center

You cannot remove a server that is referenced by any other Sterling Control Center object including server groups, rules, SLCs, and roles.

About this task

To remove a server from Sterling Control Center:

Procedure

1. In the server list, right-click the server you want to remove and select **Remove Server**.
2. Click **OK** to remove the server. The server is removed.

   The server is removed from any open monitor windows unless it is the only item displayed in the monitor. In that case, the monitor window closes.

Manage server groups

A server group is a customized grouping of your system servers. You define your server groups in the way that makes sense to you.

For example, you can group servers by processing center or by server type. You can even group all managed servers into one group to monitor all server activity in one monitor window.

Server group definitions are system wide. For example, if you define two server groups named ConnectDir and ConnectEnt, all Sterling Control Center users in your organization (if they have the necessary permissions) will see these server groups.

You can specify server groups in Sterling Control Center permissions, rules, and SLCs.

Creating a server group

You can create server groups and assign servers to those groups.

About this task

To create a server group:

Procedure

1. Select **Manage** > **Add Server Group**. The Create Server Group window is displayed.
2. Type a unique name for the group in **Name**, optionally add a **Description**, and click **Next**.
3. In **Servers**, select one or more servers to add to the group and click the Right Arrow button. Click **Next** when finished adding servers.

   Tip: Add more than one server at a time by holding down **Shift** (for adjacent servers) or **Ctrl** (for non-adjacent servers) while selecting.

   For more on filtering the list of available servers, see *Filtering Objects*.
4. To add server groups to this group, select one or more to add to the group and click the Right Arrow button. Then click **Next**.
5. Review the details of the new group on the **Confirm Choices** wizard page, then click **Finish**.
6. Click **Close**.

Viewing or changing a server group definition

After you have created a server group, you can view or change the group's properties.

About this task

To view or change a server group:

Procedure

1. Click the **Groups** tab in the Sterling Control Center window..
2. Right-click the group and select **Properties**. The Group Properties window displays.
3. Add a server to the group by clicking the **Servers** tab, selecting the server in the **Servers** list, and clicking the Right Arrow button to move it to **Selected Servers**.
4. Remove a server from the group by selecting the server in the **Selected Servers** list and clicking the Left Arrow button.
5. Add a server group to the group by clicking the **Server Groups** tab, selecting the group in the **Server Groups** list, and clicking the Right Arrow button to move it to **Selected Server Groups**.
6. Remove a server group from the group by selecting the server group in **Selected Server Groups** and clicking the Left Arrow button.

   Tip: Select more than one server at a time by pressing **Shift** (for adjacent servers) or **Ctrl** (for non-adjacent servers) while selecting. Select all servers in a list by pressing **Ctrl + A.**
7. When finished, click **OK**.

Removing a server group

You can remove servers groups you have defined.

About this task

To remove a server group:

Procedure

1. Click the **Groups** tab in the Sterling Control Center window.
2. Right-click the group to remove and select **Remove Group**.
3. Click **OK**.

Results

When you remove a server group from Sterling Control Center, any rules, SLCs, and roles that referenced the server group are automatically updated. The servers referenced in the server group are not affected.

Resolving system server group naming conflicts

If you change system server group names and a naming conflict exists, the Sterling Control Center engine does not start. To resolve the conflict, edit the systemGroups.properties file.

About this task

When the engine detects naming conflicts between system server groups and other server groups, it outputs the following message to the log and the console and stops:

```
CGRP034E Server group IDs found with matching system server Group IDs. Edit
conf\servergroups\systemGroups.properties and change these names: {0}
```

In the previous message, {*0*} is replaced with a list of the system server group names that are creating the conflict and preventing the engine from starting.

To resolve system server group name conflicts:

Procedure

1. In a text editor, open systemGroups.properties in *InstallDirectory*`\conf\servergroups\`.
2. Edit the text after the equal sign (=) to change the system server group names identified in the error message. For information on naming guidelines, see *Changing system server group names* in *Getting Started*.

   Attention: Each system server group must have a unique name. It cannot have the same name as another system server group or a user-defined server group. If a naming conflict exists, the engine will not start until the conflict is resolved. If objects reference the old system server group name, edit the object properties to reference the new system server group name.
3. Save the file.
4. Start the engine.

Managing licenses

Sterling Control Center license management supports import of server licenses to a central license management repository and ad hoc distribution to managed Sterling Connect:Direct servers. Licensing options include assignment of a unique license key to a server and a license key shared among multiple servers.

About this task

When a new license key is pushed to a managed server, the server validates the new key and, assuming a valid key, copies it to the appropriate location and begins to use it.

In addition to manually importing licenses, you can set up Sterling Control Center to automatically import license key files received via email. You can then manually push those licenses to the appropriate servers. For more information see *Pushing licenses to servers* and *Automatically importing licenses*.

Note: To push new license keys or make changes to existing keys for a Sterling Connect:Direct server, the user ID used by Sterling Control Center to connect to the server must have administrator authority on that server. For Sterling Connect:Direct for z/OS, you must also have an additional authorization flag turned on for the Update license key function. For more information about setting the authorization flag, see *Functional Authority Privileges* in *IBM Sterling Connect:Direct for z/OS Administration Guide*.

To manage licenses:

Procedure

Select **Tools** > **License Management**. The License Management listing displays. The License Management listing contains license information in two tabbed panes: **Import** and **Push**. The Import pane is for importing license data into the Sterling Control Center engine License Management repository. The **Push** pane is for pushing imported licenses to managed servers enabled for license push.

Manually importing licenses

Before you can push licenses to servers, you must import them into Sterling Control Center.

About this task

To manually import licenses into Sterling Control Center

Procedure

1. On the **Import** pane of the **License Management** listing, click **Import**. The **Import License Key File** wizard displays, starting with the **License Key Text** page.
2. Do one of the following:
   - Type or paste license key text into the **License Key Text** text box.
   - Click **File** to navigate to and import a text file containing the license key text.
3. Click **Next** to move through succeeding wizard pages, supplying license ID information and selecting servers to apply the license to.

   Tip: You can create a new version of an existing license by selecting an existing license ID. You cannot create a new version of a license if a previous version is assigned to a server to which you do not have access.
4. Click **Finish** on the **Summary** page and then **Close** to exit the **Import License Key File** wizard.

Viewing and comparing licenses

Before you push updated licenses to a managed server, you can compare a new license to the current server license.

About this task

To view and compare licenses:

Procedure

1. Do one of the following:
   - Select a license in the **License Management** listing (**Import** or **Push** tab) and click **Properties**.
   - Double-click the license.
   - Right-click the license and select **Properties**.
2. To select a license version for a managed server, on the **Push** tab of the **License Management** listing, select a server and click its **License to Push** button. Only servers that support license push are shown.
3. In the **Select a License and a Version** window, select a license and version and click **OK**.
4. To compare license details with those of the license currently assigned to a server:
5. Right-click the license in the **License Management** listing and select **Compare**. The Compare License Keys window displays. The details of the selected license key and the one currently assigned to the server are displayed side by side. If they match, the message text `Matches: True` is displayed. If they do not match, `Matches: False` is displayed in red and any differences are displayed in red.
6. To compare against a different license key on the **License Management** listing, select another license key from either drop-down list.

Deleting licenses

You can delete licenses from Sterling Control Center.

About this task

To delete a license from Sterling Control Center:

Procedure

1. Do one of the following:
   - Right-click the license in the **License Management** listing and select **Delete**.
   - Select the license and click the **Delete** button.
2. Click the appropriate version of the selected license in **Select License–Version** and click **OK**.

License import field definitions

There are many fields pertaining to importing licenses for servers in Sterling Control Center.

The following table defines the fields pertaining to importing licenses for servers.

Field	Description
License ID	The license identifier.

Field	Description
# of Versions	The number of available versions of the license.
Imported By	The user who imported the license.
Imported Date/Time	Date and time of the license import.
Platform	The operating system that this license applies to (if available).
Exp. Date	Expiration date of the license (if available).

Pushing licenses to servers

From the **License Management Push** tab, you can disable or enable licenses for pushing and view the properties of servers enabled for pushing. You can push imported licenses to servers that have been enabled for pushing.

About this task

To push licenses to servers:

Procedure

1. Enable or disable servers for pushing by doing the following as needed:
   - Enable a disabled server for pushing by selecting the server (Shift-click to select contiguous servers; Ctrl-click to select non-contiguous servers) and clicking **Enable for Push**.
   - Disable servers for pushing by selecting the servers and clicking **Disable for Push**.
2. Push a license to a server by selecting the server and clicking **Push**.
3. Cancel the push operation by clicking **Stop Push**.
4. When the push operation is complete, consult the **Last Push Result** and **Last Push Message** columns to check on the operation's success. If the operation was unsuccessful, Last Push Result is highlighted in red.

License push field definitions

There are many fields pertaining to pushing licenses to servers in Sterling Control Center.

The following table defines the fields pertaining to pushing licenses to servers.

Field	Description
✔	A checkmark indicates that the server is enabled for license push.
Server	The server to which the license is to be pushed.
License to Push	The license to be pushed, that is, sent to the selected server for validation and use.
Last Pushed License	The license that was last successfully pushed to this server.
Matches Current Server License?	Indicates whether this license matches the one currently being used by the server (Y/N).

Field	Description
Last Push Attempt	The date and time when the last license push was attempted for this server.
Last Push Result	The date and time when the last license push was attempted for this server.
Last Push Message	The message returned from the last attempted push.

Automatically importing licenses

You can configure Sterling Control Center to automatically import licenses.

About this task

Besides manually importing licenses, you can configure Sterling Control Center to monitor a POP3 or IMAP mailbox for e-mails containing license key file attachments. If it finds a license key attachment in the mailbox, Sterling Control Center validates the license and, if it is found to be valid, imports it into the License Repository. You can then push the license to the appropriate server or servers. For more information on pushing licenses, see *Pushing licenses to servers*.

Note: The e-mail mailbox should be considered as belonging to Sterling Control Center and should not be shared with any other user.

An event is generated when the license is validated and imported, or when the license does not validate. The e-mail is deleted from the mailbox whether or not it has an attachment. You can create a rule to notify you when one of these license events occurs so you can take the appropriate action.

To set up automatic license import:

Procedure

1. Click **Control Center** > **System Settings**. The **System Settings** dialog displays.
2. Click the **License Management** tab.
3. Enter the **E-mail User** and **Password** for the email account to monitor.
4. Enter the email server's **Host Name** and **Host Port** number.
5. Enter the **E-mail Protocol** (POP3 or IMAP) used.
6. Enter the **Frequency**, in minutes, with which to check for incoming emails with license attachments.
7. Click **Update**.

Chapter 5. Manage Rules and Actions

Manage rules

A rule is a system instruction that you create and Sterling Control Center executes automatically. For example, you can define a rule to monitor server status and generate an alert if a server error occurs.

For more information about rules, see *Implementation*.

Rules consist of the following parts:

- Criteria that must be met in order for the rule to be applied; for example, a certain return code generated by a file transfer. All criteria in a rule must be met for the rule to be applied. To see a complete list of criteria you can monitor, see *Keys and Fields*.
- One or more schedules that may be associated with a rule. If a schedule is associated with a rule, the rule is applied when the rule's criteria are met and a schedule associated with the rule matches. For more information about schedules, see *Schedules overview*.
- An action that is performed when the criteria are met; for example, sending a notification e-mail or generating an alert when a file transfer completes. For more information, see *About actions*.

After you create a rule, it is displayed in the Rules listing. For more information about the Rules listing, see *Displaying the rules listing*.

Sterling Control Center provides predefined actions that generate alerts and predefined rules, including ones that monitor for SLC messages. You can use these actions and rules when creating SLCs to monitor Processes or file transfers. You can also modify the actions and rules as necessary to meet your processing requirements. See *Using predefined actions and rules in SLCs* for how to use predefined rules.

Creating a rule

Create rules to provide system instructions that Sterling Control Center executes automatically.

About this task

You can also use predefined rules provided with Sterling Control Center. For more information, see *Predefined actions and rules*. For an overview of how rules are used by Sterling Control Center, see *Implementation*.

Note:

Sterling Control Center comes with a standalone utility that simplifies creation of multiple actions, rules, and other Sterling Control Center objects. The utility is described in *Create multiple objects*.

To create a single rule:

Procedure

1. Select **Manage** > **Rules and Actions** > **Rules** from the Sterling Control Center window. The **Rules** listing is displayed.
2. Click the Create button to display the **Create Rule** wizard.

   For descriptions of Rules fields, see *Rules field descriptions*.
3. Type a **Name** and **Description** for the rule, click **Enable** to enable it, and click **Next**.
4. Specify one or more parameters to further define the rule by choosing a **Key** and **Operator** and entering a **Value**. The list of operators depends on whether the parameter is numeric (Return Code and File Size) or alphanumeric. For more information on the keys you can use in parameters, see *Keys and fields*. Click **Next**.

   Tip: When choosing multiple Values for a single Key, separate the Values with a pipe (|) character and use Reg Ex as the Operator.
5. Select one or more **Schedules** to associate with the rule by moving the schedule (using the Right Arrow button) from **Rule / Metadata Schedules** to **Selected Schedules**. Click **Next**.

   Tip: Create a new schedule by clicking the Create button for **Rule / Metadata Schedules**. You can duplicate an existing schedule and modify the duplicate by clicking the Duplicate button. View the properties of a schedule in either **Rule / Metadata Schedules** or **Selected Schedules** by selecting the schedule and clicking the Properties button.
6. Select an **Action** to perform when the defined parameters and schedules are met. For a linked rule, this is the first action to complete when Sterling Control Center detects the initial condition. (For more on actions, see *About actions*.) Click **Next**.

   Tip: Create a new action by clicking the Create button next to **Action**. You can duplicate an existing action and modify the duplicate by clicking the Duplicate button. View an action's properties by selecting the action and clicking the Properties button.
7. If this is a linked rule, take the following steps: Click **Enabled** to enable the linkage. Specify the **Parameters** (conditions) under which the linked rule is to be triggered. Specify a **Resolution Action** to take if the linked rule's condition is resolved before the timeout period elapses. Specify a **Non-Resolution Action** to take if the condition remains unresolved after the timeout period has elapsed. And specify the **Timeout** period in minutes.

   Attention: Process events (Process Started, Process Step Started, Process Step Ended, and Process Ended) are all generated at the same time by Sterling Control Center for Sterling Connect:Enterprise for z/OS, Sterling Connect:Enterprise for UNIX, QuickFile, and most native FTP servers because Sterling Control Center only “sees” the file transfer ending event. Be aware of this when writing linked rules for process events for these types of servers.
8. Click **Next** and then **Finish** to add the rule to the **Rules** listing.
9. Click **Close** to close the **Create Rule** wizard.

Results

After you create a rule, it is displayed in the Rules listing. Enabled rules are applied in the order in which they are listed. Therefore, rules with specific criteria should precede rules with general criteria. Only one rule per rule set is triggered

per event, so if the first rule is too general, a match always occurs and subsequent rules are ignored.

Displaying the Rules listing

The Rules listing lists all rules along with a description and information about their status. You can display the listing and sort the columns of information.

About this task

To display the Rules listing:

Procedure

1. From the Sterling Control Center window, select **Manage** > **Rules and Actions** > **Rules**.
2. To sort on any column, click the column heading.

   The following icons are displayed in the Rules listing to indicate status of a rule:

Icon	Description
	The rule is enabled.
	The rule can be edited by the user who is viewing the rule.
	1 schedule is associated with the rule and the schedule is enabled.
	1 schedule is associated with the rule and the schedule is disabled.
	Multiple schedules are associated with the rule and all schedules are enabled.
	Multiple schedules are associated with the rule and some of the schedules are enabled.
	Multiple schedules are associated with the rule and all of the schedules are disabled.
	The rule is a linked rule.

Using data visibility groups to view rule sets

From the Rules listing, you can use data visibility groups as a means to filter rules into rule sets.

About this task

To view rules by data visibility group:

Procedure

1. From the Sterling Control Center window, select **Manage** > **Rules and Actions** > **Rules**.
2. From the **Rule Set** drop down list, select **Global** to view rules that do not have a data visibility group, or select one of the data visibility groups.

Tip:
For a data visibility restricted user, the list will contain only the data visibility groups included in the user's role. An unrestricted user will see the Global rule set and all of the data visibility groups.

3. To view a different rule set, select a data visibility group from the **Rule Set** drop down list.

Viewing or modifying rule properties

You can view and change the properties that define a rule.

About this task

To view or modify rule properties:

Procedure

1. **Select Manage** > **Rules and Actions** > **Rules** from the Sterling Control Center window to display the **Rules** listing.
2. Do one of the following to display the **Rule Properties** window:
   - Double-click a rule.
   - Select a rule and click the Properties button.
3. Select tabs to display property subgroups and modify properties as necessary. See *Rules field descriptions* for descriptions of rules fields.

   Important: You must have permission to edit the rule. Edit permission is denoted by the Edit Permissions icon.
4. Click **Update**.

   Tip: If you modify the data visibility group setting in the rule parameters, the Rules listing changes the rule set to the new data visibility group value. The updated rule is displayed in the rule listing when the update is complete.

Rules field descriptions

There are many fields pertaining to rules in Sterling Control Center.

The following table describes the fields that define a rule:

Field	Description
Rule Name	The name of the rule. Required.
Description	Text describing the rule. Optional.
Enabled	Select this option to enable the rule. By default rules are enabled when first created.

Field	Description
Parameters	Selection criteria for further defining the rule. Choose a Key and Operator and enter the Value you want to monitor. For more information about parameters, see *Keys and fields* You must enter at least one parameter. A specific server or server group is required for a server restricted role. A data visibility group is required for a data visibility restricted role. When choosing multiple values for a single key, separate the values with a pipe (|) character and use Reg Ex as the Operator. For easy message ID lookup for Sterling Control Center messages, select **Message Id as the Parameter, Matches as the Operator**, and then click the **Elliptical Icon** in the **Value** field. To find and select a message, type any part of the Message ID or text to display matching messages, and click **Insert**. Lists are provided for other keys as well, such as Event Type, Data Visibility Groups, and Servers and Server Groups.
Schedules	Schedules to associate with the rule. To add a schedule to the rule definition, highlight the schedule in **Rule / Metadata Schedules** and click the Right Arrow button. To disassociate a schedule from a rule, highlight the schedule in Selected Rule Schedules and click the Left Arrow button.
Action	The action to perform when the defined parameters and schedules are met. An action is the activity or activities that Sterling Control Center performs when an event triggers a rule. For more information about the types of activities an action can perform, see *About actions*.
Linked Rules: Enabled	Click **Enabled** to make this rule a linked rule. A linked rule specifies a second condition and an action that is performed if the second condition is not resolved within a user-specified timeout period.
Linked Rules: Parameters	The parameters that describe the condition under which the linked rule is triggered. For more information, see *Creating a rule*.
Linked Rules: Resolution Action	The action to take if the second condition specified in the Linked Rules: Parameters field is met before the timeout period elapsing.
Linked Rules: Non-Resolution Action	The action to take if the second condition specified in the Linked Rules: Parameters field is not met before the timeout period elapses.
Timeout	The amount of time after the first conditions are met within which, if the second conditions are met, the resolution action will be taken. If the second conditions are not met within the Timeout period, the non-resolution action is taken. The range is 1-64,546 minutes. Default is 5 minutes.

Changing the order of rules

Enabled rules are applied in the order in which they are listed in the **Rules** listing. Rules with specific criteria should precede rules with general criteria. Only one rule per rule set is triggered per event, so if the first rule is too general it may always result in a match, with subsequent rules being ignored.

About this task

To change the order of rules:

Procedure

1. Select **Manage** > **Rules and Actions** > **Rules** from the Sterling Control Center window to display the **Rules** listing.
2. Highlight the rule to reorder.
3. In the **Move selected to position #** field, type the position in which to place the selected rule.
4. Click **Move**.

   Note: Be patient while the rule is moved. The **Rules** listing refreshes when the move is complete.

   The rules listing must be sorted in ascending priority order before the move can be accomplished.

Enabling or disabling a rule

Rules must be enabled to be processed. When you first create a rule, it is enabled by default. When you remove the only server or server group used by a rule, the rule is automatically disabled.

About this task

To enable or disable a rule:

Procedure

1. **Select Manage** > **Rules and Actions** > **Rules** from the Sterling Control Center window to display the **Rules** listing.
2. Do one of the following to display the **Rule Properties** window:
   - Select the rule and click **Properties** button.
   - Double-click the rule.
3. Click **Enabled** to place or remove the check mark and click **OK**.

About actions

Sterling Control Center performs an action when the occurrence of an event triggers a rule.

A Sterling Control Center action can perform one or more of the following kinds of activities.

Activity	Description
E-mail	An email address or addresses, or an email list, to which notifications will be sent when the corresponding rule is triggered. Specify the address or addresses, or the email list, to which to send the e-mail, along with the sender e-mail address, a subject line, and message text. You can specify variables to define the e-mail addresses, subject line, and message. You can also send a test e-mail message to make sure an e-mail address is valid. Rather than type multiple addresses individually, you can import a list of email addresses. See *Adding a list of email addresses to an action*.
Alert	Generates a Sterling Control Center alert that an event has occurred. Alerts are displayed in the Active and Handled Alerts monitors.
SNMP trap	Generates an SNMP trap to the SNMP host defined in the Sterling Control Center SNMP Host settings (see *SNMP Host settings*). SNMP Host system settings must be configured to generate traps.
Operating system command	Executes the specified executable command file on the computer where the Sterling Control Center engine is installed, and passes an XML string of the event that triggered the rule to the command file (if no other parameters are passed to the command). You must specify the full path to the command. You can also pass parameters to the command. These parameters can use variables (such as &processName;) which are replaced by the event values. If you designate parameters to pass to the command, Sterling Control Center will not automatically pass the entire XML string of the event to the command. See *Sterling Control Center variables*, for the fields to pass as variables. A sample command may be a user-created script that, if a Process fails, writes Process statistics data to a Help desk file. Any user-created scripts should be validated thoroughly before you use them with Sterling Control Center. For an example of an operating system command, see *How-To.*
Server command	Executes the specified command on a Sterling Connect:Direct server. You can either select a command template from a list box or type the entire command. **Note:** This activity is not available for Sterling B2B Integrator, Sterling Connect:Enterprise, Sterling Connect:Direct for i5/OS, or FTP servers. The command template contains variables for Process name (&processName;) and Process ID (&processId;). When Sterling Control Center submits the command to the Sterling Connect:Direct server, it replaces the variables with the Process name and ID values from the event that triggered the rule. For example, if a Process named SENDDATA and numbered 00087654 triggers a rule that sends a DELETE command to the Sterling Connect:Direct server, the command template: delete process pname=&processName; pnumber=&processId; translates to: delete process pname=SENDDATA pnumber=00087654 See *Sterling Control Center variables* for the fields to pass as variables.

No operation	Performs no action. Useful when you do not want an alert generated or another action taken. For example, you could have two rules with the same criterion, such as Server down, and define them with differing actions: • The first rule has a schedule attached to it (for example, 22:00-23:00 Saturday) when server maintenance is applied. • The second rule has no schedule attached and sends an email to the System Administrator about the server being down. When a server down event occurs during the maintenance window, no email is sent.

You create an action to define an activity that Sterling Control Center performs when an event triggers a rule. Note the following:

- You can define more than one activity for an action.
- You can import a list of email addresses for the E-mail page. See *Adding a list of email addresses to an action* for more information.
- Sterling Control Center ships with some predefined actions. See *Predefined actions and rules* for a complete listing.

Creating an action

Sterling Control Center comes with a number of predefined actions you can use. You can also create your own new actions.

About this task

Note: Sterling Control Center comes with a standalone utility that simplifies creation of multiple actions, rules, and other Sterling Control Center objects. The utility is described in *Creating multiple objects by using the sample script*.

To create a single action:

Procedure

1. Select **Manage** > **Rules and Actions** > **Actions** to display the **Actions** listing.
2. Click the Create button to display the **Create Action** wizard.
3. Type a name and description for the action and click **Next**.
4. To create an email to send whenever the action occurs, define the **To**, **From**, **Subject**, and **Message** fields. Click **To**: to specify one or more email lists. (You can create, duplicate, or modify email lists in the **Email List** window that displays.) Sort the To: list of email addresses in ascending or descending alphabetical order by toggling Sort. Include variables, if you wish, in the Subject line or Message text area. See *Sterling Control Center variables*. To make sure an email address is valid, click **Test**, enter the email address, and click **Send**. Then make sure that the message was received at the destination.
5. To import email addresses, click **Import**. Refer to *Adding a list of email addresses to an action*.
6. Click **Next** to continue.
7. Select the type of alert to generate from the **Alert Severity** drop-down list and click **Next**.
8. Enter information in one or more of the following wizard panels to identify the action criteria:

- To create SNMP traps, turn on the **Generate SNMP Trap** option.
- To use operating system commands to define the action, type the commands or the fully-qualified name of a file that contains the commands in the **OS Command** field.
- To send a command to the Sterling Connect:Direct server for execution, type information in the **Server Command** window.

9. Identify the restricted roles that have permission to modify the action.

   Unrestricted roles automatically have permission to modify an action.
10. Specify whether the action will be visible to all users or only the restricted users in the roles you selected. If you make the action visible to all users, you cannot restrict visibility to specific roles after it is created and referenced. Click **Next**.
11. Click **Finish** to add the action to the **Actions** listing.
12. Click **Close** to close the **Create Action** wizard.

Note: For more information about these options, see *Actions field descriptions*.

Inserting variables

You can include variables, such as those specifying the action name or event type, when you define an action's email, OS command, or server command settings. The **E-mail, OS Command**, and **Server Command** tabs on the **Action Properties** window contain fields in which you can insert variables.

About this task

Note: Use the variable list in the **Select Variable** window rather than inserting variables by typing them in. If the variable you enter is not contained in the **Select Variable** list, it will not be substituted.

To insert a variable when defining an action:

Procedure

1. Click in one of the text entry fields with an associated **Insert Var** button.
2. Click **Insert Var**.
3. In the **Select Variable** window, select a variable and click **OK**.

   The variable is inserted into the text field.

Importing a list of email addresses

You can import a list of email addresses into an action.

About this task

To import a text file containing a list of email addresses into an action:

Procedure

1. Select **Manage** > **Rules and Actions** > **Actions** from the Sterling Control Center window to display the **Actions** listing. Double-click the action to open the **Action Properties** window.
2. From the **E-mail** tab, click **Import**.
3. Navigate to the text file containing the email addresses, select it, and click **Import**. The file contents are imported. If you have already made an entry, the new text replaces the existing text.

Adding a list of email addresses to an action

You can add email addresses to an action in the form of an email list or lists. You can also import a text file that contains a list of email addresses. The addresses in the text file can be delineated by commas or line breaks.

About this task

To add an email list to an action:

Procedure

1. Select **Manage** > **Rules and Actions** > **Actions** from the Sterling Control Center window to display the **Actions** listing. Double-click the action to open the **Action Properties** window.
2. From the **E-mail** tab, click **To:**. The **Email Lists** window displays.
3. Select lists from the **Email Lists** column and click the Right Arrow button to move them to **Selected Email Lists**. You can add, duplicate, or view properties of email lists here, too.
4. Click **OK**.

Sorting email addresses

You can sort email addresses that have been added to an action.

About this task

To sort a list of email addresses:

Procedure

Click **Sort** to put the email addresses on the **Create Action - E-mail** window in ascending or descending order

Displaying the Actions listing

You can display the actions you have created.

About this task

To display the Actions listing:

Procedure

1. From the Sterling Control Center window, select **Manage** > **Actions**.
2. To sort on any column, click the column heading.

Viewing or modifying actions

After you have created actions, you can view or modify them.

About this task

To view or modify an action:

Procedure

1. Select **Manage** > **Rules and Actions** > **Actions** from the Sterling Control Center window to display the **Actions** listing.
2. Do one of the following:

- Select an action and click the Properties button.
- Double-click the action.

3. Click in a field to view field-level help. Field-level help is displayed in the status bar.
4. Modify the action information as necessary. See *Actions field descriptions* for definitions of action fields.

   Note: To make changes, you must have permission to edit the action. Edit permission is denoted by the Rule Edit Icon.
5. Click **OK** when finished.

Actions field descriptions

There are many fields pertaining to actions in Sterling Control Center.

Field Name	Description
Alert Severity	A number from 0-3 that indicates how severe or critical the alert is. Severity is indicated on the Queued or Completed Activity monitors, or the Handled or Active Alerts monitors, with a color-coded icon. This field is optional. To choose a severity level, select one of the following: 0–In compliance (no alert icon generated). A severity level 0 alert deletes all previous alerts for the same SLC instance. 1–High severity (red alert icon generated) 2–Medium severity (orange alert icon generated) 3–Low severity (yellow alert icon generated)
Command Template	A template that gives you suggestions on server command syntax, for use in creating alerts. You can make changes to a command after displaying the template. For example, selecting Delete Process Command from the Command Template displays the following: delete process pname=&processName; pnumber=&processId;
Description	Text describing the action. Optional.

Field Name	Description
Enter operating system command text	Execute the specified executable command file on the computer where the Sterling Control Center engine is installed, and pass an XML string of the event that triggered the rule to the command file (if no other parameters are passed to the command). You must specify the full path to the command. You can also pass parameters to the command. These parameters can use variables (such as &processName;) which are replaced by the event values. If you designate parameters to pass to the command, Sterling Control Center does not automatically pass the entire XML string of the event to the command. Example: An action could specify an operating system command that references a user-created script which, if a Process fails, writes Process statistics data to a Help desk file. You should thoroughly validate any user-created scripts before using them with Sterling Control Center.
From	The return email address that will appear on notification e-mails. If you specify a **To:** address, the **From:** address is required.
Generate SNMP Trap	Turn on this option to generate an SNMP trap to the host defined in the Sterling Control Center SNMP Host settings. SNMP Host system settings must be configured to generate traps.
Message	The text of the email. Optional.
Name	The name of the action. An action is an activity that Sterling Control Center performs when an event triggers a rule. For more on the activities an action can perform, see *About actions*.
Restricted Roles	List of restricted roles defined in Sterling Control Center. Select a role and click the Right Arrow or Left Arrow button to move the role between this field and **Selected Roles**.
Selected Restricted Roles	Restricted roles with rights to modify this action. If no roles are selected, then only an unrestricted user (admin) can modify this action.
Server	The name of the server on which to run the server commands entered.

Field Name	Description
Server Command	A command sent to the Sterling Connect:Direct server for execution. You can type the entire command or select a command template. If you select a command template, Sterling Control Center replaces any variables fields (fields beginning with “&” and ending with ";") with the actual values from the event record. For example, selecting Delete Process Command from the Command Template displays the following command: delete process pname=&processName; pnumber=&processId; **Note:** It is not necessary to terminate server commands with an additional semicolon. Sterling Control Center replaces &processName; with the Process name and &processId; with the Process ID from the event. See *Sterling Control Center Variables*, for the fields to pass as variables. The command must use valid Sterling Connect:Direct syntax.
Subject	Text to be inserted in the email's subject line. If you specify a **To:** address, **Subject** is required.
This action is visible to all users	When selected, this option makes the action public and available for selection by all users. Once a public action is referenced by any other object, you cannot make it private by restricting visibility to specific roles/users.
This action is visible to restricted users in these Selected Restricted Roles	When restricted roles are selected, this option allows only restricted users in the selected roles to view/select/edit the action.
To	The email addresses of recipients to be notified when this action is triggered. Optional.

Use predefined actions and rules

Sterling Control Center provides predefined actions that generate alerts and predefined rules, including ones that monitor for SLC messages. You can use these actions and rules when creating SLCs to monitor Processes or file transfers. You can also modify the actions and rules as necessary to meet your processing requirements.

For more information, see *Using predefined actions and rules in SLCs* for how to use predefined rules and *Predefined actions and rules* for a listing of predefined rules and actions that are included in Sterling Control Center.

Chapter 6. Manage Service Level Criteria

Service level criteria (SLCs) are performance objectives that require processing to occur within a certain time window.

For example, a Sterling Connect:Direct process may need to begin by 20:00 and end by 20:30. An SLC can monitor for the timeliness of both events. If either does not occur within a certain window, the SLC can be used to notify you of that fact. Sterling Control Center can monitor processing start times, stop times, or durations depending on the type of SLC schedule you define. You can define a rule that creates an alert and then view the alert through the Alerts Monitor. The alert might lead you to investigate to determine why the processing did not occur as expected, and to make corresponding adjustments.

There are four types of SLCs:

- Standard—Standard SLCs monitor specific Process names, file names, etc. Use standard SLC groups when you know the specific item to monitor. For more information, see *Creating a Standard SLC group*.
- Wildcard—Wildcard SLCs monitor Processes, file names, etc. with names that do not remain constant, such as Batch IDs with the date and time in their names. To specify monitoring criteria in wildcard groups, you can use the wildcard characters asterisk and question mark, or regular expressions (regex). For more information, see *Creating a Wildcard SLC group*.
- Workflow—Workflow SLCs monitor the flow of related Processes. For example, a workflow SLC can monitor a transaction consisting of three Processes, all of which must run and finish within three hours of the first Process's initiation. For more information, see *Creating a Workflow SLC Group*.
- Simple—Simple SLCs are created using a question/answer format to define the scenario you want to monitor and to select basic parameters and specify values for those parameters. For more information about simple SLCs, see *About simple SLCs*.

For more information about the role SLCs play in Sterling Control Center, see *Implementation*.

SLCs and QuickFile

When defining SLCs, you need to be aware of specific considerations for QuickFile.

- Standard and Wildcard SLCs
  - The Remote Node value is not set in any Sterling Control Center for QuickFile servers.
  - QuickFile event values correspond to the following Sterling Control Center values:

QuickFile event value	Sterling Control Center event value	Sterling Control Center value for downloads	Sterling Control Center value for uploads
package subject	Process Name	Source File Name	Destination File Name
file name		Destination File Name	Source File Name

QuickFile event value	Sterling Control Center event value	Sterling Control Center value for downloads	Sterling Control Center value for uploads
user full name	Submitter ID		

- Workflow SLCs

  The Sterling Control Center stepName event element value is constructed for use as a milestone correlator value. The stepName consists of the QuickFile package identifier value, the recipient user email address, and the QuickFile file name. For downloads, the stepName consists of the QuickFile package identifier, the user email address, and the QuickFile file name.

  As a result, stepName has the same value for a file that is uploaded for a specific user as it does when that same file is downloaded by that user. When the stepName variable value is used as a Workflow SLC correlator, users with the appropriate authority can create one Workflow SLC to ensure that uploaded files are downloaded in a timely manner, regardless of the user or file name.

About creating SLCs

Follow this procedure to create an SLC.

About this task

To create an SLC:

Procedure

1. Review the processing schedule to determine the times when processing must start and complete, and how long processing can run. In the case of a workflow SLC, determine what relationships, such as contingency, exist among processes in the workflow.
2. Create calendars in Sterling Control Center—or use a predefined calendar—based on your review of the processing schedule. Calendars are used in schedules. The same calendar can be used in multiple schedules.
3. Set up SLC schedules in Sterling Control Center based on your review of the processing schedule and the calendars created in step 2. The same SLC schedule can be used with different SLCs. Multiple SLC schedules can be used with one SLC.
4. Review processing to group different items into SLC groups. For example, if a set of Processes runs at the same time, the Processes should be placed into one SLC group.
5. Create the SLC group.

Results

When you create an SLC group it is displayed in a listing of all groups of its type—standard, wildcard, workflow, or simple (see *Displaying an SLC group listing*).

Displaying an SLC group listing

You can display a listing of all SLCs by SLC group type (standard, wildcard, workflow, or simple). The listing shows the SLC group names, a description, and icons that show current status of the group.

About this task

To display an SLC group listing:

Procedure

From the Sterling Control Center window, select **Manage** > **Service Level Criteria (SLCs)** > select the type of SLC group. The corresponding SLC group listing displays.

Results

The SLC group listing icons are described in the following table.

Icon	Description
	The SLC group is enabled.
	The SLC group can be edited by the user who is viewing it.
	1 schedule is associated with the SLC group and the schedule is enabled.
	1 schedule is associated with the SLC group and the schedule is disabled.
	Multiple schedules are associated with the SLC group and all schedules are enabled.
	Multiple schedules are associated with the SLC group and some of the schedules are enabled.
	Multiple schedules are associated with the SLC group and all of the schedules are disabled.

Using data visibility groups to view SLC groups

From the SLC listings, you can use data visibility groups as a means to filter SLCs into sets.

About this task

To view SLC groups by data visibility group:

Procedure

1. From the Sterling Control Center window, select **Manage** > **Service Level Criteria (SLC)** and then select the type of SLC group.
2. From the SLC Set drop down list, select Global to view SLCs that do not have a data visibility group, or select one of the data visibility groups.

   Note: For a data visibility restricted user, the list will contain only the data visibility groups included in the user's role. An unrestricted user will see the Global SLC set and all of the data visibility groups.
3. To view a different SLC set, select a data visibility group from the SLC Set drop down list.

Viewing or modifying properties of an SLC group

You can view an existing SLC group and change any of its properties except for the name.

About this task

To view or change an SLC group:

Procedure

1. Select **Manage** > **Service Level Criteria (SLCs)** and then select the type of SLC group from the Sterling Control Center window to display the corresponding listing.
2. Double-click an SLC to display its properties window, or select the SLC and click the **Properties Icon**.
3. Change the information as required and click **Update**. For a description of SLC Group fields, see *Standard and Wildcard SLC field descriptions*, or *Workflow SLC field definitions*.

   The SLC information is updated.

Adding or removing schedules from an SLC group

You can add or remove schedules from an SLC group.

About this task

To add or remove one or more schedules for an SLC group:

Procedure

1. Select **Manage** > **Service Level Criteria (SLCs)** > and then select the type of SLC group from the Sterling Control Center window.
2. Double-click an SLC to display its SLC group properties window.
3. Select the **Schedules** tab to display a list of defined schedules.
4. Do one of the following:
   - Add a schedule by highlighting it in the **All Schedules** box and clicking the Right Arrow button.
   - Remove a schedule by highlighting it in the **Selected Schedules** box and clicking the Left Arrow button.
5. Click **Update** to close the SLC group properties window.

Enabling or disabling an SLC

You can disable an SLC to stop its being invoked, then enable it to resume the SLC's operation.

About this task

Note: When you delete from Sterling Control Center the only server or server group used by an SLC, the SLC is automatically disabled.

To enable or disable an SLC:

Procedure

1. Select **Manage** > **Service Level Criteria (SLCs)** and then select type of SLC group from the Sterling Control Center window.
2. Double-click the SLC you want to enable or disable. The corresponding group properties window is displayed.
3. Select the **Enabled** box on the **General** tab to enable the SLC, or deselect to disable the SLC, then click **Update**. For a Simple SLC, click **Enable this SLC** on the **How will it be identified** screen.
4. Click **Close**.

Using predefined actions and rules in SLCs

Sterling Control Center provides predefined actions and rules. You can use these actions and rules to monitor for SLC events and generate alerts when they occur. You can modify the predefined actions and rules as necessary to meet your processing requirements.

About this task

These actions and rules are displayed in the **Actions** and **Rules** listings respectively.

To modify a predefined action or rule:

Procedure

1. Create an SLC to monitor a Process or file transfer. (See *About creating SLCs*
2. Review *Predefined actions and rules* to find the rule you wish to modify.
3. Review *Message IDs for rules* to find the message IDs generated by the SLC.
4. Access the rule for each associated message ID. On the Server Groups or Servers tab, select the server group or servers to monitor. (See *Manage rules*.)
5. All predefined rules, except for one, are enabled. (The one exception is the Monitor rate out of compliance rule.) If you do not want to use a rule, you must disable it. (See *Enabling or disabling a rule*.) See *Predefined actions and rules*, for a complete listing of the predefined rules.

Creating multiple SLCs

You can create multiple SLCs rather than creating them one-by-one.

Sterling Control Center comes with a standalone utility that simplifies creation of multiple actions, rules, and other Sterling Control Center objects. The utility is described in *Create multiple objects*.

Creating a standard SLC group

Create Standard SLC groups to monitor specific items such as process names or file names. Use standard SLC groups when you know the specific item to monitor.

About this task

Standard SLC groups are used to monitor the following items:

- Sterling Connect:Direct process starts, ends, and durations
- Sterling Connect:Direct process step starts, step ends, and durations

- Sterling B2B Integrator (Sterling B2B Integrator) business process starts, ends, and durations
- Sterling B2B Integrator business process activity starts, ends, and durations
- Sterling B2B Integrator AFT transfer starts, ends, and durations
- Sterling File Gateway arrived files, routes, and delivery starts, ends, and durations
- Sterling Connect:Enterprise batch arrivals and transmissions
- QuickFile uploads and transfers of files
- FTP GETs and PUTs

You can import a text file containing a list of process names, file names within processes, submitter IDs, batch IDs, or mailbox IDs into an SLC. See *Importing information into a standard SLC group* for more information.

To create a standard SLC group:

Procedure

1. Select **Manage** > **Service Level Criteria (SLCs)** > **Standard SLC Groups**. The Standard SLC Groups listing displays.
2. Click the Create button to display the **Create Standard SLC Group** wizard.
3. Enter a **Name** and **Description** for the SLC.

   Note: For descriptions of standard SLC fields, see *Standard and wildcard SLC field descriptions*.
4. Select values for the **Monitor Window Tolerance** fields.
5. If you want to be notified when an event does not occur, select the **Generate notification if event has not occurred** field.
6. To enable the SLC, check **Enabled**.
7. Click **Next** to continue.
8. On the **Server Groups** page, identify one or more server groups to monitor by selecting the name in **Groups** and clicking the Right Arrow button to move it to **Server Groups**. Click **Next** to continue.
9. Identify individual servers to monitor by selecting the server name in **Servers** and clicking the Left Arrow button to move it to **Selected Servers**. Click **Next** to continue.

   Note: You must select at least one server group or server from the lists on the Server Groups and Servers wizard pages.
10. On the **Data Visibility Groups** page, select the data visibility group to associate with this SLC by selecting the name in **Data Visibility Groups** and clicking the Right Arrow button to move it to **Selected** Data **Visibility Groups**.

    Note: If you are a data visibility restricted user, you are required to select a data visibility group for the SLC.

    Click **Next** to continue.
11. On the **Schedules** page, identify one or more schedules to associate with the SLC. At least one schedule is required. Click **Next** to continue.

12. In the **Processes/Batches**, **File Names**, **Submitters/Senders**, and **Remote Servers/Recipients** pages, enter the item or items to monitor, or click **Import** to import files containing this information. Click **Next** to move through each of these wizard pages.

    To allow one SLC to monitor multiple instances of the same process or file name, check **Allow Duplicates** on the Processes/Batches or File Names pages.
13. On the **Confirm Choices** page, click **Finish**. The SLC is added to Sterling Control Center.
14. Click **Close** on the **Finish** page to close the wizard.

What to do next

If you want the SLC to generate an alert, you must create and enable the corresponding action and rule. See *About actions* and *Manage rules* for more information.

Standard and wildcard SLC field descriptions

The following fields are used to define standard and wildcard SLCs.

Field	Description
Allow Duplicates	Check to allow Sterling Control Center to monitor multiple Processes or batches with the same name.
All Schedules	The list of schedules to choose from.
Concurrence Count (Wildcard SLC)	For a wildcard SLC associated with a calendar schedule, the number of SLC instances expected to be seen during the scheduled time. For a wildcard SLC associated with a duration schedule, the number of instances of the SLC that may run at one time. The range is 1-100. Default is 1.
Data Visibility Groups	The list of visibility groups to choose from.
Description	Descriptive information to further identify the SLC.
End Window Tolerance	The number of hours after the expected end of processing to stop monitoring. The default is **6 hours after the schedule requirements**. The range is 0–24 hours.
Expression (Wildcard SLC)	For wildcard SLCs, the regular expression or wildcard definition used in constructing matching criteria (against Processes/batch IDs, filenames, submitters/mailboxes, remote servers). This expression must follow RegEx or wildcard syntax. Regular expressions can be used to match text or numeric strings that follow a particular pattern. Special characters are allowed. To test the value you define in this field, click **Test**.
File Names	A list of the destination file names of files copied by a Process. At least one entry among Process Names/Batch IDs, File Names, Submitters/Sender Mailbox IDs, and Remote Servers/Recipient Mailbox IDs is required.
Groups	The server groups to choose from.
Name	A unique name for the SLC.
Other: Enabled	Click to enable the SLC.

Field	Description
Other: Generate notification if event has not occurred	Check this option to generate notification of events (an alert) for an SLC when an event fails to occur. If this option is checked and one or more calendar schedules are associated with the SLC, events are generated when service-level criteria are not met. If it is unchecked, events (positive or negative) are generated only if the SLC criteria are met. For example, you might create an SLC to monitor a Process that normally runs at 1pm on Fridays. If the process never runs on Friday, an SLC event would be generated only if this box is checked. If it is not checked, SLC events would be generated only if the Process ran (whether early, on time, or late).
Process Names/Batch IDs	The Sterling Connect:Direct Process names or Sterling Connect:Enterprise batch IDs to monitor. At least one entry among Process Names/Batch IDs, File Names, Submitters/Sender Mailbox IDs, and Remote Servers/Recipient Mailbox IDs is required.
Selected Data Visibility Groups	The data visibility group (chosen from **Data Visibility Groups**) that is associated with this SLC. Only one data visibility group can be selected for an SLC. Data visibility group restricted users must select a data visibility group when creating an SLC (their first Data Visibility Group is automatically selected). Only events applicable to the data visibility group specified will be processed by the SLC.
Selected Groups	The server groups (chosen from Groups) that this SLC is to monitor. At least one server or server group is required.
Selected Schedules	Schedule or schedules to apply to the SLC. At least one schedule is required.
Selected Servers	The servers (chosen from Servers) that this SLC is to monitor. At least one server or server group is required.
Servers	The list of servers to choose from.
Start Window Tolerance	The number of hours before the expected start of processing to begin monitoring. The default is **6 hours before the schedule requirements**. The range is 0–24 hours.
Submitters/Sender Mailbox IDs	A list of submitters or sender mailbox IDs to monitor. At least one entry among Process Names/Batch IDs, File Names, Submitters/Sender Mailbox IDs, and Remote Servers/Recipient Mailbox IDs is required.
RegEx (Regular Expression)	For wildcard SLCs, check to indicate that the referenced expression is a regular expression.
Remote Servers/Recipient Mailbox IDs	A list of remote servers or recipient mailbox IDs to monitor. At least one entry among Process Names/Batch IDs, File Names, Submitters/Sender Mailbox IDs, and Remote Servers/Recipient Mailbox IDs is required.

Importing information into a standard SLC group

You can import a text file into a standard SLC group.

About this task

The text file may include information about:

- Sterling Connect:Direct or FTP Process names and Sterling B2B Integrator business process names
- File names within Sterling Connect:Direct or FTP Processes or Sterling B2B Integrator business process activities
- Sterling Connect:Direct or FTP remote servers/recipients
- Sterling Connect:Direct or FTP Process or Sterling B2B Integrator business process submitter IDs
- Sterling Connect:Enterprise Batch IDs
- Sterling Connect:Enterprise sender and recipient Mailbox IDs

To import a file into an SLC:

Procedure

1. Click **Import** on one of the following SLC Create wizard or Properties pages:
   - **Processes/Batches**
   - **File Names**
   - **Submitters/Senders**
   - **Remote Servers/Recipients**
2. In the Import window that displays, navigate to the text file, select it, and click **Import**. The text is imported. Multiple items must be separated by commas. You can edit the imported text if necessary.
3. Click **Next** to continue.

Exporting information from a standard SLC Group

You can export the information from a standard SLC group to a text file.

About this task

The following types of information can be exported:

- Sterling Connect:Direct or FTP process names and Sterling B2B Integrator business process names
- File names within Sterling Connect:Direct or FTP processes or Sterling B2B Integrator business process activities
- Sterling Connect:Direct or FTP remote servers/recipients
- Sterling Connect:Direct or FTP process or Sterling B2B Integrator business process submitter IDs
- Sterling Connect:Enterprise batch IDs
- Sterling Connect:Enterprise sender and recipient mailbox IDs

To export information from an SLC to a text file:

Procedure

1. Click **Export** on one of the following SLC Create wizard or Properties pages:
   - **Processes/Batches**
   - **File Names**
   - **Submitters/Senders**
   - **Remote Servers/Recipients**
2. Select a location to store the text file.
3. Type a name for the text file and click **Export**. The information is exported.

4. Click **Next** to continue.

Creating a wildcard SLC group

Use wildcard SLC groups when you do not know or cannot specify the servers, Processes, destination file names, submitter IDs, batch IDs, or mailbox IDs to monitor.

About this task

To specify the monitoring criteria for wildcard SLCs, you can use either the wildcard characters asterisk (*) or question mark (?) (the default), or regular expressions. See *Regular expressions*, for basic regular expression syntax and examples.

To create a wildcard SLC group:

Procedure

1. Select **Manage** > **Service Level Criteria (SLCs)** > **Wildcard SLC Groups**. The Wildcard SLC Groups listing displays.
2. Click the Create button to display the **Create Wildcard SLC Group** wizard.
3. Type a **Name** for the SLC and, optionally, a **Description**.

   Note: For field descriptions, see *Standard and Wildcard SLC field descriptions*.
4. For **Start Window Tolerance**, specify the number of hours before a schedule requirement to begin monitoring for SLC activity. For **End Window Tolerance**, specify the number of hours after a schedule requirement to stop monitoring for SLC activity.
5. Specify the **Concurrence Count**. For a wildcard SLC associated with a calendar schedule, specify the number of SLC instances expected to be seen during the scheduled time. For a wildcard SLC associated with a duration schedule, specify the number of instances of the SLC that may run at one time.
6. If you want to be notified when an event does not occur, enable the **Generate notification if event has not occurred** field.
7. To enable the SLC, check **Enabled**.
8. Click **Next** to continue.
9. On the **Server Groups** page, identify a server group to monitor by selecting the name in **Groups** and clicking the Right Arrow button to move it to **Server Groups**. You must select at least one server group or server from the lists on this or the Servers wizard page. Click **Next** to continue.
10. Identify servers to monitor by entering an **Expression**. Select **RegEx** if the expression is a regular expression. You can test the expression by clicking **Test**. (See *Testing expressions*.) You must make an entry either here or on the Server Groups wizard page. Click **Next** to continue.
11. On the **Data Visibility Groups** page, select the data visibility group to associate with this SLC by selecting the name in **Data Visibility Groups** and clicking the Right Arrow button to move it to **Selected Data Visibility Groups**.

    Note: If you are a data visibility restricted user, your own data visibility group will be automatically selected.

Click **Next** to continue.

12. On the **Schedules** page, identify one or more schedules to associate with the SLC. At least one schedule is required. Click **Next** to continue.
13. In the **Processes/Batches**, **File Names**, **Submitters/Senders**, and **Remote Servers/Recipients** pages, identify the items to monitor by entering an **Expression**. Select **RegEx** if the expression is a regular expression. You can test the expression by clicking **Test**. (See *Testing expressions* Click **Next** to move through each wizard page.
14. On the **Confirm Choices** page, click **Finish**. The SLC is added to Sterling Control Center.
15. Click **Close** on the **Finish** page to close the wizard.
16. If you want the SLC to generate an alert, you must create and enable the corresponding action and rule. See *About actions* and *Manage rules* for more information.

Testing expressions

Sterling Control Center allows you to test standard wildcard and regular expressions.

About this task

The **Expression Tester** window enables you to test standard wildcard and regular expressions. (See *Regular expressions*.)

To test an expression:

Procedure

1. In the Servers, Processes/Batch IDs, File Names, Submitters/Mailbox IDs, or Remote Servers page of the Create Wildcard SLC wizard, or the Create Workflow Milestone page of the Create Workflow Wizard, type an expression in the **Expression** text box and click **Test** (see *Creating a Wildcard SLC Group* or *Creating a Workflow SLC Group*). The **Expression Tester** window is displayed with the expression you typed.
2. Type a **Test Value** to test the expression against. For example, to test the wildcard expression ServX*, you could type ServX45. This field is case sensitive.
3. Select **RegEx (Regular Expression)** to test a regular expression.
4. Click **Match**. Depending on whether the value matches the expression, True or False is displayed following the **Match** button. If necessary, verify your wildcard syntax and test again.
5. Click **OK** or **Cancel** to return.

Creating a workflow SLC Group

You use workflow SLC groups to monitor a group of related or sequential processes or process steps. Workflow SLCs monitor related or contingent processes and process steps by tracking them as milestones in a workflow.

About this task

In creating a workflow SLC group, you specify information in the following categories:

- General information, such as name and description of the workflow SLC group

- An overall schedule or schedules for the SLC
- Milestones representing the processes or process steps
- A time range/duration for each milestone. These values can be based on the workflow SLC's actual start or its scheduled start.
- Parameters, including optional message lists for generating workflow SLC messages. These messages include jeopardy messages and fire-once messages.

If you want the workflow SLC to generate an alert, you must create and enable the corresponding action and rules. See *Manage rules* and *About actions* for more information.

To create a workflow SLC group:

Procedure

1. Select **Manage** > **Service Level Criteria (SLCs)** > **Workflow SLC Groups**. The Workflow SLC Groups listing displays.
2. Click the Create button to display the **Create Workflow SLC Group** wizard.
3. On the **General** page, enter general information about the workflow SLC and click **Next** to continue to the next page. For a description of each field, see *Workflow SLC field definitions*.
4. On the **Data Visibility Groups** page, select the data visibility group to associate with this SLC by selecting the name in **Data Visibility Groups** and clicking the Right Arrow button to move it to **Selected Data Visibility Groups**.

   Tip: If you are a data visibility restricted user, your own data visibility group will be automatically selected.

   Click **Next** to continue.
5. On the **Schedules** page, move one or more schedules from All Schedules to Selected Schedules by selecting it and clicking the Right Arrow button. To move a schedule out of the Selected Schedules list, select it and click the Left Arrow button. Click **Next** to continue to the next page.
6. On the **Parameters** page, enter details regarding how milestone time values are to be handled, the SLC concurrence count, an optional correlator value, and optional Jeopardy and Fire-Once Message Lists.

   For more information on the values you can select for a correlator source, see *Sterling Control Center variables*. For more information on message lists, see *Maintain message lists*.
7. Click **Next** to continue to the next page.
8. On the **Milestones** page, add one or more milestones by clicking **+** and creating the milestone. See *Creating a milestone* for more information.
9. Click **Finish** on the **Confirm Choices** page to confirm the selections you've made.
10. Click **Close** on the **Finish** page to add the SLC to the Workflow SLC listing.

Workflow SLC field definitions

There are many fields pertaining to Workflow SLCs in Sterling Control Center.

The following table describes the fields that make up a workflow SLC.

Field	Description
Name	The workflow SLC name.
Description	Text describing the workflow SLC. Optional.
Enabled	Check to enable the workflow SLC. Default is enabled.
Generate notification if event has not occurred	If this option is checked and one or more calendar schedules are associated with the workflow, and if the workflow does not run when specified, notifications of events are generated. If the option is unchecked, notifications of events (positive or negative) are generated only if the workflow runs.
Suppress Milestone Messages	Check this option to prevent notifications that pertain to workflow SLC milestones. When this option is checked, only notifications that refer to the workflow SLC itself are generated.
Monitor Window Tolerances: Start	The number of hours before a schedule requirement to monitor for workflow SLC activity. The default is **6 hours** before the schedule requirement. The range is 0–24 hours.
Monitor Window Tolerances: End	The number of hours after a schedule requirement to monitor for SLC activity. The default is 6 hours after the schedule requirement. The range is 0–24 hours.
Data Visibility Groups	The list of data visibility groups to choose from.
Selected Data Visibility Groups	The data visibility group (chosen from **Data Visibility Groups**) that is associated with this SLC. Only one data visibility group can be selected for an SLC. Data visibility group restricted users will have their first data visibility group automatically selected. Only events applicable to the DVG specified will be processed by the SLC.
Schedules	The schedule or schedules to associate with the workflow SLC.
Milestone times Relative to: Actual Start of Workflow SLC	Select this option to indicate that milestone times in the workflow SLC are relative to the time that the SLC actually starts. This option and the following option are mutually exclusive, and one is required.
Milestone times Relative to: Scheduled Start of Workflow SLC	Select this option to indicate that milestone times in the workflow SLC are relative to the time that the SLC is scheduled to start. This option and the preceding option are mutually exclusive, and one is required.
Concurrence Count	For a workflow associated with a calendar schedule, the number of workflow instances expected to be seen during the scheduled time. For a workflow associated with a duration schedule, the number of instances of the workflow that may run at one time. The range is 1-100. Default is 1.
Correlator Source	The value Sterling Control Center obtains and uses at runtime to correlate milestones in the workflow SLC. Click **Insert Var** and then select the event element variable to use as the value required in all events making up the workflow SLC instance to be considered complete. For more information on variables you can use, see *Sterling Control Center variables*. You can use a different correlator for an individual milestone to override this general Correlator Source, which is used for the entire SLC. For more information, see *Creating a milestone*.

Field	Description
Jeopardy List: Message ID	A list of messages used to indicate that a workflow SLC milestone is in danger of failing to complete normally due to a problem with a previous milestone. When a message in the jeopardy list is generated for any milestone, then a jeopardy event will be generated for all milestones in the same workflow that have yet to start. A jeopardy event is an SLC event containing the jeopardy message ID (CSLC229I) along with the name of the milestone and the reason that the milestone is in jeopardy. See *Maintain Message lists*.
Fire-Once List: Message ID	Fire-once messages are generated only once per workflow, no matter how many times the condition that triggers them may occur. See *Maintain Message lists*.
Milestones	The milestones that comprise the workflow. For more information, see *Creating a milestone*.

Maintain message lists

As part of the process of managing workflow SLCs, you can create, modify, duplicate, and delete message lists. Message lists can be used as a source of jeopardy messages or fire-once messages. Jeopardy messages signal that a milestone is in danger of failing to complete as scheduled due to a problem with a previous milestone. Fire-once messages display a maximum of once per workflow no matter how many times the condition that triggers them occurs.

You can select any message list to use as a jeopardy list or fire-once list. In other words, in setting up a message list you do not define it as jeopardy or fire-once.

Creating a message list

You can create a message list that contains jeopardy or fire-once messages. The list can then be used with workflow SLCs.

About this task

To create a message list:

Procedure

1. Select **Manage** > **Service Level Criteria (SLCs)** > **Message Lists**.

   Note: You can also manage message lists as part of creating or modifying a workflow SLC. (See *Creating a workflow SLC group*.)
2. Click the Create button. The **Create Message List** wizard displays.
3. On the **General** page, provide a name and description for the message list and click **Next** to go to the next page. For details on the fields that make up a message list, see *Message list field definitions*
4. On the **Messages** page, select messages to include in the list by any of the following methods and click **Next** to go to the next page:
   - Individually select messages to include in the list by checking them.
   - To select all messages, right-click the listing and select **Select All**.
   - To deselect all messages, right-click the listing and select **Deselect All**.
   - To get suggestions, right-click in the message listing and select **Suggest Jeopardy List** or **Suggest Fire-Once List**. Messages typical of the kind you

asked for are automatically checked. You can modify the list by deselecting suggested ones or selecting ones not suggested.

5. On the **Permissions** page, confine permission to manage the message list to a selected role by selecting the role and clicking the Right Arrow button. Move a role out of **Selected Roles** by selecting it and clicking the Left Arrow button.
6. Specify whether the message list will be visible to all users or only to the users in the roles you selected. If you make the message list visible to all users, you cannot restrict visibility to specific roles once it has been referenced. Click **Next**.
7. On the **Confirm Choices** page, review your choices and click **Finish**.
8. On the **Finish** page, click **Close**.

Modifying a message list

After you have created message lists, you can modify them.

About this task

To modify a message list:

Procedure

1. Select **Manage** > **Service Level Criteria (SLCs)** > **Message Lists**.
2. Double-click an item in the **Message Lists** screen, or select it and click the **Properties Icon**. The **Message List Properties** screen displays.
3. Change any of the information detailed in steps 3 and 7 of the *Creating a message list* procedure. Click **Update** to finish. For details on the fields that make up a message list, see *Message list field definitions*.

Message list field definitions

There are many fields pertaining to Message lists in Sterling Control Center.

The following table defines the fields that make up a message list.

Field	Description
Name	The name of the message list.
Description	Text describing the message list.
Messages	The messages that make up the message list.
All Roles	The roles available to select from.
Selected Roles	The restricted roles that have permission to modify this message list. If none is selected, only unrestricted roles have such permission.
This message list is visible to all users	When selected, this option makes the message list public and available for selection by all users. Once a public message list is referenced by any other object, you cannot make it private by restricting visibility to specific roles/users.
This message list is visible to restricted users in these Selected Restricted Roles	When restricted roles are selected, this option allows only restricted users in the selected roles to view/select/edit the message list.

Maintain Milestones

Creating a milestone

Use milestones to specify the processes or process steps to be monitored in a workflow SLC.

About this task

To create a milestone:

Procedure

1. On the **Milestones** page of the **Create Workflow SLC Group Wizard** or **Workflow SLC Group Properties**, click the Create button. The **Create Milestone** wizard is displayed.
2. On the **General** page, enter general information about the milestone and click **Next** to go to the next page.

   Note: For descriptions of the fields that make up a milestone, see *Milestone Field Definitions*.
3. On the **Parameters** page, select one or more **Key**s, select an **Operator**, and enter a **Value**. An entry that specifies either Server or Server Group is required. Also, either Process Name or Step Name is required. To see information about additional keys you can specify, see *Keys and Fields*.

   Optionally, you can also enter a Correlator Source. For more information, see *Sterling Control Center variables*.

   Click **Next** to go to the next page.

   Note: Users with a restricted role must always specify a server group. In addition, they can specify a server. By specifying both a server and server group, the SLC applies only to activity on the server specified as opposed to all servers in the server group.
4. On the **Schedule** page, define duration or calendar schedule values (or both) and press **Next** to continue. A duration schedule requires **Minimum Duration** and **Maximum Duration** values. For a calendar schedule, enter **Normal Start Range Start (NSRs)** and **Normal Start Range End (NSRe)** or **Normal End Range Start (NERs)** and **Normal End Range End (NERe)** values, or both.
5. Confirm choices by clicking **Finish** on the **Confirm Choices** page, then click **Close** on the **Finish** page.

Modifying a milestone

After you create a milestone, you can modify it.

About this task

To modify a milestone:

Procedure

1. On the **Milestones** page of the **Create Workflow SLC Group** wizard or **Workflow SLC Group Properties**, double-click the milestone or select it and click the **Properties Icon**. The **Milestone Properties** window is displayed.
2. Change any of the information, except for Name, as detailed in steps 2 through 4 of the *Creating a milestone* procedure for creating a milestone. Click **Update** on any page to finish.

Milestone field definitions

There are many fields pertaining to milestones in Sterling Control Center.

The following table defines the fields that make up a milestone.

Field	Description
Name	A name for the milestone.
Description	Text describing the milestone.
Key	The selection criteria for this milestone, such as Process Name or Submitter ID. To see information on parameters you can use as keys, see *Keys and fields*.
Operator	The operator for the selection criterion. Depending on the value you choose for Key, choose from: • Matches • Wildcard • RegEx
Value	The value of the Key to set as the selection criterion.
Correlator Source	The value Sterling Control Center obtains and uses at runtime to correlate this individual milestone to other milestones in the workflow SLC. This will override the Correlator Source value set in the Workflow SLC for this milestone only. Click Insert Var and then select the event element variable. For more information on variables you can use, see *Sterling Control Center variables*. **Note:** If you use a correlator for an individual milestone, you must either specify a correlator for each milestone or one for the workflow SLC itself to use as a default correlator.
Minimum Duration	The minimum amount of time the milestone item is expected to run, in the format hhh:mm:ss. Hours and minutes are required if you specify a value. Example: Type 1 hour and 15 minutes as 1:15. Type 20 minutes as 0:20. Type 15 seconds as 0:00:15.
Maximum Duration	The maximum amount of time the milestone item is expected to run, in the format hhh:mm:ss. Hours and minutes are required if you specify a value. Example: Type 1 hour and 15 minutes as 1:15. Type 20 minutes as 0:20. Type 15 seconds as 0:00:15.
Normal Start Range: Start	The beginning of a time range within which processing is expected to start for a milestone item. This time range is relative to the actual or scheduled start of the workflow. Expressed in 24-hour format. For example, enter 18 hours as 18:00 or 30 minutes as 0:30.
Normal Start Range: End	The endpoint of a time range within which processing is expected to start for a milestone item. This time range is relative to the actual or scheduled start of the workflow. Expressed in 24-hour format. For example, enter 18 hours as 18:00 or 30 minutes as 0:30. End Time cannot be the same as Start time. If the start time is later than the end time, the NSR spans two days.

Field	Description
Normal End Range: Start	The beginning point of a time range within which processing is expected to end for a milestone item. This time range is relative to the actual or scheduled start of the workflow. Expressed in 24-hour format. For example, enter 18 hours as 18:00 or 30 minutes as 0:30.
Normal End Range: End	The endpoint of a time range within which processing is expected to end for a milestone item. This time range is relative to the actual or scheduled start of the workflow. Expressed in 24-hour format. For example, enter 18 hours as 18:00 or 30 minutes as 0:30. End time cannot be the same as Start time. If the start time is later than the end time, the NER spans two days.

Tip: Start range and end range times are relative to the scheduled or actual start of the workflow SLC, depending upon whether Milestone Times Relative to: Actual Start of Workflow SLC or Milestone Times Relative to: Scheduled Start of Workflow SLC is checked.

About simple SLCs

Simple SLCs enable you to create an SLC by answering a few basic questions, specifying values for basic parameters, and giving the SLC a name and description. When you create a simple SLC, all necessary objects to support the SLC, such as rules, actions, and schedules, are also created.

The following considerations apply to simple SLCs:

- Although simple SLCs are based on workflow SLCs, simple SLCs support only one milestone.
- After you create them, simple SLC groups are displayed in both the Simple SLC Groups list and in the Workflow SLC Groups list. You can view simple SLC properties from the Workflow SLC Group list, but you cannot edit them from this list. They must be edited from the Simple SLC Groups list.
- Any milestones, calendars, schedules, or actions created for a simple SLC will have the same name as the SLC. Any rules created for a simple SLC will have a rule name of <SLC_Name>_CSLC0XXE or <SLC_Name>_ignored_msgs.
- Any objects created for the SLC are displayed with the listings for those object types, for example, actions. You can view an action created by a simple SLC from the Actions list, but that action can be edited only from the Show Simple SLC Groups.
- When you delete a simple SLC, the objects created for the SLC that have the same name as the simple SLC are also deleted.
- You cannot create a simple SLC that has the same name as an existing calendar, schedule, action, rule, or workflow SLC. Conversely, you cannot create a workflow SLC that has the same name as a simple SLC.
- Because the rules generated by simple SLCs are created with specific parameters, they appear at the beginning of the priority list.
- If your role does not have manage permissions for the objects used to create simple SLCs, such as calendars, schedules, and actions, you will only be able to select existing objects when creating simple SLCs. If your role has view-only permissions, you will not be able to create or update simple SLCs.

Using the Create Simple SLC Group Wizard

The Create Simple SLC Group wizard walks you through the creation of a simple SLC using a question/answer format.

Your answer to the first question: "What interests you?" defines the starting point and structure for building the SLC. When you select an answer, a synopsis of the SLC is displayed on the first page. For example, when you select "My process didn't start on time," the following is displayed:

The synopsis of the SLC contains the basic parameters for the scenario you chose. From this first page, you can proceed as follows:

- Click the underlined text to provide values for the basic parameters.

Important: If you have view-only permissions, you cannot edit the underlined text.

- Click **Next** to cycle through the pages of the wizard to answer the five questions used to define the SLC. As you select answers to the questions, the parameters associated with those answers are displayed in the synopsis. When using this method, you can select additional or different parameters than the basic parameters.
- Click **Final** to move to the last question where you provide a name, description, and data visibility group for the SLC and provide values for the basic parameters required for the SLC.

At anytime before you click **Finish** to complete the SLC, you can click **Back** to return to previous pages to select different answers and to provide values for the parameters associated with those answers.

Creating a simple SLC group

You create a simple SLC group using the Create Simple SLC Group wizard.

About this task

To create a simple SLC group:

Procedure

1. Select **Manage** > **Service Level Criteria (SLCs)** > **Simple SLC Groups** > **Create Simple SLC**. The Simple SLC Group wizard displays.
2. On the **What interests you?** page, select the general scenario that you want to monitor and click **Next**.

   Note: As you are answering questions to create a simple SLC, the box on the page contains a synopsis of the simple SLC scenario you have chosen. To edit the basic SLC parameters, you can click the underlined text. If you do not want to cycle through the wizard pages, you can click **Final** to go to the Summary page, where you can also edit the basic parameters.
3. On the **How do you define it?** page, select the parameters that specifically define what will be monitored. To specify values for the parameters, click the underlined text. Click **Next** to continue.
4. On the **When should it occur?** page, specify whether the time constraints for the SLC will be based on an existing or a new schedule (with a start/end time range and recurrence), or on a duration of time. To specify values for the time constraints, click the underlined text. Click **Next** to continue.

5. On the **What do you want done?** page, select the action that will be taken when this scenario occurs. To specify values for the action you chose, click the underlined text. Click **Next** to continue.
6. On the **How will it be identified?** page, specify a name and description for the SLC and select a data visibility group.
7. Click **Summary** to review the parameters for the SLC or **Finish** to complete the SLC.
8. Click **Close**.
9. You are notified when the SLC has been created. Click **Close**.

Viewing or modifying properties of a simple SLC group

You can view an existing simple SLC group and change any of its properties except for the name.

About this task

To view or change a simple SLC group:

Procedure

1. Select **Manage** > **Simple SLC Group** > **Show Simple SLC Groups** from the Sterling Control Center window.
2. Double-click a simple SLC to display its properties window, or select the SLC and click the Properties button. The **Create Simple SLC Group** wizard displays. To update the simple SLC, either:
   - Click the underlined text to provide values for the basic parameters on the first page.
   - Click **Next** to cycle through the pages of the wizard to update the answers to the five questions used to define the SLC. Click the underlined text to edit parameter values in the synopsis.
   - Click **Final** to move to the last question where you can edit the description and select a data visibility group for the SLC and provide values for the parameters required for the SLC.
3. When you have completed your updates, click **Finish**.
4. You are notified when the SLC has been updated. Click **Close**.

Enabling or disabling a simple SLC group

After you create a simple SLC group, you can enable or disable it for use by Sterling Control Center.

About this task

To enable or disable a simple SLC group:

Procedure

1. Select **Manage** > **Simple SLC Group** > **Show Simple SLC Groups** from the Sterling Control Center window.
2. Double-click a simple SLC group to display its properties window, or select the SLC and click the **Properties** button. The Create Simple SLC Group wizard displays.
3. Click **Final** to move to the last question. On this page, select **Enable this SLC** or clear this option to disable the SLC.

4. Click **Finish**.
5. You are notified when the SLC has been updated. Click **Close**.

Chapter 7. Schedules overview

Schedules are associated with SLCs to specify when or for how long monitoring occurs. They are associated with rules to specify when events will be matched against rule criteria and when they will not.

For example, if you do not want a rule to be applied during scheduled downtime, you can create two calendar schedules: one that excludes the downtime and one that includes only the downtime. For the schedule with only downtime, specify an action of "No Operation." For the other schedule, specify an action that produces an alert when the rule criteria are met. Then, associate the two schedules with the rule.

Note: You can create a schedule as part of the process of creating or editing a rule. For more information, see *Creating a rule*.

For information about the types of schedules and how they are used with SLCs and rules and, see *Implementation*.

Creating an SLC calendar schedule

Create an SLC calendar schedule to specify when processing occurs.

About this task

To create an SLC calendar schedule:

Procedure

1. Click **Manage** > **Service Level Criteria (SLCs)** > **SLC Schedules**. The **SLC Schedules** listing displays.
2. Click the Create button to display the **Create SLC Schedule** wizard.
3. Select **Calendar Schedule** in the **Schedule Type** field.
4. Type a **Name** and **Description** for the schedule.
5. Select **Enabled** if you want to enable the schedule.
6. Click **Next**.
7. Select an existing **Calendar Name** to use in the schedule.

   Note: You can create a new calendar by clicking **+** for **Calendar Name**. You can duplicate an existing calendar and modify the duplicate by clicking the **Duplication Icon**. View the properties of a calendar by selecting the calendar name and clicking **Properties**.
8. Select the **Time Zone** to be used for monitoring.
9. Type the **Normal Start Range (NSR) Start Time** and **End Time**, or the **Normal End Range (NER) End Day**, **Start Time**, and **End Time**, as desired, for the schedule.
   - Enter the times according to the time zone you selected in the previous step.
   - Type the time in 24-hour format. For example, enter 6:00 a.m. as 06:00. Enter 6 p.m. as 18:00. Enter 12:30 a.m. as 00:30.
   - If you specify a time range, supply both the Start Time and End Time.

- The Start Time and End Time cannot be the same.
- The maximum difference between the Start Time and End Time, without using End Day, is 23 hours, 59 minutes. Using End Day, you can specify start and end times that are as much as 7 days apart.
- If the Start Time is later than the End Time, the schedule spans 2 days.

10. Optionally, identify the restricted roles that have permission to modify the schedule. Highlight a restricted role in the **All Roles** window and click the Right Arrow button to move it to the **Selected Roles** window.

    Note: Unrestricted roles already have permission to modify schedules and are not displayed in the list of All Roles.
11. Specify whether the schedule will be visible to all users or only to the users in the roles you selected. If you make the schedule visible to all users, you cannot restrict visibility to specific roles after it has been referenced.
12. Click **Next** and then, on the **Finish** page, click **Finish.**
13. Click **Close** to close the **Create SLC Schedule** window.

Creating a rule calendar schedule

Create a rule calendar schedule to specify when events will be matched against the rule's criteria and when they won't be.

About this task

To create a rules calendar schedule:

Procedure

1. Click **Manage** > **Rules and Actions** > **Rule Schedules**. The **Rule/Metadata Schedules** listing displays.
2. Click the Create button to display the **Create Rule/Metadata Schedule** wizard.
3. Type a **Name** and **Description** for the schedule.
4. Select **Enabled** if you want to enable the schedule.
5. Click **Next**.
6. Select a **Calendar Name** to use in the schedule.

   Note: You can create a new calendar by clicking the Create button next to **Calendar Name**. You can duplicate an existing calendar and modify the duplicate by clicking the Duplicate button. View a calendar's properties by selecting the calendar name and clicking the Properties button.
7. Select the **Time Zone** to be used for monitoring.
8. Type the **Start Time**, **End Day**, and **End Time** for the schedule.
9. If you want to check the time that the event occurred to determine if the rule conditions are met, turn on **Check Schedule against when event occurred**.
10. Optionally, identify the restricted roles that have permission to modify the schedule. Highlight a restricted role in the **Restricted Roles** list and click the Right Arrow button to move it to **Selected Restricted Roles**.

    Note: Unrestricted roles already have permission to modify schedules and are not displayed in the list of Restricted Roles.
11. Specify whether the schedule will be visible to all users or only to the users in the roles you selected. If you make the schedule visible to all users, you cannot restrict visibility to specific roles after it has been referenced.

12. Click **Next**, then, on the **Finish** page, click **Finish.**
13. Click **Close** to close the **Rule Schedule** window.

Creating a metadata calendar schedule

You can create a calendar schedule to use in defining metadata rules.

About this task

For more information on metadata rules, see *Metadata rules overview*.)

To create a metadata calendar schedule:

Procedure

1. Click **Manage** > **Metadata** > **Metadata Schedules**.
2. Follow the *Creating a rule calendar schedule* procedure beginning with step 2.

Creating an SLC duration schedule

Create an SLC duration schedule that can be used in conjunction with SLCs to specify that processing can begin at any time, but once it has begun, it must be completed within a specified amount of time (hours, minutes, seconds). For example, processing must complete within 15 minutes of when a file transfer starts.

About this task

To create an SLC duration schedule:

Procedure

1. Click **Manage** > **Service Level Criteria (SLCs)** > **SLC Schedules**. The **SLC Schedules** listing displays.
2. Click the Create button to display the **Create SLC Schedule** wizard.
3. Select **Duration Schedule** in the **Schedule Type** field.
4. Type a **Name** and **Description** for the schedule.
5. Select **Enabled** if you want to enable the schedule.
6. Click **Next**.
7. Select a **Calendar** to use in the schedule.
8. Type the **Minimum Duration** in the format hhh:mm:ss. Hours and minutes are required. For example, type 1 hour and 15 minutes as 1:15. Type 20 minutes as 0:20. Type 15 seconds as 0:00:15.
9. Type the **Maximum Duration** in the format hhh:mm[:ss]. Hours and minutes are required. For example, type 1 hour and 15 minutes as 01:15. Type 20 minutes as 00:20. Type 15 seconds as 00:00:15. You must supply both a minimum and a maximum duration. They cannot be the same values. The maximum duration is 167 hours, 59 minutes, and 59 seconds (7 days).
10. Click **Next.**
11. Optionally, identify the restricted roles that have permission to modify the schedule. Highlight a restricted role in **All Roles** and click the Right Arrow button to move it to **Selected Roles**.

Tip: Unrestricted roles already have permission to modify schedules and are not displayed in the list of All Roles.

12. Specify whether the schedule will be visible to all users or only to the users in the roles you selected. If you make the schedule visible to all users, you cannot restrict visibility to specific roles after it is created. Click **Next**.
13. On the Confirm Choices page, click **Finish.**
14. Click **Close** on the **Finish** page to close the **Create SLC Schedule** window.

Displaying a schedules listing

After you have created schedules, you can view them in a schedules listing.

About this task

To display a schedules listing:

Procedure

1. From the Sterling Control Center window, select one of the following:
   - **Manage > Service Level Criteria (SLCs)** > **SLC Schedules**
   - **Manage > Rules and Actions** > **Rules Schedules**
   - **Manage > Metadata > Metadata Schedules**
2. To sort on any column, click on the column heading.

Viewing or modifying schedule properties

After you have created schedules, you can view and modify their properties.

About this task

To view or modify the properties of a schedule:

Procedure

1. Select one of the following:
   - **Manage > Service Level Criteria (SLCs)** > **SLC Schedules**
   - **Manage > Rules and Actions** > **Rules Schedules**
   - **Manage > Metadata > Metadata Schedules**
2. Double-click a schedule in the listing to display the **Rule/Metadata Schedule** or **SLC Schedule Properties** window.
3. Click in a field to view field-level help.
4. Modify the fields you want to change. See *Schedule field descriptions* for descriptions of the fields.

   Note: To make changes, you must have permission to edit the schedule. Edit permission is denoted by the Edit icon.
5. Click **Update** when finished. Click **Cancel** to exit without saving your changes.

Schedule field descriptions

You can use the following fields to define a schedule.

Field	Description
All Roles	A list of all restricted roles not yet permitted to modify the schedule.

Field	Description
Calendar Name	A calendar for defining when to run the schedule. Sterling Control Center ships with a number of calendars from which to choose; or you can add your own.
Check Schedule Against When Event Occurred	(Rules Schedule) Check this option to use the time that the event occurs to determine whether rule conditions are met. This option is automatically checked when you create a new rule. Uncheck to use engine time to determine whether rule conditions are met.
Description	Text describing the schedule.
Enabled	Select to enable the schedule.
End Day	(Rules Schedule) The day on which the schedule ends. Select from the following options: Calendar Start Day or Start Day + 1-6 days.
End Time	(Rules Schedule) The time to end the schedule. Enter the time in 24-hour format. If you specify a start time, you must also supply an end time. The start time and end time cannot be the same time. If start time is later than end time, the schedule spans two days.
Minimum Duration	(SLC Duration Schedule) The minimum duration processing normally takes.
Maximum Duration	(SLC Duration Schedule) The maximum duration processing normally takes.
Name	A name for the schedule.
Normal End Range End Day	(SLC Calendar Schedule) The day on which the schedule ends. Ranges from calendar start day to calendar start day plus six days.
Normal End Range End Time (NERe)	(SLC Calendar Schedule) The end of a time range that defines when processing normally ends for a monitored item, in 24-hour format. NER end time cannot be the same time as start time. If the start time is later than the end time, NER spans two days.
Normal End Range Start Time (NERs)	(SLC Calendar Schedule) The start of a time range that defines when processing normally ends for a monitored item, in 24-hour format. NER end time cannot be the same time as start time. If the start time is later than the end time, NER spans two days.
Normal Start Range End Time (NSRe)	(SLC Calendar Schedule) The end of a time range when processing normally starts for a monitored item, expressed in 24-hour format. NSR end time cannot be the same time as start time. If the start time is later than the end time, NSR spans two days.
Normal Start Range Start Time (NSRs)	(SLC Calendar Schedule) The beginning of a time range when processing normally starts for a monitored item, in 24-hour format.
Selected Roles	The restricted roles permitted to modify the schedule. Unrestricted roles already have permission to modify schedules.
Schedule Type	Type of Schedule. For a rule schedule, the type is always Calendar. An SLC schedule can be a Calendar or Duration schedule.
Start Time	(Rules Schedule) The time to begin the schedule. Enter the time according to the time zone you selected and in 24-hour format. If you specify a start time you must also supply an end time. The start time and end time cannot be the same. If the start time is later than the end time, the schedule spans two days.
Time Zone	The time zone to use for the SLC, rule, or schedule. Select a time zone from the pull-down menu. This field also shows the difference between the time zone and Coordinated Universal Time (UTC, also known as Greenwich Mean Time). Arizona has its own time zone, because Arizona does not recognize Daylight Saving Time.

Field	Description
This schedule is visible to all users	When selected, this option makes the schedule public and available for selection by all users. Once a public schedule is referenced by any other object, you cannot make it private by restricting visibility to specific roles/users.
This schedule is visible to restricted users in these Selected Restricted Roles	When restricted roles are selected, this option allows only restricted users in the selected roles to view/select/edit the schedule.

Enabling or disabling a schedule

You can enable or disable a schedule for use by Sterling Control Center.

About this task

To enable or disable a schedule:

Procedure

1. From the **Rule/Metadata Schedules** or the **SLC Schedules** listing, double-click the schedule that you want to enable or disable. The **Rule/Metadata Schedule** or **SLC Schedule Properties** window is displayed.
2. Select **Enabled** to add or remove the check mark and click **Update**.

About calendars

A calendar specifies the dates used in a calendar schedule. This includes how long the calendar remains in effect, and how often processing is repeated (recurrence).

Sterling Control Center comes with predefined calendars for each weekday as well as a daily schedule. You can use these calendars for both rule schedules and SLC schedules, and you can create additional calendars to meet your processing needs.

Creating a calendar

Create calendars to specify days/dates, how long the calendar remains in effect, and how often processing is repeated (recurrence).

About this task

To create a calendar:

Procedure

1. Select **Manage** > **Calendars**.
2. Click the Create button to display the **Create Calendar** wizard.
3. Type a unique meaningful **Name** for the calendar, for example, Month End. The name can be up to 25 characters.
4. Type a **Description** for the calendar.
5. Click **Next** to display the **Recurrence** panel. The **Recurrence** panel specifies how often processing occurs and how long the calendar remains in effect.
6. To select the starting date for the calendar:

Click the **Recurrence Range Start** field to display the calendar.

Select the month, year, and date that you want the calendar to take effect.

Click **OK**.

7. Select **No end date** to leave the calendar permanently in effect, or select an end date for the calendar by doing the following:

   Select **Recurrence Range End by**.

   Click the date button to display the calendar.

   Select the month, year, and date that you want the calendar to end.

   Click **OK**.
8. Select a **Recurrence Pattern** (Daily, Weekly, Monthly, or Yearly). The display changes according to the pattern you selected.
9. Select details for the recurrence pattern you selected. See *Recurrence patterns* for more information.
10. Click **Next** to display the **Modifications** panel. The processing dates are highlighted on the calendars based on the recurrence pattern.
11. Click on individual dates to remove them from the recurrence pattern. Click the Right Arrow or Left Arrow button to move forward or backward through the calendar. Click **Reset** to remove all modifications to the calendar. Click **Next to continue.**

    Note: Modifications to a recurrence pattern remain in effect until December 31 of the following year, regardless of the recurrence end date. After December 31 of the following year, you must make the modifications again.
12. Optionally, identify the restricted roles that have permission to modify the calendar. Select a role in **Restricted Roles** and click the Right Arrow button to move it to **Selected Restricted Roles**.

    Note: Unrestricted roles already have permission to modify calendars and are not displayed.
13. Specify whether the calendar will be visible to all users or only to the users in the roles you selected. If you make the calendar visible to all users, you cannot restrict visibility to specific roles after it has been referenced. Click **Next**.
14. Click **Next** to continue.
15. On the **Confirm Choices** page, click **Finish.**
16. Click **Close** on the **Finish** page.

Recurrence patterns

Each recurrence pattern has its own set of parameters. You use these parameters to create calendars to match your processing dates.

The following table describes the four types of recurrence patterns:

Pattern	Description
Daily	Processing occurs every 1–7 days (Monday through Sunday) or every 1–5 weekdays (Monday through Friday). An example is processing that occurs every weeknight.
Weekly	Processing occurs at a specified weekly interval on specified days. An example is payroll processing that occurs every Friday.

Pattern	Description
Monthly	Processing occurs at a specified monthly interval on a specified day, such as the 7th of each month, or the third Monday of each month. An example is accounts receivable processing that occurs on the last day of each month. If you select the 31st as the date, Sterling Control Center sets the date to the last day of the month.
Yearly	Processing occurs once a year on a specified day or date. An example is year-end processing that occurs on January 15.

Viewing or modifying a calendar

After you create calendars, you can view or modify their properties.

About this task

To view or modify a calendar:

Procedure

1. Select **Manage** > **Calendars**.
2. Select a calendar name and click the Properties button or double-click a calendar name to display the **Calendar Properties** window.
3. Click a tab to view its information, or click the **Summary** tab to view an overview of the calendar's definition.
4. Type in the fields you want to change. See *Calendar field descriptions* for descriptions of the fields.

   Note: To make changes, you must have permission to edit the calendar. Edit permission is denoted by the Rule Edit icon.
5. Click **Update** when finished.

Calendar field descriptions

You can use many fields to define a calendar.

The following table describes the fields that comprise a calendar.

Field	Description
Name	A name for the calendar.
Description	Text that describes the calendar.
Recurrence Range: Start	Date when the calendar is to start (defaults to creation date).
Recurrence Range: End: No End Date	No end date is set for this calendar.
Recurrence Range: End: End By	The date on which this calendar ends. Defaults to the last day of the year after the creation date. You cannot set it beyond that date.

Field	Description
Recurrence Pattern	The frequency of occurrence (daily, weekly, monthly, or yearly). Select an end time for the recurrence range by clicking the calendar and selecting a date or select No end date to create a nonending recurrence range. Select Daily, Weekly, Monthly, or Yearly to identify how often to run the schedule. For each option, select the recurrence pattern to use. See *Recurrence patterns*.
Permissions: Restricted Roles	Restricted roles to select from. Select a role and move to **Selected Restricted Roles** by clicking the Right Arrow button.
Permissions: Selected Restricted Roles	Restricted roles that have permission to modify this calendar.
Permissions: This calendar is visible to all users	When selected, this option makes the calendar public and available for selection by all users. Once a public calendar is referenced by any other object, you cannot make it private by restricting visibility to specific roles/users.
Permissions: This calendar is visible to restricted users in these Selected Restricted Roles	When restricted roles are selected, this option allows only restricted users in the selected roles to view/select/edit the calendar.
Modifications	Shows active and inactive dates for the selected calendar. Active dates are shaded yellow. Click a date to activate or deactivate. Click **Reset** to reset the calendar to the dates originally set by choosing the **Recurrence Pattern** on the previous page. Click the Left Arrow button to move to a prior month. Click the Right Arrow button to move forward to the next month.

Calendar example - Monday through Friday processing

This example shows how to create a calendar for Monday through Friday processing.

About this task

To create a calendar for Monday through Friday processing:

Procedure

1. Create a calendar with the following values (see *Creating a calendar*):

Panel	Field	Value
General	Name	Monday-Friday
	Description	Monday through Friday
Recurrence	Start	Today's date
	End	No end date
	Recurrence Pattern	Every 1 weekday(s)
Modification	Modifications	Remove holidays per your company schedule

2. Leave all other fields blank or at their default values.

Chapter 8. Manage email lists

You can create lists of email addresses for groups of users who need to be contacted when an event occurs.

These lists can be selected when you create actions.

Creating an email list

Create an email list that can be used in actions to send notifications to a list of users.

About this task

To create an email list:

Procedure

1. Select **Manage > Email Lists** to display the **Email List** listing.
2. Click the Create button to display the **Add Email List** wizard.
3. Type a name and description for the email list and click **Next**.
4. To add email addresses to the list, click the **To**: field and type the addresses. To import email addresses from a text file, locate the file and click **Import**. To sort the addresses in ascending or descending order, click **Sort**.
5. Click **Next** to continue.
6. Identify the restricted roles that have permission to modify the email list.

   Tip: Unrestricted roles automatically have permission to modify an action.
7. Specify whether the email list will be visible to all users or only to the users in the roles you selected. If you make the email list visible to all users, you cannot restrict visibility to specific roles after it is created. Click **Next**.
8. Click **Finish** to add the email list to the **Email List** listing.
9. Click **Close** to close the **Add Email List** wizard.

Exporting information from an email list

You can export to a text file a list of addresses that have been entered into an email list's To: field.

About this task

To export a list of email addresses:

Procedure

1. Select **Manage > Email Lists** from the Sterling Control Center window to display the **Email List** listing. Double-click an email list to display its properties.
2. From the **E-mail** tab, click **Export**. A file selection window is displayed.
3. Select a location for the text file.

4. Type a name for the text file and click **Export**. The information is exported to a text file.

Exporting email information from an action

You can export to a text file a list of addresses that have been entered into an action's **To:** field.

About this task

To export a list of email addresses:

Procedure

1. Select **Manage** > **Rules and Actions** > **Actions** from the Sterling Control Center window to display the **Actions** listing. Double-click an action to display its properties.
2. From the **E-mail** tab, click **Export**. A file selection window is displayed.
3. Select a location for the text file.
4. Type a name for the text file and click **Export**. The information is exported to a text file.

Displaying a listing of email lists

After you have created email lists, you can display a listing of them.

About this task

To display the Email List listing:

Procedure

1. From the Sterling Control Center window, select **Manage > Email Lists**.
2. To sort on any column, click the column heading.

Viewing or modifying email lists

You can view or modify email lists.

Procedure

To view or modify an email list:

1. Select **Manage** > **Email Lists** from the Sterling Control Center window to display the **Email List** listing.
2. Do one of the following:
   - Select an email list and click the Properties button.
   - Double-click the email list.
3. Click in a field to view field-level help. Field-level help is displayed in the status bar.
4. Modify the email list information as necessary. See *Email list field descriptions* for definitions of email list fields.

   Attention: To make changes, you must have permission to edit the email list. Edit permission is denoted by the Rule Edit icon.
5. Click **OK** when finished.

Email list field descriptions

The following table describes the fields that define an email list.

Field Name	Description
Description	Text describing the action. Optional.
Name	The name of the email list.
Restricted Roles	List of restricted roles defined in Sterling Control Center. Select a role and click the Left Arrow or Right Arrow button to move the role between this field and Selected Restricted Roles.
Selected Restricted Roles	Restricted roles with rights to modify this email list. If no roles are selected, only an unrestricted user (admin) can modify this email list.
This email list is visible to all users	When selected, this option makes the email list public and available for selection by all users. Once a public email list is referenced by any other object, you cannot make it private by restricting visibility to specific roles/users.
This email list is visible to restricted users in these Selected Restricted Roles	When restricted roles are selected, this option allows only restricted users in the selected roles to view/select/edit the email list.
To	The list of email addresses. Email lists can be used to notify addressees when an action is triggered.

Chapter 9. Metadata rules overview

Using metadata rules, you can append additional elements and values to Sterling Control Center events before they are processed by both the Rule and SLC services.

Metadata rules are applied to all Sterling Control Center events, unless you explicitly set them not to be, for statistics collected from specific managed servers. The additional metadata type elements and values are logged in the Sterling Control Center Events database. When a metadata rule matches an event, Sterling Control Center appends metadata to the event as lists of key value pairs. You can use these metadata fields as matching criteria when defining conventional rules. Metadata can also be used as filter criteria for reports and alert monitor or activity monitor data.

Metadata rules be used to simplify the specification of your rule and SLC criteria. They can also be used to simplify specification of your report criteria. For more information about metadata rules and how they differ from regular rules, see *Implementation*.

Note: Metadata can be used to analyze only new activity. You cannot do retroactive analysis of existing data.

Creating a metadata rule

Create metadata rules Metadata rules to append additional elements and values to Sterling Control Center events before they are processed by the SLC service or normal rule processing.

About this task

To create a metadata rule:

Procedure

1. Select **Manage** > **Metadata** > **Metadata Rules** to display the **Metadata Rules** listing.
2. Click the Create button to display the **Create Metadata Rule** wizard.
3. Type a **Name** and **Description** for the metadata rule and click **Next**.

   Note: For detailed definitions of metadata rules fields, see *Creating a metadata rule*.
4. Select a server group or groups on which to apply the metadata rule by moving the group (using the Right Arrow button) from **Groups** to **Selected Groups**. Click **Next**.
5. Select individual servers on which to apply the metadata rule by moving the server (using the Right Arrow button) from **Servers** to **Selected Servers**. Click **Next**.

   Note: At least one server or server group is required for a restricted role.

6. Optionally, select one or more **Schedules** to associate with the metadata rule by moving the schedule (using the Left Arrow and Right Arrow buttons) from **Rule/Metadata Schedules** to **Selected Schedules**.

   Note: Create a new schedule by clicking the Create button for the **Rule/Metadata Schedules**. You can duplicate an existing schedule and modify the duplicate by clicking the Duplicate button. View the properties of a schedule in either **Rule/Metadata Schedules** or **Selected Schedules** by selecting the schedule and clicking the Properties button.
7. Click **Next**.
8. Specify one or more selection criteria to further define the metadata rule by choosing a **Key**, an **Operator**, and a **Value** for each parameter. The list of operators depends on whether the key is numeric (for example, Return Code and File Size) or alphanumeric. For more information on keys you can use as rule criteria, see *Keys and Fields*. Click **Next**.
9. Select a **Metadata Action** to perform when the parameters and schedules are met.

   Note: Create a new metadata action by clicking the Create button for the **Action**. Duplicate an existing metadata action and modify the duplicate by clicking the Duplicate button. View the properties for a metadata action by selecting the action and clicking the Properties button. For more on metadata action properties, see *Creating metadata actions*.
10. Click **Next** and then **Finish** to add the metadata rule to the **Metadata Rules** listing.
11. Click **Close** to close the **Create Metadata Rule** wizard.

Displaying the metadata rules listing

After you have defined metadata rules, you can display a metadata rules listing.

About this task

To display the Metadata Rules listing:

Procedure

From the Sterling Control Center window, select **Manage** > **Metadata** > **Metadata Rules**. The **Metadata Rules** listing is displayed.

Viewing or modifying a metadata rule

After you have created metadata rules, you can view or modify them.

About this task

To view or modify a metadata rule:

Procedure

1. Select **Manage** > **Metadata** > **Metadata Rules** to display the **Metadata Rules** listing.
2. Do one of the following to display the **Metadata Rule Properties** window for a rule:
   - Double-click the metadata rule

- Select the metadata rule and click the Properties button.

3. Select from among the tabs to display property subgroups and modify properties as needed. See *Metadata rules field definitions* for descriptions of metadata rule fields.

   Note: To make changes, you must have permission to edit the metadata rule. Edit permission is denoted by the Editable Icon.
4. Click **Update**.

Reordering metadata rules

As with standard rules processing, an event can match at most one metadata rule. When it matches a metadata rule, all metadata rules lower in the hierarchy are ignored and thus not matched on for that event. You can change the hierarchical order of metadata rules to change which will be matched upon first.

About this task

To change the order of metadata rules:

Procedure

1. In the **Metadata Rules** listing, select the metadata rule to reorder.
2. In the **Move selected to position #** field, type the position in which to place the metadata rule.
3. Click **Move**.

   Note: You must sort metadata rules in Priority ascending order prior to changing their position in the listing.

Enabling metadata rules

After you have created metadata rules, you can enable or disable them.

About this task

To enable or disable a metadata rule:

Procedure

1. In the **Metadata Rules** listing, do one of the following:
   - Select the metadata rule and click the Properties button.
   - Double-click the metadata rule.
2. In the **Metadata Rule Properties** window, click **Enabled** to place or remove the check mark.
3. Click **Update**.

   Note: When you remove the only server or server group used by a metadata rule, the metadata rule is automatically disabled.

Metadata rules field definitions

You can use many fields to define metadata rules.

Following are definitions for the fields that make up a metadata rule.

Field	Description
Name	The name of the metadata rule.
Description	Text describing the metadata rule.
Groups	Server groups to choose from.
Selected Groups	The server group the metadata rule applies to.
Servers	The list of servers to choose from.
Selected Servers	Servers to which you want the metadata rule to apply.
Rule Schedules	The list of schedules to choose from.
Selected Schedules	The schedules you want associated with the metadata rule.
Parameters	Selection criteria for further defining the rule. Choose a Key and Operator and enter the Value you want to monitor. For more information on parameters, see *Metadata rules field definitions*.
Parameters: Operator	Operator for defining the metadata rule's match criteria.
Parameters: Value	A value for further defining the metadata rule's match criteria.
Actions	The actions to perform when the metadata rule criteria are met.

Managing metadata type mapping

You can append as many as four metadata elements, and values, per Sterling Control Center event using metadata actions. The element names are called metadata types. Changing the way metadata elements are labeled is called mapping metadata types.

About this task

Attention: Unlike other configuration data, the Metadata Type Mapping for User Data and Server Data is stored in the database, rather than in the local Sterling Control Center configuration. If you switch to a new database or reinitialize the existing database during upgrading or for any other reason, the Metadata Type Mapping data will be lost. Make note of these values before switching or initializing the database and reconfigure them afterwards.

To map metadata types:

Procedure

1. Select **Manage** > **Metadata** > **Metadata Type Mapping**.
2. On the Rules/Actions tab, for each metadata type you wish to map, enter a name that describes the metadata.
3. On the Server Metadata Titles tab, for each server metadata type you wish to map, enter a name that describes the metadata.
4. When finished, click **OK**.

Note: Once you map a metadata type to a new value, that value appears in place of the default in lists of Key selections when you create rules or set filters for metadata actions (for Rules/Actions metadata fields), or when you specify server metadata (for Server Metadata Titles) or for both when you generate reports containing metadata.

About metadata actions

In Sterling Control Center, metadata actions act similarly to conventional ones, but they are used only by metadata rules (and metadata rules can only refer to metadata actions). You manage metadata actions in much the same way as conventional ones.

The values in a metadata action are added to events when the metadata rules they are part of match the events.

Creating metadata actions

You can create metadata actions that can be used in metadata rules.

About this task

To create a metadata action:

Procedure

1. Select **Manage** > **Metadata** > **Metadata Actions** to display the **Metadata Actions** listing.
2. Click the Create button. The **Create Metadata Action** wizard displays.
3. Type a **Name** and **Description** for the new metadata action and click **Next** to continue.
4. Enter a metadata value for any field you want to have set when the metadata action is performed.

   Note: To change the label of a metadata field, see *Metadata rules overview*.
5. To include a variable as part of the metadata value for a field, click **Insert Var** next to the field. Select a variable from the **Variable** listing. Click **OK** to insert a variable and return to the **Create Metadata Action** wizard.

   Note: For a description of variables, see *Sterling Control Center variables*.
6. Click **Next**.
7. If you want to restrict use of this metadata action to certain roles, highlighting the roles in **All Roles** and click the Right Arrow button to move them to **Selected Roles**. You can also add, duplicate, or check the properties of roles using the buttons that follow All Roles.
8. Click **Next**.
9. Click **Finish** and then **Close** to add the action to the **Metadata Actions** listing.

Displaying metadata actions

You can display a list of the metadata actions you have created.

About this task

To display the Metadata Actions listing:

Procedure

Select **Manage** > **Metadata** > **Metadata Actions**. The **Metadata Actions** listing displays.

Viewing and modifying metadata actions

You can view and modify metadata actions.

About this task

To view or modify a metadata action:

Procedure

1. From the **Metadata Actions** listing, do one of the following:
   - Select an action and click the **Properties** Icon.
   - Double-click an action
2. Modify the metadata action information as necessary.

   Note: To make changes, you must have permission to edit the metadata action. Edit permission is denoted by the **Rule Edit** Icon.
3. Click **Update** when finished.

Chapter 10. Perform guided node discovery

Guided Node Discovery (Node Discovery) allows you to find Sterling Connect:Direct servers deployed in your Enterprise Network.

Node Discovery can be performed on servers managed by Sterling Control Center and ones not managed by Sterling Control Center.

Note: Sterling Connect:Enterprise, FTP, and Sterling B2B Integrator servers do not support Node Discovery.

Summary of node discovery process

The first step in Node Discovery is to specify the time frame and the servers on which to perform it. Then, after you start Node Discovery, the following occurs:

1. Sterling Control Center tries to contact each enabled Explorer server.
2. After a server is contacted, Sterling Control Center obtains the data transmission facility (DTF) address, DTF port, license, and node name and populates the Explorer List with this information. It updates the Last Discovery Date/Time in the Explorer List. Then information from the server's network map and statistics records (for the time specified) is scanned for other servers with whom the server communicates.
3. If a server cannot be contacted, the MsgID and Return Code fields in the Explorer List are updated with information concerning the errors that prevented the connection.
4. For each unique trading partner identified in the server's network map or statistics record, a server entry is added to the Discovery List.
5. When Node Discovery is complete, other fields in the Explorer List are populated, including return code, last explore range, and last successful Discovery.

Identify servers for node discovery

Before doing Node Discovery, you add Sterling Connect:Direct servers to the Explorer List. You can add servers already managed by Sterling Control Center and unmanaged servers not defined in Sterling Control Center.

In order to perform Node Discovery on a server, the credentials specified must be authorized to access a server's network map information. After you add a node to the Explorer List, it is displayed with **CD Stopped Function Icon**, indicating that the node has not been contacted. To determine whether it can be contacted, enable the node for Node Discovery.

Note: If a server is located during Node Discovery and it is already defined in the Discovery List, Explorer List, or My List, the server is ignored. Servers with identical DTF address and DTF port values are considered duplicates.

Adding a managed server to the Explorer List

Before you perform node discovery on managed servers, you have to add them to the Explorer List.

About this task

To add a managed server to the Explorer List:

Procedure

1. Select **Tools** > **Node Discovery**.
2. From the **Explorer List** tab, click the Create button. The **Add Server to Explorer List wizard** is displayed.
3. Select **Control Center-Managed Server** and click **Next**.
4. In the **All Managed Servers** box, highlight one or more managed servers to add to the list and click the Right Arrow button to add them to the **Explorer List**.
5. Click **Next**.
6. Review the selected servers. If the list is correct, click **Finish** to add the servers. If the list is not correct, click **Back** to make any changes and repeat this procedure.
7. To add more servers, click **Add Another Server** and repeat steps 3–6.
8. Click **Close** to close the wizard.

Adding an unmanaged server to the Explorer List

Before you perform node discovery on unmanaged servers, you have to add them to the Explorer List.

About this task

To add an unmanaged server to the Explorer List:

Procedure

1. Select **Tools** > **Node Discovery**.
2. From the Explorer List tab, click the Create button. The **Add Server to Explorer List wizard** is displayed.
3. Select **Unmanaged Server** and click **Next**.
4. Select the type of server and click **Next**: Sterling Connect:Direct with TCP/IP API or Sterling Connect:Direct for i5/OS. Sterling Connect:Direct server platforms that operate under TCP/IP API include:
   - Sterling Connect:Direct for HP NonStop
   - Sterling Connect:Direct for z/OS
   - Sterling Connect:Direct for UNIX
   - Sterling Connect:Direct for Microsoft Windows
5. Do one of the following:
   - If you chose Sterling Connect:Direct platforms with TCP/IP API, provide the following required information about the server:
     - API Address
     - API Port
     - User ID
     - Password
   - If you chose Sterling Connect:Direct for i5/OS, provide the following information:
     - Host Name

- Library Name
- User ID
- Password

6. Fill in optional fields with any available information. Refer to the context-sensitive Help for each field for more information.
7. Click **Test Connection** to validate the login information provided.
8. Click **Next**.
9. Review the information about the server. If the information is correct, click **Finish** to add the server.
10. To add another server, click **Add Another Server** and repeat steps 3–9.
11. Click **Close**.

Manage the Explorer List

Viewing or modifying a server definition after node discovery

After node discovery, you can modify server definitions for servers listed in the Explorer List.

About this task

To modify a server defined in the Explorer List:

Procedure

1. From the **Node Discovery** window, highlight the server.
2. Click **Properties**.
3. Modify property fields as desired and click **OK**.

Enabling a server for discovery

Before you can run node discovery, you need to enable servers for discovery.

About this task

To enable a server for Node Discovery:

Procedure

1. From the **Node Discovery** window, highlight the server to enable and click **Enable for Discovery**.
2. You are informed if a selected server cannot be enabled. Do the following to enable the node for Node Discovery:

   Click **Yes** to configure the node.

   Type the correct information about the server.

   Click **OK**.

Disabling a server for discovery

You can disable a server for node discovery.

About this task

To disable a server for Node Discovery:

Procedure

From the **Node Discovery** window, highlight the server and click **Disable for Discovery**.

Removing a server from the Explorer List

You can remove a server from the Explorer List.

About this task

To remove a server from the Explorer list:

Procedure

Highlight the server to remove from the **Node Discovery** window and click the Remove button.

Note: When you remove a server, all discovered nodes associated with this node in either the Discovery List or My List are removed. However, if a node in the Discovery List or My List is associated with the deleted node and another Explorer node, it is not removed.

Running node discovery

After you add servers to the Explorer List and enable them for Node Discovery, you are ready to run Node Discovery. Node Discovery searches the statistics records and network map of the servers to identify other servers with which they have communicated.

About this task

After you start Node Discovery, you can close the **Node Discovery** window. Node Discovery continues to search statistics records and network maps of the enabled nodes. A progress bar displays the status of the Node Discovery activity when you reopen the Node Discovery window.

After Node Discovery is complete, Sterling Control Center updates the Last Discovery and Last Successful Discovery Date/Time (when applicable) for each enabled Explorer node.

If Sterling Control Center cannot contact an enabled Explorer server for Node Discovery, the Return Code, Msg ID, and Message Text fields are updated with information about why the connection failed.

To run Node Discovery:

Procedure

1. If necessary, select **Tools > Node Discovery** to open the **Node Discovery** window.
2. From the **Explorer List** tab, click **Run Discovery**. The **Discovery Date Range** dialog is displayed.
3. To identify the date range of statistics records searched:
   - Click **Start Date**.
   - Select a date on which to begin searching statistics records.

- Click **OK**.
- Click **End Date**.
- Select an end date for the statistics record search.
- Click **OK**.

4. Click **OK**.

Identify the status of servers in the node discovery list

The **Node Discovery** window displays the servers that you added to the Explorer List with information about each server.

The following icons are displayed with a server to indicate its status:

Icon	Description
	The server is connected and available for Node Discovery.
	The node either has not been enabled for Node Discovery or cannot be contacted.
	The server is enabled for Node Discovery.
	The server is managed by Sterling Control Center.

Manage the Discovery List and My List

After Node Discovery has been performed, the **Discovery List** window displays information about servers found during Node Discovery. After Node Discovery has identified a server, the server can be moved to the Explorer List and used to discover additional servers, or it can be moved to My List.

My List provides a work area and a place to move discovered nodes to prevent the Discovery List from getting cluttered. The server can also be added to the list of managed servers.

Moving a server to My List

After a server has been identified using Node Discovery, you can move it from the Discovery List to My List.

About this task

To move a server to My List:

Procedure

From the **Discovery List** tab, do one of the following:

- Highlight the server to move and click **Move to My List**.
- Right-click the server and select **Move to My List** from the contextual menu.

Moving a server to the Discovery List

You can move a server from My List to the Discovery List.

About this task

To move a server to the Discovery List:

Procedure

1. From the **My List** tab, do one of the following:
   - Highlight the server to move and click **Move to Discovered List**.
   - Right-click the server and select **Move to Discovered List** from the contextual menu.
2. Completed the required server and license information (at minimum).
3. Click **Test Connection** to test the connection to this server.
4. Click **OK** to move the server.

Moving a server to the Explorer List

You can move a server to the Explorer List from the Discovery List or My List.

About this task

To move a server to the Explorer List:

Procedure

1. From the **Discovery List** tab or **My List** tab, do one of the following:
   - Highlight the server to move and click **Move to Explorer List**.
   - Right-click the server and select **Move to Explorer List**.
2. Select the type of server: Sterling Connect:Direct with TCP/IP API or Sterling Connect:Direct for i5/OS. Sterling Connect:Direct server platforms that operate under the TCP/IP API include:
   - Sterling Connect:Direct for HP NonStop
   - Sterling Connect:Direct for z/OS
   - Sterling Connect:Direct for UNIX
   - Sterling Connect:Direct for Microsoft Windows
3. Do one of the following:
   - If you chose Sterling Connect:Direct with TCP/IP API, provide the following required information about the server:

     API Address

     API Port

     User ID

     Password
   - If you chose Sterling Connect:Direct for i5/OS, provide the following information:

     Host Name

     Library Name

     User ID

     Password
4. Fill in optional fields with any available information. Refer to the Help displayed for each field for more information.
5. Click **Test Connection** to validate the connection to the server.

6. Click **OK** to move the server. To add a server in the Explorer List to the list of managed servers, see *Adding a managed server to the Explorer List*.

Showing partners

The Partners Table lists all nodes that have communicated with the selected explorer or discovered node. A node contained in the explorer node's netmap or that shows up in node statistics may also be listed in this table, even if the node in question has never communicated with the selected node. This status is indicated by the check mark in the netmap or statistics column.

About this task

To view the partners of an explorer node:

Procedure

1. In the **Node Discovery Explorer List** or **Discovery List**, right-click a server.
2. Select **Show Partners**. The Partners Table displays a listing of partner nodes. The columns that comprise the listing are defined in the following table:

Column	Description
#	Row number.
Name or Alias	The server ID.
Node Name	The Sterling Connect:Direct node name.
Node Type	Type of Sterling Connect:Direct node (D = Discovered, E=Explorer).
From Netmap	A check mark indicates that this node was identified as a partner by virtue of being in the selected node's netmap.
From Stats	A check mark indicates that this node was identified as a partner by virtue of being included in node statistics.
Discovered Time	Time the node was found during Node Discovery.
Comments	User-entered comments.

Adding discovered node comments

You can add comments about servers in the Discovery List. Examples of useful comments might include a note to the effect that a server is no longer in use and needs to be removed from the network, or that a server's license needs updating.

About this task

To add comments about servers in the Discovery List:

Procedure

1. In the **Discovery List**, do one of the following:
   - Right-click a server and select **Comments**.
   - Double-click the server.
2. Type comments in the **Discovered Node Comments** window text box. The maximum number of characters is 2048.
3. Click **OK**.

Removing a server from the Discovery List or My List

You can remove a server from the Discovery List or My List.

About this task

To remove a server from one of these lists::

Procedure

1. Click the **Discovery List** tab or **My List** tab.
2. Highlight the server or servers to remove from the **Node Discovery** window and click the Remove button.

   Note: When you remove a server from the Explorer List, all discovered nodes associated with that server in either the Discovery List or My List are removed—unless they are associated with another Explorer node.

Chapter 11. About Sterling Control Center reports

Sterling Control Center allows you to define and run a variety of reports.

There are four types of Sterling Control Center reports:

- Standard Sterling Control Center reports are produced from the Sterling Control Center console, either on demand (**Reports** > **Define/Run**) or by scheduling them to be run at a certain time and sent to designated recipients via email (**Reports** > **Automate**). You can run existing reports using the Web Console.

  The Audit Log is a standard report of changes made to Sterling Connect:Direct server configuration objects. It can be run as an on-demand report or displayed on screen (by selecting **Tools** > **Audit Log**).
- Database reports use SQL queries or a third-party tool such as Crystal Reports to extract data from the Sterling Control Center databases and create the reports. Sterling Control Center provides several sample reports in Crystal Reports format that you can use with the Sterling Control Center databases if you already have Crystal Reports. You can also use these samples as templates to design your own reports. For more information on database schemas, including database tables and field definitions, see *Data for third-party reporting tools* in *Reports*.
- Log files on standard reports are saved to the Cognos/logs folder. After using these logs for general debugging and maintenance purposes, you may want to clear out these backups on a regular basis to keep this directory to a reasonable size.
- The SLC Debug Report is useful for troubleshooting an SLC. To access this report, select **Tools** > **Run SLC Debug Report**. The report is saved to the Sterling Control Center engine log folder and the name of the file is SLCDebugReport.html

Important: When you add an IBM Sterling Connect:Direct node to Sterling Control Center for monitoring, you must run configuration management on the node before you can run reports on it. To manage a configuration option, such as, functional authorities, Sterling Control Center polls the node and puts the information in the database. After the database is populated with the information, you can run reports on the node.

Chapter 12. Sterling Control Center settings

Sterling Control Center settings control system behavior and performance. Most settings are specified during system installation and do not need to be changed. However, you may need to change some settings to accommodate new requirements.

For more information on both engine and console logs, see *Modify log4j to retain log files*. The following table describes the tabs on the **Sterling Control Center System Settings** window:

System Setting	Description
Application Log	Displays the location of the console application log file. The application log stores information about Sterling Control Center console activity. The log name is system generated. The log is stored in the `ControlCenter\log` directory as a text file. If you access the console through Java™ Web Start, the log file location is shown. The application log setting is view-only. You cannot change it.
Console	**Default Graphic Activity Monitor Expected Maximum Processes** specifies the default value that constitutes a high level of server activity, as depicted by the bar graph for the server in the Servers listing and in graphic visualizations of server activity. **Default Console Auto Refresh Setting** sets the default number of seconds between automatic refreshes of the activity monitors for users with permission levels that allow for automatic refresh. The **Enter Default Console Timeout values** settings specify the default number of minutes a user session is inactive before the user is logged out and the default number of minutes before the inactivity timeout has been reached that a warning message will be displayed.
Database	Defines the location and type of Sterling Control Center databases (production and staging), how the connections to the databases are established, when to automatically handle alerts, when and how to send data to the staging database, and when and how to automatically purge it from the staging database. See *Database settings field definitions* for field definitions. Refer to *Database administration* for more information on staging and purging. These settings are established during installation. Take caution when changing them because they affect Sterling Control Center operation.
E-mail	Specifies the communications parameters used to send email messages. Display only. **Important:** To change SMTP email settings, run the configCC utility. If you change email settings, you must also configure Cognos Business Intelligence server using the configCC utility. In Sterling Control Center, you can create an action to send an email. That action can be referenced by one or more rules, which when triggered will send an email. See *Email settings* for field definitions. You can also customize the email subject and contents. See *Creating an action*.

System Setting	Description
Engine Connection	These setting specify the port that the Sterling Control Center engine is configured to listen on for connections from the Sterling Control Center console. This setting is defined during Sterling Control Center installation and is view only.
File Agent	Settings on the **File Agent** tab let you specify settings Sterling Control Center uses to listen for process submissions from file agents associated with managed Sterling Connect:Direct servers.
License Management	**License Key Versions** defines the number of license key versions to keep in history. This tab also allows you to control email settings for importing license key information via email.
SNMP Hosts	Specifies the host computers where Simple Network Management Protocol (SNMP) traps are sent. You can define a Sterling Control Center action that sends a trap to an SNMP tool. These traps contain information from the event that can be used for diagnostics. The action can be referenced by one or more rules, which when triggered will send the SNMP trap. See *SNMP host settings* for information about adding, changing, or deleting SNMP hosts.
Services	Controls the number of simultaneous pollers, as well as settings relating to configuration management. See *Services field descriptions*.

These settings are all system-wide. See *Changing system settings* for the procedures to change them.

You can also specify how to display time on your Sterling Control Center console. This setting, which is not system-wide, is described in *Console Preferences*.

Changing system settings

If you have privileges to do so, you can change any of the system settings.

About this task

To change system settings:

Procedure

1. Take one of the following actions:
   - Select **Control Center** > **System Settings**.
   - Right-click the Sterling Control Center icon and select **Properties**. The **System Settings** panel is displayed.
2. To change database settings, select the **Database** tab and change the values. For definitions of database fields, see *database settings*.
3. To change email connection settings, select the **E-mail** tab and change the values. For definitions of the email fields, see *Email settings*.
4. To change the SNMP Hosts settings, select the **SNMP Hosts** tab and change the values. For more, see *SNMP Host Settings*.
5. To view the log file name, select the **Application Log** tab. For a definition of this field, see *Application log field description*.

6. To change the simultaneous pollers setting, select the **Services** tab. For a definition of this field, see *Services field descriptions*. For more considerations and general information, see *Tune the Sterling Control Center engine*.
7. To view the ports that are used to connect to the Sterling Control Center engine, select the **Engine Connection** tab. For definitions of the Engine Connection fields, see *Engine connection field descriptions*.
8. To change the default values for the console settings, select the **Console Settings** tab. You can change the following settings:
   - Default Graphical Activity Monitor expected maximum processes
   - Default Console Auto Refresh System Setting in seconds
   - Default Timeout values

   For a definition of these settings, see *Console settings field descriptions*.
9. To change license management settings, including settings for the email address to which license expirations are sent, select the **License Management** tab. For definitions of these fields, see *Managing licenses*.
10. To change File Agent settings, select the **File Agent** tab. For definitions of these fields, see *File Agent field descriptions*.
11. Click **Update** when you complete the changes.

Database settings

Database settings are viewable on the Database tab of System Settings. You can modify database settings depending on your role privileges.

About this task

To manage database settings:

Procedure

1. Click **Control Center** > **System Settings**.
2. Modify database settings as required (depending on your role privileges). Click **Update** to save changes.
3. View detailed display-only information about the Sterling Control Center databases by doing one of the following from the Database tab of System Settings:
   - Click **Production DB Info** (for the production database).
   - Click **Staging DB Info** (for the staging database).
4. To view more detailed database setup information, statistics, and other information, click tabs on the Staging Database or Production Database panel.
5. Refresh the information by clicking **Refresh**.
6. Click **Close** to close the panel.

Database settings field definitions

You can use the following fields to define database settings.

Field	Definition
Automatically Handle Alerts Older Than (Hours)	The number of hours after which alerts are automatically moved from the Active Alerts monitor to the Handled Alerts Monitor. If this value is set to 0, no alerts are moved.

Field	Definition
Average Delete Time	Average time in milliseconds required to move rows from production to staging database. Display only.
Average Insert Time	Average time in milliseconds required to add rows to the production database. Display only.
Average Update Time	Average time in milliseconds required to update rows in the production database. Display only.
CD Stats table rows	Number of table rows of Sterling Connect:Direct statistical data. Display only.
CE Stats table rows	Number of table rows of Sterling Connect:Enterprise statistical data. Display only.
CX Stats table rows	Number of table rows of Sterling Connect:Express statistical data. Display only.
Database Name	Name of the production database. Set at installation. Display only.
Database Type	Type of production database. Set at installation. Display only. Values include: • Oracle • DB2® • Microsoft SQL
Data Movements Status	Whether or not currently running. Display only.
Event table rows	Number of table rows of event data in the production database. Display only.
Host Name	The computer where the production database is installed. Set at installation. Display only.
Last Data Movement Duration	Time that last data movement took. Display only.
Last Data Movement End	Date/time of end of last data movement. Display only.
Last Data Movement Start	Date/time of beginning of last data movement. Display only.
Last Purge Duration	Time that last purge required. Display only.
Last Purge End	Date/time of end of last purge. Display only.
Last Purge Start	Date/time of beginning of last data purge. Display only.
Movement of Data to Staging Database: Audit Data Older Than (days)	The number of days after which configuration management audit data are moved from the production database to the staging database. The default value is 7. The minimum value is 2.

Field	Definition
Movement of Data to Staging Database: Data Older Than (days)	The number of days after which statistical and event data are moved from the production database to the staging database. The default value is 7. The minimum value is 2. **Note:** If the Production Database is partitioned or no Staging Database is defined, the removed data is discarded. If the Production Database is not partitioned and a Staging Database has been defined, the removed data is added to the Staging Database. **Note:** This setting determines how far back Sterling Control Center can resume monitoring when a user pauses and then resumes monitoring. For example if this parameter specifies seven days and the user pauses the server for two weeks, Sterling Control Center will resume monitoring seven days back, not all the way back to the pause point when data is requested from the server. For more information, see *Pausing and resuming process activity monitors* in *User*.
Movement of Data to Staging Database: Number of Rows to Select per DB Transaction	The maximum number of production database rows Sterling Control Center reads into memory in preparation for moving to the staging database row by row. The default is 4000.
Movement of Data to Staging Database: When to Begin Moving Data	The number of minutes between attempts by Sterling Control Center to move data from the production database to the staging database. Or, the time of day to begin moving data to the staging database.
Next Scheduled Data Movement	Date/time of end of next scheduled data movement. Display only.
Next Scheduled Purge	Date/time of end of next scheduled purge. Display only.
Number of Rows to Select per DB Transaction	The maximum number of database rows Control Center reads into memory in preparation for purging data from the staging database row by row. The default is 4000.
Oldest Record	Oldest record in the production database, in days. Display only.
Port	The port number used to access the production database. Set at installation. Display only.
Purge Status	Whether or not purge is currently running. Display only.
Purging of Data from Staging Database: Audit Data Older Than (Days)	Automatically purge configuration management audit data older than the days defined in this field from the events and statistics tables in the staging database. The default value is 30.
Purging of Data from Staging Database: Data Older Than (Days)	Automatically purge data older than the days defined in this field from the events and statistics tables in the Sterling Control Center staging database. The default value is 30.
Purging of Data from Staging Database: When To Begin Purging Data: Run Daily at time.	The time at which to do a daily purge. Defined as Sterling Control Center engine time.

Field	Definition
Purging of Data from Staging Database: When To Begin Purging Data: Run Every n Minutes	The number of minutes between database purge attempts.
Removal of data from production database: Data Older than (days)	The number of days after which statistical and event data are removed from the production database. The default value is 7. The minimum value is 2.
Removal of data from production database: Audit Data Older than (days)	The number of days after which configuration management audit data are removed from the production database. The default value is 7. The minimum value is 2.
Removal of data from production database: When to begin moving data	The number of minutes between attempts by Sterling Control Center to remove data from the production database. Or, the time of day to begin removing data.
Removal of data from production database: Number of rows to select per DB transaction	The maximum number of production database rows Sterling Control Center reads into memory in preparation for removing row by row. The default value is 4000.
User ID	The user ID you assign to access the database. Display only.

Email settings

Sterling Control Center provides proactive email notifications for events. Email settings are configured during installation. To configure or change email settings after installation, use the configCC utility.

The email settings you configure are displayed on the E-Mail tab in System Settings. These settings cannot be edited using the console.

SNMP host settings

SNMP Hosts settings specify the host computers where SNMP traps are sent from Sterling Control Center.

Adding an SNMP host

Add an SNMP Hosts settings to specify the host computers where SNMP traps are sent from Sterling Control Center

About this task

To add an SNMP host:

Procedure

1. Select **Control Center** > **System Settings** to display the **System Settings** window.
2. Select the **SNMP Hosts** tab.
3. Click **Add** to display the **Add Host** window.
4. Type the following information (see *SNMP Host Settings* for details):
   - Host Name

- Port
- Community (optional)

5. Click **OK**.
6. Click **Add** to add another SNMP host, or click **OK** to close the **System Settings** window.

Editing an SNMP host

You can edit SNMP host settings.

About this task

To edit an SNMP host:

Procedure

1. Select **Control Center > System Settings** to display the **System Settings** window.
2. Select the **SNMP Hosts** tab.
3. Double-click the table row to edit, enter your changes, and click **OK**.

Removing an SNMP host

You can remove an SNMP host.

About this task

To remove an SNMP host:

Procedure

1. Select **Control Center > System Settings** to display the **System Settings** window.
2. Select the **SNMP Hosts** tab.
3. Select the host you want to remove.
4. Click **Remove**.
5. Click **OK** on the confirmation window.

SNMP host settings field definitions

There are three field definitions to define SNMP host settings.

Following are field definitions for the SNMP Host Settings:

Field Name	Definition
Host Name	The IP address of the server that Sterling Control Center sends SNMP traps to. This field is required if you configure the host settings.
Port	The optional 1- to 5-digit port number that the SNMP host listens for traps on. The default value is **162**. The maximum value is 65535.
Community	The SNMP community string included in the SNMP traps generated by Sterling Control Center. The maximum length is 64 characters. No special characters allowed. Required if you configure host settings.

Application log field description

There is one field description for an application log.

The following table defines the single field on the Application Log tab in System Settings.

Field	Definition
Log File Name	The application log stores information about Sterling Control Center console activity. The name is system generated. The log is stored in the ControlCenter\log directory as a text file. The application log file name setting is view only. You cannot change it.

Services field descriptions

You can use many fields to define services in Sterling Control Center.

The following table defines the fields on the Services tab in System Settings.

Field	Definition
Simultaneous Pollers	The number of threads Sterling Control Center uses to poll Connect servers in collecting server statistics. The minimum and default value is **7**. **Note:** A good rule of thumb for setting this value is to make it the larger of either 7 or 20% of the total number of managed servers. That is, if the number of servers is less than 35, set Simultaneous Pollers to 7; if the number is 35 or greater, set Simultaneous Pollers to the total number of managed servers times 0.20.
Check for configuration changes on servers	How often Sterling Control Center should check for changes to configuration objects on managed servers. Select Never or specify a time for Run Daily at.
Minimum number of configuration versions	The minimum number of configuration versions Sterling Control Center should retain for each configuration object type.
Minimum age of configuration versions	The minimum age of configuration versions that Sterling Control Center should retain.

Field	Definition
Start certificate expiry notification	The number of days before expiry of trusted or key certificates when Sterling Control Center will begin generating events. The default is **60 days**. Certificate expiry checking works only for certificates in Sterling Control Center's object repository. To ensure that your certificates are in the repository, you can manually check and add them using **Configure Servers** > **Secure+** > **Secure+ Key Certificates** or > **Secure+ Trusted Certificates**. Or, you can automatically check for configuration changes on a daily basis using the **Check for Configuration Changes on Servers** system setting. This option is available only for servers that support configuration management. When a certificate has reached the point when expiry notifications are to be generated, notifications are generated once a day until the certificate's expiration time changes. To act upon certificate expiry events, or notifications, you can use the Certificate Expiry Warning predefined rule to define the number of days before expiry that action will be taken. For more information, see *How can I know when my Sterling Connect:Direct Secure Plus certificates are about to expire?* in *How-To*.

Engine connection field descriptions

There are two fields to define engine connections.

The following table defines the fields on the Engine Connection tab in System Settings.

Field	Definition
Engine HTTP Port	The HTTP port (for nonsecure connections) that the Sterling Control Center engine listens on. This setting is defined during Sterling Control Center installation. Display only.
Engine HTTPS Port	The HTTPS port (for secure connections) that the Sterling Control Center engine listens on. This setting is defined during Sterling Control Center installation. Display only.

Console settings field descriptions

Console settings deal with graphic visualizations of server activity, how often activity monitors are refreshed, and inactivity timeout for console sessions.

Following are field definitions for the Console settings:

Field	Definition
Default Graphical Activity Monitor expected maximum processes	The maximum number of processes servers are likely to handle simultaneously. This value can be overridden for a particular server in Server Properties, the Settings tab (see *Viewing or modifying a server definition after node discovery*).

Field	Definition
Default Console Auto Refresh System Setting in seconds	The default number of seconds to elapse between automatic refreshes of the activity monitors. Users with permission can override this value by setting **Change Auto Refresh To** under **Control Center** > **Console Preferences**. For more information about overriding this value, see *Changing console preferences* in *Getting Started*.

Field	Definition
Time out after *n* minute(s) of inactivity	The amount of time that a user session is inactive before the user is logged out. • The range is 0-10000 minutes. • The default is 0 minutes, which indicates no inactivity timeout. • This value cannot be less than or equal to the **Display warning message *n* minute(s) before timing out** parameter value. However, if the **Time out after *n* minute(s) of inactivity parameter value** is set to 0, the **Display warning message *n* minute(s) before timing out** must be 0. • The browser session timeout value is the console timeout value + 1 minute. When the console timeout is set to 0, the browser session timeout is 10 minutes. • The console timeout value must be greater than the Auto Refresh value. • If Auto Refresh is enabled and console timeout is enabled (set greater than 0), the web *browser session* will not time out. However, if the user does not explicitly press keys or click the mouse, the *console timeout* will trigger. Example 1 Setting of: Auto Refresh=120 seconds Time out after 30 minute(s) of inactivity. Display warning message 2 minute(s) before timing out. Means: Data in console monitors would refresh every 120 seconds. User would get a dialog pop up with a 2 minute count down after 28 minutes of inactivity (no keyboard or mouse activity). Example 2 Setting of: Auto Refresh=120 seconds Time out after 30 minute(s) of inactivity. Display warning message 0 minute(s) before timing out. Means: Data in console monitors would refresh every 120 seconds. User would get logged out of console after 30 minutes of inactivity (no keyboard or mouse activity). There will be no warning dialog. Example 3 Setting of: Auto Refresh=120 seconds Time out after 0 minute(s) of inactivity. Display warning message 0 minute(s) before timing out. Means: Data in console monitors would refresh every 120 seconds. User does not have to do any keyboard or mouse activity to keep logged on. User will never be logged out due to inactivity. Example 4 Setting of: Auto Refresh permission=none Time out after 10 minute(s) of inactivity. Display warning message 1 minute(s) before timing out. Means: Data in console monitors will not be automatically refreshed. User would get a dialog pop up with a 1 minute count down after 9 minutes of inactivity (no keyboard or mouse activity).

Field	Definition
Display warning message *n* minute(s) before timing out	Number of minutes before the inactivity timeout has been reached, that the warning message will be displayed. The default is 0. The range is 0-9999. The warning message contains a counter that shows the minutes and seconds remaining until the user is logged off. • When the warning message is displayed, if the user clicks **OK**, the dialog closes and the inactivity timer is reset. • When the inactivity timeout is reached, the user session is canceled and the user is logged out of the console.

License management field descriptions

You can use many fields to define license management.

The following table defines the fields on the License Management tab in System Settings.

Field	Definition
License key versions	The number of license key versions to keep in history.
Email user	The user who is sent emails containing license key information to be imported into Sterling Control Center via License Management.
Email user password	The user password for the email user who is sent emails with licenses.
Email hostname	The email system hostname.
Email host port	The email system host port.
Email protocol	The protocol used by the email system (IMAP or POP3).
Frequency (minutes)	How often, in minutes, to check for new license information arriving via email.

File Agent field descriptions

You can use many fields to define a Sterling Connect:Direct File Agent.

The following table defines the fields on the File Agent tab in System Settings.

Field	Definition
SNMP Listener Address	IP address from which Sterling Control Center listens for process submissions from file agents.
SNMP Listener Port	Port Sterling Control Center uses to listen for process submissions from file agents.
Generate No Process Submited Notifications Every x Minutes After Last Submit	The number of minutes Sterling Control Center will wait for a “Process was submitted” trap from a monitored Sterling Connect:Direct File Agent before generating an event stating that no submits have recently been initiated.
File Agent Service Status	The status of the Sterling Connect:Direct File Agent service. (Display only.)

Chapter 13. Administering Other systems

Sterling Control Center allows for direct access to Sterling B2B Integrator, Sterling File Gateway, and Sterling Connect:Direct. Your access depends in part on your credentials on those other systems.

Accessing the Sterling Connect:Direct Browser User Interface

With authorization, you can access Sterling Connect:Direct from Sterling Control Center through the Sterling Connect:Direct Browser User Interface. From this user interface an administrator can log into Sterling Connect:Direct, sign onto a Sterling Connect:Direct server, change initialization parameters, and maintain netmap and user authorization information.

About this task

To access the Sterling Connect:Direct Browser User Interface:

Procedure

1. Log in by right-clicking a Sterling Connect:Direct server in the list of servers and then click **Connect Direct Browser** > **Login Page**. The **Sign On to a** Sterling Connect:Direct Node screen displays.
2. Sign onto a Sterling Connect:Direct server by right-clicking it in the list of servers, then click **Connect Direct Browser > Sign On**. The **Sign On Request Response** screen displays.
3. To change initialization parameters, right-click a Sterling Connect:Direct server in the list of servers and click **Connect Direct Browser** > **InitParms**. The **Change Initialization Parameters** screen displays.
4. To maintain netmap information:, right-click a Sterling Connect:Direct server in the list of servers and click **Connect Direct Browser** > **NetMap**. The **Select Netmap** screen displays.
5. To maintain user authorizations, right-click a Sterling Connect:Direct server in the list of servers and click **Connect Direct Browser** > **User Auth**. The **Select User Authorities Results** screen displays.

Accessing Sterling B2B Integrator

With authorization, you can access Sterling B2B Integrator from Sterling Control Center.

About this task

Note: The Dashboard port value in Server Properties (Connection tab) must be specified; otherwise, the Sterling B2B Integrator Dashboard option cannot be used.

To access the Sterling B2B Integrator Dashboard and sign onto a Sterling B2B Integrator server as the user designated in server properties:

Procedure

1. Right-click the Sterling B2B Integrator server.

2. Select Sterling B2B Integrator Dashboard > **Sign On**. The Sterling B2B Integrator Dashboard Login screen is displayed.
3. Provide valid Sterling B2B Integrator credentials and click **Sign In**. The **Admin Console Home** screen displays.

   Note: For information on administering Sterling B2B Integrator via the Sterling B2B Integrator Dashboard, consult the Sterling B2B Integrator documentation.

Accessing Sterling File Gateway

With authorization, you can access Sterling File Gateway from Sterling Control Center.

About this task

To access Sterling File Gateway:

Procedure

1. Right-click the Sterling File Gateway server.
2. Select **Sterling File Gateway** > **Login Page**.
   The **Sterling File Gateway Login** screen displays.
3. You must provide valid Sterling File Gateway credentials and click **Sign In**.

Chapter 14. Database administration

Sterling Control Center information is stored in an Oracle, Microsoft SQL Server, or DB2 database. To maintain optimal system performance, your database should regularly be staged, purged, and backed up. For all database types, your database administrator should use the database utilities provided with those products to perform this maintenance.

Automatically maintain Sterling Control Center databases

When you first install Sterling Control Center you are asked to set up two Sterling Control Center databases, a production database and a staging database. Staging is the act of moving data from the production database to the staging database. Once in the staging database the data can then be purged or archived and then purged by the database administrator. You can access the staging database for purging or archival without disrupting data collection into the production database. You can establish an automated staging schedule for the production database and an automated purge schedule for the staging database.

Move data in bulk to the staging database

Note: This method of transferring data refers only to systems where the production and staging databases reside on the same database instance, that is, on the same physical machine and in the same database server. In addition, the production database user ID must have permission to access the staging database tables.

To speed up the transfer of data from the production to the staging database, Sterling Control Center automatically moves data in bulk instead of row by row whenever it is possible. To use this more efficient method, Sterling Control Center goes through these steps:

- Copies n number of rows from production database table to a temporary table

Note: n is the Number of rows to select per DB transaction specified on the System Settings window. For more information, see *Sterling Control Center settings*.

- Copies all the data from the temporary table to the staging database table
- Using the data in the temporary table, deletes all the data from the production database table that has been copied to staging database table

Sterling Control Center repeats these steps until all the data up to the desired date is moved to the staging database.

Chapter 15. Tune Sterling Control Center

The major components of Sterling Control Center are the Sterling Control Center Engine, the Sterling Control Center Console, and the database server. All three affect the overall performance and must be run separately on high-powered hardware. Running any component on an underpowered machine will have a negative impact on the overall performance.

Sterling Control Center does much more than display the status of managed servers—it collects activity data from servers, processes the data and, as part of the processing, stores the data in the database. In addition, data processing includes applying rules and SLCs. Sterling Control Center's performance is measured by the number of events it processes per second.

Review the following guidelines and implement those that will work in your environment.

General Tuning

Multiple threads and services on the Sterling Control Center engine simultaneously collect data from different managed servers, process data, and issue database commands to the database server. The database server must be powerful enough to handle all these concurrent requests. Because database operation is I/O intensive, the database server should be run on a machine with fast I/O devices.

Review the following general guidelines related to your environment and network:

- For both UNIX and Microsoft Windows systems, no other application should be installed on the same file system or drive where Sterling Control Center is installed.

  This stems from the fact that Sterling Control Center uses checkpoint files to determine the last time it collected activity data from a managed server, and keeps these files in the location where Sterling Control Center is installed.
- Do not run any other application, including anti-virus software, on the machine where the Sterling Control Center engine is running.
- Make sure that the network connectivity between the Sterling Control Center engine and the database server is on a high-speed network.
- Use a multi-CPU machine for the Sterling Control Center engine when monitoring a large number of servers. No other tuning will help an underpowered machine.

Tune the Sterling Control Center engine

Be sure to review these general guidelines when tuning the Sterling Control Center engine.

Review the following general guidelines to tune the Sterling Control Center engine:

- Make sure that the Sterling Control Center engine is running on adequate hardware.

  To estimate the engine requirements appropriate for your environment, see *Determining Engine and Database Requirements* in *Getting Started*, which outlines

the steps for finding the required hardware. Worksheets and a utility program are provided to assist you in this planning.

- Adjust the number of simultaneous pollers.

  As noted earlier, multiple services simultaneously collect data from different managed servers. The number of simultaneous services that collect data from managed servers is determined by the Simultaneous Pollers setting, which you can change by going to **Control Center** > **System Settings** > **Services**. The recommended setting is 20% of the total number of managed servers. If you specify a number greater than the default setting of 7, you must adjust your heap size.

- If necessary, increase the Java heap memory size to accommodate the number of simultaneous pollers Sterling Control Center needs. By default, the Java process in Sterling Control Center uses up to 512 MB.

  To calculate your memory requirement, use the following formula:

  ```
  Heap = 45 MB +
         (Number of simultaneous pollers * 30 MB) +
         (Number of servers *.5 MB) +
         (Number of Completed Processes cached * 1 KB * Number of servers * Average
     Number of Data Visibility Group Activity per servers)
  ```

  If more than 1.5 GB of heap is required, you must use a 64-bit Operating System and install Sterling Control Center with the 64-bit JRE. On a 32-bit system, even if you have more than 2 GB physical RAM, the Java process cannot use it.

- If required, add more physical memory to your system.

  You should never allocate more memory to heap than the available physical memory on the machine. For example, if your computer has 1 GB physical memory (some of which is used by the operating system), the physical memory available for other processes is less than 1 GB. In that case, you should not specify 1 GB as the max heap size for the Java process.

- Reduce the completed processes cache size. To access this setting for a particular server, right-click the server, select **Properties**, click the **Settings** tab, and then click **Advanced**. Adjust the value for the Max Completed Processes accordingly.

  By default, the last 100 completed processes are kept in memory for each server. This cache uses heap memory and approximately 1 KB per entry. When managing a large number of servers, a significant amount of heap memory is used. Reducing the completed processes cache size also reduces the heap memory usage.

- Do not specify too high a value for the system setting, Number of rows to select per DB transaction (the default is 4000 rows) because a high value requires a great deal of heap memory if the production and staging databases are in separate database instances.

  In addition, the database server will be forced to do a table scan to select that number of rows instead of using an index, which also slows down the process. To access this setting, go to **Control Center** > **System Settings** > **Database**.

- To reduce processing overhead, including less database usage, consider not collecting process step statistics for Sterling Connect:Direct servers. To access this option, select the server, and go to **Properties** > **Connection**.

Attention: If you have any rules or SLCs that depend on the step start and step end events, those SLCs and rules will not work if you do not collect the step statistics. For example, if you enabled this option and you had a rule that watches for a copy step failure, the rule would not work.

- To reduce processing overhead, remove or disable any unused rules and SLCs.

- Adjust both the Production database and Staging database maintenance settings (**Control Center** > **System Settings** > **Database**) to keep the minimum amount of data you need.

  When databases have less data, they perform better, and their insert, update, and seek times are faster. When your performance starts degrading, it could be because there is too much data in the Sterling Control Center databases and the activity data collection from the managed servers is falling behind.

  The staging database is not an archive database for permanent storage. You must move the data to a data warehousing type of database.
- Schedule reports to run when there is less activity on the database server, which results in less activity in the database server. Running reports during off-peak hours reduces database contention and helps in collecting data from managed servers.
- Set up Server groups and restricted roles, and then assign users to restricted roles. Linking specific users to the specific servers they need to monitor avoids different users monitoring the same server's activities, which reduces overhead on the Sterling Control Center engine.
- Do not change the engine's default log level unless necessary.

  Excessive logging involves intensive file system I/O and slows down processing significantly, thus, severely degrading performance. Sterling Control Center log files are used to troubleshoot exceptions. The default logging level is set up to log all abnormal situations and is sufficient in normal production environments. Change the log level only when troubleshooting issues, and after you resolve the issue, change the log level back to the default level.
- To reduce the engine overhead, increase the size of the engine log file (the default size is 5000 KB) by opening the CCEngine.log4j file and changing the value in the line log4j.appender.R.MaxFileSize=8000KB.

  If you are monitoring a large number of servers, you may be required to do this because of the growing number of file switches required to keep up with the amount of information going into the log. When the size of the log reaches 5000 KB, a new file is created and the old file is renamed with a number suffixed to the end. If the log file fills up quickly, a log file switch occurs, which slows the engine performance. If the log file size is larger, fewer log file switches occur, resulting in less engine overhead.
- When running reports, narrow the report to a specific server and specific date. By specifying criteria that use an index for the database table involved in the report, less database I/O is performed, making the report run faster. When indexes are used, database table scans are avoided, resulting in less overhead on the database server. To make your report run faster, also specify as many columns as possible.

  The EVENTS table contains the following indexes and associated columns for the EVENTS and CD_STATS_LOG database tables:

  ```
  EVENT_ID_INDEX (EVENT_ID)
  SEQ_NUM_INDEX (DATE_TIME, SEQ_NUM, NODE_ID)
  EVENTS_ALERTS_DEL (ALERT, ALERT_DELETED)
  EVENTS_COMPLETED (ACTIONS_COMPLETED)
  EVENTS_TYPE_INDEX (EVENT_TYPE, NODE_ID, NODE_TYPE)
  EVENTS_SLC_INDEX (SLC_SRC_EVENT_ID, SLC_INSTANCE_ID, ALERT,
  ALERT_DELETED)
  EVENTS_STAT_IDX (NODE_ID, PROC_NAME, PROC_ID, DATE_TIME)
  ```

  The CD_STATS_LOG table contains the following indexes and associated columns:

```
CD_STAT_INDEX (LOG_DATE_TIME, SEQ_NUM, NODE_ID)
CD_STAT_NODE_INDEX (NODE_ID, PROC_NAME, PROC_NUMBER)
CD_STAT_NAME_INDEX (NODE_ID, PROC_NAME, PROC_NUMBER, LOG_DATE_TIME)
CD_EVENT_ID_IX (EVENT_ID)
```

- Pause the monitoring on servers that will be down for an extended period of time. By not polling inactive servers, processing overhead for the Sterling Control Center engine is reduced.
- Increase the monitor rest time to reduce how often Sterling Control Center collects data from the managed server while increasing the amount of data Sterling Control Center collects in a single poll. The maximum monitor rest time varies for each type of managed server. For more information, see *Server Field Descriptions*.
- Use an unencrypted connection between the engine and managed servers to reduce CPU usage and improve performance.
- For greater efficiency, Sterling Control Center keeps caches of information rather than going to the database repeatedly. For example, Sterling Control Center keeps a cache of alerts for each data visibility group (DVG) defined to the system in addition to a cache for all completed processes. To turn off the initialization of these caches at startup, you edit the CCEngineService.xml configuration file to change the initializeCachesAtStartup element to "false," as shown in the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<service>
     <serviceId>CCEngineService</serviceId>
     <serviceType>0</serviceType>
     <serviceClass>com.sterlingcommerce.scc.agent.SCCAgent</serviceClass>
     <serviceName>CCenter</serviceName>
     <initializeCachesAtStartup>false</initializeCachesAtStartup>
     <nodeCheckMonitorFudgeFactor>30</nodeCheckMonitorFudgeFactor>
     <nodeCheckRestTimeMultiplier>2</nodeCheckRestTimeMultiplier>
     <nodeCheckMonitorRate>30</nodeCheckMonitorRate>
     <batchEventQueueDepth>50</batchEventQueueDepth>
     <simultaneousCdPollers>7</simultaneousCdPollers>
     <recordLimit>2500</recordLimit>
     <maxEventQueueSize>40000</maxEventQueueSize>
     <maxCompletedProcs>100</maxCompletedProcs>
     <maxAlerts>1000</maxAlerts>
     <maxDeletedAlerts>1000</maxDeletedAlerts>
     <maxProcessQueueEventSize>250</maxProcessQueueEventSize>
     <versionCount>3</versionCount>
     <minVersionAge>10</minVersionAge&gt>
     <synchObjectTime>NEVER</synchObjectTime&>
     <batchInsertLimit>100</batchInsertLimit>
     <dontPopulateStatsTable>false</dontPopulateStatsTable>
     <serverTimeZoneId>America/Chicago</serverTimeZoneId>
     <certificateExpiry&gt;60</certificateExpiry>
     </service>
```

Use the Sterling Control Center console wisely

The Sterling Control Center console obtains activity data from the engine for only those servers for which an activity monitor is opened. Server status events and alerts are always collected from the engine regardless of which monitors are opened.

Review the following general guidelines related to using a console:

- Close any unneeded Completed and Queued Activity monitors. The Sterling Control Center console periodically gets activity data from the engine. (The frequency is based on the Auto Refresh rate.) If monitors are not open, the

Console does not need to collect activity data, which reduces the processing overhead on the Console and related I/O activities.

- To reduce the overhead on the Console, open Completed and Queued Activity monitors only on the servers whose activities you really want to see. For example, if you are monitoring 1000 servers and the Completed Activity Monitor is opened on all 1000 servers, the monitor will be constantly filled with new activities. This will not only make it difficult for you to find what you are looking for, it will also simultaneously increase the processing overhead for the Console by making it retrieve the activity data for all those servers.
- Use a non-secure connection between the engine and console, unless you are connecting to the engine over the internet. If you are using the internet, use a secure connection.
- To reduce the overhead on the Console, increase the Auto Refresh settings using one of the following methods:
  - Change the Default Console Auto Refresh System Setting in seconds setting (**Control Center** > **System Settings**).
  - Specify a new value for the **Change Auto Refresh to:** setting (**Control Center** > **Console Preferences** > **Auto Refresh Settings**).
- To reduce the number of data requests to the engine, require manual refresh for users who do not need to actively monitor managed servers. Set up roles that use the Manual option for the Console Auto Refresh Permission.
- When you are not using the Console, log out of it. Each console connected to the engine increases the events processing by approximately six events per second on the engine.
- To further improve the engine performance, set up alerts to send e-mail notifications as alert conditions occur instead of requiring users to monitor alerts using the Console.
- When monitoring a large number of servers, use the option, Sterling Control Center Console - Large Configuration (Greater Than 512 MB, Less Than 1 GB), on the Sterling Control Center Launch Page. The large configuration allocates up to 1 GB max heap size, which will improve performance.
- When monitoring a large number of servers, avoid using VPN to connect to the engine. VPN connections are secure and encrypted and as a result, are 2 to 3 times slower than non-secure connections. When you open an activities monitor which covers a large number of managed servers and activities on those servers, a lot of data has to be transferred over the secure connection, which will slow down performance.

Tune the database server

The database plays a crucial role in Sterling Control Center by acting as the repository for the data Sterling Control Center collects from the monitored servers. The database server must be able to handle all database operation requests issued by the Sterling Control Center engine. The ability of the Sterling Control Center engine to perform optimally depends on the capacity of the database server, and its hard disk speed is an important factor in providing better performance.

It is important to size the database appropriately. For more information on sizing the database, see *Determining Engine and Database Requirements* and *Database Sizing Worksheet*.

General database tuning

Review these guidelines before performing general database tuning.

- Check for known hardware and software problems pertaining to your system.

- Never tune more than one level of your system at a time.
- Put tracking and fallback procedures in place before you install and begin to use Sterling Control Center.
- Do not share the database instance with other applications.
- If you use a virus scanner, disable it if it is on the database server. If you cannot disable the virus scanner, at least exclude the database files and directories from the Virus Scanner operation. Also, schedule the scan during off-peak times.
- To avoid disk contention, use different physical disks for data files and log files.
- Rebuild indexes periodically. For the main tables, EVENTS, CD_STATS_LOG, CE_STATS_LOG, rebuild these indexes at least every week.
- Increase the database buffer.
- Use hardware-based RAID (Redundant Array of Independent Disks) technology.
- Use database clustering.

Guidelines for Oracle databases

Review the following guidelines to tune Oracle databases:

- Use Oracle Real Application Clusters (RAC).
- Use hardware-based RAID (Oracle-recommended RAID 1 for performance).
- The key initialization parameters in Oracle are SGA_MAX_SIZE, PGA_AGGREGATE_TARGET, DB_CACHE_SIZE, and SHARED_POOL_SIZE. If you use ASMM, SGA_TARGET is the key initialization parameter. Tune the following database parameters by using the recommended values:
  - Number of open cursors: at least 2000
  - Database block buffers: at least 19200. IBM recommends that you set this value to 0 if SGA memory is equal to or greater than 0.
  - System Global Area (SGA) memory (10g/11g only): greater than 0
  - Shared pool size: at least 900000000
  - Large pool size: at least 614400
  - Number of processes: at least 500
  - Log Buffer: MAX (0.5, (128K * number of CPUs))
  - Sort Area Size: at least 65536
  - Redo Log Files: The behavior of the database writer and archive processes depends on the size of redo logs, thus also influencing performance. Generally, the larger the redo log files, the better the performance. Undersized log files increase checkpoint activity and reduce performance. In addition, to reduce redo log operations, consider the NOLOGGING option.
  - Keep the Hit Ratio for the Data cache greater than 95%.
  - Create enough dispatchers. For more information about creating dispatchers, see the Oracle website.
  - Make sure that the SGA is large enough to accommodate memory reads since physical memory is generally much faster than retrieving data from disk.
  - Measure hit ratios for the library cache of the shared pool with the V$LIBRARYCACHE view. A hit ratio of greater than 95% is optimal.
  - The general rule of thumb is to make the SHARED_POOL_SIZE parameter 50–150% of the size of your DB_CACHE_SIZE.
  - Adjust the PGA_AGGREGATE_TARGET parameter, which determines how efficiently sorting and hashing operations are performed in your database. Use the following formula to get the optimal value:

```
SELECT ROUND(pga_target_for_estimate/1024/1024) target_mb,
estd_pga_cache_hit_percentage cache_hit_perc, estd_overalloc_count
FROM V$PGA_TARGET_ADVICE
```

Guidelines for MS SQL Servers

Be sure to review these guidelines before tuning an MS SQL server:

- Make the computer use background services rather than programs. To change your current setting, right-click on **My Computer** > **Advanced** > **Settings for Performance.**
- For Server properties, select the Boost SQL server priority.
- To avoid frequent checkpoints, adjust the Recovery interval.

Note: All transactions are very short ones (less than a second).

- Use File Groups for database files.
- To watch for I/O bottlenecks, use the System Performance Monitor to check the Physical Disk :% Disk Time and Physical Disk: Avg. Disk Queue Length parameters. Consistently high values indicate an I/O bottleneck. To improve performance, use a faster disk drive, move files to a second disk, or add disks to a RAID array.
- Adjust the memory allocated to the SQL server.
- Keep an eye on the SQLServer:Buffer Manager: Page reads/sec and SQL Server:Buffer Manager: Page writes/sec parameters.
- Store temporary databases on a fast disk.
- Use hardware-based RAID.

Guidelines for DB2 databases

Be sure to review these guidelines before tuning DB2 databases including the DB2 Universal Database™ (UDB) multi-user version of DB2.

- Ensure that you have enough disks (6–10 per CPU is a good start). The container for each table space should span all available disks. Some table spaces, such as SYSCATSPACE, and those with a small number of tables do not need to be spread across all disks, while those with large user or temporary tables should.
- Buffer pools should use about 75% (OLTP) or 50% (OLAP) of available memory.
- Perform runstats on all tables, including system catalog tables.
- To configure the database manager, use the Configuration Advisor.
- To restrict logging to a separate high-speed disk, specify this disk by using the NEWLOGPATH database configuration parameter.
- To avoid sort overflows, increase the value specified for the SORTHEAP parameter.
- Table space type should be SMS for the system catalog table space and temporary table spaces and DMS raw (device) or file for the rest. Run db2empfa to enable multi-page file allocation for the SMS table spaces; this will allow SMS table spaces to grow an extent at a time (instead of a page), which can speed up heavy insert operations and sorts which spill to disk.
- Set the database's Transaction per Minute (tpm) parameter to a value closer to your system's events/second figure. At minimum, this value should be set to 3000.
- To reduce database locks, set the isolation level to Uncommitted Read.

Additional reference information

These sources provide more information about database performance and tuning.

Topic	See
General tuning	Database Tuning: Principles, Experiments, and Troubleshooting Techniques by Dennis Shasha and Philippe Bonnet ISBN:9781558607538 Morgan Kaufmann Publishers © 2003 (415 pages)
Oracle databases	Oracle Database 10g Performance Tuning Tips & Techniques by Richard J. Niemiec ISBN: 9780072263053 Oracle Press Copyright The McGraw-Hill Companies, Inc. © 2007
Tuning SQL servers	Professional SQL Server 2005 Performance Tuning by Steven Wort and et al. ISBN: 9780470176399 John Wiley & Sons (US) Copyright Wiley Publishing, Inc. © 2008
Tuning MS SQL	Filegroups in SQL Server 2005
Tuning DB2 UDB version 8.1 and its databases	Best practices for tuning DB2 UDB v8.1 and its databases

Chapter 16. Event type descriptions

This table describes all Sterling Control Center event types.

Event Type	Event Name	Description	Possible Use
01	Process Step Started	For Sterling Connect:Direct, indicates that a Process step started. For Sterling Connect:Enterprise, indicates that a batch transmission started. For Sterling B2B Integrator, a business Process activity or AFT file transfer started. For Sterling File Gateway, a Delivery or Route started. For FTP, a file transfer started. For Sterling Connect:Express, a file transfer started. For QuickFile, a transfer started. For MQ MFT, a file transfer or step started.	To track Process step starts.
02	Process Step Ended	For Sterling Connect:Direct, indicates that a Process step ended. For Sterling Connect:Enterprise, indicates that a batch transmission ended. For Sterling B2B Integrator, indicates that a business Process activity ended or AFT file transfer completed. For Sterling File Gateway, a Delivery or Route completed. For FTP, a file transfer completed. For Sterling Connect:Express, a file transfer ended. For QuickFile, a transfer ended. For MQ MFT, a file transfer or step ended.	To track completions of steps within Processes.

Event Type	Event Name	Description	Possible Use
03	Process Started	For Sterling Connect:Direct, indicates that Process started. For Sterling Connect:Enterprise, indicates that a batch transmission started. For Sterling B2B Integrator, indicates that a business Process started. For Sterling File Gateway, an Arrived File started. For FTP, a file transfer started. For Sterling Connect:Express, a file transfer process started. For QuickFile, indicates one or more file transfers are about to start. For MQ MFT, indicates one or more file transfers or steps have started.	To track Process starts.
04	Process Ended	For Sterling Connect:Direct, indicates that a Process ended. For Sterling Connect:Enterprise, indicates that a batch transmission ended. For Sterling B2B Integrator, indicates that a business Process ended. For Sterling File Gateway, an Arrived File completed. For FTP, a file transfer completed. For Sterling Connect:Express, a file transfer process ended. For QuickFile, one or more file transfers ended. For MQ MFT, indicates one or more file transfers or steps have ended.	To track Process completions.
05	Server Status	Relates various types of server status information.	To track server status.
06	SLC Notification	Service Level Criteria	Use Message ID to determine specific type of SLC event.
07	Server Shutdown Started	Not currently used.	Not currently used.

Event Type	Event Name	Description	Possible Use
08	Server Shutdown	Indicates a server shutdown.	To track times when Sterling Connect:Express servers shutdown.
09	Process Status	Generated by a Sterling Connect:Direct or MQ MFT server and contains details about a queued Process or file transfer.	Used to track queue movement by Sterling Connect:Direct processes or MQ MFT file transfers.
10	Server License	Results from a license management check on a managed server.	For notification of expiring licenses.
11	Server Error	Indicates that an error occurred on a managed server.	To track server status.
12	Server Command	Indicates that a monitored server initiated a command. For a list of Sterling Connect:Direct commands associated with this event, see *Event type: Sterling Connect:Direct statistic record ID cross reference*.	To track Process commands, such as delete, suspend, and resume. To track Netmap modifications on managed Sterling Connect:Direct servers. To track request for transfers initiated by Sterling Connect:Express servers.
13	Connection Started	Indicates that a managed server initiated a session/connection.	To track initiation of sessions which are created for performing file transfers.
14	Connection Shutdown Started	Indicates that a connection, or session, by a managed server started to shut down. **Attention:** Currently used only for Sterling B2B Integrator managed servers and Sterling Connect:Express servers.	To track session status.
15	Sterling Control Center Status	Indicates the status of the Sterling Control Center server.	To track Sterling Control Center server status.
16	Process Queue	Contains data on active and queued Processes on managed servers. Sterling Connect:Direct, Sterling B2B Integrator, Sterling Connect:Express, and QuickFile only.	This event is used internally within Sterling Control Center.
17	Process Interrupted	Indicates that a process session was interrupted and the Process will be restarted later. Sterling Connect:Direct only.	To track Sterling Connect:Direct Processes that ended but will restart.
66	Suppressed SLC Notification	Service Level Criteria Workflow notification suppressed because of "Fire-Once" List. May also occur if the server for which the SLC references is paused.	Used for debugging.

Event type: Sterling Connect:Direct statistic record ID cross-reference

You can use statistic record information to determine what Sterling Connect:Direct activities produce associated Sterling Control Center event types. If a statistic record ID is not listed, Sterling Control Center does not use it.

This table cross-references event types to the Sterling Connect:Direct statistic IDs.

Event Type	Statistic Record ID	Description	Platform				
			i5/OS	HP NonStop	z/OS	UNIX	Microsoft Windows
Connection Started	SB	Session Begin			X		
	SSTR	Session started				X	X
	SMSES	Session Begin	X				
	SESSSTART	Session Begin		X			
Server Command	ADNADD	Net map entry added	X				
	ADNCHG	Net map entry changed	X				
	ADNDLT	Net map entry deleted	X				
	CDSTOP	Stop command issued	X				
	CH	Change Process			X		
	CHGP	Change Process Command Issued				X	X
	DELP	Delete Process command issued				X	X
	DP	Delete Process			X		
	FLSP	Flush Process command issued				X	X
	FP	Flush Process			X		
	FS	Suspend Process			X		
	FT	Flush Task			X		
	IK	Inq. AP file			X		
	IT	Inq. Trap			X		
	LCOA	Signon failure					X
	NM	Change Netmap			X		
	NMPR	Change Netmap				X	X
	NUTR	Sterling Connect:Direct termination requested					X
	PCDEL	Delete Process	X				

Event Type	Statistic Record ID	Description	Platform				
			i5/OS	HP NonStop	z/OS	UNIX	Microsoft Windows
Server Command (cont.)	PCFLU	Flush process	X				
	PCHOLD	Held Process	X				
	PCREL	Release Process	X				
	PCSUB	Submit Process	X				
	PCSUS	Suspend Process	X				
	PFLS	Process flushed				X	X
	PS	Process submitted			X		
	SI	Signon attempt			X		
	ST	Stop Sterling Connect:Direct command issued			X		
	STOP	Stop Sterling Connect:Direct command issued				X	X
	SUBMIT	Submit		X			
	SUBP	Submit command issued				X	X
	TS	Suspend Task			X		
	UM	Update Network Map			X		
	UU	Update User			X		
	XCMM	UNIX sign-on failure					
Server Error	PERR	Process error detected				X	X
	SERR	System error				X	
Server License	APCK	Asset Protection Check					X
	LIEX	License has expired				X	X
	LWEX	License will expire in 14 days				X	X

Event Type	Statistic Record ID	Description	Platform				
			i5/OS	HP NonStop	z/OS	UNIX	Microsoft Windows
Process Status	LEXC	An unknown exception has occurred					X
	QCEX	Queue Change to Exec Queue				X	X
	QCHO	Queue Change to Hold Queue				X	X
	QCTI	Queue Change to Timer Queue				X	X
	QCWA	Queue Change to Wait Queue				X	X
	QE	Queue Change to Exec Queue			X		
	QH	Queue Change to Hold Queue			X		
	QT	Queue Change to Timer Queue			X		
	QW	Queue Change to Wait Queue			X		
Server Status	SD	Sterling Connect:Direct Starting			X		
	TF	TCQ Full					
	TL	TCQ Below Defined Threshold					
	TW	TCQ Above Defined Threshold					
	XSTA	User Exit Program Started					
Process Ended	PRED	Process Ended				X	X
	PROCEND	Process Ended		X			
	PT	Process Termination			X		
	SMPTM	Process Ended	X				
	USEC	User Security check issued				X	X
	ZT	Process Termination			X		
Process Started	PI	Process Started			X		
	PROCSTART	Process Started		X			
	PSTR	Process Started				X	X
	SMPST	Process Started	X				
	ZI	Process Started			X		

Event Type	Statistic Record ID	Description	Platform				
			i5/OS	HP NonStop	z/OS	UNIX	Microsoft Windows
Process Step Ended	CT	Copy Termination			X		
	CTRC	Copy Control record written				X	X
	IFED	IF statement ended				X	X
	MC	PDS Member Copy			X		
	RJ	Run Job			X		
	RJED	Run Job command completed				X	X
	RT	Run Task			X		
	RTED	Run Task command completed				X	X
	SBED	Submit complete				X	X
	SMSTTM	Process Step Ended	X				
	STEPEND	Process Step Ended		X			
Process Step Started	CI	Copy Step Start			X		
	IF	If statement started			X		
	JI	Run Job Start			X		
	LSST	Local Process Step Started				X	X
	RSST	Remote Process Step Started				X	X
	SMSTST	Process Step Started	X				
	STEPSTART	Process Step Started		X			
	SW	Submit within a Process			X		
	TI	Run Task Start			X		
	UM	Update Network Map			X		

Chapter 17. Administrative troubleshooting

When you encounter issues administering Sterling Control Center, there are solutions that can help you fix them.

The following table provides solutions to common Sterling Control Center system issues:

Issue	Solution
Logging off UNIX kills the Sterling Control Center process.	Log on as root to the computer where the engine is installed, then start Sterling Control Center.
java.lang.OutOfMemoryError message received when logging on to Sterling Control Center on an HP-UX computer.	Set the HP-UX kernel parameters to the following values to avoid this error: • kernel maxusers–2000 • kernel nproc–5120 • kernel max_thread_proc–3000 • kernel nkthread–8976 • kernel nfile–83968 • kernel maxfiles–4096 • kernel maxfiles_lim–4096 • kernel ncallout–8992 • kernel maxdsiz–2063835136 • sndd tcp_conn_request_max–2048 See the HP-UX documentation for instructions to set these parameters.
Not enough space errors received during installation.	• Delete unnecessary files to provide more room on your computer. • Close all open applications and rerun the installation.

Issue	Solution

Getting out-of-memory errors on the Sterling Control Center engine server	By default, the maximum heap size of the Sterling Control Center engine is set to 512 MB. You can increase this value when getting out-of-memory errors or when you increase Simultaneous Pollers in Systems Settings. The guidelines and steps apply both to 32-bit and 64-bit platforms.
	
	To calculate your heap requirements, use the following formula:
	`Maximum heap size = 45 MB +`
	`(# simultaneous pollers * 30 MB) +`
	`(# servers * .5 MB) +`
	`(# completed processes cached *`
	`1 KB * # servers)`
	
	If more than 1.5 GB of heap is required, you must use a 64-bit system.
	
	Changing Java heap settings in both Microsoft Windows and UNIX environments involves editing the InstallationInfo.properties file to add an entry. Next, you must run the configCC.bat/sh configuration script and restart the Sterling Control Center engine.
	
	To change Java heap settings:
	1. Make a backup of the file InstallationInfo.properties at ControlCenterInstallDirectory\conf.
	2. Open InstallationInfo.properties (at ControlCenterInstallDir\conf) with a text editor (such as Notepad on Microsoft Windows or vi on UNIX).
	3. Look for line that starts with MAX_HEAP_SIZE. (If it is there, change the value to the wanted number). If it is not there, add a line at the end of the file as shown in the following example:
	MAX_HEAP_SIZE=-Xmx???m
	4. Replace ??? with the wanted number.
	Example: MAX_HEAP_SIZE=-Xmx1024m
	5. Save the file.
	6. Run the configCC.sh (UNIX) or configCC.bat (Microsoft Windows) file at ControlCenterInstallDirectory/bin.
	7. Answer no to all the questions. Merely running the script makes the necessary updates to different runEngine scripts.
	8. Stop the engine by using stopEngine.sh (UNIX) or stopEngine.bat (Microsoft Windows).
	9. Start the engine by using runEngine.sh (UNIX) or runEngine.bat Microsoft Windows).

Rules produce no results.	• If you specify multiple criteria, all criteria must be met for the rule to take effect. Try reducing the number of criteria. • Rule values are case-sensitive. Verify that you are using the proper case. • Earlier rule criteria was met. Verify that the rules are in proper order. • Verify that the rule is enabled. If the rule has a schedule associated with it, the schedule is enabled and active during the time in question. • For more information, see *Troubleshooting rules* in *How-To*.

Issue	Solution
Expected User and Server Data statistics are not being produced.	Unlike other configuration data, the Metadata Type Mapping for User Data and Server Data are stored in the database, rather than in the local Sterling Control Center configuration. If you switched to a new database or reinitialized the existing database during upgrading or for any other reason, the Metadata Type Mapping values were lost. For instructions on how to map metadata types, see *Managing metadata type mapping*.
No WS_FTP statistics or events are being produced even though no errors occurred during installation of the WS_FTP agent. There are no obvious configuration errors in Sterling Control Center.	Verify that the name of the directory where you installed the Sterling Control Center FTP agent does not contain any blanks. If it does, reinstall the agent and make sure that the name of the new directory does not contain any blanks.
The Sterling Control Center engine shutdown unexpectedly.	When an SQL exception occurs within the Sterling Control Center engine that is not a truncation or duplication exception, Sterling Control Center sends out a notification message CJDB026E. It then shuts down Sterling Control Center. If you want to send a notification that Sterling Control Center shutdown, create a rule that identifies this error message and sends a notification.
A driver exception occurred.	When a driver exception occurs, Sterling Control Center sends out a CJDB013E or CLI025E message.
Cannot find the Control Center Engine log file to identify an installation issue.	The Sterling Control Center Engine log file is in the log directory under the Sterling Control Center engine installation directory. The engine log file name starts with CCEngine.
The Sterling Control Center Engine shuts down while it is running, caused by the shutdown of the database server.	Check the Sterling Control Center engine log file for details. If the database server was shut down, restart the database server and restart the Sterling Control Center engine.
When using the Microsoft SQL Server, Sterling Control Center creates too many connections on the SQL Server. This can be caused by Sterling Control Center using the JDBC connection pooling mechanism, which maintains a fixed number of connections with the SQL server or by using statement pooling which reuses the same JDBC connection with many different SQL Statements. For more details refer the following link: PRB: Unexpected Connections to SQL Server with JDBC	If you want to reduce the Connection Pool Size: • Stop the Sterling Control Center engine. • From the Sterling Control Center engine installation location, edit the following lines in the *InstallDirectory*/conf/services/system/JDBCService.xml file and change the values to the desired number: <maxpool>50</maxpool> <maxconn>100</maxconn> <initsize>16</initsize> **Important:** Setting the value of any of these fields to less than 16 severely impacts the performance of the Sterling Control Center engine. • Save the modified file. • Restart the Sterling Control Center engine.

Issue	Solution
Cannot log on when trying to manage a Sterling Connect:Direct for i5/OS server where the correct user ID and password are provided. The following error is displayed in the log file: `ERROR CDTask - javax.security.auth.login. FailedLoginException: com.sterlingcommerce.component. persistence.PersistenceException: java.sql.SQLException: [SQL0204] INITPARMS in <Library name> type *FILE not found.`	Fix the invalid library name specified for server connection properties.
Cannot start the engine due to a system server group naming conflict. The following error is displayed in the console and the log file: `CGRP034E Server group IDs found with matching system server Group IDs. Edit conf\servergroups\systemGroups.properties and change these names: {0}`	Edit the systemGroups.properties in *InstallDirectory*`\conf\servergroups\` to resolve the naming conflict and restart the engine. For more information, see *Resolving system server group naming conflicts*.
Cannot start the engine due to a role referencing an unknown server group. The following error is displayed in the console and the log file: `CROL009E Error while loading role. The role definition file name is {0}`	Edit the referenced file and change the old system server group name to the new system server group name and restart the engine.
Cannot access the web console using Internet Explorer.	In Internet Explorer, the website for the Sterling Control Center web console cannot not be displayed in compatibility mode. To disable compatibility mode for the web console: 1. In Internet Explorer, click **Tools** > **Compatibility View Settings**. 2. If the Sterling Control Center web console website (referenced in the launch URL) is listed in the websites that have been added to the compatibility view, select it and click **Remove**.

Chapter 18. Predefined actions and rules

The following topics describe the predefined rules and actions that ship with Sterling Control Center.

Predefined actions

This table lists and describes the predefined actions that ship with Sterling Control Center.

Action	Alert Severity/Result	Comments
no operation	none	Specified when no action is warranted. **Note:** You will not find this pre-defined action in the list of defined actions to edit.
alert0	0-In compliance	Associated with in-compliance SLC rules. An alert0 causes any previous alerts associated with its SLC instance to be automatically handled. For linked rules, can be used for either of the resolution and nonresolution actions.
alert1	1-High	
alert2	2-Medium	
alert3	3-Low	

Predefined rules

This table lists and describes the predefined rules that ship with Sterling Control Center. For information on the SLC message IDs referred to in the descriptions, see *Message IDs for rules*.

Attention: Changing the action defined for a rule may affect the behavior of SLCs that use that rule.

Rule	Description	Event Type
Bad return code	RC not equal zero - alert1	Process Step Ended
Did not start by end of monitor window	CSLC228E - alert1	SLC Notification
On-time completion in jeopardy	CSLC229I - alert2	SLC Notification
Monitor rate out of compliance	Alert 2 if servers not being polled.	Server Status
Process not submitted by File Agent	CCFA006I - Process not submitted by File Agent in timely fashion	Server Command

Rule	Description	Event Type
File Agent Service Initialization Error	CCFA014E - Triggered if File Agent Service initialization error occurs	Server Command
Certificate Expiry Warning	CCFG229I - alert 1 CCFG230I - alert 1	Server Status
Proc duration exceeded	CSLC044E - alert1	SLC Notification
Proc duration not determ.	CSLC050E - alert3	SLC Notification
Proc duration not ended	CSLC043E - alert2	SLC Notification
Proc duration okay	CSLC042I - alert0	SLC Notification
Proc duration running	CSLC049E - alert3	SLC Notification
Proc duration short	CSLC041E - alert2	SLC Notification
Proc duration suspended	CSLC046E - alert2	SLC Notification
Proc duration way over	CSLC045E - alert1	SLC Notification
Process already running	CSLC031E - alert3	SLC Notification
Process ended early	CSLC036E - alert0	SLC Notification
Process ended late	CSLC039E - alert0	SLC Notification
Process ended on-time	CSLC037I - alert0	SLC Notification
Process has not ended	CSLC038E - alert2	SLC Notification
Process has not started	CSLC034E - alert2	SLC Notification
Process not ended warn	CSLC048E - alert3	SLC Notification
Process not even started	CSLC026E - alert2	SLC Notification
Process not started late	CSLC027E - alert1	SLC Notification
Process not started warn	CSLC047E - alert3	SLC Notification
Process started early	CSLC032E - alert3	SLC Notification
Process started late	CSLC035E - alert2	SLC Notification
Process started on-time	CSLC033I - alert0	SLC Notification
Process still not ended	CSLC040E - alert2	SLC Notification
Process suspended	CSLC046E - alert2	SLC Notification
Staging database down	CJDB032E - alert1	Server Status
Trans dur exceeded	CSLC063E - alert2	SLC Notification
Trans dur exceeded-late	CSLC064E - alert2	SLC Notification
Trans dur not determined	CSLC070E - alert1	SLC Notification
Trans dur okay	CSLC062I - alert0	SLC Notification
Trans dur really late	CSLC065E - alert1	SLC Notification
Trans dur running	CSLC069E - alert0	SLC Notification
Trans dur short	CSLC061E - alert2	SLC Notification
Trans dur suspended	CSLC066E - alert2	SLC Notification
Trans ended - late	CSLC059E - alert3	SLC Notification
Trans ended early	CSLC056E - alert3	SLC Notification
Trans ended ontime	CSLC057I - alert0	SLC Notification

Rule	Description	Event Type
Trans not ended - late	CSLC058E - alert2	SLC Notification
Trans not ended	CSLC068E - alert2	SLC Notification
Trans not even start late	CSLC029E - alert2	SLC Notification
Trans not even started	CSLC028E - alert2	SLC Notification
Trans not started - late	CSLC054E - alert1	SLC Notification
Trans not started	CSLC067E - alert2	SLC Notification
Trans running early	CSLC051E - alert3	SLC Notification
Trans started early	CSLC052E - alert3	SLC Notification
Trans started late	CSLC055E - alert2	SLC Notification
Trans started ontime	CSLC053I - alert0	SLC Notification
Trans still not ended	CSLC060E - alert2	SLC Notification
Trans suspended	CSLC066E - alert2	SLC Notification
Transfer ahead of schedule - 25 dMax	CSLC177I - alert3	SLC Notification
Transfer ahead of schedule - 25 dMin	CSLC171I - alert3	SLC Notification
Transfer ahead of schedule - 50 dMax	CSLC179I - alert3	SLC Notification
Transfer ahead of schedule - 50 dMin	CSLC173I - alert2	SLC Notification
Transfer ahead of schedule - 75 dMax	CSLC181I - alert3	SLC Notification
Transfer ahead of schedule - 75 dMin	CSLC175I - alert3	SLC Notification
Transfer behind schedule - 25 dMax	CSLC178E - alert2	SLC Notification
Transfer behind schedule - 25 dMin	CSLC172E - alert2	SLC Notification
Transfer behind schedule - 50 dMax	CSLC180E - alert2	SLC Notification
Transfer behind schedule - 50 dMin	CSLC174E - alert2	SLC Notification
Transfer behind schedule - 75 dMax	CSLC182E - alert2	SLC Notification
Transfer behind schedule - 75 dMin	CSLC176E - alert2	SLC Notification

Chapter 19. Message IDs for rules

You can use message IDs when creating rules and SLCs.

Messages IDs specific to Sterling Connect:Direct

You can use message IDs specific to Sterling Connect:Direct when creating rules.

These messages are related to server and Process commands. This list is sorted by message ID.

Event Type	Event Name	Message ID	Message Text
Server and Process Command			
12	Server Command	CNCD015E	Process delete failed. ServerID, Command, Reason
12	Server Command	CNCD016E	Process change failed. ServerID, Command, Reason
12	Server Command	CNCD017E	Process suspend failed. ServerID, Command, Reason
12	Server Command	CNCD018E	Stop server failed. ServerID, Command, Reason
12	Server Command	CNCD031E	Server Added, Id: ServerID, by: UserID
12	Server Command	CNCD032E	Server Updated, Id: ServerID, by: UserID
12	Server Command	CNCD033E	Server Deleted, Id: ServerID, by: UserID
12	Server Command	CNCD034E	Process Processname has been deleted by user UserID
12	Server Command	CNCD035E	Process Processname has been suspended by user UserID
12	Server Command	CNCD036E	Process Processname has been changed by user UserID
12	Server Command	CNCD044E	Server servername stopped by user UserID.
9	Process Status	CNCD053I	Process moved to the Execution queue.
9	Process Status	CNCD054I	Process moved to the Hold queue. Status is Held initially.
9	Process Status	CNCD055I	Process moved to the Timer queue.
9	Process Status	CNCD056I	Process moved to the Wait queue.
9	Process Status	CNCD061I	Process moved to Hold queue. Status is Held in Error.
9	Process Status	CNCD062I	Process moved to Hold queue. Status is Held by Operator.
9	Process Status	CNCD063I	Process moved to Hold queue. Status is Held Retained.
9	Process Status	CNCD064I	Process moved to Hold queue. Status is Held Due to Suspension.
9	Process Status	CNCD065I	Process moved to Hold queue. Status is Held for Call.
9	Process Status	CNCD066I	Process moved to Hold queue. Status is Held Initial.

Message IDs specific to Sterling Connect:Enterprise

You can use message IDs specific to Sterling Connect:Enterprise when creating rules.

The following table lists Sterling Control Center message IDs specific to Sterling Connect:Enterprise servers.

Event Type	Event Name	Message ID	Message Text
13	Connection Started	CNCE022E	Error connecting to server. Server ID: \{3\} Host Name: \{0\} API Port: \{1\} Source Port: \{5\} User ID: \{2\} Details: \{4\}
14	Connection Shutdown Started	CNCE023E	Error disconnecting from server. Server ID: \{3\} Host Name: \{0\} API Port: \{1\} User ID: \{2\}
3 1 2 4	Process Start Process Step Start Process Step End Process End	CNCE001I	AutoConnect (AC) SEND Operation Performed. (IBM Sterling Connect:Enterprise for z/OS only)
3 1 2 4	Process Start Process Step Start Process Step End Process End	CNCE002I	AutoConnect (AC) RECV Operation Performed. (Sterling Connect:Enterprise for z/OS only)
3 1 2 4	Process Start Process Step Start Process Step End Process End	CNCE003I	RemoteConnect (RC) ADD Operation Performed.
13	Connection Started	CNCE009I	RemoteConnect (RC) CONNECT Operation Performed.
12	Server Command	CNCE007I	RemoteConnect (RC) DEL Operation Performed.
12	Server Command	CNCE006I	RemoteConnect (RC) DIR Operation Performed.
14	Connection Shutdown Started	CNCE010I	RemoteConnect (RC) DISCON Operation Performed.
3 1 2 4	Process Start Process Step Start Process Step End Process End	CNCE005I	RemoteConnect (RC) REQ Operation Performed.
3 1 2 4	Process Start Process Step Start Process Step End Process End	CNCE011I	Offline (OFF) EXT Operation Performed. (IBM Sterling Connect:Enterprise for UNIX only)
3 1 2 4	Process Start Process Step Start Process Step End Process End	CNCE012I	Offline (OFF) ADD Operation Performed. (Sterling Connect:Enterprise for UNIX only)

Event Type	Event Name	Message ID	Message Text
3 1 2 4	Process Start Process Step Start Process Step End Process End	CNCE013I	AutoConnect (AC) Collect (C) Operation Performed. (Sterling Connect:Enterprise for UNIX only)
3 1 2 4	Process Start Process Step Start Process Step End Process End	CNCE014I	AutoConnect (AC) Transmit (T) Operation Performed. (Sterling Connect:Enterprise for UNIX only)
3 1 2 4	Process Start Process Step Start Process Step End Process End	CNCE015I	Offline (OFF) ERA Operation Performed. (Sterling Connect:Enterprise for UNIX only)
3 1 2 4	Process Start Process Step Start Process Step End Process End	CNCE016I	Offline (OFF) STA Operation Performed. (Sterling Connect:Enterprise for UNIX only)
13	Connection Started	CNCE018I	AutoConnect (AC) RNFR operation Performed.
13	Connection Started	CNCE019I	AutoConnect (AC) RNTO operation Performed.
13	Connection Started	CNCE020I	RemoteConnect (RC) RNFR operation Performed.
13	Connection Started	CNCE021I	RemoteConnect (RC) RNTO operation Performed.
13	Connection Started	CNCE113I	AutoConnect (AC) Failure. (Sterling Connect:Enterprise for UNIX only)
5	Server Status	CNCE114I	IBM Sterling Connect:EnterpriseDaemon is running. ID: DaemonID
5	Server Status	CNCE115I	Sterling Connect:Enterprise Daemon is down. ID: DaemonID
5	Server Status	CNCE116I	Sterling Connect:Enterprise Daemon added/removed/changed. ID: DaemonID
13	Connection Started	CNCE209I	AutoConnect (AC) CONNECT Operation Performed. (Sterling Connect:Enterprise for Sterling Connect:Enterprise for z/OS only)
14	Connection Shutdown Started	CNCE210I	AutoConnect (AC) DISCON Operation Performed. (Sterling Connect:Enterprise for z/OS only)
13	Connection Started	CNCE211I	AutoConnect (AC) SessionStart Performed.
13	Connection Started	CNCE212I	AutoConnect (AC) SessionEnd Performed.
13	Connection Started	CNCE213I	AutoConnect (AC) ULOG Performed.

Messages IDs specific to QuickFile

You can use message IDs specific to QuickFile when creating rules.

The following table lists Sterling Control Center message IDs specific to QuickFile.

Event Type	Event Name	Message ID	Message Text
1	Process Step Start	CIVCC1001I	CIVCC1001I: {0} sent file {1} with package subject {2} to {3}
2	Process Step End	CIVCC1001I	CIVCC1001I: {0} sent file {1} with package subject {2} to {3}
1	Process Step Start	CIVCC1004I	CIVCC1004I: {0} downloaded file {1} with package subject {2}
2	Process Step End	CIVCC1004I	CIVCC1004I: {0} downloaded file {1} with package subject {2}
5	Server Status	CIVCC1006I	CIVCC1006I: {0} deleted file {1} with package subject {2}
1	Process Step Start	CIVCC1008E	CIVCC1008E - Contains virus and will not be transferred
2	Process Step End	CIVCC1008E	CIVCC1008E - Contains virus and will not be transferred
1	Process Step Start	CIVCC1009I	CIVCC1009I - Successfully scanned for viruses
2	Process Step End	CIVCC1009I	CIVCC1009I - Successfully scanned for viruses
3	Process Start	CIVCC1017I	CIVCC1017I: Transfer package with subject {0} started
4	Process End	CIVCC1018E	CIVCC1018E - Transfer package with subject (0) ended with error
4	Process End	CIVCC1018I	CIVCC1018I: Transfer package with subject {0} ended
5	Server Status	CIVCC1019I	CIVCC1019I: Summary for package with subject {0}
1	Process Step Start	CIVCC1022E	CIVCC1022E - Contains sensitive information (DLP)
2	Process Step End	CIVCC1022E	CIVCC1022E - Contains sensitive information (DLP)
1	Process Step Start	CIVCC1023I	CIVCC1023I - Successfully scanned for sensitive information (DLP)
2	Process Step End	CIVCC1023I	CIVCC1023I - Successfully scanned for sensitive information (DLP)
5	Server Status	CIVID1011I	CIVID1011I: {0} enabled the advanced file transfer
5	Server Status	CIVID1008I	CIVID1008I: {0} logged out
5	Server Status	CIVCF1020I	CIVCF1020I - Successfully deleted ICAP server
5	Server Status	CIVCF1030I	CIVCF1030I - Successfully enabled system policy for Data Loss Prevention
5	Server Status	CIVCF1030E	CIVCF1030E - ICAP Configuration error
5	Server Status	CIVCF1032E	CIVCF1032E - Could not connect to ICAP server

Messages IDs specific to Sterling Connect:Express

You can use message IDs specific to Sterling Connect:Express when creating rules.

The following table lists Sterling Control Center message IDs specific to Sterling Connect:Express servers. The Sterling Connect:Express platform is denoted by the first letter of the message ID: U is UNIX and W is Microsoft Windows.

Important: Sterling Connect:Express logs errors differently than other server types supported by Sterling Control Center. If you want to use the predefined Bad Return Code rule or create a rule to watch for failed Sterling Connect:Express transfers, you need to watch for non-zero return codes in the Server Status and Server Error event types in addition to the Process Step Ended event type.

Event Type	Event Name	Message ID	Message Text
5	Server Status	UMBL124I	Monitor information - C:X INITIALIZATION COMPLETE V150-2 RUN=(C)
8	Server Shutdown	UMEL300I	Monitor ended - C:X TERMINATION COMPLETE
5	Server Status	UMIL125I	Monitor information - LARGE FILE (>2Gbytes) SUPPORT AVAILABLE
12	Server Command	URIL058I	Request information - REQUEST nnnnnnnn PURGED BY REMAPI
12	Server Command	URKL021I	Request accepted - REQUEST nnnnnnnn <- xxxxxx ACCEPTED (N)
11	Server Error	URLL145W	Request rejected - REQUEST nnnnnnnn REJECTED <- XXXXXXXX SRC=xxxx TRC=yyyyL PRC=zzzz
11	Server Error	URRL012I	Request error - REQUEST nnnnnnnn FILE cccccccc SRC=xxxx TRC=yyyyL PRC=zzzz
1	Process Step Started	UTBL132I	Transfer started - REQUEST nnnnnnnn FILE TRANSFER STARTED STRF xxxxxxxxxx
2	Process Step Ended	UTEL130I	Transfer ended - REQUEST nnnnnnnn FILE TRANSFER ENDED STRF xxxxxxxxxx
4	Process Ended	UTEL136I	Transfer ended - REQUEST nnnnnnnn RECEIVING <- cccccccc FILE FILE NUMBER OF RECORDS: nnnnnnnnnn
4	Process Ended	UTEL137I	Transfer ended - REQUEST nnnnnnnn TRANSMITTING -> cccccccc FILE FILE NUMBER OF RECORDS: nnnnnnnnnn
3	Process Started	UTKL131I	Transfer accepted - REQUEST nnnnnnnn FILE TRANSFER ACCEPTED STRF xxxxxxxxxx
11	Server Error	UTRL142E	Transfer error - REQUEST nnnnnnnn FILE ERROR DURING SELECTION TRC=yyyyL PRC=zzzz
5	Server Status	UXAL151W	Communication aborted - COMMUNICATION ABORTED WITH XXXXXXXX REQ: nnnnnnn
14	Connection Shutdown Started	UXCL139I	Communication ended - COMMUNICATION CLOSED (I) WITH: XXXXXXXX REQ: nnnnnnnnn (P) (T)
14	Connection Shutdown Started	UXDL138I	Communication ended - COMMUNICATION CLOSED (O) WITH: XXXXXXXX REQ: nnnnnnnn (P) (T)
13	Connection Started	UXOL134I	Communication started - COMMUNICATION OPENED (I) WITH: XXXXXXXX REQ: nnnnnnnn (P) (T)
13	Connection Started	UXPL133I	Communication started - COMMUNICATION OPENED (O) WITH: XXXXXXXX REQ: nnnnnnnnn (P) (T)
5	Server Status	UXRL143I	Communication error - COMMUNICATION NOT OBTAINED -> XXXXXXXX REQ: nnnnnnnnn RETRY IN: xx MINUTES
5	Server Status	UXRL144E	Communication error - REQUEST nnnnnnnn SESSION ERROR CALL NRC=nnnn
13	Connection Started	UXWL140I	Communication retry - REQUEST nnnnnnnn RETRY WITH PARTNER XXXXXXXX
5	Server Status	WMBL055I	Monitor initialization - THE MONITOR IS STARTED
5	Server Status	WMSL067I	Monitor start - MONITOR INITIALISATION IN PROGRESS...
4	Process Ended	WOIL040I	Transfer end - XXXXXXXX – DISABLED
1	Process Step Started	WTBL077I	Transfer begin - XXXXXXXX - FILE - TRANSFER STARTED (RECEIVE)

Event Type	Event Name	Message ID	Message Text
2	Process Step Ended	WTEL078I	Transfer end - XXXXXXXX - FILE - TRANSFER ENDED
3	Process Started	WTKL076I	Transfer accepted - XXXXXXXX - TRANSFER ACCEPTED
12	Server Command	WTRL081E	Client error - Cnnnnnnnn - ERROR - TRC= Axxxx SRC= xxxx NRC= xxxx ERC=xxxx
12	Server Command	WWRL035E	Client error - Cnnnnnnnn - TCP/IP RC= xxxx
13	Connection Started	WXBL021I	Communication begin - nnnnnnnnnn - COMMUNICATION OPENED (IN) WITH cccccc (p)
14	Connection Shutdown Started	WXEL022I	Communication end - XXXXXXXX - COMMUNICATION CLOSED WITH cccccc (p)

Message IDs specific to Sterling B2B Integrator

You can use message IDs specific to Sterling B2B Integrator when creating rules.

The following table lists Sterling Control Center message IDs specific to Sterling B2B Integrator servers.

Event Type	Event Name	Message ID	Message Text
5	Server Status	CGIS010I	Sterling B2B Integrator Adapter is enabled. ID: {0}
5	Server Status	CGIS011I	Sterling B2B Integrator Adapter has stopped. ID: {0}
5	Server Status	CGIS012I	Sterling B2B Integrator Adapter added/removed.
5	Server Status	CGIS013I	Sterling B2B IntegratorNode status is down. Node: {0}
5	Server Status	CGIS014I	Sterling B2B Integrator Node status is up. Node: {0}
5	Server Status	CGIS015I	Sterling B2B Integrator Node removed. Node: {0}
12	Server Command	CGIS016I	Process Name: Name cleared from Process Queue by User: UserID
5	Server Status	CGIS018I	Sterling B2B Integrator Node added. Node: {0}
5	Server Status	CGIS031I	Sterling B2B Integrator Perimeter server has been enabled. Name: {0}
5	Server Status	CGIS032I	Sterling B2B Integrator Perimeter Server has been disabled : Name : {0}
5	Server Status	CGIS033I	Sterling B2B Integrator Perimeter Server connected : Name : {0}
5	Server Status	CGIS034I	Sterling B2B Integrator Perimeter Server disconnected : Name : {0}
5	Server Status	CGIS035I	Sterling B2B Integrator Perimeter Server added/removed.

Message IDs (Event Codes) specific to Sterling File Gateway

Sterling File Gateway "event codes" are mapped to Sterling Control Center event message IDs. For more information on a particular event code, search for that code.

Message IDs for Sterling Control Center

There are a variety of events and messages generated in Sterling Control Center related to Sterling Control Center status and components, such as server groups, roles, rules, databases, users, and schedules. Message IDs related to Sterling Connect:Direct File Agent are also included.

This list is sorted by message ID within the event type.

Event Type	Event Name	Message ID	Message Text
Sterling Control Center Status Messages			
10	Server License	CCNS004E	License Expiry Warning. License is about to expire. Days left: {0}
5	Server Status	CCNS006E	Maximum concurrent Processes changed.
5	Server Status	CCNS010I	Server running with emergency key.
5	Server Status	CCNS018E	Monitor rate out of compliance. Server ID: {0} Last poll Date/time: {1} Monitor Rest Time: {2}
5	Server Status	CCNS019E	Certificate expiry notification. Server ID: (0) Certificate: {1} Expires: {2} Days left: {3}
5	Server Status	CCNS020E	Monitored Queue Limit has been exceeded. Server ID: {0} Queue: {1} Limit: {2} Depth: {3}
5	Server Status	CCNS022I	Monitoring paused. Server ID: {0} User ID: {1}
5	Server Status	CCNS023I	Monitoring resumed from pause point. Server ID: {0} User ID: {1}
5	Server Status	CCNS024I	Monitoring resumed from current time. Server ID: {0} User ID: {1}
5	Server Status	CCNS025I	At startup, server found to be paused. Server ID: {0}
5	Server Status	CCNS029I	Monitor rate back in compliance. Server ID: {0} Last poll Date/time: {1} Monitor Rest Time: {2}
5	Server Status	CCNS030I	Monitored Queue Limit back in compliance. Server ID: {0} Queue: {1} Limit: {2} Depth: {3}
5	Server Status	CCTR033E	Server is up. **Note:** For monitored server.
5	Server Status	CCTR034E	Server is down. **Note:** For monitored server.
5	Server Status	CCTR035E	Unable to establish a connection to server. Check Server Service configuration parameters for invalid ID and/or password value, or unsupported level of server.
10	Server License	CCTR040E	License management key file in use only valid for {0} more day(s).
10	Server License	CCTR041E	License expired. A new license management key file must be obtained to restart the product.
10	Server License	CCTR046E	Emergency license management key file in use. Valid for {0} more day(s).
5	Server Status	CCTR051E	Connection cannot be established to a Connect:Direct server.
12	Server Command	CCTR052I	Simultaneous pollers value changed by user UserID to nn.
5	Server Status	CCTR055E	Server is up. **Note:** For managed but not monitored server.
5	Server Status	CCTR056E	Server is down. **Note:** For managed but not monitored server.
5	Server Status	CCTR074E	Connection to server established.
5	Server Status	CCTR083E	Engine shutdown has been initiated by user name.

Event Type	Event Name	Message ID	Message Text
5	Server Status	CCTR101E	Service {0} Updated.
Server Group Messages			
12	Server Command	CGRP012I	Group created
12	Server Command	CGRP013I	Group updated
12	Server Command	CGRP014I	Group deleted
Role Messages			
12	Server Command	CROL017E	New role created, ID: {0}, by: {1}, Role: {2}
12	Server Command	CROL018E	Role updated
12	Server Command	CROL019E	Role deleted
Rule Messages			
12	Server Command	CRUL043E	New Rule Created, ID: RuleID, by: UserID
12	Server Command	CRUL044E	Rule Updated, ID: RuleID, by: UserID
12	Server Command	CRUL045E	Rule Deleted, ID: RuleID, by: UserID
12	Server Command	CRUL050E	Alert Deleted
12	Server Command	CRUL077E	Rule moved down
12	Server Command	CRUL078E	Rule moved up
Metadata Rule Messages			
12	Server Command	CMDR043E	New metadata rule created, ID, by: UserID.
12	Server Command	CMDR044E	Metadata rule updated, ID, by: UserID.
12	Server Command	CMDR045E	Metadata rule deleted, ID, by: UserID.
12	Server Command	CMDR077E	Metadata rule moved down, ID, by: UserID.
12	Server Command	CMDR078E	Metadata rule moved up, ID, by: UserID.
12	Server Command	CMDR148E	Server metadata field map updated.
12	Server Command	CMDR149E	Metadata field map updated.
Rule Action Messages			
12	Server Command	CACT025E	New action created, ID: ActionID, by: UserID
12	Server Command	CACT026E	Action updated, ID: ActionID, by: UserID
12	Server Command	CACT027E	Action deleted, ID: ActionID, by: UserID
12	Server Command	CRUL099I	Server command performed successfully. Server ID: {0}, Command: {1}
12	Server Command	CRUL140I	Server command to be performed. Rule ID: {0}, Action ID: {1}, Event ID: {2}, Server ID: {3}, Command: {4}
Metadata Rule Action Messages			
12	Server Command	CMDA025E	New action created. ID: ActionID, by: UserID.
12	Server Command	CMDA026E	Action updated. ID: ActionID, by: UserID.
12	Server Command	CMDA027E	Action deleted. ID: ActionID, by: UserID.
Database Messages			
12	Server Status	CJDB026E	Database outage has occurred. System shutdown initiated.
12	Server Status	CJDB032E	Staging database unavailable.
User Maintenance Messages			
12	Server Command	CUSR030E	New User Created, ID: UserID, by: UserID

Event Type	Event Name	Message ID	Message Text
12	Server Command	CUSR031E	User Updated, ID: UserID, by: UserID
12	Server Command	CUSR032E	User Deleted, ID: UserID, by: UserID
Node Discovery Messages			
12	Server Command	CDIS016E	Deleted Explorer node: NodeID.
12	Server Command	CDIS017E	Deleted Discovery node: NodeID.
12	Server Command	CDIS019E	Changed enabled state for node: NodeID.
12	Server Command	CDIS028E	Discovery complete.
12	Server Command	CDIS031E	Discovery initiated.
Report Service Messages			
12	Server Command	CRPT006E	Updated report: ReportID.
12	Server Command	CRPT007E	Deleted report: ReportID.
12	Server Command	CRPT008E	Created report: ReportID.
5	Server Status	CRPT012I	High Water Mark Report complete.
License Service Messages			
5	Server Status	CLIC019I	License removed. ID: NodeID, Version: Version#, User: UserID.
5	Server Status	CLIC020I	License added. ID: NodeID, Version: Version#, User: UserID.
5	Server Status	CLIC027I	License push operation complete.
5	Server Status	CLIC028I	License validation operation complete.
5	Server Status	CLIC050E	License import failed. ID: {0} Version: {1} User: {2}
File Agent Service Messages			
5	Server Status	CCFA001I	File Agent {0} added for Server ID {1}.
5	Server Status	CCFA002I	File Agent {0} removed from Server ID {1}
5	Server Status	CCFA003I	File Agent {0} for Server ID {1} is up.
5	Server Status	CCFA004I	File Agent {0} for Server ID {1} is down.
12	Server Command	CCFA005I	File Agent {0} for Server ID {1} configuration updated.
5	Server Status	CCFA006I	File Agent {0} for Server ID {1} has not submitted a Process lately. Minutes since submit: {2}
5	Server Status	CCFA007I	File Agent {0} for Server ID {1} submitted a Process.
15	Control Center Status	CCFA008I	File Agent Settings for no process submitted warning time value changed by user {0} to {1}.
15	Control Center Status	CCFA009I	File Agent Settings for SNMP listener port value changed by user {0} to {1}.
15	Control Center Status	CCFA010I	File Agent Settings for heart beat interval value changed by user {0} to {1}.
15	Control Center Status	CCFA0014I	Error starting File Agent trap receiver logic. SNMP Listener port specified may already be in use. Error: {0}
15	Control Center Status	CCFA021I	File Agent Settings for SNMP listener address value changed by user {0} to {1}.
15	Control Center Status	CCFA022I	File Agent Service listening on specified SNMP listener address and port. Address: {0} Port: {1}
15	Control Center Status	CCFA023I	File Agent peak unprocessed trap count: {0}

Event Type	Event Name	Message ID	Message Text
Email List Messages			
12	Server Command	CEDL025E	New Email List Created, ID: {0}, by: {1}
12	Server Command	CEDL026E	Email List Updated, ID: {0}, by: {1}
12	Server Command	CEDL027E	Email List Deleted, ID: {0}, by: {1}
Report Schedule Messages			
12	Server Command	CRSC028E	Report Schedule Created. ID: {0}, by: {1}
12	Server Command	CRSC029E	Report Schedule Updated. ID: {0}, by: {1}
12	Server Command	CRSC030E	Report Schedule Deleted. ID: {0}, by: {1}
	Automated Reports Messages		
12	Server Command	CRSC051I	Automated Report Created. ID: {0}, by: {1}
12	Server Command	CRSC052I	Automated Report Updated. ID: {0}, by: {1}
12	Server Command	CRSC053I	Automated Report Deleted. ID: {0}, by: {1}
Calendar Schedule Messages			
12	Server Command	CCAL006E	Updated calendar: CalendarID, by: UserID.
12	Server Command	CCAL007E	Deleted calendar: CalendarID, by: UserID.
12	Server Command	CCAL008E	Created calendar: CalendarID, by: UserID.
	Rule Schedule Messages		
12	Server Command	CRSC025E	New rule schedule created, RuleID, by: UserID.
12	Server Command	CRSC026E	Rule schedule updated, RuleID, by: UserID.
12	Server Command	CRSC027E	Rule schedule deleted, RuleID, by: UserID.
Calendar Schedule SLC-Generated Messages			
6	SLC	CSLC026E	Workflow/Milestone/Step/Process did not start by NERs. SLC: SLCID
6	SLC	CSLC027E	Workflow/Milestone/Step/Process did not start by NERe. SLC:SLCID
6	SLC	CSLC030E	Workflow/Milestone/Step/Process started. SLC: SLCID
6	SLC	CSLC031E	Step/Process running prior to start of monitoring. SLC: SLCID
6	SLC	CSLC032E	Workflow/Milestone/Step/Process started prior to NSRs. SLC: SLCID
6	SLC	CSLC034E	Workflow/Milestone/Step/Process did not start by NSRe. SLC: SLCID
6	SLC	CSLC035E	Workflow/Milestone/Step/Process started after NSRe. SLC: SLCID
6	SLC	CSLC036E	Workflow/Milestone/Step/Process ended before NERs. SLC: SLCID
6	SLC	CSLC037I	Workflow/Milestone/Step/Process ended. SLC: SLCID
6	SLC	CSLC038E	Workflow/Milestone/Step/Process did not end by NERe. SLC: SLCID
6	SLC	CSLC039E	Workflow/Milestone/Step/Process ended after NERe. SLC: SLCID
6	SLC	CSLC040E	Workflow/Milestone/Step/Process did not complete before the end of the monitoring window. SLC: SLCID
6	SLC	CSLC046E	Workflow/Milestone/Step/Process suspended. SLC: SLCID

Event Type	Event Name	Message ID	Message Text
6	SLC	CSLC047E	Workflow/Milestone/Step/Process did not start by NSRs. SLC: SLCID
6	SLC	CSLC048E	Workflow/Milestone/Step/Process running after NERs. SLC: SLCID
Duration Schedule SLC-Generated Messages			
6	SLC	CSLC033I	Workflow/Milestone/Step/Process started. SLC: SLCID
6	SLC	CSLC041E	Workflow/Milestone/Step/Process ended before dMin. SLC: SLCID
6	SLC	CSLC042I	Workflow/Milestone/Step/Process ended when expected - between dMin and dMax. SLC: SLCID
6	SLC	CSLC043E	Workflow/Milestone/Step/Process did not end by dMax. SLC: SLCID
6	SLC	CSLC044E	Workflow/Milestone/Step/Process ended after dMax. SLC: SLCID
6	SLC	CSLC045E	Workflow/Milestone/Step/Process did not complete before the end of the monitoring window. SLC: SLCID
6	SLC	CSLC049E	Workflow/Milestone/Step/Process did not end by dMin. SLC: SLCID
6	SLC	CSLC050E	Workflow/Milestone/Step/Process duration could not be determined - was running before monitoring started.
6	SLC	CSLC171I	File Transfer ahead of schedule (25% dMin)
6	SLC	CSLC172E	File Transfer behind schedule (25% dMin)
6	SLC	CSLC173I	File Transfer ahead of schedule (50% dMin)
6	SLC	CSLC174E	File Transfer behind schedule (50% dMin)
6	SLC	CSLC175I	File Transfer ahead of schedule (75% dMin)
6	SLC	CSLC176E	File Transfer behind schedule (75% dMin)
6	SLC	CSLC177I	File Transfer ahead of schedule (25% dMax)
6	SLC	CSLC178E	File Transfer behind schedule (25% dMax)
6	SLC	CSLC179I	File Transfer ahead of schedule (50% dMax)
6	SLC	CSLC180E	File Transfer behind schedule (50% dMax)
6	SLC	CSLC181I	File Transfer ahead of schedule (75% dMax)
6	SLC	CSLC182E	File Transfer behind schedule (75% dMax)
SLC Group Messages			
12	Server Command	CSLC080I	SLC group created
12	Server Command	CSLC081I	SLC group updated
12	Server Command	CSLC082I	SLC group deleted
12	Server Command	CSLC086I	SLC wildcard group created
12	Server Command	CSLC087I	SLC wildcard group updated
12	Server Command	CSLC088I	SLC wildcard group deleted
12	Server Command	CSLC089I	SLC wildcard group order change
12	Server Command	CSLC220I	New SLC Workflow Group Created, ID, by UserID.
12	Server Command	CSLC221I	SLC Workflow Group Updated, ID, by UserID.
12	Server Command	CSLC222I	SLC Workflow Group Deleted, ID, by UserID.

Event Type	Event Name	Message ID	Message Text
SLC Schedule Messages			
12	Server Command	CSLC083I	SLC schedule created
12	Server Command	CSLC084I	SLC schedule updated
12	Server Command	CSLC085I	SLC schedule deleted
SLC Calendar Messages			
12	Server Command	CSLC112I	Calendar created
12	Server Command	CSLC113I	Calendar updated
12	Server Command	CSLC114I	Calendar deleted
SLC Message List Messages			
12	Server Command	CSLC223I	New MessageList Created, ID, by UserID.
12	Server Command	CSLC224I	MessageList Updated, ID, by UserID.
12	Server Command	CSLC225I	MessageList Deleted, ID, by UserID.
SLC Workflow Messages			
6	SLC	CSLC228E	Workflow/Milestone/Step/Process did not start before the end of the monitoring window. SLC: SLCID
6	SLC	CSLC229I	Workflow/Milestone/Step/Process on time completion for SLC SLCID may be in jeopardy. Reason: ReasonID.

Message IDs specific to configuration management

Many messages related to configuration management are generated in Sterling Control Center.

The following table lists Sterling Control Center message IDs specific to configuration management.

Event Type	Event Name	Message ID	Message Text
12	Server Command	CCFG021I	Operation beginning Netmap node create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG022I	Operation beginning Netmap mode create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG023I	Operation beginning Netmap commpath create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG024I	Operation beginning Initparms create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG025I	Operation beginning Translation table create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG026I	Operation beginning Proxy create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG027I	Operation beginning User auth create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG028I	Operation beginning Secure+ node create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG029I	Operation beginning Secure+ Key Certificate create. User ID: {0} Server ID: {1} Job ID: {2}

Event Type	Event Name	Message ID	Message Text
12	Server Command	CCFG030I	Operation beginning Secure+ Trusted Certificate create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG031I	Operation beginning Netmap node delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG032I	Operation beginning Netmap mode delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG033I	Operation beginning Netmap commpath delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG034I	Operation beginning Initparms delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG035I	Operation beginning Translation table delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG036I	Operation beginning Proxy delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG037I	Operation beginning User auth delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG038I	Operation beginning Secure+ node delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG039I	Operation beginning Secure+ Key Certificate delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG040I	Operation beginning Secure+ Trusted Certificate delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG041I	Operation beginning Netmap node refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG042I	Operation beginning Netmap mode refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG043I	Operation beginning Netmap commpath refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG044I	Operation beginning Initparms refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG045I	Operation beginning Translation table refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG046I	Operation beginning Proxy refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG047I	Operation beginning User auth refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG048I	Operation beginning Secure+ node refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG049I	Operation beginning Secure+ Key Certificate refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG050I	Operation beginning Secure+ Trusted Certificate refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG051I	Operation beginning Netmap node update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG052I	Operation beginning Netmap mode update. User ID: {0} Server ID: {1} Job ID: {2}

Event Type	Event Name	Message ID	Message Text
12	Server Command	CCFG053I	Operation beginning Netmap commpath update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG054I	Operation beginning Initparms update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG055I	Operation beginning Translation table update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG056I	Operation beginning Proxy update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG057I	Operation beginning User auth update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG058I	Operation beginning Secure+ node update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG059I	Operation beginning Secure+ Key Certificate update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG060I	Operation beginning Secure+ Trusted Certificate update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG071I	Operation successful Netmap node create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG072I	Operation successful Netmap mode create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG073I	Operation successful Netmap commpath create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG074I	Operation successful Initparms create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG075I	Operation successful Translation table create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG076I	Operation successful Proxy create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG077I	Operation successful User auth create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG078I	Operation successful Secure+ node create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG079I	Operation successful Secure+ Key Certificate create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG080I	Operation successful Secure+ Trusted Certificate create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG081I	Operation successful Netmap node delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG082I	Operation successful Netmap mode delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG083I	Operation successful Netmap commpath delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG084I	Operation successful Initparms delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG085I	Operation successful Translation table delete. User ID: {0} Server ID: {1} Job ID: {2}

Event Type	Event Name	Message ID	Message Text
12	Server Command	CCFG086I	Operation successful Proxy delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG087I	Operation successful User auth delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG088I	Operation successful Secure+ node delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG089I	Operation successful Secure+ Key Certificate delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG090I	Operation successful Secure+ Trusted Certificate delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG091I	Operation successful Netmap node refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG092I	Operation successful Netmap mode refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG093I	Operation successful Netmap commpath refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG094I	Operation successful Initparms refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG095I	Operation successful Translation table refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG096I	Operation successful Proxy refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG097I	Operation successful User auth refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG098I	Operation successful Secure+ node refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG099I	Operation successful Secure+ Key Certificate refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG100I	Operation successful Secure+ Trusted Certificate refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG101I	Operation successful Netmap node update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG102I	Operation successful Netmap mode update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG103I	Operation successful Netmap commpath update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG104I	Operation successful Initparms update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG105I	Operation successful Translation table update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG106I	Operation successful Proxy update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG107I	Operation successful User auth update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG108I	Operation successful Secure+ node update. User ID: {0} Server ID: {1} Job ID: {2}

Event Type	Event Name	Message ID	Message Text
12	Server Command	CCFG109I	Operation successful Secure+ Key Certificate update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG110I	Operation successful Secure+ Trusted Certificate update. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG111E	Operation failed Netmap node create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG112E	Operation failed Netmap mode create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG113E	Operation failed Netmap commpath create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG114E	Operation failed Initparms create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG115E	Operation failed Translation table create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG116E	Operation failed Proxy create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG117E	Operation failed User auth create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG118E	Operation failed Secure+ node create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG119E	Operation failed Secure+ Key Certificate create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG120E	Operation failed Secure+ Trusted Certificate create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG121E	Operation failed Netmap node delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG122E	Operation failed Netmap mode delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG123E	Operation failed Netmap commpath delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG124E	Operation failed Initparms delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG125E	Operation failed Translation table delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG126E	Operation failed Proxy delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG127E	Operation failed User auth delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG128E	Operation failed Secure+ node delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG129E	Operation failed Secure+ Key Certificate delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG130E	Operation failed Secure+ Trusted Certificate delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG131E	Operation failed Netmap node refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}

Event Type	Event Name	Message ID	Message Text
12	Server Command	CCFG132E	Operation failed Netmap mode refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG133E	Operation failed Netmap commpath refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG134E	Operation failed Initparms refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG135E	Operation failed Translation table refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG136E	Operation failed Proxy refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG137E	Operation failed User auth refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG138E	Operation failed Secure+ node refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG139E	Operation failed Secure+ Key Certificate refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CFG140E	Operation failed Secure+ Trusted Certificate refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG141E	Operation failed Netmap node update. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG142E	Operation failed Netmap mode update. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG143E	Operation failed Netmap commpath update. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG144E	Operation failed Initparms update. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG145E	Operation failed Translation table update. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG146E	Operation failed Proxy update. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG147E	Operation failed User auth update. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG148E	Operation failed Secure+ node update. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG149E	Operation failed Secure+ Key Certificate update. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG150E	Operation failed Secure+ Trusted Certificate update. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG151E	Operation failed. Job ID: {0} UserID: {1} Server ID: {2} Operation: {3} Object type: {4} Reason: {5}
12	Server Command	CCFG152E	Configuration Job completed. Job ID: {0} User ID: {1} Operation: {2} Object type: {3} Return Code: {4} Error: {5}
12	Server Command	CCFG158E	Scheduled Configuration Job canceled by System at startup. Job should have already run. Job ID: {0} Operation: {1} Object type: {2}
12	Server Command	CCFG159E	Configuration Job canceled by System at startup. Job had been canceled or was running previously. Job ID: {0} Operation: {1} Object type: {2}

Event Type	Event Name	Message ID	Message Text
12	Server Command	CCFG160E	Cancel Configuration Job failed, nothing to cancel. User: {0} Job ID: {1}
12	Server Command	CCFG161I	Configuration Job submitted. Job ID: {0} User ID: {1} Operation: {2} Object type: {3} Status: {4}
12	Server Command	CCFG162I	Configuration Job held. Job ID: {0} User ID: {1} Operation: {2} Object type: {3}
12	Server Command	CCFG163I	Configuration Job canceled. Job ID: {0} User ID: {1} Operation: {2} Object type: {3}
12	Server Command	CCFG164I	Configuration Job completed. Job ID: {0} User ID: {1} Operation: {2} Object type: {3} Return Code: {4}
12	Server Command	CCFG165I	Configuration Job starting. Job ID: {0} User ID: {1} Operation: {2} Object type: {3}
12	Server Command	CCFG166I	Cancel Configuration Job initiated. User: {0} Job ID: {1}
12	Server Command	CCFG167I	Configuration Job updated. Job ID: {0} User ID: {1} Operation: {2} Object type: {3} Status: {4}
12	Server Command	CCFG168I	Configuration Job released. Job ID: {0} User ID: {1} Operation: {2} Object type: {3} Status: {4}
12	Server Command	CCFG169I	Configuration Job restarted. Job ID: {0} User ID: {1} Operation: {2} Object type: {3} Status: {4}
12	Server Command	CCFG184I	Template created. User ID: {0} ID: {1} Type: {2}
12	Server Command	CCFG185I	Template updated. User ID: {0} ID: {1} Type: {2}
12	Server Command	CCFG186I	Template deleted. User ID: {0} ID: {1} Type: {2}
12	Server Command	CCFG188I	Versions of all objects associated with server being deleted by System. Server: {0}
12	Server Command	CCFG189I	Version being deleted. User ID: {0} Version ID: {1} Server: {2} Object type: {3}
12	Server Command	CCFG191I	New Netmap node version created. Server ID: {0}
12	Server Command	CCFG192I	New Netmap mode version created. Server ID: {0}
12	Server Command	CCFG193I	New Netmap commpath version created. Server ID: {0}
12	Server Command	CCFG194I	New Initparms version created. Server ID: {0}
12	Server Command	CCFG195I	New Translation table version created. Server ID: {0}
12	Server Command	CCFG196I	New Proxy version created. Server ID: {0}
12	Server Command	CCFG197I	New User auth version created. Server ID: {0}
12	Server Command	CCFG198I	New Secure+ Node version created. Server ID: {0}
12	Server Command	CCFG199I	New Secure+ Key Certificates version created. Server ID: {0}
12	Server Command	CCFG200I	New Secure+ Trusted Certificates version created. Server ID: {0}
12	Server Command	CCFG208E	Operation failed Secure+ cipher suite refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG209I	Operation beginning Secure+ cipher suite refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG210I	Operation successful Secure+ cipher suite refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG211E	Operation failed Secure+ alias create. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}

Event Type	Event Name	Message ID	Message Text
12	Server Command	CCFG212E	Operation failed Secure+ alias delete. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG213E	Operation failed Secure+ alias refresh. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG214E	Operation failed Secure+ rekey parm file. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG215E	Operation failed Secure+ synch parm file. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG216E	Operation failed Secure+ validate parm file. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG221I	New Secure+ Cipher Suites version created. Server ID: {0}
12	Server Command	CCFG222I	Operation beginning Secure+ alias create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG222I	Operation beginning Secure+ alias create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG223I	Operation beginning Secure+ alias delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG224I	Operation beginning Secure+ alias refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG225I	Operation successful Secure+ alias create. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG226I	Operation successful Secure+ alias delete. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG227I	Operation successful Secure+ alias refresh. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG228I	New Secure+ aliases version created. Server ID: {0}
5	Server Status	CCFG229I	Trusted Certificate Expiry notification. Server ID: {0} Certificate: {1} Expires: {2} Days left: {3}
5	Server Status	CCFG230I	Key Certificate Expiry notification. Server ID: {0} Certificate: {1} Expires: {2} Days left: {3}
12	Server Command	CCFG232I	Operation beginning Secure+ rekey parm file. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG233I	Operation beginning Secure+ synch parm file. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG234I	Operation beginning Secure+ validate parm file. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG235I	Operation successful Secure+ rekey parm file. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG236I	Operation successful Secure+ synch parm file. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG237I	Operation successful Secure+ validate parm file. User ID: {0} Server ID: {1} Job ID: {2} Response: {3}
12	Server Command	CCFG241I	Operation beginning Copy parameters. User ID: {0} Server ID: {1} Job ID: {2}
12	Server Command	CCFG242I	Operation successful Copy parameters. User ID: {0} Server ID: {1} Job ID: {2}

Event Type	Event Name	Message ID	Message Text
12	Server Command	CCFG248E	Operation failed Copy parameters. User ID: {0} Server ID: {1} Job ID: {2} Reason: {3}
12	Server Command	CCFG250E	User ID: {0} not permitted to manage {1}

Chapter 20. Regular expressions

Regular expressions (or regex) can be used in wildcard SLCs and other Sterling Control Center entities to match text or numeric strings that follow a particular pattern. They consist of normal characters and special characters. Normal characters are uppercase and lowercase letters and numbers. Special characters have specific meanings in the expression.

For example, the regular expression ABCDEF contains only normal characters. When used as a match criterion, it will match only ABCDEF text strings. The regular expression [ABCDEF] contains normal characters and special characters (the brackets). It will match any text string that includes A, B, C, D, E, or F.

Regular expressions can be very complex. This topic describes basic expression characters and some simple examples for Sterling Control Center. If you want to learn more about regular expressions, an Internet search on the terms “regular expression” or “regex” will provide many sites that explain regular expressions in greater detail.

The following table lists some common regular expression special characters and examples. Multiple special characters can be used in the same expression to create more criteria.

Note: Regular expression patterns are case sensitive. Case sensitivity can be controlled within a pattern using the inline modifier (?i).

Special Character	Description	Examples
[ ]	Matches any character between the brackets. Ranges are specified by a hyphen ([a-z], [0-9]).	Proc4[123] matches the strings Proc41, Proc42, and Proc43. Proc4[a-e]7 matches the strings Proc4a7, Proc4b7, Proc4c7, Proc4d7, and Proc4e7.
[^]	Matches any character not appearing between the brackets. Ranges are specified by a hyphen ([a-z], [0-9]).	Proc4[^789] matches all strings that contain Proc4, except for strings containing Proc47, Proc48, or Proc49.
. (period)	Matches any single character.	Proc4.567 matches the strings Proc41567, Proc42567, Proc4a567, and so on. It does not match Proc412567.
+ (plus)	Matches strings containing one or more occurrences of the character immediately preceding the plus sign.	Proc456+ matches Proc456, Proc4566, Proc45666 and so on.
* (asterisk)	Matches strings containing zero or more occurrences of the character preceding the asterisk. The search treats the character preceding the asterisk as optional.	Proc456* matches Proc45, Proc456, Proc4566, Proc45666 and so on.

Special Character	Description	Examples
?	Matches strings containing zero or one occurrence of the character immediately preceding the question mark. The character preceding the question mark is treated as optional by the search.	Proc456? matches Proc45 and Proc456. Proc4[5-8]? matches Proc4, Proc45, Proc46, Proc47, and Proc48.
| (pipe)	Matches the characters on either side of the pipe.	Proc456|Proc459|Proc460 matches Proc456, Proc459, or Proc460.
\	Escape character that converts a special character to a normal character.	Node\.Atlanta matches Node.Atlanta.
(?i)	Used to control case sensitivity. This inline modifier affects all characters to the right and in the same enclosing group. Affected characters are allowed to be case insensitive.	In the pattern w (x (?i) y) z, only the letter y is allowed to be case insensitive.

Chapter 21. Sterling Control Center variables

The following table lists Sterling Control Center event elements that you can use as variables in operating system and server command actions, email actions, metadata actions, and workflow SLC correlators. A brief description of each element is also included.

The event elements are listed in alphabetical order. For each variable, the relevant server types are indicated by an x in one or more of the following columns:

- CD (Sterling Connect:Direct)
- CE (Sterling Connect:Enterprise)
- CX (Sterling Connect:Express)
- SI (Sterling B2B Integrator, including Sterling File Gateway)
- QF (QuickFile)
- MQ (MQ MFT)
- FTP (FTP servers of all types)
- SCC (Sterling Control Center)

Event Element	CD	CE	CX	SI	QF	MQ	FTP	SCC	Description
action								x	Action performed on Sterling Control Center entity.
actionId								x	Name of an action called by a rule.
activityType								x	A code that indicates the type of SLC activity an SLC event is associated with. • WF=Workflow • M=Milestone • S=Process Step • P=Process
alert	x	x	x	x	x	x	x	x	Alert level/severity.
applAgentType		x							Application Agent type
batchId		x							Batch ID
batchNumber		x							Batch number
bytesRead	x	x		x					Number of bytes read from the source file.
bytesSent	x	x		x					Number of bytes sent to the destination file.
bytesXferred	x		x			x			Number of bytes received by the destination file.
CBEA	x								Control Block Encryption Algorithm
CERI	x								Certificate Issuer
CERT	x								Certificate Subject
CKPT	x								Check Point

Event Element	CD	CE	CX	SI	QF	MQ	FTP	SCC	Description
CLAS	x								Class
CNOD	x								CT Node
controlCenterName								x	Sterling Control Center name
CPUS	x								CPU Time (milliseconds)
CSPE	x								Sterling Connect:Direct Secure Plus
CSPP	x								Secure Protocol
CSPS	x								Secure Cipher Suite
CSTN	x								Current® Signature Verified
CX.EVT			x						Event type. Possible values are: • NodeCommand • NodeStatus • NodeStarted • NodeShutdown • NodeError • ProcessStepStart • ProcessStepEnd • ProcessStepProgress • ProcessEnded • ConnectionError • ConnectionShutdownStarted • ProcessStarted • TimerEvent
CX.FBYT			x						File bytes transferred.
CX.FLAB			x						File label (PeSIT pi37).
CX.FNRD			x						Number of records transferred.
CX.LNAM			x						Local node name.
CX.LPHN			x						Local file name.
CX.NBYT			x						Network bytes transferred.
CX.NRC			x						Network return code.
CX.OS			x						Operating system.
CX.PNAM			x						Other node name.
CX.PRC			x						Protocol return code.
CX.PROT			x						File transfer protocol. Possible values are: • E=PsSIT Type E • D=PeSIT Type D • A=PeSIT E "PROF=ANY" • F=FTP • O=Odette
CX.SRC			x						System return code.

Event Element	CD	CE	CX	SI	QF	MQ	FTP	SCC	Description
CX.TBDA			x						Beginning of transfer date/time.
CX.TDIR			x						Transfer direction. Possible values are: • T=Transmit • R=Receive
CX.TDST			x						Transfer destination.
CX.TEDA			x						End of transfer date/time.
CX.TIDT			x						Transfer identified.
CX.TOM			x						Server name.
CX.TORG			x						Transfer origin.
CX.TRC			x						Return code.
CX.TRCV			x						Receiver of the file.
CX.TSND			x						Sender of the file.
CX.TYPL			x						Type of link. Possible values are: • T=TCPIP • S=SNA
CX.TYPR			x						Request type. Possible values are: • N=Normal request • M=Message • E=End-to-End Response • H=Hold request • I=Inquiry request
CX.TYPU			x						Process originator. Possible values are: • I=Local node is the originator • E=Remote node is the originator
CX.USDR			x						User data received (PeSIT Pi99), associated to file.
CX.USDS			x						User data sent (PeSIT pi99), associated to file.
daemonHost		x							DNS host name or IP address of the system the Sterling Connect:Enterprise daemon is on.
daemonName		x							Name of the Sterling Connect:Enterprise daemon.
daemonOriginator		x							Originator of the Sterling Connect:Enterprise daemon.
daemonPid		x							Process identifier of the Sterling Connect:Enterprise daemon.

Event Element	CD	CE	CX	SI	QF	MQ	FTP	SCC	Description
daemonResource		x							Resource of the Sterling Connect:Enterprise daemon.
daemonSid		x							Session identifier of the Sterling Connect:Enterprise daemon.
daemonState		x							State of the Sterling Connect:Enterprise daemon.
daemonType		x							Type of the Sterling Connect:Enterprise daemon. Sterling Control Center monitors only daemons of type master.
dateTime	x	x	x	x	x	x	x	x	The date and time that the event was generated.
daysBeforeExpiry	x								An integer value that tells the number of days before certificate expiration.
DBUG	x								Debug
DBYW	x								Bytes Written
DBYX	x								Bytes Received
DDS1	x								Destination Disposition 1
DDS2	x								Destination Disposition 2
DDS3	x								Destination Disposition 3
destFile	x	x	x	x	x	x	x	x	Destination file name. For Sterling Connect:Direct, the file name at the destination in a copy step of a Process. For QuickFile, QF.File when file is downloaded and QF.packageSubject when file is uploaded.
direction	x		x	x		x	x		Indicates direction of file transmissions. • inBound • outBound
DRCW	x								Records written
DRUX	x								RUs received
ECMP	x								Extended compression
EPRT	x								Execution Priority
eventId	x	x	x	x	x	x	x	x	The ID number assigned by the system to each event.
eventType	x	x	x	x	x	x	x	x	A code indicating the type of event. See *Event Type Descriptions* for a listing of event types and descriptions.

Event Element	CD	CE	CX	SI	QF	MQ	FTP	SCC	Description
eventTypeDescr	x	x	x	x	x	x	x	x	A description for the event type.
executingProcs	x			x					Number of Processes in execution state.
FDBK	x								Feedback
FG.CONS_ORG_KEY				x					Sterling File Gateway Consumer Org Key
FG.DATA_FLOW_ID				x					Sterling File Gateway Data Flow ID
FG.EVENT_CODE				x					Sterling File Gateway Event Code.
FG.FILE_NAME				x					Sterling File Gateway Arrived File Name.
FG.PROD_ORG_KEY				x					Sterling File Gateway Arrived File Producer Org Key
FG.STATE				x					Sterling File Gateway Arrived File State
fgActivityType				x					Sterling File Gateway activity type • D=Delivery • R=Route • A=Arrived File
fileSize	x	x	x	x	x	x	x		The size of the file transferred
fromNode	x		x	x	x	x	x		The node that sent the file: • P=Pnode • S=Snode Indicates which server, local or remote, is sending the file. When the value is P, the server initiating the Process is the sender; otherwise, the server initiating the Process is the receiver.
FUNC	x								Function information
groupId								x	SLC name
HOLD	x								Hold
inError				x					Indicates an error occurred during business process execution
isBP				x					Event is associated with a Sterling B2B Integrator business process.
jobId								x	Job ID
jobName		x				x			Job Name
LCCD	x								Local Return Code

Event Element	CD	CE	CX	SI	QF	MQ	FTP	SCC	Description
lineName		x							Line Name
listName		x							List Name
LKFL	x								Link Fail
LMSG	x								Local Message ID
LNOD	x								Local Node
localNode	x			x		x			Server that processed the file.
mailboxFlags		x							Mailbox Flags
mailBoxId		x							Mailbox ID
maxExecutingProcs	x			x					Maximum number of concurrently executing Processes.
MCSI	x								Merged signature
MEMA	x								Alias Member Name
MEMB	x								Target Member Name
mepLastOccurrence	x			x					The last occurrence of maximum number of concurrently executing Processes.
mepOccurrences	x			x					Number of times maximum number of concurrently executing Processes occurred.
messageId	x	x	x	x	x	x	x	x	Server or Sterling Control Center message ID issued with the event.
milestoneId								x	Name of milestone
MPEA	x								Merge EA
MQMFT.action						x			The MQ MFT action type.
MQMFT.action.time						x			The MQ MFT action time.
MQMFT.call.crslt.oc						x			The call outcome.
MQMFT.call.crslt.rslt.error						x			The call result error.
MQMFT.call.crslt.rslt.oc						x			The call result outcome.
MQMFT.call.crslt.rslt.rc						x			The call result return code.
MQMFT.call.crslt.rslt.stderr						x			The call result stderr output.
MQMFT.call.crslt.rslt.stdout						x			The call result stdout output.
MQMFT.call.crslt.rslt.time						x			The call result time.
MQMFT.call.crslt.retries						x			The call result retries.
MQMFT.call.cmd.argument						x			The call command arguments.
MQMFT.call.cmd.name						x			The call command name.
MQMFT.call.cmd.retryCount						x			The call command retry count.

Event Element	CD	CE	CX	SI	QF	MQ	FTP	SCC	Description
MQMFT.call.cmd.retryWait						x			The call command retry wait.
MQMFT.call.cmd.successRC						x			The call command successful return code.
MQMFT.call.cmd.type						x			The call command type.
MQMFT.destAgent.QMgr						x			The destination queue manager.
MQMFT.destAgent.agent						x			The destination agent.
MQMFT.destAgent.bridgeURL						x			The destination bridge URL.
MQMFT.destAgent.systemInfo.arch						x			The destination operating system arch.
MQMFT.destAgent.systemInfo.name						x			The destination operating system name.
MQMFT.destAgent.systemInfo.ver						x			The destination operating system version.
MQMFT.ID						x			The MQ MFT identifier for the transfer.
MQMFT.job.name						x			The job name (if provided), otherwise, "MQMFT_transfer".
MQMFT.metaData.metaData						x			User provided metadata.
MQMFT.originator.hostName						x			Hostname of the originator.
MQMFT.originator.mqmdUserID						x			The originator MQMD user ID.
MQMFT.originator.userID						x			The originator user ID.
MQMFT.postdestCall.crslt.oc						x			The postdest call outcome.
MQMFT.postdestCall.crslt.rslt.error						x			The postdest call result error.
MQMFT.postdestCall.crslt.rslt.oc						x			The postdest call result outcome.
MQMFT.postdestCall.crslt.rslt.rc						x			The postdest call result return code.
MQMFT.postdestCall.crslt.rslt.stderr						x			The postdest call result stderr.
MQMFT.postdestCall.crslt.rslt.stdout						x			The postdest call result stdout.
MQMFT.postdestCall.crslt.rslt.time						x			The postdest call result time.
MQMFT.postdestCall.crslt.retries						x			The postdest call result retries.
MQMFT.postdestCall.cmd.argument						x			The postdest command arguments.
MQMFT.postdestCall.cmd.name						x			The postdest command name.
MQMFT.postdestCall.cmd.retryCount						x			The postdest command retry count.

Event Element	CD	CE	CX	SI	QF	MQ	FTP	SCC	Description
MQMFT.postdestCall.cmd.retryWait						x			The postdest command retry wait.
MQMFT.postdestCall.cmd.successRC						x			The postdest command successful return.
MQMFT.postdestCall.cmd.type						x			The postdest command type.
MQMFT.postsrcCall.crslt.oc						x			The postsrc call outcome.
MQMFT.postsrcCall.crslt.rslt.error						x			The postsrc call error.
MQMFT.postsrcCall.crslt.rslt.oc						x			The postsrc call result outcome.
MQMFT.postsrcCall.crslt.rslt.rc						x			The postsrc call result return code.
MQMFT.postsrcCall.crslt.rslt.stderr						x			The postsrc call result stderr output.
MQMFT.postsrcCall.crslt.rslt.stdout						x			The postsrc call result stdout output.
MQMFT.postsrcCall.crslt.rslt.time						x			The postsrc call result time.
MQMFT.postsrcCall.crslt.retries						x			The postsrc call result retries.
MQMFT.postsrcCall.cmd.argument						x			The postsrc command arguments.
MQMFT.postsrcCall.cmd.name						x			The postsrc command name.
MQMFT.postsrcCall.cmd.retryCount						x			The postsrc command retry count.
MQMFT.postsrcCall.cmd.retryWait						x			The postsrc command retry wait.
MQMFT.postsrcCall.cmd.successRC						x			The postsrc command successful return.
MQMFT.postsrcCall.cmd.type						x			The postsrc command type.
MQMFT.predestCall.crslt.oc						x			The predest call outcome.
MQMFT.predestCall.crslt.rslt.error						x			The predest call result error.
MQMFT.predestCall.crslt.rslt.oc						x			The predest call result outcome.
MQMFT.predestCall.crslt.rslt.rc						x			The predest call result return code.
MQMFT.predestCall.crslt.rslt.stderr						x			The predest call result stderr output.
MQMFT.predestCall.crslt.rslt.stdout						x			The predest call result stdout output.
MQMFT.predestCall.crslt.rslt.time						x			The predest call result time.
MQMFT.predestCall.crslt.retries						x			The predest call result retries.
MQMFT.predestCall.cmd.name						x			The predest call command name.
MQMFT.predestCall.cmd.retryCount						x			The predest call result retry count.

Event Element	CD	CE	CX	SI	QF	MQ	FTP	SCC	Description
MQMFT.predestCall.cmd.retryWait						x			The predest call result retry wait.
MQMFT.predestCall.cmd.successRC						x			The predest call result successful return.
MQMFT.predestCall.cmd.type						x			The predest call command type.
MQMFT.presrcCall.crslt.oc						x			The presrc call outcome.
MQMFT.presrcCall.crslt.rslt.error						x			The presrc call result error.
MQMFT.presrcCall.crslt.rslt.oc						x			The presrc call result.
MQMFT.presrcCall.crslt.rslt.rc						x			The presrc call result return code.
MQMFT.presrcCall.crslt.rslt.stderr						x			The presrc call result stderr output.
MQMFT.presrcCall.crslt.rslt.stdout						x			The presrc call result stdout output.
MQMFT.presrcCall.crslt.rslt.time						x			The presrc call result time.
MQMFT.presrcCall.crslt.retries						x			The presrc call result retries.
MQMFT.presrcCall.cmd.argument						x			The presrc command arguments.
MQMFT.presrcCall.cmd.name						x			The presrc command name.
MQMFT.presrcCall.cmd.retryCount						x			The presrc command retry count.
MQMFT.presrcCall.cmd.retryWait						x			The presrc command retry wait.
MQMFT.presrcCall.cmd.successRC						x			The presrc command successful return.
MQMFT.presrcCall.cmd.type						x			The presrc command type.
MQMFT.srcAgent.QMgr						x			The source agent queue manager.
MQMFT.srcAgent.agent						x			The source agent name.
MQMFT.srcAgent.bridgeURL						x			The source agent bridge URL.
MQMFT.srcAgent.systemInfo.arch						x			The source agent operating system arch.
MQMFT.srcAgent.systemInfo.name						x			The source agent operating system name.
MQMFT.srcAgent.systemInfo.ver						x			The source agent version.
MQMFT.statistics.actualStartTime						x			Statistics actual start time.
MQMFT.statistics.numFileFailures						x			Statistics number of file failures.
MQMFT.statistics.numFileWarnings						x			Statistics number of file warnings.
MQMFT.statistics.retryCount						x			Statistics retry count.
MQMFT.status.rsltCode						x			The result code.
MQMFT.status.supplement						x			MQ MFT message.
MQMFT.ts.item.dest.cs						x			The destination checksum.

Event Element	CD	CE	CX	SI	QF	MQ	FTP	SCC	Description
MQMFT.ts.item.dest.cs.meth						x			The destination checksum method.
MQMFT.ts.item.dest.exist						x			The destination exists.
MQMFT.ts.item.dest.lmod						x			The destination last modification.
MQMFT.ts.item.dest.queue.groupId						x			The destination queue group ID.
MQMFT.ts.item.dest.queue.msgCount						x			The destination queue message.
MQMFT.ts.item.dest.queue.msgId						x			The destination queue message ID.
MQMFT.ts.item.dest.queue.msgLength						x			The destination queue message.
MQMFT.ts.item.dest.size						x			The destination file size.
MQMFT.ts.item.mode						x			The transfer mode.
MQMFT.ts.item.src.cs						x			The source checksum.
MQMFT.ts.item.src.cs.meth						x			The source checksum method.
MQMFT.ts.item.src.disp						x			The source disposition.
MQMFT.ts.item.src.lmod						x			The source last modified date/time.
MQMFT.ts.item.src.queue.groupId						x			The source queue group ID.
MQMFT.ts.item.src.queue.msgCount						x			The source queue message count.
MQMFT.ts.item.src.queue.msgId						x			The source queue message ID.
MQMFT.ts.item.src.queue.msgLength						x			The source queue message length.
MQMFT.ts.item.src.size						x			The source file size.
MQMFT.ts.item.status.rsltCode						x			The transfer result code.
MQMFT.ts.item.status.supplement						x			The transfer message.
MQMFT.ts.startTime						x			The transfer start time.
nodeId	x	x	x	x	x		x		The server alias.
nodeName	x		x	x	x	x	x		The actual name of the server. For QuickFile, comes from QF.serverName.

Event Element	CD	CE	CX	SI	QF	MQ	FTP	SCC	Description
nodeType	x	x	x	x	x	x	x	x	The code indicating the type of server. The server types are: • 0 = Sterling Control Center • 1 = Sterling Connect:Direct • 2 = Sterling Connect:Enterprise • 3 = Sterling B2B Integrator • 4 = FTP • 5 = Sterling Connect:Express • 6 = QuickFile • 7 = MQ MFT
nodeTypeDescr	x	x	x	x	x	x	x	x	A description of the server type
nonExecutingProcs	x			x					Number of nonexecuting Processes
objectId								x	ID of object associated with the event
objectType								x	Type of object associated with the event
objectVersion								x	Version of object associated with the event
OCCD	x								Other Return Code
oid		x							Object Identifier
OMSG	x								Other Message ID
origNode	x		x	x	x	x			The originating node of a process. QuickFile, comes from QF.serverName.
PACC	x								Pnode Accounting Information
PCSI	x								Pnode Signature
PEAL	x								Pnode Encryption Algorithm List
percentComplete	x					x		x	The percent complete of the file copy or transfer.
PPEA	x								Pnode Encryption Data
PPLX	x								Pnode Plex Class
processData				x					Sterling B2B Integrator process data
processId	x	x	x	x	x		x		The Process ID or batch number. QuickFile, comes from QF.packageId.

Event Element	CD	CE	CX	SI	QF	MQ	FTP	SCC	Description
processIds	x			x					A list of Process IDs or batch numbers in a Process Queue event.
processName	x	x	x	x	x		x		The Process name or batch ID.
processNames								x	A list of Process names or batch IDs in a Process Queue event.
processQueue	x		x	x	x	x			The queue containing the Process.
processQueues								x	A list of queues in a Process Queue event.
protocol		x							Protocol
PRTY	x								Priority
PSIN	x								Previous Signature Verified
QF.eventType					x				Type of QuickFile event
QF.file					x				Name of file
QF.operation					x				Event operation
QF.recipient.userEmail					x				Recipient user email address
QF.recipient.userFullname					x				Recipient user full name
QF.recipient.userId					x				Recipient user ID
QF.userEmail					x				User email address
QF.userRegistered					x				Boolean indicator as to whether QuickFile user is registered or not. Values are true | false.
QUEU	x								Queue
RCCT	x								Record Category
recCat	x	x							Record Category
recipientMailboxId		x							Recipient Mailbox ID
recordId	x	x							The type of statistics record from the event. For a list of record IDs, see *Event type descriptions*.
relativeSelectStmt		x							Relative Select Statement
remoteName		x							Remote Name
remoteNode	x	x	x	x		x	x		Name of the remote server involved in a process or file transfer.
remoteNodes	x			x					A list of remote servers in a Process Queue event.
RETN	x								Retain

Event Element	CD	CE	CX	SI	QF	MQ	FTP	SCC	Description
returnCode	x	x	x	x	x	x	x	x	A numeric code returned from a completed process that indicates failure or success. For QuickFile, based on last letter of the messageId. If the last letter is l, the return code is 0; otherwise, it is 8.
RSTR	x								Restart
ruleId	x	x	x	x	x	x	x	x	The name of the rule triggered by the event.
ruleInstanceId	x	x	x	x	x	x	x	x	Rules Instance ID used when there is a linked rule
ruleMemberName		x							Rule Member Name
ruleName		x							Sterling Connect:Enterprise for z/OS Rule Name
RUSZ	x								RU Size
SACC	x								Snode Accounting Information
SBND	x								Submit Node
SCHD	x								Scheduled Date/Time
SCMP	x								Standard Compression
SCSI	x								Snode Signature
SDS1	x								Source Disposition 1
SDS2	x								Source Disposition 2
SDS3	x								Source Disposition 3
SEAL	x								Snode Encryption Algorithm List
seqNum	x	x	x	x	x	x	x	x	Sequence
session				x					Sterling B2B Integrator Session
SESSION.ADAPTER_ NAME				x					Sterling B2B Integrator system adapter name.
SESSION.ADAPTER_ TYPE				x					Sterling B2B Integrator adapter type.
SESSION.CHILD_ SESSIONID				x					Sterling B2B Integrator Session child session ID
SESSION.CON_END_ TIME				x					Sterling B2B Integrator Session connection end time.
SESSION.CON_IS_ SUCCESS				x					Sterling B2B Integrator Session connection successful.
SESSION.CON_START_ TIME				x					Sterling B2B Integrator Session connection start time.
SESSION.DIS_END_TIME				x					Sterling B2B Integrator Session disconnect end time.

Event Element	CD	CE	CX	SI	QF	MQ	FTP	SCC	Description
SESSION.DIS_IS_ SUCCESS				x					Sterling B2B Integrator Session disconnect is success.
SESSION.DIS_START_ TIME				x					Sterling B2B Integrator Session disconnect start time.
SESSION.END_WFID				x					Sterling B2B Integrator Session end workflow ID.
SESSION.END_WFSTEP				x					Sterling B2B Integrator Session end workflow step.
SESSION.ENDPOINT1				x					Sterling B2B Integrator Session end point 1.
SESSION.ENDPOINT2				x					Sterling B2B Integrator Session end point 2.
SESSION.ENDPORT1				x					Sterling B2B Integrator Session end port 1.
SESSION.ENDPORT2				x					Sterling B2B Integrator Session end port 2.
SESSION.ERROR_MSG				x					Sterling B2B Integrator Session error message.
SESSION.IS_LOCAL_INIT				x					Sterling B2B Integrator Session is local init.
SESSION.PRINCIPAL				x					Sterling B2B Integrator Protocol Activity Session principal.
SESSION.PROTOCOL				x					Sterling B2B Integrator protocol of file movement.
SESSION.PS_INSTANCE				x					Sterling B2B Integrator Protocol Activity Session PS instance.
SESSION.SECURE_MODE				x					Sterling B2B Integrator Protocol Activity Session secure mode.
SESSION.SESSION_ ARCHIVE_ID				x					Sterling B2B Integrator Protocol Activity Session archive ID.
SESSION.SESSION_ID				x					Sterling B2B Integrator Protocol Activity Session ID.
SESSION.START_WFID				x					Sterling B2B Integrator Protocol Activity Session start workflow ID.
SESSION.START_WFSTEP				x					Sterling B2B Integrator Protocol Activity Session start workflow step.
SESSION.STATUS_CODE				x					Sterling B2B Integrator Protocol Activity Session status code.
shortText	x	x	x	x	x	x	x	x	Message text associated with the Message ID.

Event Element	CD	CE	CX	SI	QF	MQ	FTP	SCC	Description
SI.MESSAGE_ID				x					Sterling B2B Integrator/Sterling File Gateway message ID
slcId								x	A system-assigned name of the SLC that triggered the event.
slcInstanceId								x	Unique SLC identifier. Includes the SLC name, schedule name, and unique number.
slcSource1								x	SLC recovery data 1.
slcSource2								x	SLC recovery data 2.
SMEM	x								Source Member Name
SOPT	x								Sysopts
sourceEventTime								x	The time that the event triggering an SLC event occurred.
sourceFile	x	x	x	x	x		x		The source file name in a Copy. Also the target in a Submit, Run Task, or Run Job Sterling Connect:Direct Process step. For QuickFile, QF.File when file is uploaded and QF.package when file is downloaded.
SPEA	x								Snode Encryption Data
SPLX	x								Snode Plex Class
SRCR	x								Records Read
SRUX	x								RUs Sent
SRVR	x								Server Name
STAT	x								Status
status	x	x							Status
stepName	x			x					The name of the Sterling Connect:Direct Process step or Sterling B2B Integrator business Process activity.
STPT	x								Stop Date/Time
STRT	x								Start Date/Time
SUBI	x								Submitter Node
submitter	x	x		x			x		User ID of the Process submitter.
submitterId	x	x	x	x	x	x	x	x	The user ID of the work submitter. For QuickFile, user fullname.
submitterIds	x			x					A list of Submitter IDs in a Process Queue event.
suspended	x								Indicates if a Process is suspended.

Event Element	CD	CE	CX	SI	QF	MQ	FTP	SCC	Description
TDSB	x								Submit Date/Time
timeUp		x							Time Up
triggerMilestoneId								x	Name of milestone that triggered the jeopardy SLC event.
url		x							URL
userData1	x	x	x	x	x	x	x	x	Metadata user data field 1.
userData2	x	x	x	x	x	x	x	x	Metadata user data field 2.
userData3	x	x	x	x	x	x	x	x	Metadata user data field 3.
userData4	x	x	x	x	x	x	x	x	Metadata user data field 4.
userId								x	User associated with the event.
WF.ACTIVITYINFO_ID				x					Business Process Activity Info ID.
WF.ADV_STATUS				x					Business Process advanced status.
WF.BASIC_STATUS				x					Business Process basic status.
WF.END_TIME				x					Business Process end time.
WF.NEXT_AI_ID				x					Business Process next AI ID.
WF.NODEEXECUTED				x					Node where Business Process executed.
WF.SERVICE_NAME				x					Service name in Business Process.
WF.START_TIME				x					Business Process / Business Process Step start time
WF.STEP_ID				x					Business Process step ID.
WF.WFD_ID				x					Business Process Definition ID.
WF.WFD_NAME				x					Business Process name.
WF.WFD_VERSION				x					Business Process Definition version.
WF.WFE_STATUS				x					Business Process execution status
WF.WORKFLOW_ID				x					Business Process instance ID
WFD_NAME				x					Business Process name
wkFlow		x							Workflow
XFER.DOC_ID				x					Sterling B2B Integrator Protocol Activity Transfer document ID
XFER.DOC_NAME				x					Sterling B2B Integrator Protocol Activity document name.
XFER.END_TIME				x					Sterling B2B Integrator Protocol Activity Transfer end time.

Event Element	CD	CE	CX	SI	QF	MQ	FTP	SCC	Description
XFER.FILE_SIZE				x					Sterling B2B Integrator Protocol Activity Transfer file size.
XFER.IS_BIN_XFER				x					Sterling B2B Integrator Protocol Activity Transfer is binary
XFER.IS_PUT				x					Sterling B2B Integrator Protocol Activity Transfer is put.
XFER.IS_SECURE				x					Sterling B2B Integrator Protocol Activity Transfer is secure.
XFER.IS_SUCCESS				x					Sterling B2B Integrator Protocol Activity Transfer is success.
XFER.KBYTES_XFER				x					Sterling B2B Integrator Protocol Activity KBytes transferred
XFER.MAILBOX_PATH				x					Sterling B2B Integrator Protocol Activity/Sterling File Gateway Arrived File Mailbox Path
XFER.MBOX_PATH				x					Sterling B2B Integrator Protocol Activity SI mailbox path.
XFER.MESSAGE_ID				x					Sterling B2B Integrator Protocol Activity Transfer message ID
XFER.MESSAGE_NAME				x					Sterling B2B Integrator Protocol Activity message name
XFER.REMOTE_ FILENAME				x					Sterling B2B Integrator Protocol Activity Transfer remote filename
XFER.START_TIME				x					Sterling B2B Integrator Protocol Activity Transfer start time
XFER.WFID				x					Sterling B2B Integrator Protocol Activity Transfer work ID.
XFER.WFSTEP				x					Sterling B2B Integrator Protocol Activity Transfer workflow step
XFER.XFER_ERROR_MSG				x					Sterling B2B Integrator Protocol Activity Transfer error message.
XFER.XFER_ID				x					Sterling B2B Integrator Protocol Activity Transfer ID.
XFER.XFER_STATUS_ CODE				x					Sterling B2B Integrator Protocol Activity Transfer status code.

Event Element	CD	CE	CX	SI	QF	MQ	FTP	SCC	Description
XLAT	x								Translate

Variables by event type

This table shows a breakdown of event elements available for use as variables by the event types they may occur in.

Note: Because the Server Shutdown Started and Server Shutdown event types (numbers 7 and 8) are not currently used, they are omitted from the table.

Event Type	1	2	3	4	5	6	9	10	11	12	13	14	15	16	17
Variable	Process Step Started	Process Step Ended	Proc Started	Proc Ended	Server Status	SLC	Proc Status	Server License	Server Error	Server Cmd	Connection Started	Connection Shutdown Started	Control Center Status	Proc Queued	Process Interrupted
action						x				x					
actionId	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
activityType						x									
alert	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
applAgentType	x	x	x	x											
batchId	x	x	x	x											
batchNumber	x	x	x	x											
bytesRead		x													
bytesSent		x													
bytesXferred							x								
CBEA		x									x				
CERI		x									x				
CERT		x									x				
CKPT		x													
CLAS										x					
CNOD		x													
controlCenterName	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
CPUS		x		x											
CSPE		x									x				
CSPP		x									x				
CSPS		x									x				
CSTN							x			x					
CX.EVT	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

Event Type	1	2	3	4	5	6	9	10	11	12	13	14	15	16	17
Variable	Process Step Started	Process Step Ended	Proc Started	Proc Ended	Server Status	SLC	Proc Status	Server License	Server Error	Server Cmd	Connection Started	Connection Shutdown Started	Control Center Status	Proc Queued	Process Interrupted
CX.FBYT		x		x							x				
CX.FLAB			x												
CX.FNRD		x		x							x				
CX.LNAM			x								x		x	x	
CX.LPHN			x								x				
CX.NBYT		x		x							x				
CX.NRC		x		x							x				
CX.OS	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
CX.PNAM			x										x	x	
CX.PRC		x		x							x	x			
CX.PROT			x										x		
CX.SRC		x		x							x	x			
CX.TBDA	x														
CX.TDIR			x	x											
CX.TDST			x												
CX.TEDA		x		x											
CX.TIDT			x												
CX.TOM	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
CX.TORG			x												
CX.TRC		x		x							x	x			
CX.TRCV			x									x			
CX.TSND			x									x			
CX.TYPL			x										x		
CX.TYPR			x												
CX.TYPU			x								x		x		
CX.USDR			x												
CX.USDS			x												
daemonHost					x										
daemonName					x										
daemonOriginator					x										
daemonPid					x										
daemonResource					x										

Event Type	1	2	3	4	5	6	9	10	11	12	13	14	15	16	17
Variable	Process Step Started	Process Step Ended	Proc Started	Proc Ended	Server Status	SLC	Proc Status	Server License	Server Error	Server Cmd	Connection Started	Connection Shutdown Started	Control Center Status	Proc Queued	Process Interrupted
daemonSid					x										
daemonState					x										
daemonType					x										
dateTime	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
daysBeforeExpiry					x										
DBUG			x												
DBYW		x													
DBYX		x													
DDS1		x													
DDS2		x													
DDS3		x													
destFile	x	x	x	x		x	x			x	x	x			
direction	x	x													
DRCW		x													
DRUX		x													
ECMP		x													
EPRT										x					
eventId	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
eventType	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
eventTypeDescr	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
executingProcs														x	
FDBK	x	x	x	x											x
FG.CONS_ORG_KEY	x	x	x	x			x								
FG.DATA_FLOW_ID	x	x	x	x			x								
FG.EVENT_CODE	x	x	x	x			x								
FG.FILE_NAME	x	x	x	x			x								
FG.PROD_ORG_KEY	x	x	x	x			x								
FG.STATE	x	x	x	x			x								
fgActivityType	x	x	x	x			x								
fileSize		x													
fromNode	x	x													
FUNC							x								

Event Type	1	2	3	4	5	6	9	10	11	12	13	14	15	16	17
Variable	Process Step Started	Process Step Ended	Proc Started	Proc Ended	Server Status	SLC	Proc Status	Server License	Server Error	Server Cmd	Connection Started	Connection Shutdown Started	Control Center Status	Proc Queued	Process Interrupted
groupId						x									
HOLD										x					
inError	x	x	x	x											
isBP	x	x	x	x							x	x		x	
jobId										x					
jobName	x	x	x	x											
LCCD		x													
lineName	x	x	x	x											
listName	x	x	x	x											
LKFL	x	x	x	x											
LMSG		x													
LNOD		x													
localNode	x	x	x	x			x								
mailboxFlags	x	x	x	x											
mailBoxId	x	x	x	x											
maxExecutingProcs														x	
MCSI											x				
MEMA		x													
MEMB	x	x			x										
mepLastOccurrence														x	
mepOccurrences														x	x
messageId	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
milestoneId						x									
MQMFT.action	x	x	x	x											
MQMFT.action.time	x	x	x	x											
MQMFT.call.crslt.oc		x													
MQMFT.call.crslt.rslt.error		x													
MQMFT.call.crslt.rslt.oc		x													
MQMFT.call.crslt.rslt.rc		x													
MQMFT.call.crslt.rslt.stderr		x													
MQMFT.call.crslt.rslt.stdout		x													
MQMFT.call.crslt.rslt.time		x													

Event Type	1	2	3	4	5	6	9	10	11	12	13	14	15	16	17
Variable	Process Step Started	Process Step Ended	Proc Started	Proc Ended	Server Status	SLC	Proc Status	Server License	Server Error	Server Cmd	Connection Started	Connection Shutdown Started	Control Center Status	Proc Queued	Process Interrupted
MQMFT.call.crslt.retries		x													
MQMFT.call.cmd.argument	x	x													
MQMFT.call.cmd.name	x	x													
MQMFT.call.cmd.retryCount	x	x													
MQMFT.call.cmd.retryWait	x	x													
MQMFT.call.cmd.successRC	x	x													
MQMFT.call.cmd.type	x	x													
MQMFT.destAgent.QMgr	x	x	x	x	x										
MQMFT.destAgent.agent	x	x	x	x	x										
MQMFT.destAgent.bridgeURL	x	x	x	x	x										
MQMFT.destAgent.systemInfo.arch	x	x	x	x	x										
MQMFT.destAgent.systemInfo.name	x	x	x	x	x										
MQMFT.destAgent.systemInfo.ver	x	x	x	x	x										
MQMFT.ID	x	x	x	x	x										
MQMFT.job.name	x	x	x	x	x										
MQMFT.metaData.metaData	x	x	x	x	x										
MQMFT.originator.hostName	x	x	x	x	x										
MQMFT.originator.mqmdUserID	x	x	x	x	x										
MQMFT.originator.userID	x	x	x	x	x										
MQMFT.postdestCall.crslt.oc		x													
MQMFT.postdestCall.crslt.rslt.error		x													
MQMFT.postdestCall.crslt.rslt.oc		x													
MQMFT.postdestCall.crslt.rslt.rc		x													
MQMFT.postdestCall.crslt.rslt.stderr		x													
MQMFT.postdestCall.crslt.rslt.stdout		x													
MQMFT.postdestCall.crslt.rslt.time		x													
MQMFT.postdestCall.crslt.retries		x													
MQMFT.postdestCall.cmd.argument	x	x													
MQMFT.postdestCall.cmd.name	x	x													
MQMFT.postdestCall.cmd.retryCount	x	x													
MQMFT.postdestCall.cmd.retryWait	x	x													
MQMFT.postdestCall.cmd.successRC	x	x													

Event Type	1	2	3	4	5	6	9	10	11	12	13	14	15	16	17
Variable	Process Step Started	Process Step Ended	Proc Started	Proc Ended	Server Status	SLC	Proc Status	Server License	Server Error	Server Cmd	Connection Started	Connection Shutdown Started	Control Center Status	Proc Queued	Process Interrupted
MQMFT.postdestCall.cmd.type	x	x													
MQMFT.postsrcCall.crslt.oc		x													
MQMFT.postsrcCall.crslt.rslt.error		x													
MQMFT.postsrcCall.crslt.rslt.oc		x													
MQMFT.postsrcCall.crslt.rslt.rc		x													
MQMFT.postsrcCall.crslt.rslt.stderr		x													
MQMFT.postsrcCall.crslt.rslt.stdout		x													
MQMFT.postsrcCall.crslt.rslt.time		x													
MQMFT.postsrcCall.crslt.retries		x													
MQMFT.postsrcCall.cmd.argument	x	x													
MQMFT.postsrcCall.cmd.name	x	x													
MQMFT.postsrcCall.cmd.retryCount	x	x													
MQMFT.postsrcCall.cmd.retryWait	x	x													
MQMFT.postsrcCall.cmd.successRC	x	x													
MQMFT.postsrcCall.cmd.type	x	x													
MQMFT.predestCall.crslt.oc		x													
MQMFT.predestCall.crslt.rslt.error		x													
MQMFT.predestCall.crslt.rslt.oc		x													
MQMFT.predestCall.crslt.rslt.rc		x													
MQMFT.predestCall.crslt.rslt.stderr		x													
MQMFT.predestCall.crslt.rslt.stdout		x													
MQMFT.predestCall.crslt.rslt.time		x													
MQMFT.predestCall.crslt.retries		x													
MQMFT.predestCall.cmd.name	x	x													
MQMFT.predestCall.cmd.retryCount	x	x													
MQMFT.predestCall.cmd.retryWait	x	x													
MQMFT.predestCall.cmd.successRC	x	x													
MQMFT.predestCall.cmd.type	x	x													
MQMFT.presrcCall.crslt.oc	x	x													
MQMFT.presrcCall.crslt.rslt.error		x													
MQMFT.presrcCall.crslt.rslt.oc		x													
MQMFT.presrcCall.crslt.rslt.rc		x													

Event Type	1	2	3	4	5	6	9	10	11	12	13	14	15	16	17
Variable	Process Step Started	Process Step Ended	Proc Started	Proc Ended	Server Status	SLC	Proc Status	Server License	Server Error	Server Cmd	Connection Started	Connection Shutdown Started	Control Center Status	Proc Queued	Process Interrupted
MQMFT.presrcCall.crslt.rslt.stderr		x													
MQMFT.presrcCall.crslt.rslt.stdout		x													
MQMFT.presrcCall.crslt.rslt.time		x													
MQMFT.presrcCall.crslt.retries		x													
MQMFT.presrcCall.cmd.argument	x	x													
MQMFT.presrcCall.cmd.name	x	x													
MQMFT.presrcCall.cmd.retryCount	x	x													
MQMFT.presrcCall.cmd.retryWait	x	x													
MQMFT.presrcCall.cmd.successRC	x	x													
MQMFT.presrcCall.cmd.type	x	x													
MQMFT.srcAgent.QMgr	x	x	x	x											
MQMFT.srcAgent.agent	x	x	x	x											
MQMFT.srcAgent.bridgeURL	x	x	x	x											
MQMFT.srcAgent.systemInfo.arch	x	x	x	x											
MQMFT.srcAgent.systemInfo.name	x	x	x	x											
MQMFT.srcAgent.systemInfo.ver	x	x	x	x											
MQMFT.statistics.actualStartTime			x	x											
MQMFT.statistics.numFileFailures			x	x											
MQMFT.statistics.numFileWarnings			x	x											
MQMFT.statistics.retryCount			x	x											
MQMFT.status.rsltCode		x													
MQMFT.status.supplement		x													
MQMFT.ts.item.dest.cs	x	x													
MQMFT.ts.item.dest.cs.meth	x	x													
MQMFT.ts.item.dest.exist	x	x													
MQMFT.ts.item.dest.lmod	x	x													
MQMFT.ts.item.dest.queue.groupId	x	x													
MQMFT.ts.item.dest.queue.msgCount		x													
MQMFT.ts.item.dest.queue.msgId		x													
MQMFT.ts.item.dest.queue.msgLength		x													
MQMFT.ts.item.dest.size		x													
MQMFT.ts.item.mode	x	x													

Event Type	1	2	3	4	5	6	9	10	11	12	13	14	15	16	17
Variable	Process Step Started	Process Step Ended	Proc Started	Proc Ended	Server Status	SLC	Proc Status	Server License	Server Error	Server Cmd	Connection Started	Connection Shutdown Started	Control Center Status	Proc Queued	Process Interrupted
MQMFT.ts.item.src.cs	x	x													
MQMFT.ts.item.src.cs.meth	x	x													
MQMFT.ts.item.src.disp	x	x													
MQMFT.ts.item.src.lmod	x	x													
MQMFT.ts.item.src.queue.groupId	x	x													
MQMFT.ts.item.src.queue.msgCount		x													
MQMFT.ts.item.src.queue.msgId		x													
MQMFT.ts.item.src.queue.msgLength		x													
MQMFT.ts.item.src.size	x	x													
MQMFT.ts.item.status.rsltCode	x	x													
MQMFT.ts.item.status.supplement	x	x													
MQMFT.ts.startTime	x	x													
nodeId	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
nodeName	x	x	x	x			x	x	x	x	x	x		x	x
nodeType	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
nodeTypeDescr	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
nonExecutingProcs														x	
objectId					x	x				x					
objectType					x	x				x			x		
objectVersion					x										
OCCD		x													
oid	x	x	x	x											
OMSG		x													
origNode	x	x	x	x			x								x
PACC		x													
PCSI		x									x				
PEAL		x									x				
percentComplete						x	x								
PPEA		x									x				
PPLX		x													
processData	x	x	x	x											
processId	x	x	x	x	x	x	x	x	x	x	x	x			

Event Type	1	2	3	4	5	6	9	10	11	12	13	14	15	16	17
Variable	Process Step Started	Process Step Ended	Proc Started	Proc Ended	Server Status	SLC	Proc Status	Server License	Server Error	Server Cmd	Connection Started	Connection Shutdown Started	Control Center Status	Proc Queued	Process Interrupted
processIds														x	
processName	x	x	x	x		x	x				x	x			
processNames														x	
processQueue						x	x								
processQueues														x	
protocol	x	x	x	x											
PRTY										x					
PSIN		x													
QF.eventType	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
QF.file		x	x		x										
QF.operation	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
QF.recipient.userEmail	x	x													
QF.recipient.userFullname	x	x													
QF.recipient.userId	x	x													
QF.userEmail	x	x	x	x	x										
QF.userRegistered	x	x	x	x	x										
QUEU				x			x								
RCCT	x	x	x	x						x	x	x			
recCat	x	x	x	x				x	x	x	x	x			x
recipientMailboxId	x	x	x	x											
recordId	x	x	x	x				x	x	x	x	x			x
relativeSelectStmt	x	x	x	x											
remoteName	x	x	x	x											
remoteNode	x	x	x	x		x	x			x	x	x			x
remoteNodes														x	
RETN							x			x					
returnCode	x	x	x	x		x		x	x	x	x	x			x
RSTR		x													
ruleId	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
ruleInstanceId	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
ruleMemberName	x	x	x	x											
ruleName	x	x	x	x											

Event Type	1	2	3	4	5	6	9	10	11	12	13	14	15	16	17
Variable	Process Step Started	Process Step Ended	Proc Started	Proc Ended	Server Status	SLC	Proc Status	Server License	Server Error	Server Cmd	Connection Started	Connection Shutdown Started	Control Center Status	Proc Queued	Process Interrupted
RUSZ		x													
SACC		x													
SBND	x	x	x	x						x	x				
SCHD			x	x											
SCMP		x													
SCSI		x									x				
SDS1		x													
SDS2		x													
SDS3		x													
SEAL		x									x				
seqNum	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
session	x	x	x	x											
SESSION.ADAPTER_NAME	x	x			x						x	x			
SESSION.ADAPTER_TYPE	x	x			x						x	x			
SESSION.CHILD_SESSIONID	x	x									x	x			
SESSION.CON_END_TIME	x	x									x	x			
SESSION.CON_IS_SUCCESS	x	x									x	x			
SESSION.CON_START_TIME	x	x									x	x			
SESSION.DIS_END_TIME	x	x									x	x			
SESSION.DIS_IS_SUCCESS	x	x									x	x			
SESSION.DIS_START_TIME	x	x									x	x			
SESSION.END_WFID	x	x									x	x			
SESSION.END_WFSTEP	x	x									x	x			
SESSION.ENDPOINT1	x	x									x	x			
SESSION.ENDPOINT2	x	x									x	x			
SESSION.ENDPORT1	x	x									x	x			
SESSION.ENDPORT2	x	x									x	x			
SESSION.ERROR_MSG	x	x									x	x			
SESSION.IS_LOCAL_INIT	x	x									x	x			
SESSION.PRINCIPAL	x	x									x	x			
SESSION.PROTOCOL	x	x									x	x			
SESSION.PS_INSTANCE	x	x									x	x			

Event Type	1	2	3	4	5	6	9	10	11	12	13	14	15	16	17
Variable	Process Step Started	Process Step Ended	Proc Started	Proc Ended	Server Status	SLC	Proc Status	Server License	Server Error	Server Cmd	Connection Started	Connection Shutdown Started	Control Center Status	Proc Queued	Process Interrupted
SESSION.SECURE_MODE	x	x									x	x			
SESSION.SESSION_ARCHIVE_ID	x	x									x	x			
SESSION.SESSION_ID	x	x									x	x			
SESSION.START_WFID	x	x									x	x			
SESSION.START_WFSTEP	x	x									x	x			
SESSION.STATUS_CODE	x	x									x	x			
shortText	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
SI.MESSAGE_ID	x	x	x	x											
slcId						x									
slcInstanceId						x									
slcSource1						x									
slcSource2						x									
SMEM		x													
SOPT		x													
sourceEventTime						x									
sourceFile	x	x	x	x			x								
SPEA		x													
SPLX		x													
SRCR		x													
SRUX		x													
SRVR	x	x	x		x		x			x	x				
STAT							x			x					
status	x	x	x	x								x	x		x
stepName	x	x	x	x			x								x
STPT		x	x	x											
STRT	x	x	x	x	x					x	x				
SUBI	x	x	x	x						x	x				
submitter						x									x
submitterId	x	x	x	x		x	x			x	x	x			x
submitterIds														x	
suspended				x											
TDSB			x	x											

Event Type	1	2	3	4	5	6	9	10	11	12	13	14	15	16	17
Variable	Process Step Started	Process Step Ended	Proc Started	Proc Ended	Server Status	SLC	Proc Status	Server License	Server Error	Server Cmd	Connection Started	Connection Shutdown Started	Control Center Status	Proc Queued	Process Interrupted
timeUp	x	x	x	x											
triggerMilestoneId						x									
url	x	x	x	x											
userData1	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
userData2	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
userData3	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
userData4	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
userId					x					x					
WF.ACTIVITYINFO_ID	x	x	x	x											
WF.ADV_STATUS	x	x	x	x											
WF.BASIC_STATUS	x	x	x	x											
WF.END_TIME	x	x	x	x											
WF.NEXT_AI_ID	x	x	x	x											
WF.NODEEXECUTED	x	x	x	x											
WF.SERVICE_NAME	x	x	x	x											
WF.START_TIME	x	x	x	x											
WF.STEP_ID	x	x	x	x											
WF.WFD_ID	x	x	x	x											
WF.WFD_NAME	x	x	x	x											
WF.WFD_VERSION	x	x	x	x											
WF.WFE_STATUS	x	x	x	x											
WF.WORKFLOW_ID	x	x	x	x											
WFD_NAME	x	x	x	x											
wkFlow	x	x	x	x											
XFER.DOC_ID	x	x													
XFER.DOC_NAME	x	x													
XFER.END_TIME	x	x													
XFER.FILE_SIZE	x	x													
XFER.IS_BIN_XFER	x	x													
XFER.IS_PUT	x	x													
XFER.IS_SECURE	x	x													
XFER.IS_SUCCESS	x	x													

Event Type	1	2	3	4	5	6	9	10	11	12	13	14	15	16	17
Variable	Process Step Started	Process Step Ended	Proc Started	Proc Ended	Server Status	SLC	Proc Status	Server License	Server Error	Server Cmd	Connection Started	Connection Shutdown Started	Control Center Status	Proc Queued	Process Interrupted
XFER.KBYTES_XFER	x	x													
XFER.MAILBOX_PATH	x	x	x	x			x								
XFER.MBOX_PATH	x	x													
XFER.MESSAGE_ID	x	x													
XFER.MESSAGE_NAME	x	x													
XFER.REMOTE_FILENAME	x	x													
XFER.START_TIME	x	x													
XFER.WFID	x	x													
XFER.WFSTEP	x	x													
XFER.XFER_ERROR_MSG	x	x													
XFER.XFER_ID	x	x													
XFER.XFER_STATUS_CODE	x	x													
XLAT		x													

Chapter 22. Modify log4j to retain log fies

Sterling Control Center uses CCEngine.log4j to configure the engine logs and CCClient.log4j file for the console logs. You can modify these two properties files to change how the log files are rolled over and then rolled off. After the log file settings are configured, you could create a backup/archival process, either manual or through some separate process outside of Sterling Control Center. If the content of a log file is empty, the log file will not be rolled over.

This documentation contains samples of the CCEngine.log4j and CClient.log4j properties files, which when used as-is will cause log files to roll over every 12 hours (midday and midnight) without ever rolling off or being limited by size.The last section provides some notes about the types of parameters changed within the sample files.

The file format of the log files ends with either –am or –pm, for example, CCEngine_20081105_140306184.log.2008-11-06-AM. This filename format enables you to easily identify and move or copy all logfiles for a given time period, such as 90 days.

To use a sample configuration file, you must replace the existing log4j file contents with the content of the sample configuration file.

Each time, you upgrade to a new version of Sterling Control Center or install a maintenance release, you must replace the contents of the log4j file to keep the settings you want.

For more information on the latest parameters changed in the sample files, see *Parameters modified in the sample log4j files*.

Sample CCEngine.log4j file

The sample log4j file for the ccengine log causes log files to roll over every 12 hours, that is, creates a new log file every 12 hours, and does not roll off any log files.

```
#
# CCEngine Log4j Properties
#
log4j.appender.stdout=org.apache.log4j.ConsoleAppender
log4j.appender.stdout.layout.ConversionPattern=%d{dd MMM yyyy HH:mm:ss,SSS} %r
[%t] %-5p %c{1} - %m%n
log4j.appender.stdout.layout=org.apache.log4j.PatternLayout
log4j.logger.com.sterlingcommerce.scc=INHERITED
log4j.logger.org.apache.commons.beanutils=OFF
log4j.appender.R.File=${CONFIG_DIR}/../log/CCEngine_${current.time}.log
log4j.appender.R.DatePattern='.'yyyy-MM-dd-a
log4j.appender.R.layout=org.apache.log4j.PatternLayout
log4j.appender.R.layout.ConversionPattern=%d{dd MMM yyyy HH:mm:ss,SSS} %r [%t]
%-5p %c{1} - %m%n
log4j.appender.R=org.apache.log4j.DailyRollingFileAppender
log4j.loggerFactory=com.sterlingcommerce.component.common.logging.log4j.LogFactory
log4j.renderer.java.lang.Throwable=com.sterlingcommerce.component.common.logging.
.log4jExceptionRenderer
log4j.rootLogger=INFO, R
log4j.category.RuleSession=INHERITED
log4j.category.RuleSession=, RuleSessionAppender
```

```
log4j.additivity.RuleSession=false
log4j.appender.RuleSessionAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.RuleSessionAppender.File=../log/RuleSession_${current.time}.log
log4j.appender.RuleSessionAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.RuleSessionAppender.layout=org.apache.log4j.PatternLayout
log4j.additivity.RuleSessionAppender=false
log4j.appender.RuleSessionAppender.layout.ConversionPattern=%d{dd MMM yyyy
HH:mm:ss,SSS} %r [%t] %-5p %c{1} - %m%n
log4j.category.RuleSession=INHERITED
log4j.category.RuleSession=, RuleSessionAppender
log4j.additivity.RuleSession=false
log4j.appender.RuleSessionAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.RuleSessionAppender.File=../log/RuleSession_${current.time}.log
log4j.appender.RuleSessionAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.RuleSessionAppender.layout=org.apache.log4j.PatternLayout
log4j.additivity.RuleSessionAppender=false
log4j.appender.RuleSessionAppender.layout.ConversionPattern=%d{dd MMM yyyy
HH:mm:ss,SSS} %r [%t] %-5p %c{1} - %m%n
log4j.category.PurgeService=INHERITED
log4j.category.PurgeService=, PurgeServiceAppender
log4j.additivity.PurgeService=false
log4j.appender.PurgeServiceAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.PurgeServiceAppender.File=../log/CCPurgeStagingService_$
{current.time}.log
log4j.appender.PurgeServiceAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.PurgeServiceAppender.layout=org.apache.log4j.PatternLayout
log4j.additivity.PurgeServiceAppender=false
log4j.appender.PurgeServiceAppender.layout.ConversionPattern=%d{dd MMM yyyy
HH:mm:ss,SSS} %r [%t] %-5p %c{1} - %m%n
log4j.category.BulkDataMover=INHERITED
log4j.category.BulkDataMover=, BulkDataMoverAppender
log4j.additivity.BulkDataMover=false
log4j.appender.BulkDataMoverAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.BulkDataMoverAppender.File=../log/BulkDataMover_${current.time}.log
log4j.appender.BulkDataMoverAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.BulkDataMoverAppender.layout=org.apache.log4j.PatternLayout
log4j.additivity.BulkDataMoverAppender=false
log4j.appender.BulkDataMoverAppender.layout.ConversionPattern=%d{dd MMM yyyy
HH:mm:ss,SSS}%r [%t] %-5p %c{1} - %m%n
log4j.category.ReportService=INHERITED
log4j.category.ReportService=INFO, ReportServiceAppender
log4j.additivity.ReportService=false
log4j.appender.ReportServiceAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.ReportServiceAppender.File=../log/ReportService_${current.time}.
log
log4j.appender.ReportServiceAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.ReportServiceAppender.layout=org.apache.log4j.PatternLayout
log4j.additivity.ReportServiceAppender=false
log4j.appender.ReportServiceAppender.layout.ConversionPattern=%d{dd MMM yyyy
HH:mm:ss,SSS}%r [%t] %-5p %c{1} - %m%n
log4j.category.EngineStartup=INHERITED
log4j.category.EngineStartup=, EngineStartupAppender
log4j.additivity.EngineStartup=false
log4j.appender.EngineStartupAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.EngineStartupAppender.File=../log/CCEngineStartup_${current.time}.
log
log4j.appender.EngineStartupAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.EngineStartupAppender.layout=org.apache.log4j.PatternLayout
log4j.additivity.EngineStartupAppender=false
log4j.appender.EngineStartupAppender.layout.ConversionPattern=%d{dd MMM yyyy
HH:mm:ss,SSS}%r [%t] %-5p %c{1} - %m%n
log4j.category.org.mortbay.log=INHERITED
log4j.category.org.mortbay.log=, JettyServiceAppender
log4j.additivity.org.mortbay.log=false
log4j.appender.JettyServiceAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.JettyServiceAppender.File=../jetty/log/Jetty_${current.time}.log
log4j.appender.JettyServiceAppender.DatePattern='.'yyyy-MM-dd-a
```

```
log4j.appender.JettyServiceAppender.layout=org.apache.log4j.PatternLayout
log4j.additivity.JettyServiceAppender=false
log4j.appender.JettyServiceAppender.layout.ConversionPattern=%d{dd MMM yyyy
HH:mm:ss,SSS}%r [%t] %-5p %c{1} - %m%n
log4j.category./cdbrowser=INHERITED
log4j.category./cdbrowser=, JettyServiceAppender
log4j.additivity./cdbrowser=false
log4j.category.SLCService=ERROR,SLCServiceAppender
log4j.additivity.SLCService=false
log4j.appender.SLCServiceAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.SLCServiceAppender.File=../log/SLCService_${current.time}.log
log4j.appender.SLCServiceAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.SLCServiceAppender.layout=org.apache.log4j.PatternLayout
log4j.additivity.SLCServiceAppender=false
log4j.appender.SLCServiceAppender.layout.ConversionPattern=%d{dd MMM yyyy
HH:mm:ss,SSS}[%t] - %m%n
log4j.category.SCCHealthChecker=INFO,SCCHealthCheckerAppender
log4j.additivity.SCCHealthChecker=false
log4j.appender.SCCHealthCheckerAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.SCCHealthCheckerAppender.File=../log/SCCHealthChecker_${current.time}
.log
log4j.appender.SCCHealthCheckerAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.SCCHealthCheckerAppender.layout=org.apache.log4j.PatternLayout
log4j.additivity.SCCHealthCheckerAppender=false
HH:mm:ss,SSS}log4j.appender.SCCHealthCheckerAppender.layout.ConversionPattern=%d
{dd MMM yyyy[%t] - %m%n
```

Sample CCClient.log4j file

The sample log4j file for the ccclient log causes log files to roll over every 12 hours, and does not roll off any log files.

```
# ccclient.Log4j
# Tue Mar 02 02:20:09 CST 2004
log4j.appender.stdout=org.apache.log4j.ConsoleAppender
log4j.logger.com.sterlingcommerce.scc=INHERITED
log4j.appender.R.File=${CONFIG_DIR}/../log/CCClient_${current.time}.log
log4j.appender.R.layout=org.apache.log4j.PatternLayout
log4j.appender.R.DatePattern='.'yyyy-MM-dd-a
log4j.appender.R.layout.ConversionPattern=%d{dd MMM yyyy HH:mm:ss,SSS} %r [%t] %-5p
%C{1} - %m%n
log4j.appender.stdout.layout.ConversionPattern=%d{dd MMM yyyy HH:mm:ss,SSS} %r [%t]
%-5p %C{1} - %m%n
log4j.appender.stdout.layout=org.apache.log4j.PatternLayout
log4j.appender.R=org.apache.log4j.DailyRollingFileAppender
log4j.loggerFactory=com.sterlingcommerce.component.common.logging.log4j.LogFactory
log4j.renderer.java.lang.Throwable=com.sterlingcommerce.component.common.
logging.log4j.ExceptionRenderer
log4j.rootLogger=INFO, R
log4j.category.ReportService=INHERITED
log4j.category.ReportService=INFO, ReportServiceAppender
log4j.additivity.ReportService=false
log4j.appender.ReportServiceAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.ReportServiceAppender.File=../log/ReportService_${current.time}.log
log4j.appender.ReportServiceAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.ReportServiceAppender.layout=org.apache.log4j.PatternLayout
log4j.additivity.ReportServiceAppender=false
log4j.appender.ReportServiceAppender.layout.ConversionPattern=%d{dd MMM yyyy
HH:mm:ss,SSS}%r [%t] %-5p %c{1} - %m%n
```

Parameters modified in the sample log4j files

Some parameters have been modified in the sample log4j files.

Note: This may not be a complete list.

Lines similar to the following have been added to the CCEngine.log4j file:

```
log4j.appender.R.DatePattern='.'yyyy-MM-dd-a
log4j.appender.RuleSessionAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.PurgeServiceAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.BulkDataMoverAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.ReportServiceAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.EngineStartupAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.JettyServiceAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.SLCServiceAppender.DatePattern='.'yyyy-MM-dd-a
log4j.appender.SCCHealthCheckerAppender.DatePattern='.'yyyy-MM-dd-a
```

The '.'yyyy-MM-dd-a item specifies to roll over the files every 12 hours. You can also choose from the following options:

- '.'yyyy-MM:—Rolls log file on the first of each month
- '.'yyyy-ww:—Rolls log file at the beginning of each week
- '.'yyyy-MM-dd:—Rolls log file at midnight every day
- '.'yyyy-MM-dd-a:—Rolls log file at midnight and midday every day
- '.'yyyy-MM-dd-HH:—Rolls log file at the beginning of each hour
- '.'yyyy-MM-dd-HH-mm:—Rolls log file at the beginning of each minute

Lines similar to the following have been removed:

```
log4j.appender.R.MaxFileSize=1000KB
log4j.appender.R.MaxBackupIndex=20
```

Lines similar to the following have been replaced:

```
log4j.appender.R=org.apache.log4j.RollingFileAppender
```

For example, the previous line was replaced with the following:

```
log4j.appender.R=org.apache.log4j.DailyRollingFileAppender
```

Chapter 23. Failover configuration

Although Sterling Control Center has been designed to handle a wide variety of system failures, it may not able to recover in the case of a hardware failure but there are other measures you can take.

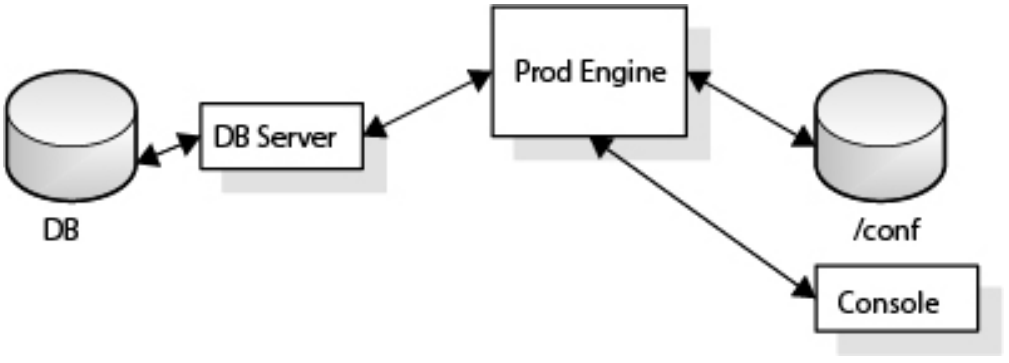
Attention: There are several measures and precautions you can take to provide failover support required in a high-availability environment. For information on configuring high availability options, see the IBM Support Portal.

This documentation discusses the configuration and manual steps for recovering from hardware failures in Sterling Control Center in two different types of environments–one in which the Sterling Control Center engine is installed on a storage area network (SAN) and one where it is not.

The typical Sterling Control Center environment consists of the following components:

- Production Engine (Prod Engine in the following diagram). The Sterling Control Center engine collects information from servers and writes that information to a database. It uses information configured in the /conf directory for system definitions.
- Database server (DB Server).
- Two databases:
  - Production Database—Contains production statistics and event data, Node Discovery-related data, auditing data, and service level criteria recovery-related data.
  - Staging Database—Contains statistics data and event data that have been moved from production.
- Console—The graphical user interface.
- Installation directory/conf— Configuration directory includes managed server definitions and checkpoint data, rules, actions, and service level criteria.

The following diagram shows the base configuration:



Failover may be required in the following situations, which can occur in both types of environments (storage area networks and non-SAN systems):

- Sterling Control Center engine computer failure
- Database server (for production database) computer failure

- Sterling Control Center engine and database server (for production database) computer failure

Important: If the production database is partitioned, Sterling Control Center does not require a staging database. If you use a production database and a staging database, Sterling Control Center requires access to both databases when it is installed and configured. Assuming the staging database resides on a different database server than the production database, Sterling Control Center continues to run even if the staging database is not available. Because recovery from staging database failures is not required for Sterling Control Center to run, this documentation does not address staging database failure as a failover/recovery scenario. Although Sterling Control Center can continue to run with a staging database server failure, eventually the staging database server must be recovered for Sterling Control Center to run with the expected level of performance.

Handling failures when the engine is installed on a SAN

When the Sterling Control Center engine is installed on a storage area network (SAN), there is a procedure you can use before a production engine failure occurs.

About this task

To handle a failure when the engine is installed on a SAN:

Procedure

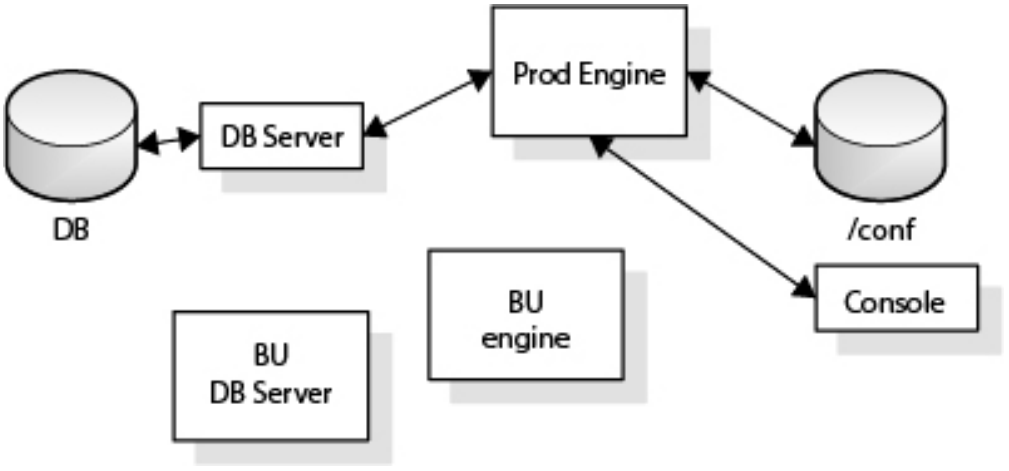
1. Identify the standby computer for the Sterling Control Center engine.
2. Identify a standby database server for the production database.
3. Create a production database and user on the standby database server for Sterling Control Center use.

Results

After you perform this procedure, two new components are added to the base diagram:

- Backup Engine (BU Engine)—Acts as the failover Sterling Control Center engine
- Backup database server (BU DB Server)—For the production database.

The following diagram shows the base configuration with these added components.



Note that when the Sterling Control Center engine is installed on a SAN, there is no requirement to install an engine on the standby computer. It is assumed that the SAN will be available even when the production engine's computer fails.

SAN scenario 1—the server on which the Sterling Control Center engine is executing fails

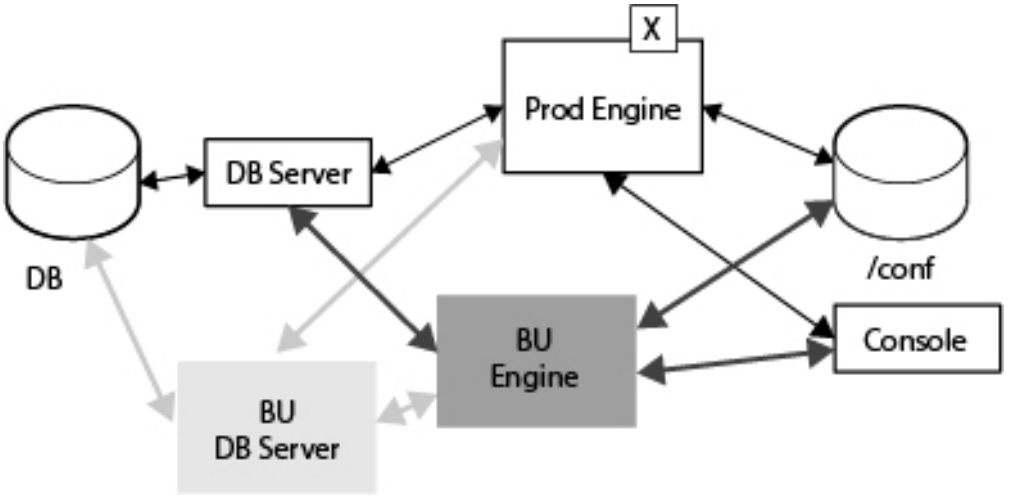
This scenario describes the action you can take when the production engine fails.

Before you begin

In this scenario, it is assumed that you have added both a backup engine and database server by performing the general procedure outlined in *Handling failures when the engine is installed on a SAN*.

About this task

In this scenario, the Production Engine has failed, so the system switches to using the backup engine, called the BU Engine. The backup database server, called the BU DB Server, is configured, but it is not active, because the primary database server is still operational.



Procedure

Start the Sterling Control Center engine from the standby computer using the console. The backup engine has access to both the database server where the production database resides and the production engine configuration data. The backup engine is brought up (without using the standby database server).

SAN scenario 2—the computer where the database server is executing fails

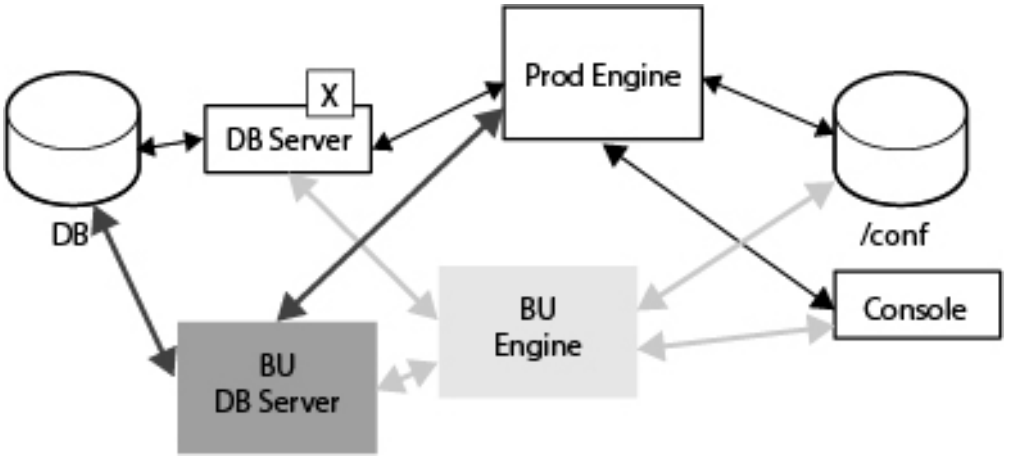
This scenario describes the action you can take when the primary database server fails.

Before you begin

In this scenario, it is assumed that you have performed the general procedure outlined in *Handling failures when the engine is installed on a SAN* and that the standby Sterling Control Center computer will not be used.

About this task

In this scenario, the primary database server, called the DB Server, has failed, so the system switches to using the backup database server, called the BU DB Server. The backup engine, called the BU Engine is configured, but is not active, because the Production Engine is still operational.



Procedure

1. Run (SAN-based) production Sterling Control Center engine's configuration script (configCC.sh/configCC.bat) and configure the engine to point to the standby database server. (The configCC.sh/configCC.bat file is located in the ControlCenterInstallLoc/bin directory.)
2. Start the (SAN-based) production Sterling Control Center engine.

Results

The Production engine has access to the backup database server because you configured and pointed it to the backup database server, which may require supplying the IP address of the backup database server. After you reconnect to the production engine using the console, the production engine can use a different production database (on a standby database server) on another computer.

SAN Scenario 3—The Computer Where the Engine Is Executing and the Computer Where the Database Server Is Executing Both Fail

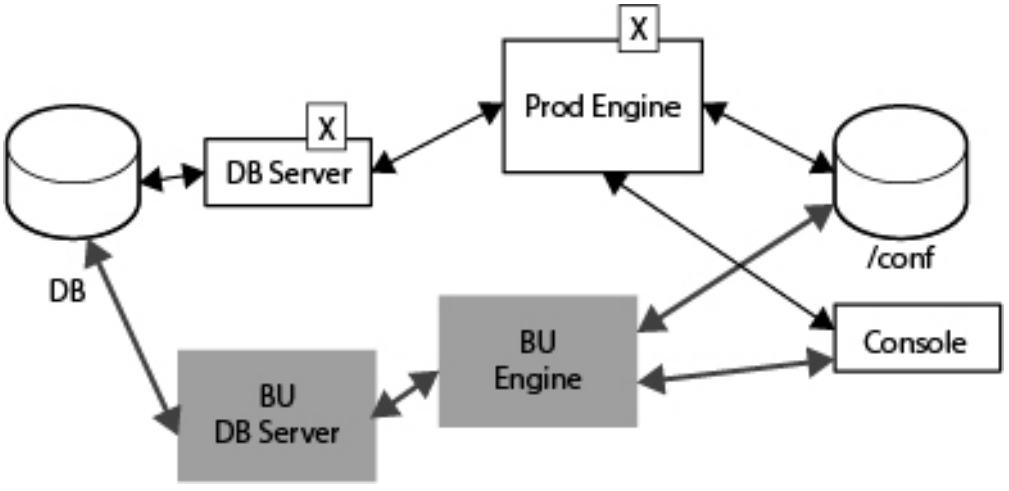
This scenario describes the action you can take when the Sterling Control Center is not installed on a SAN and the Production Engine fails and the primary database server fails.

Before you begin

In this scenario, it is assumed that you have performed the general procedure outlined in *Handling failures when the engine is installed on a SAN* and that the storage area network is available even after the Sterling Control Center production engine computer has failed.

About this task

In this scenario, the Production Engine has failed, so the system switches to using the backup engine, called the BU Engine, and the primary database server, called the DB Server, has failed, so the system switches to using the back up database server, called the BU DB Server.



Procedure

1. Run the (SAN-based) Sterling Control Center engine's configuration script from another computer (configCC.sh/configCC.bat) and configure the engine to point to the standby database server. (The ConfigCC.sh /configCC.bat file is located in the ControlCenterInstallLoc/bin directory.)
2. Start the (SAN-based) Sterling Control Center engine (from another computer).

Results

The backup database server can access the Production database. In addition, the backup engine can access the Production Engine configuration data. When the primary database server fails, the backup database server is brought up and the backup engine is brought up when the production engine fails. (You may have to configure the backup database server's IP address.) To bring up the system, you contact the backup engine using the console.

Handling failures when the engine is not installed on a SAN

There is a procedure you can follow when the Sterling Control Center engine is not installed on a storage area network.

About this task

To prepare for any type of failure in a non-SAN environment:

Procedure

1. To recover from a production Sterling Control Center engine failure, you must have copies of the most recent configuration files.
2. Identify the standby computer for Sterling Control Center engine.
3. Identify a standby database server.
4. Create a production database and user on the standby database server for Sterling Control Center use.
5. Install the Sterling Control Center engine on the standby computer.
6. On a regular basis, copy the entire /conf directory of the production Sterling Control Center engine to the standby Sterling Control Center engine install location.
   - The /conf directory is located in the same directory where Sterling Control Center is installed.
   - It is recommended that you copy the /conf directory (including the subdirectories) of the production Sterling Control Center engine to the standby Sterling Control Center engine install location at least once a day. (In other words, replace the contents of the standby Sterling Control Center engine's /conf directory with the contents of the production Sterling Control Center engine's /conf directory.)
   - Ideally, the periodic copy should be based on the frequency of changes to the Sterling Control Center configuration data (rules, actions, SLCs, managed servers, etc.).

Safeguarding the managed server's checkpoint data

It is crucial that you systematically copy the managed server's checkpoint data in the /conf directory to the standby Sterling Control Center engine install location. The managed server's checkpoint data keeps track of the last time ("savedDateTime") data from that managed server was saved. Each managed server's checkpoint data is kept separately under the /conf directory.

About this task

Whenever the Sterling Control Center engine is restarted, the engine uses the checkpoint data of each managed server to collect data beginning with the last time data was collected. Likewise, when you start the standby engine after a primary engine fails, the Sterling Control Center engine uses the checkpoint data of each managed server to collect this data.

Procedure

To avoid collecting data that has already been collected, perform a cold start at the standby location. To do a cold start, do one of the following from the command line. These scripts are located in the ControlCenterInstallLoc/bin directory.

- Run the runEngineCold.bat script file (Microsoft Windows)

- Run the runEngineCold.sh script bat file (UNIX)
- After you replicate the production database and copy the /conf directory to the standby Sterling Control Center engine install location, two new components have been added to the base diagram:
  - DB—The replicated database which acts as the Failover Sterling Control Center database.
  - /conf—The manual copy of the production /conf directory.

Testing the standby Sterling Control Center engine

Although it is not necessary for the standby Sterling Control Center engine to run all the time, you should test it periodically.

About this task

To test the standby engine:

Procedure

1. Shut down the production Sterling Control Center engine.
2. Copy the contents of the production Sterling Control Center engine's /conf directory to the standby Sterling Control Center engine.
3. Start the standby Sterling Control Center engine.

Scenario 1—The computer where the Sterling Control Center engine is executing fails

This scenario describes the action you can take when the production engine fails.

Before you begin

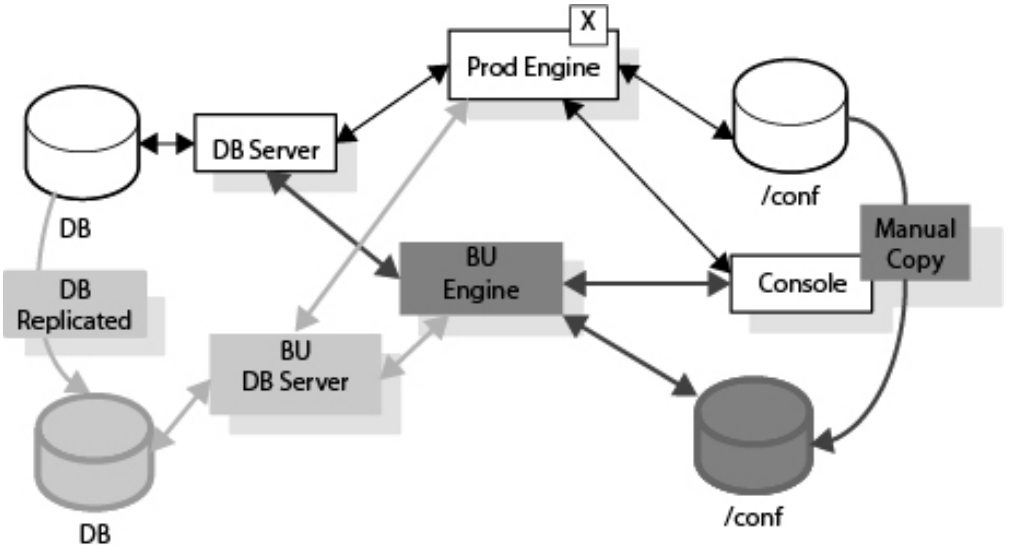
In this scenario, it is assumed that you have followed all procedures outlined in *Handling failures when the engine is not installed on a SAN* before the production Sterling Control Center engine computer failure. The following assumptions are also in place:

- The standby engine will use the same database server used by the production Sterling Control Center engine.
- This also implies that the standby database server will not be used.

The backup Sterling Control Center engine has access to the production database. You must manually copy the production engine configuration data to enable the backup engine to be brought up properly.

About this task

In this scenario, the Production Engine has failed, so the system switches to using the backup engine, called the BU Engine. The backup database server, called the BU DB Server, is configured, but it is not active, because the primary database server is still operational. Since the engine is not installed on a storage area network, the main Database replication is indicated in the diagram between the main Database and the backup database, and the manual copy that you make between /conf and the backup /conf is indicated on the diagram.



Procedure

Start the standby Sterling Control Center engine using the console. When you contact the backup engine, the backup engine is brought up using the copied /conf configuration data.

Scenario 2—the computer where the primary database is executing fails

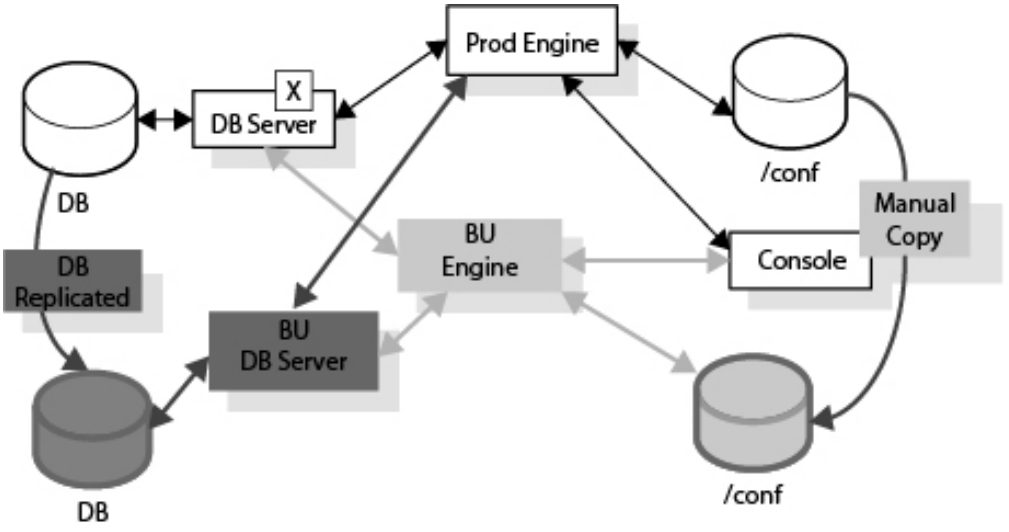
This scenario describes the action you can take when the Sterling Control Center is not installed on a SAN and the primary database server fails.

Before you begin

In this scenario, it is assumed that you have followed all procedures outlined in *Handling failures when the engine is not installed on a SAN* before the production Sterling Control Center engine computer failure. It is also assumed that the standby Sterling Control Center engine will not be used. This situation can be handled simply by configuring the Sterling Control Center engine to use a different production database (standby database server) on another computer.

About this task

In this scenario, the primary database server, called the DB Server, has failed, so the system switches to using the backup database server, called the BU DB Server. The backup engine, called the BU Engine is configured, but is not active, because the Production Engine is still operational. Since the engine is not installed on a storage area network, the main Database replication is indicated in the diagram between the main Database and the backup database, and the manual copy that you make between /conf and the backup /conf is indicated on the diagram.



Procedure

1. Run the production Sterling Control Center engine's configuration script (configCC.sh/configCC.bat) and configure the engine to point to the standby database server.
2. Start the production Sterling Control Center engine.

Results

The primary database has been replicated to the backup database server. The production engine is brought back up by pointing to the backup database server (which may require you to configure the IP address for the backup database).

Note: As mentioned earlier, Sterling Control Center uses the database mainly to store auditing and statistics data. Since all configuration data is stored where the Sterling Control Center engine is installed, the engine can be started using a new database and function normally. As a result, the standby Sterling Control Center database does not need up-to-date data from the primary Sterling Control Center database. This also implies that database replication does not need to be set up for high-availability purposes alone.

Scenario 3—The Computer Where the Engine Is Executing and the Computer Where the Database Server Is Executing Both Fail

This scenario describes the action you can take when the production engine and the primary database both fail.

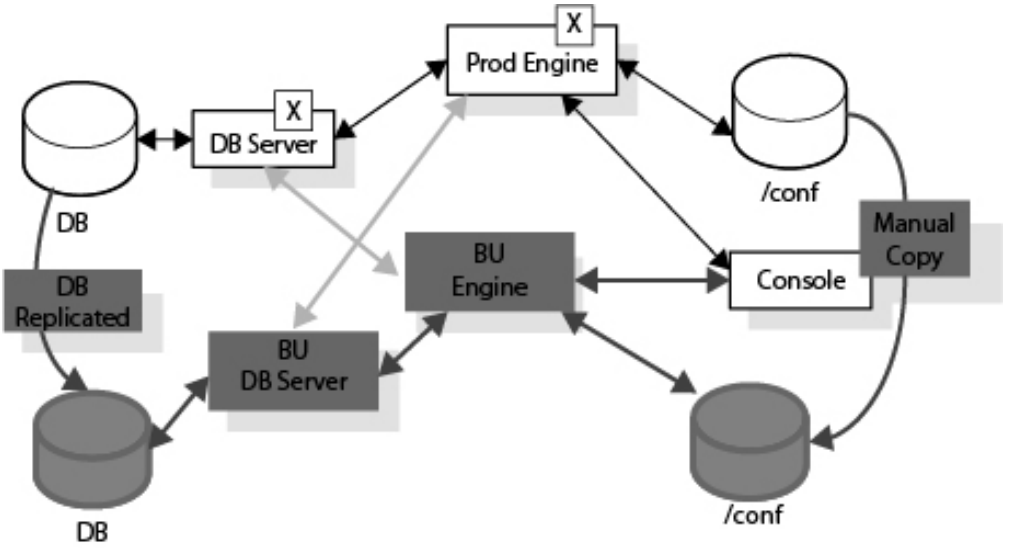
Before you begin

In this scenario, it is assumed that you have followed all procedures outlined in *Handling failures when the engine is not installed on a SAN* before the production environment failure.

About this task

In this scenario, the Production Engine has failed, so the system switches to using the backup engine, called the BU Engine, and the primary database server, called

the DB Server, has failed, so the system switches to using the back up database server, called the BU DB Server. Since the engine is not installed on a storage area network, the main Database replication is indicated in the diagram between the main Database and the backup database, and the manual copy that you make between /conf and the backup /conf is indicated on the diagram.



Procedure

1. Run the standby Sterling Control Center engine's configuration script (configCC.sh/configCC.bat) and configure the engine to point to the standby database server. (The configCC.sh /configCC.bat file is located in the ControlCenterInstallLoc/bin directory.)
2. Start the standby Sterling Control Center engine.

Results

In this case, both the standby Sterling Control Center engine and standby database server are used.

Chapter 24. Keys and fields

In Sterling Control Center, you can specify a key to define the criteria for a report, rule, or SLC. You can also specify a key to act as a filter to limit the number of items that display in many Sterling Control Center listings. A parameter consists of a key, an operator, and a value.

For more information, see *Filtering objects*.

Statistics, properties, and other system-generated information are displayed in various listings, Activity Monitors, and Process Monitors. They give you information about alerts, file transfers, business processes, and other status information. These informational fields are also included here.

The keys and fields are listed in alphabetic order. For each key or field, a brief description is provided along with server-specific information, if applicable. For some items, mapping of terms is included to translate values to a specific server type. Not all keys are available for use in all situations.

Key/Field	Description
Action	Action performed on Sterling Control Center entity.
Actions Flag	Time stamp indicated when event processing completed.
Activity Type	The type of activity an SLC event is associated with. Possible values include: • WF = Workflow • M = Milestone • P = Process • S = Process Step
Alert level	The severity level of the Alert. Possible values include: • 1 = High • 2 = Medium • 3 = Low
Batch ID	Batch identifier used in Sterling Connect:Enterprise.
Batch Number	Batch number used in Sterling Connect:Enterprise.
Bytes Read	Number of bytes read from the source file by the sending server.
Bytes Received	Number of bytes received by the receiving server.
Bytes Sent	Number of bytes sent by the sending server to the receiving server.
Bytes Written	Number of bytes written to the destination file by the receiving server.
Check Point (Y or N)	Indicates whether the checkpoint feature of Sterling Connect:Direct is enabled to facilitate recovery if an interruption in data transfer occurs.
Condition Code	Return code associated with Process steps and Process ends. Possible values include: • 0 = Successful execution. • 4 = A warning-level error was encountered. • 8 = An error occurred during execution. • 16 = A catastrophic error occurred during execution.
Control Center Name	Name of the Sterling Control Center engine.

Key/Field	Description
Cipher Suite	The cipher suite, such as SSL_RSA_WITH_DES_CBC_SHA, used in secure Sterling Connect:Direct sessions.
CX.Event Type	Event type. Possible values are: • NodeCommand • NodeStatus • NodeStarted • NodeShutdown • NodeError • ProcessStepStart • ProcessStepEnd • ProcessStepProgress • ProcessEnded • ConnectionError • ConnectionShutdownStarted • ProcessStarted • TimerEvent
CX.File Bytes Transferred	File bytes transferred.
CX.File Label	File label (PeSIT pi37).
CX.File Transfer Protocol	File transfer protocol. Possible values are: • E=PsSIT Type E • D=PeSIT Type D • A=PeSIT E "PROF=ANY" • F=FTP • O=Odette
CX.Local File Name	Local file name.
CX.Local Node Name	Local node name.
CX.Network Bytes Transferred	Network bytes transferred.
CX.Network Return Code	Network return code.
CX.Number of Records Transferred	Number of records transferred.
CX.Operating System	Operating system.
CX.Other Node Name	Other node name.
CX.Process Originator	Process originator. Possible values are: • I=Local node is the originator • E=Remote node is the originator
CX.Protocol Return Code	Protocol return code.
CX.Receiver of File	Beginning of transfer date/time.Receiver of the file.
CX.Request Type	Request type. Possible values are: • N=Normal request • M=Message • E=End-to-End Response • H=Hold request • I=Inquiry request
CX.Return Code	System return code.
CX.Sender of File	Sender of the file.

Key/Field	Description
CX.Server Name	Server name.
CX.System Return Code	Return code.
CX.Transfer Destination	Transfer destination.
CX.Transfer Direction	Transfer direction. Possible values are: • T=Transmit • R=Receive
CX.Transfer Identified	Transfer identified.
CX.Transfer Origin	Transfer origin.
CX.Type of Link	Type of link. Possible values are: • T=TCPIP • S=SNA
CX.User Data Received	User data received (PeSIT Pi99), associated to file.
CX.User Data Sent	User data sent (PeSIT pi99), associated to file.
Daemon Host	DNS host name or IP address of the system the Sterling Connect:Enterprise daemon is on.
Daemon Name	Name of the Sterling Connect:Enterprise daemon.
Daemon Originator	Originator of the Sterling Connect:Enterprise daemon. Same as Remote ID.
Daemon PID	Process identifier of the Sterling Connect:Enterprise daemon.
Daemon Resource	Resource of the Sterling Connect:Enterprise daemon.
Daemon SID	Session identifier of the Sterling Connect:Enterprise daemon.
Daemon State	State of the Sterling Connect:Enterprise daemon.
Daemon Type	Type of the Sterling Connect:Enterprise daemon. Sterling Control Center monitors only daemons of type master.
Data Visibility Group	Name of the data visibility group. **Note:** If the user who creates a rule or SLC is data visibility restricted, a data visibility group must be specified.
Date Time	The date and time that the event was generated. For FTP W3C servers and IIS logs, this value can be the date and time when the event started or ended. For date and time for end events, this value is the date time plus the time taken.
Days Before Expiry	Number of days before a certificate expires.
Dest Agent	Destination MQ MFT Agent.
Dest Disp1	The status of the destination file before the transfer begins.

Key/Field	Description
Destination File	Destination file name. For Sterling Connect:Direct, the file name at the destination in a copy step of a Process. For Sterling Connect:Enterprise the file name, if received by Sterling Connect:Enterprise, or the userid requesting the file if sent by Sterling Connect:Enterprise. For FTP, in a PUT, the name of the file as found in the FTP transfer log. In a GET, the ID of the user who initiated the transfer. For FTP W3C servers, in the case of an inBound destination file, check the cs-uri-stem if the FTP command is in the cs-method field. Otherwise, check the cs-uri-query field. For FTP W3C servers, in the case of an outBound destination file, check the cs-username if available. Otherwise, check the c-ip field. For FTP IIS logs, in the case of an inBound destination file, check the cs-uri-stem. For an outBound destination file, check the cs-username field.
Direction (inBound or outBound)	Indicates direction of Sterling B2B Integrator and FTP file transmissions. For FTP W3C servers, depends on the FTP command. SENT, RETR, GET, and DOWNLOADED commands are considered inbound. CREATED, STOR, STOU, PUT, UPLOADED, APPE, and APPENDED commands are considered outbound. For FTP II logs, depends on the FTP command in the cs-method field.
EMail Flag	Indicates when email action processing completed.
Event ID	The ID number assigned by the system to each event.
Event ID/Number	The ID number assigned by the system to each event.
Event Type	A code that indicates the type of event. For a listing of event types and descriptions, see *Event type descriptions*.
Executing Processes	The number of Processes in the Execution queue.
Extended Compression	Indicates whether the extended compression was used while transferring the file.
Feedback	The feedback code generated from a Sterling Connect:Direct Process statement.
fgActivityType	The activity associated with the Sterling File Gateway file transfer. Possible values include: • A = Arrival • R = Route • D = Delivery
FG.Activity (A or R or D)	The activity associated with the Sterling File Gateway file transfer. Possible values include: • A = Arrival • R = Route • D = Delivery
FG.Arrived File Name	The name of the arrived file involved in the Sterling File Gateway file transfer.

Key/Field	Description
FG.Arrived File Status	The status of the arrived file involved in the Sterling File Gateway file transfer. Possible values include: • Arrived • Failed • Ignored
FG.Business Process Name	Sterling B2B Integrator business process name.
FG.Consumer	The name of the partner who received the arrived file involved in the Sterling File Gateway file transfer.
FG.Consumer ContentType	The content type of the file to be delivered.
FG.Consumer Mailbox Path	The mailbox path to deliver to a consumer.
FG.ConsumerType	File type the consumer receives.
FG.Data Flow ID	The ID of a data flow document associated with a correlation entry or file transfer event.
FG.DOCUMENT_ID	Sterling File Gateway Arrived File Document ID
FG.Event Code	The Sterling File Gateway equivalent of a message ID.
FG.FILE_NAME	Sterling File Gateway Arrived File Name.
FG.FILE_SIZE	Sterling File Gateway Arrived File Size.
FG.Layer Count	Layers in the file structure.
FG.Layer Description	Descriptive string for the layer type.
FG.Layer Filename	Name of the file in a layer.
FG.Layer Type	Type of layer, such as ZIP, PGP, Text.
FG.PayloadName	Name of the file delivered.
FG.PROD_ORG_KEY	Sterling File Gateway Producer Org Key.
FG.Producer	The name of the partner who created and sent the arrived file involved in the Sterling File Gateway file transfer.
FG.Producer Payload	Name of the file produced.
FG.Route Count	Number of routes for the arrived file.
FG.Routing Channel Template Name	The routing channel template (RCT) defines the structure through which routing occurs.
FG.REVIEWED	Sterling File Gateway Reviewed Arrived File
FG.ROUTES_REMAIN	Sterling File Gateway Remaining Routes
FG.ROUTE_EVENT_KEY	Sterling File Gateway Route Event Key
FG.STATE	Sterling File Gateway Arrived File State
FG.TIME	Sterling File Gateway Event Time
FG.WFID	Sterling File Gateway Arrived File Workflow ID
File Agent Name	The unique name for the file agent specified during file agent configuration.
File Agent Rule	The rule configured on File Agent that determines which Process to use to submit the file to Sterling Connect:Direct
File Agent Trigger File	The file that triggers the rule or the default Process.
File Gateway Time	Date and time that events occurred in Sterling File Gateway. Format: yyyy/mm/dd hh:mm:ss.msmsms (UTC +/- hhmm).

Key/Field	Description
File Size	Size of file transferred in bytes. For FTP W3C servers and IIS logs, file size = cs-bytes + sc-bytes (or 0 if neither is available). For WS_FTP servers, this information is not available.
From Node	Indicates which server, local or remote, is sending the file. When the value is P, the server that is initiating the Process is the sender; otherwise, the server that is initiating the Process is the receiver. • P = PNODE • S = SNODE
From Server	Same as From Node.
ftpLogRecord	Actual contents of the FTP log record that caused the event to be generated. For FTP W3C servers and IIS logs, (date time GMT) plus all fields from the log. **Note:** For more information, see the sections on FTP xferlog and IIS Log Formats and W3C FTP Server Logs in *Getting Started*.
Group ID	SLC Name
In Error	Indicates that one or more activities within a Sterling B2B Integrator business process failed. • True • False
Is BP	Indicates whether the event is associated with a Sterling B2B Integrator business process. • True • False
Link Fail	Indicates whether a communications error occurred. • True • False
Local Node (P or S)	The server that processed the file. P = Primary S = Secondary
Local Condition Code	The return code of the local Sterling Connect:Direct server.
Local Message ID	The message ID of the local Sterling Connect:Direct server.
Local Server	The name of the local Sterling Connect:Direct server
Log Date/Time	Date and time that the event occurred. Format: yyyy/mm/dd hh:mm:ss.msmsms (UTC +/- hhmm). For Sterling File Gateway, this value is the date and time that events were logged in the database. To see a chronological listing of events, open the Statistics viewer, right-click a column heading, select Manage Columns, and add File Gateway Time to Selected Columns. To sort, right-click the File Gateway Time column.
Mailbox ID	Mailbox identifier used in Sterling Connect:Enterprise.
Message	The server or Sterling Control Center message ID issued with the event.

Key/Field	Description
Message ID	The server or Sterling Control Center message ID issued with the event. For Sterling File Gateway, Event Code is mapped to Message ID.
Message Text	Message description.
Minutes Since Last Submit	Number of minutes since the previous submission to the File Agent.
MQMFT.The MQ MFT message id	Server or Sterling Control Center message ID issued with the event.
MQMFT.The MQ MFT action type	MQ FTE action type. The values are started, progress, or completed.
MQMFT.The action time	Action time. The format is yyyy-mm-ssThh:mm:ss.nnnZ.
MQMFT.-call's outcome	The outcome of the call.
MQMFT.-call result's error	The resulting error of the call.
MQMFT.-call result's outcome	The resulting outcome of the call.
MQMFT.-call result's return code	The resulting return code of the call.
MQMFT.-call result's stderr output	The call stderr output.
MQMFT.-call result's stdout output	The call stdout output.
MQMFT.-call result's time	The call result time.
MQMFT.-call result's retries	The number of retries for the call.
MQMFT.-call command arguments	The call command arguments.
MQMFT.-call command name	The call command name.
MQMFT.-call command retry count	The call retry count.
MQMFT.-call command retry wait	The call retry wait time.
MQMFT.-call command successful return code	The call specification of a successful RC.
MQMFT.-call command type	The call command type.
MQMFT.Destination queue manager	Name of the destination agent.
MQMFT.Destination agent	Name of the destination agent queue manager.
MQMFT.Destination bridge URL	The URL if the MQ MFT process bridged the file from MQ to some other protocol (like FTP).
MQMFT.Destination's OS arch	Architecture of the destination agent.
MQMFT.Destination's OS name	Name of the destination agent operating system.
MQMFT.Destination's OS version	Version of the destination agent operating system.
MQMFT.MQ MFT identifier for the transfer	MQ MFT identifier for the file transfer.
MQMFT.Job name (if provided). Otherwise, "MQMFT_transfer".	Job name (if provided). Otherwise, the value isMQ MFT_transfer.
MQMFT.User provided metadata	User metadata. Format is [key1=value1].[key2=value2]...
MQMFT.Hostname of the originator	Hostname of the request originator.
MQMFT.The originator's MQMD userid	MQMD userid of the originator.
MQMFT.The originator's userid	Originator userid.
MQMFT.-postdest call's outcome	The postdest call outcome.
MQMFT.-postdest call's error	The postdest call result error.
MQMFT.-postdest call result's outcome	The postdest call result outcome.
MQMFT.-postdest call result's return code	The postdest call result return code.

Key/Field	Description
MQMFT.-postdest call result's stderr output	The postdest call result stderr.
MQMFT.-postdest call result's stdout output	The postdest call result stdout.
MQMFT.-postdest call result's time	The postdest call result time.
MQMFT.-postdest call result's retries	The postdest call result retries.
MQMFT.-postdest command arguments	The postdest command arguments.
MQMFT.-postdest command name	The postdest command name.
MQMFT.-postdest command retry count	The postdest command retry count.
MQMFT.-postdest command retry wait	The postdest command retry wait.
MQMFT.-postdest command successful return code	The postdest command successful return.
MQMFT.-postdest command type	The postdest command type.
MQMFT.-postsrc call's outcome	The postsrc call outcome.
MQMFT.-postsrc call's error	The postsrc call error.
MQMFT.-postsrc call result's outcome	The postsrc call result outcome.
MQMFT.-postsrc call result's return code	The postsrc call result return code.
MQMFT.-postsrc call result's stderr output	The postsrc call result stderr output.
MQMFT.-postsrc call result's stdout output	The postsrc call result stdout output.
MQMFT.-postsrc call result's time	The postsrc call result time.
MQMFT.-postsrc call result's retries	The postsrc call result retries.
MQMFT.-postsrc command arguments	The postsrc command arguments.
MQMFT.-postsrc command name	The postsrc command name.
MQMFT.-postsrc command retry count	The postsrc command retry count.
MQMFT.-postsrc command retry wait	The postsrc command retry wait.
MQMFT.-postsrc command successful return code	The postsrc command successful return.
MQMFT.-postsrc command type	The postsrc command type.
MQMFT.-predest call's outcome	The predest call outcome.
MQMFT.-predest call result's error	The predest call result error.
MQMFT.-predest call result's outcome	The predest call result outcome.
MQMFT.-predest call result's return code	The predest call result return code.
MQMFT.-predest call result's stderr output	The predest call result stderr output.
MQMFT.-predest call result's stdout output	The predest call result stdout output.
MQMFT.-predest call result's time	The predest call result time.
MQMFT.-predest call result's retries	The predest call result retries.
MQMFT.-predest command name	The predest call command name.
MQMFT.-predest command retry count	The predest call result retry count.
MQMFT.-predest command retries	The predest call result retry wait.

Key/Field	Description
MQMFT.-predest command successful return code	The predest call result successful return.
MQMFT.-predest command type	The predest call command type.
MQMFT.-presrc call's outcome	The presrc call outcome.
MQMFT.-presrc call result's error	The presrc call result error.
MQMFT.-presrc call result's outcome	The presrc call result.
MQMFT.-presrc call result's return code	The presrc call result return code.
MQMFT.-presrc call result's stderr output	The presrc call result stderr output.
MQMFT.-presrc call result's stdout output	The presrc call result stdout output.
MQMFT.-presrc call result's time	The presrc call result time.
MQMFT.-presrc call result's retries	The presrc call result retries.
MQMFT.-presrc command arguments	The presrc command arguments.
MQMFT.-presrc command name	The presrc command name.
MQMFT.-presrc command retry count	The presrc command retry count.
MQMFT.-presrc command retry wait	The presrc command retry wait.
MQMFT.-presrc command successful return code	The presrc command successful return.
MQMFT.-presrc command type	The presrc command type.
MQMFT.Source agent queue manager	The source agent queue manager.
MQMFT.Source agent name	The source agent name.
MQMFT.Source agent bridge URL	The URL if MQ MFT received a file from some other protocol other than MQ (like FTP).
MQMFT.Source agent's OS arch	The source agent operating system arch.
MQMFT.Source agent's OS name	The source agent operating system name.
MQMFT.Source agent's OS version	The source agent version.
MQMFT.Statistics actual start time	Statistics actual start time.
MQMFT.Statistics number of file failures	Statistics number of file failures.
MQMFT.Statistics number of file warnings	Statistics number of file warnings.
MQMFT.Statistics retry count	Statistics retry count.
MQMFT.rslt code	The result code.
MQMFT.MQ MFT msg	MQ MFT message.
MQMFT.Destination checksum	Destination file checksum.
MQMFT.Destination checksum method	Destination file checksum method.
MQMFT.Destination exists	The exists= specification.
MQMFT.Destination last modification date/time	Last modified date/time of the destination file. The format is yyyy-mm-ssThh:mm:ss.nnnZ.
MQMFT.Destination queue group id	Destination queue group ID.
MQMFT.Destination queue message count	Count of messages to queue.
MQMFT.Destination queue message id	Destination queue message ID.
MQMFT.Destination queue message length	Length of message.

Key/Field	Description
MQMFT.Destination file size	Destination file size.
MQMFT.Transfer mode	The transfer mode.
MQMFT.Source checksum	The source checksum.
MQMFT.Source checksum method	The source checksum method.
MQMFT.Source disposition	The source disposition.
MQMFT.Source last modified date/time	The source last modified date/time.
MQMFT.Source queue group id	The source queue group ID.
MQMFT.Source queue message count	The source queue message count.
MQMFT.Source queue message id	The source queue message ID.
MQMFT.Source queue message length	The source queue message length.
MQMFT.Source file size	The source file size.
MQMFT.Transfer result code	The transfer result code.
MQMFT.Transfer message	The transfer message.
MQMFT.Transfer start timeOrig Node	The transfer start time.
Name	Same as Process name.
Node Name	The name of the server.
Node Type	The code that indicates the type of server. The server types are: • 0 = Sterling Control Center • 1 = Sterling Connect:Direct • 2 = Sterling Connect:Enterprise • 3 = Sterling B2B Integrator • 4 = FTP • 5 = Sterling Connect:Express • 6 = QuickFile • 7 = MQ MFT
Non-Executing Processes	The number of Processes not being executed, that is, in the Wait, Hold, or Timer queues.
Number	Same as Process number.
Orig Node	The originating node of a Sterling Connect:Direct or Sterling B2B Integrator Process. For FTP W3C servers, check the cs-username field if available; otherwise, the c-ip field. For FTP IIS logs, check the cs-username field if available.
Originating Node/Server	The name of the server or node (PNODE) that initiated the process. For FTP, the submitter ID. User ID of the user that is initiating the work.
Other Condition Code	The return code of the remote Sterling Connect:Direct server.
Other Message ID	The message ID of the remote Sterling Connect:Direct server.
Percent Complete	For Sterling Connect:Direct servers, the percent complete of the file copy or transfer. Relevant only to events with the event type of Process Status.
Pnode	The Sterling Connect:Direct primary node.
Pnode Acct Info	Accounting information associated with the Sterling Connect:Direct primary node.

Key/Field	Description
Process ID	For Sterling File Gateway, the ID for the business process. For Sterling Connect:Direct, same as Process number.
Process Name	The name of the Process or batch ID. (The name of an FTP Process is always either GET or PUT.) For FTP W3C servers, this value comes from the cs-method field if available; otherwise, it is the cs-uri field. For FTP IIS logs, this value comes from the cs-method field.
Process Name/Batch ID	This key or field maps to the following values: • Process name (Sterling Connect:Direct) • Business Process name (Sterling B2B Integrator) • Batch ID (Sterling Connect:Enterprise) • GET or PUT (FTP servers) • Arrived File Name (Sterling File Gateway)
Process Number	The number that identifies the process.
QF.eventType (also QuickFile Event Type)	The type of QuickFile event.
QF.file	The name of the QuickFile file.
QF.operation (also QuickFile Operation)	The QuickFile event operation.
QF.recipient.userEmail (also QuickFile Recipient Email Addr)	The email address of the QuickFile recipient user.
QF.recipient.userId (also QuickFile Recipient User ID)	The user ID of the QuickFile recipient.
QF.userEmail (also QuickFile User Email Address)	The email address of the QuickFile user.
QF.userId (also QuickFile User ID)	The user ID of the QuickFile user.
QF.userRegistered (also QuickFile User Registered)	Boolean indicator as to whether the QuickFile user is registered or not. Values are true | false.
Queue ID	In Sterling Connect:Direct, there are 4 processing queues: Exec, Hold, Timer, and Wait. In Sterling B2B Integrator, there are 10 queues: Q0 through Q9.
Record Category	Statistics record category. Possible values include: • CAEV=The record is related to a Sterling Connect:Direct event, such as a Sterling Connect:Direct shutdown. • CAPR=The record is related to a Sterling Connect:Direct Process.
Record ID	The record (or statistic ID) used to indicate what Sterling Connect:Direct activities produce associated Sterling Control Center event types, for example, CH (Change Process) has an Event type of Server Command. For more information, see *Event type: Sterling Connect:Direct statistic record ID cross-reference*.
Records Read	The number of records read from the source file.
Records Written	The number of records written to the destination file.
Remote Node/Server	The server or remote node name involved in a Process or file transfer. For Sterling Connect:Direct, the remote node is the SNODE name. For Sterling Connect:Enterprise, the remote node is the recipient mailbox ID.
Remote Server	The remote server name.

Key/Field	Description
Restart	Indicates if the restart feature of Sterling Connect:Direct is enabled to facilitate recovery should an interruption in data transfer occur.
Restart (Y or N)	Indicates if the restart feature of Sterling Connect:Direct is enabled to facilitate recovery should an interruption in data transfer occur.
Return Code	Same as condition code. Return code associated with Process steps and Process ends. Possible values include: • 0 = Successful execution. • 4 = A warning-level error was encountered. • 8 = An error occurred during execution. • 16 = A catastrophic error occurred during execution. For FTP W3C servers, this comes from the sc-win32-status field if available; else, sc-status field. For FTP IIS logs, this comes from the sc-win32-status field if available.
RUS Received	The number of buffers received by the destination server.
RUS Sent	The number of buffers sent to the destination file by the sending server.
RU Size	In Sterling Connect:Direct, the size of blocks in number of bytes sent in a transmission.
Rule ID	The name of the rule triggered by the event.
Secure+ Enabled (Y or N)	Indicates if the Secure+ Option feature for a Sterling Connect:Direct file transfer was enabled.
Secure Protocol	The protocol, such as TLS or SSL, used in secure Sterling Connect:Direct sessions.
Sequence	For Sterling File Gateway, the sequence number.
Sequence Number	Sequence number of the statistics record.
Server	Actual name of monitored server.
Server Alias	Monitored server name used by Sterling Control Center.
Server Data/Metadata 1-10	Server metadata fields for analyzing server information according to the needs of your organization. See *Metadata rules overview*.
Server Groups	Sterling Control Center server group names.
Server ID	The name or alias of the server.
Server ID/Server Alias	Sterling Control Center Name/Alias of managed server.
Server Name	Name of the managed server.
Server Type	The type of server. (Also same as NodeType event element variable.) • 0 = Sterling Control Center • 1 = Sterling Connect:Direct • 2 = Sterling Connect:Enterprise • 3 = Sterling B2B Integrator • 4 = FTP • 5 = Sterling Connect:Express • 6 = QuickFile
Server Type Name	Type of Server.
SESSION.ADAPTER_DISPLAY_ NAME	For a protocol activity, the display name for the Sterling B2B Integrator adaptor.

Key/Field	Description
SESSION.ADAPTER_NAME	For a protocol activity, the system name for the Sterling B2B Integrator adaptor.
SESSION.ADAPTER_TYPE	For a protocol activity, the display name for the Sterling B2B Integrator adaptor.
SESSION.CON_END_TIME	For a protocol activity, the time the Sterling B2B Integrator session connection ended.
SESSION.CON_IS_SUCCESS	For a protocol activity, indicates the Sterling B2B Integrator session connection was successful.
SESSION.DIS_IS_SUCCESS	For a protocol activity, indicates the Sterling B2B Integrator session disconnection was successful.
SESSION.DIS_START_TIME	For a protocol activity, the time the Sterling B2B Integrator session disconnection started.
SESSION.END_WFID	For a protocol activity, the workflow ID for the Sterling B2B Integrator session end.
SESSION.END_WFSTEP	For a protocol activity, the workflow step for the Sterling B2B Integrator session end.
SESSION.ENDPOINT1	Sterling B2B Integrator session end point 1.
SESSION.ENDPOINT2	Sterling B2B Integrator session end point 2.
SESSION.ENDPORT1	Sterling B2B Integrator session end port 1.
SESSION.ENDPORT2	Sterling B2B Integrator session end port 2.
Short Msg	The short message text of a message ID. (Also same as shortText event element variable.)
Short Text	Message text associated with the Message ID.
SI.Adapter Name	Name of the Sterling B2B Integrator adapter.
SI.Adapter Type	Type of Sterling B2B Integrator adapter.
SI.Document Name	Name of the business document that the business Process works on.
SI.Is Put(true/false)	Indicates if a file to a Sterling B2B Integrator mailbox was delivered successfully.
SI.Mailbox Path	A storage area path for business documents. The Sterling B2B Integrator mailbox path provides an administrative hierarchy that is easy to manage and understand.
SI.Message ID	Message ID of the business information communicated through the business Process.
SI.Message Name	Name of the business information communicated through the business Process.
SI.Process Data	Data that is accumulated in an XML document about a business process during the life of the process.
SI.Session Protocol	Protocol that the adapter handles.
SI.Type	For Sterling B2B Integrator server, indicates the source of the event: • FG = Sterling File Gateway • BP = Business Process • PR = Protocol
SLC Flag	Indicates when SLC processing completed.
SLC ID	A system-assigned name of the SLC that triggered the event.
SLC Identification	A system-assigned name of the SLC that triggered the event.

Key/Field	Description
SLC Instance ID	Unique SLC identifier. Includes the SLC name, schedule name, and unique number.
SLC Name	The name of the SLC.
SLC Source 1	SLC recovery data 1
SLC Source Event ID	A system assigned number that identifies the SLC that triggered the event. Used by the system to relate multiple SLC events to the same SLC source.
SLC Source Event Time	The time that the event triggering an SLC event occurred.
Snode	The secondary Sterling Connect:Direct server involved in the Process. The initiating node in a Process is the Pnode, or primary node.
Snode Acct Info	Accounting information associated with the Sterling Connect:Direct secondary node.
Source Agent	Source MQ MFT Agent.
Source File	For a Sterling Connect:Direct server, the source file name in a Copy. Also the target in a Submit, Run Task, or Run Job Sterling Connect:Direct Process step. For Sterling Connect:Enterprise, the file name if sent by Sterling Connect:Enterprise or the userid sending the file if received by Sterling Connect:Enterprise. For FTP, in a PUT, the ID of the user who did the transfer. In a GET, the name of the file received. For FTP W3C servers, in the case of an inBound source file, this comes from the cs-username field if available; else this comes from the c-ip field. For FTP W3C servers, in the case of an outBound source file, this comes from the cs-uri-stem field if the FTP command is in the cs-method field; else, this comes from the cs-uri-query field. For FTP IIS logs, in the case of an inBound source file, this comes from the cs-username field. In the case of an outBound source file, this comes from the cs-uri-stem field.
Standard Compression	Indicates if the standard compression was used while transferring the file.
Start Time	The date and time the event started.
Start Date/Time	The date and time the event started.
Step Name	The Sterling Connect:Direct Process step name or Sterling B2B Integrator business Process activity. **Note:** This key cannot be used for Sterling Connect:Direct for i5/OS.
Stop Time	The date and time the event stopped.
Stop Date/Time	The date and time the event stopped.
Submit Node	The server name that initiated the Process.
Submitter/ID	The name or user ID of the person who submitted the Process or Sterling Connect:Enterprise mailbox.
SUBMITTER NODE	The name of the node the Process was submitted from.
Translation	For Sterling Connect:Direct, the type of translation performed for a Process copy.
trapFlag	Indicates when trap operation action completed.

Key/Field	Description
Type	• For Sterling B2B Integrator server, the type of activity. • FG = Sterling File Gateway • BP = Business Process • PR = Protocol
User Data 1–4	Metadata fields for analyzing activity in ways unique to your organization. See *Metadata rules overview*.
userOpFlag	Indicates when a user operation action completed.
WF.ACTIVITYINFO_ID	Business Process Activity Info ID.
WF.BASIC_STATUS	Business Process basic status.
WF.END_TIME	Business Process end time.
WF.NEXT_AI_ID	Business Process next AI ID.
WF.NODEEXECUTED	Node where Business Process executed.
WF.SERVICE_NAME	Service name in Business Process.
WF.START_TIME	Business Process / Business Process Step start time
WF.STEP_ID	Business Process step ID.
WF.WFD_ID	Business Process WFD ID.
WF.WFD_NAME	Business Process WFD name.
WF.WFD_VERSION	Business Process WFD version.
WF.WFE_STATUS	Business Process execution status
WF.WORKFLOW_ID	Business Process instance ID
WFD_NAME	Business Process name

Chapter 25. Monitor a Sterling B2B Integrator server

You can use Sterling Control Center to monitor various aspects of a Sterling B2B Integrator server.

You can monitor:

- Adaptor status
- Queue depths: Q0 through Q9
- Business process activity
- Sterling File Gateway activity
- File transfers using one or more of the various protocols supported by the Sterling B2B Integrator server

When you are defining Sterling B2B Integrator server properties, consider the following when choosing monitoring options:

- To monitor business process activities, set Monitor Business Processes to **Yes**.

  After Sterling Control Center has connected to the Sterling B2B Integrator server, you can limit the data collected on business processes by Sterling Control Center. To limit data, click the BP List button on the Settings tab of the Server Properties window.

  On the Business Process Selection dialog, select up to 255 business processes that will not be monitored. In this dialog, you can enter the XPath expression for retrieval of process data for specific business processes. For more information, see *Collecting Sterling B2B Integrator process data*.
- To monitor Sterling File Gateway activity, set **Monitor File Gateway** to **Yes**.
- To monitor file transfers directly that are initiated by business processes and Sterling File Gateway, select one or more of the protocols listed on the Settings tab.

  If no protocols or business processes are selected for monitoring, Sterling Control Center does not monitor the adaptor status for the Sterling B2B Integrator server, regardless of the value set for Adapter Status Monitor Rest Time.
- To monitor queue depths, you can specify which queues to monitor at what limit on the Queue Limits tab.

  Sterling Control Center watches the specified queues and generates events when the specified limit is exceeded and when the queue depth returns to the limit, as shown in the following example:

  ```
  CCNS020E Monitored Queue Limit has been exceeded.  Server ID: {0}  Queue: {1}
  Limit: {2}  Depth: {3}
  CCNS030I Monitored Queue Limit back in compliance.  Server ID: {0}  Queue: {1}
  Limit: {2}  Depth: {3}
  ```

  For information on using these events in rules, see *How can I know if the number of items being executed by a server exceeds a specified threshold?* in *How-To*.

Collecting Sterling B2B Integrator process data

During the life of a business process Sterling B2B Integrator collects process data in an XML document, which can become quite large. Typically, business processes act on the document or payload data, such as a customer's purchase order, and extract information from the document and place it in the process data. Process data can be used for various purposes including determining what the next step of the business process will be.

Sterling Control Center can track elements and components within the process data, such as the name of a file being transferred or a purchase order number. When you select a specific business process to monitor on a Sterling B2B Integrator server, you can specify the Process Data XPath to enable Sterling Control Center to access the information you need in the process data XML document. The extracted process data is part of the other statistical elements collected for each business process step.

Using collected Sterling B2B Integrator process data

You can also use the collected process data in rules, metadata rules, SLCs, and reports.

The following items related to using process data in Sterling Control Center:

- The element name in Sterling Control Center event for the process data is SI.Process Data.
- The XPath must always start with the prefix, `/ProcessData`, for example, `/ProcessData/FTPClientBeginSessionServiceResults/ServerResponse/Text`.
- Only one XPath can be specified for a specific business process in Sterling Control Center.
- If a business process (parent) invokes another business process (child), you must specify the same XPath for both the parent and child business processes to collect the process data for all the steps in a workflow instance.

The following XML document example of a parent business process (SCC_Process1) invokes a child business process (CCC_GetInfo) in INLINE mode:

```
<process name="SCC_Process1">
  <sequence>
    <operation>
      <participant name="InvokeSubProcessService" />
      <output message="Xout" >
        <assign to="INVOKE_MODE">INLINE</assign>
        <assign to="WFD_NAME">CCC_GetInfo</assign>
      </output>
      <input message="Xin" >
        <assign to="." from="*"></assign>
      </input>
</operation>
<operation name="Wait">
      <participant name="WaitService"/>
      <output message="WaitServiceTypeInputMessage">
        <assign to="WAIT_INTERVAL">2</assign>
        <assign to="." from="*"></assign>
      </output>
      <input message="inmsg">
        <assign to="." from="*"></assign>
      </input>
    </operation>
  </sequence>
```

In this example, Step 2 is part of business process CCC_GetInfo. To collect process data for all steps of Instance ID 157547, the XPath must be specified for both SCC_Process1 and CCC_GetInfo.

Chapter 26. Monitor file transfers performed by Sterling File Gateway

The underlying platform for Sterling File Gateway is Sterling B2B Integrator. To monitor Sterling File Gateway activities, add a Sterling B2B Integrator server and specify the Monitor File Gateway option on the Settings panel. If you are already monitoring the underlying Sterling B2B Integrator server and want to monitor Sterling File Gateway activities, update the settings for the Sterling B2B Integrator server by clicking the Monitor File Gateway option.

The following Sterling File Gateway activities can be monitored:

- Arrived File events
- Route events
- Delivery events

Related to Sterling File Gateway activities, Sterling Control Center also allows monitoring activities of Mailbox Service, MBI (Mailbox Browser Interface). Sterling File Gateway uses Mailbox Service to place files in mailboxes. You can monitor those activities by selecting the Mailbox Service protocol in the server settings panel.

Viewing Sterling File Gateway activities

For each arrived file, depending on its status, an entry may appear either in the Queued Activity Monitor or Completed Activity Monitor.

You can view the following:

- To view all arrived file events, route events, and delivery events for a particular arrived file, right-click on the item in the activity monitor, and choose Select Statistics.
- To see a chronological listing of events, right-click a column heading, select Manage Columns, and add File Gateway Time to Selected Columns.
- To sort, right-click the File Gateway Time column. The Log Date/Time column displays when the event was logged in the database where as the File Gateway Time column displays when the event occurred.

In the Activity Monitor display panels, the SI.Type field can show one of the following types of activity for a Sterling B2B Integrator server:

- FG indicates a Sterling File Gateway activity.
- BP indicates a business process activity.
- PR indicates a protocol activity.

Sterling File Gateway activities are collected using the following Sterling File Gateway database tables:

- FG_ARRIVEDFILE
- FG_ROUTE
- FG_DELIVERY
- FG_ROUTE_EVENT
- FG_EVENT_ATTR

Statistics Viewer

All Sterling File Gateway source information is displayed in the Statistics Viewer. In the Statistics Viewer, fields with the prefix FG relate to columns in Sterling File Gateway database tables.

Sterling File Gateway terms

Sterling File Gateway terms are mapped to standard Sterling Control Center terms in the Activity Monitor displays

The following Sterling File Gateway terms are mapped to standard Sterling Control Center terms:

- SFG Arrived File is mapped to Process Name.
- SFG Event Code is mapped to Message ID in statistics.
- The return codes for the arrived file and its events are based on status and are set to either 0 (completed) or 8 (failed).

Chapter 27. Monitor file transfers performed by QuickFile

QuickFile file transfers consist of upload and download operations. QuickFile allows packages, consisting of one or more files, to be uploaded for one or more recipients. Files in those packages can be downloaded by the designated recipients.

Sterling Control Center monitors a QuickFile appliance by subscribing to event messages generated as it performs tasks such as uploads and downloads. These event messages are:

- Consumed by Sterling Control Center
- Converted into Sterling Control Center events (by a QuickFile node service that is created to monitor it)
- Passed on to the Metadata Rule Service, Rule Service, Data Visibility Service, SLC Service, and other Sterling Control Center internal services, as appropriate

As a result, all the typical monitoring functions that can be performed for other server types that are supported by Sterling Control Center, can also be performed for QuickFile servers.

QuickFile event messages contain various elements, with corresponding values, including:

eventType
The type of event for which the message was generated

file The file name

fileSize
The size of the file

operation
The type of operation

packageSubject
The package subject

recipient.userEmail
The recipient email address

recipient.userFullName
The full name of the recipient

recipient.userId
The user ID of the recipient

recipient.userRegistered
A true or false value that depends upon the status of the recipient

userEmail
The user's email address

userRegistered
A true or false value that depends upon the status of the user

serverName
Typically the IP address of the QuickFile appliance

Some of these QuickFile event variables are also directly accessible through Rules, SLCs, and more. QuickFile event variables begin with QF, followed by the QuickFile event element name, for example, QF.operation. For more information, see *Sterling Control Center variables*.

A subset of the QuickFile event message values is mapped to Sterling Control Center event elements and values as follows:

- QF.dateTime is dateTime
- QF.file is destFile for downloads and sourceFile for uploads
- QF.fileSize is fileSize
- QF.packageId is processId
- QF.packageSubject is processName. It is also sourceFile for downloads and destFile for uploads
- QF.serverName is both nodeName and origNode
- QF.userFullName is submitterId

QuickFile messages are generated when packages that are uploaded consist of the following event types:

- packageStart
- fileStart – one per file, per recipient, in the package
- fileEnd – one per file, per recipient, in the package
- fileEvent – one per file, per recipient in the package
- packageEnd

QuickFile messages are generated when files in packages that are downloaded consist of the following event types:

- packageStart
- fileStart
- fileEnd
- fileEvent
- packageEnd

As these messages are processed by a QuickFile node service, the following Sterling Control Center events are generated:

- Process Start event for every packageStart message
- Step Start and Step End events (with the same time stamp) for every fileEvent message
- Process End event for every packageEnd message

The fileStart and fileEnd messages are not used by the QuickFile node service because they do not contain recipient information. However, the fileEvent messages have recipient information and all the information that is contained in the fileStart and fileEnd messages. Because both Step Start and Step End events are generated from a single fileEvent message when transfers complete, step-based SLCs that use Calendar schedules should only specify NER (Normal End Range) values and not NSR (Normal Start Range) values.

Important: Users cannot write rules to monitor for failed QuickFile transfers because QuickFile messages make no distinction between transfers that failed versus transfers that succeeded.

Completed Process Activity Monitor

For each package uploaded by a QuickFile user, there is a single entry in the Sterling Control Center Completed Process Activity Monitor. As users download files related to a package, that same entry is updated, as opposed to having more entries added to the monitor. The same entry is updated because all statistics related to the upload of packages have the same Sterling Control Center Process ID. This ID is set to the value of the QuickFile package identifier. All downloads from the same QuickFile package have the same QuickFile package identifier.

Queued Process Activity Monitor

You may or may not see transfers in progress in a Sterling Control Center Queued Process Activity Monitor depending on the following factors:

- The number of files that are being uploaded in a package
- The speed of either upload and download file transfers
- The monitor rest time value for the QuickFile node service

File transfers can start and finish before Sterling Control Center has a chance to display them.

Important: QuickFile does not generate message events as transfers are in flight. As a result, no indication of a transfer's progress is available in the Queued Process Activity Monitor for QuickFile. Therefore, rules set up to watch for the SLC events that are related to Steps ahead or behind schedule (message IDs CSLC171I through CSLC182E) are not triggered for QuickFile transfers.

QuickFile event variables

QuickFile has the following event variables:

Event variable	Description
QF.dateTime	Date and time the event occurred
QF.eventType	Type of QuickFile event
QF.file	Name of file
QF.fileSize	Size of file
QF.operation	Event operation
QF.packageFileCount	Count of files in package
QF.packageId	QuickFile package identifier
QF.packageSubject	QuickFile package subject
QF.packageTotalSize	Size of all files in package
QF.recipient.userEmail	Recipient user email address
QF.recipient.userFullname	Recipient user full name
QF.recipient.userId	Recipient user ID
QF.recipient.userRegistered	Boolean indicator as to whether QuickFile recipient is registered or not
QF.serverName	QuickFile server name
QF.serverOS	QuickFile server operating system
QF.serverVersion	QuickFile version
QF.statusCode	QuickFile event status code

Event variable	Description
AF.userEmail	User email address
QF.userFullName	User full name
QF.userId	User ID
QF.userRegistered	Boolean indicator as to whether QuickFile user is registered or not. Vales are true | false
QF.utcOffset	UTC offset of QuickFile server

Chapter 28. Monitor MQ MFT file transfers

MQ MFT activity consists of file transfers between MQ MFT agents and execution of commands on the source or destination agent.

The MQ MFT coordination queue manager logs the results of these operations in to the appropriate topic in MQ (SYSTEM.FTE). Sterling Control Center subscribes to the MQ topic (and its subtopics). Sterling Control Center handles these messages in the following ways:

- Consumes them
- Converts them into Sterling Control Center events by an MQ MFT node service that is created to monitor MQ MFT servers
- Passes them on to the Metadata Rule Service, Rule Service, Data Visibility Service, SLC Service, and other Sterling Control Center internal services

Queued Process Activity Monitor

Inflight file transfers may or may not display in the Queued Process Activity Monitor depending on the following factors:

- The file transfer is so quick that MQ MFT does not generate a progress event for the transfer.
- The file transfer completes quickly.
- The monitor rest time that is specified for the MQ MFT node service prevents the transfer from displaying.

Completed Process Activity Monitor

MQ MFT allows multiple files to be transferred in a single request. Each of the files transferred is treated by Sterling Control Center as separate steps within the same process. So, when you choose Select Statistics on a completed process, you see the following steps:

- Process Started
- Step Started
- Step Ended
- Step Started
- Step Ended
- :
- Process Ended

Attention: Sterling Control Center activities that use ANT scripts produce a separate process for each ANT step.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

19-21, Nihonbashi-Hakozakicho, Chuo-ku

Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be

incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA 95141-1003

U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© IBM 2013. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2013.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Connect Control Center®, Connect:Direct®, Connect:Enterprise, Gentran®, Gentran®:Basic®, Gentran:Control®, Gentran:Director®, Gentran:Plus®, Gentran:Realtime®, Gentran:Server®, Gentran:Viewpoint®, Sterling Commerce™, Sterling Information Broker®, and Sterling Integrator® are trademarks or registered trademarks of Sterling Commerce®, Inc., an IBM Company.

Other company, product, and service names may be trademarks or service marks of others.

Index

A

account lockout policy
  configuring 39
action
  field descriptions 77
  predefined 169
actions
  adding a list of email addresses 76
  creating 74
  displaying the listing 76
  exporting email addresses 114
  importing email addresses 75
  inserting variables 75
  modifying 76, 114
  overview 72
  predefined 85
  sorting email addresses 76
adding
  server 45
administering other systems 145
application log
  field description 140
application log settings 133
application programming interface 18
audit log
  obtaining for an object 5
auto refresh settings 141

B

buttons 1

C

calendar
  viewing or modifying 110
calendar example
  Monday through Friday processing 111
calendar field descriptions 110
calendar schedule
  creating a metadata 105
  creating a rule calendar schedule 104
calendar schedule template 13
calendars
  creating a 108
  overview 108
  recurrence patterns 109
CCAPI 17, 18
CCClient.log4j file sample 227
CCEngine.log4j file sample 225
certificate expiry notification setting
  field description 140
changing order 72
checkpoint data
  safeguarding 234
comments
  adding discovered node 129
configuration management
  message IDs 184
configuration objects
  copying between installations 19
  copying between Microsoft Windows installations 21
  copying between UNIX installations 20
console
  using efficiently 152
console settings
  field descriptions 141
Create Simple SLC Group Wizard 99
creating 99
  SLCs 82
creating milestones 96
cross-referencing objects 8

D

data visibility group 25
  create 25
  display listing 26
  field descriptions 26
  viewing or changing 26
data visibility groups
  using to view rule sets 69
  view SLC groups by 83
database
  general tuning 153
database administration 147
  automatically maintain 147
  move bulk data to staging database 147
database server
  tuning 153
database settings 133, 135
  changing 135
DB2 databases
  tuning 155
deleting
  licenses 63
Discovery List
  moving server from My List to 128
  overview 127
  removing server 130
duplicating objects 4
duration schedule template 13
DVG 25

E

e-mail schedule template 13
email address
  sorting 76
email list
  field descriptions 115
email lists
  creating 113
  exporting email addresses 113
  overview 113
Email lists
  displaying listing 114
email settings 133
email system settings 138
enabling or disabling
  schedules 108
Engine connection system setting 141
engine failures
  non-SAN procedure 234
event type descriptions 157
event types
  Sterling Connect:Direct statistic record ID cross-reference 160
Event types 157
Explorer list
  adding a managed server 124
  adding an unmanaged server 124
Explorer List
  moving a server to 128
  removing a server 126
expressions 91

F

failover
  non-SAN engine failure 235
  non-SAN primary database server failure 236
  non-SAN production engine and primary database server failure 237
  safeguarding managed server's checkpoint data 234
failover configuration 229
  SAN database server failure 232
  SAN engine failure 231
  testing standby engine 235
  when the engine is installed on a SAN 230
field definitions 135
  license push 64
Field definitions
  license import 63
fields 239
File Agent
  field descriptions 144
File agents
  monitoring 49
filtering objects 2

G

Graphic Activity Monitor 141
guided node discovery 123
  adding a managed server to the Explorer List 124
  adding an unmanaged server to the Explorer List 124

I

importing
licenses 62
inactivity timeout 141
inactivity warning message 141

K

keys 239

L

license import field definitions 63
license management
field descriptions 144
license push field definitions 64
licenses
comparing 63
deleting 63
importing 62
importing automatically 65
managing 62
pushing to servers 64
viewing 63
log files
retaining by modifying log4j 225
log4j 225
log4j files samples
parameters modified 228

M

managing
Sterling Control Center objects 1
maximum concurrent session count
resetting
maximum concurrent session count 59
servers 59
message IDs
configuration management 184
creating rules and SLCs using 173
general Sterling Control Center 179
QuickFile 176
Sterling B2B Integrator 178
Sterling Connect:Direct 173
Sterling Connect:Direct File Agent 179
Sterling Connect:Enterprise 173
Sterling Connect:Express 176
Sterling File Gateway 179
Message IDs
rules 179
Sterling Connect:Enterprise 174
Message list
field descriptions 95
message lists
overview 94
workflow SLCs 94
message lists for workflow SLCs
creating 94
metadata
creating a calendar schedule 105
managing type matching 120
overview 117
metadata actions
creating 121
displaying 122
overview 121
viewing and editing 122
metadata rules
creating 117
displaying list 118
enabling 119
field definitions 120
reordering 119
viewing or modifying 118
Microsoft Windows installations
copying configuration objects 21
milestone field definitions 97
milestones
creating 96
modifying 96
modifying milestones 96
MQ MFT
monitoring file transfers 265
MS SQL servers
tuning 155
multiple object
batch creation utility 9
creating 9
multiple objects
creating using the sample script 10
My List
moving server from Discovery List to 127
overview 127
removing server 130

N

new objects
adding 3
node configuration
permissions 33
node discovery 123
disabling a server for 125
enabling servers for 125
identifying servers for 123
running 126
viewing or modifying server definitions after 125
Node Discovery
showing a list of partners 129
Node Discovery List
server status icons 127
non-SAN scenario
engine server and database server fail 237
engine server fails 235
primary database server fails 236

O

object listings
printing 6
saving object listings 6
object properties
checking 4
objects
creating and maintaining 17
objects *(continued)*
cross-referencing 8
duplicating 4
filtering 2
removing 8
saving listings 7
operation system commans template 13
Oracle databases
tuning 154

P

Partners Table
showing a list of partners 129
password policy
modifying 40
sample 41
setting 40
performance 156
permissions 31
node configuration 33
predefined actions 79
predefined actions and rules 169
using 85
predefined rules 79
preferences
setting console 141
printing object listings 6

Q

QuickFile
message IDs 176
monitoring file transfers 261

R

recurrence patterns in calendars 109
refresh monitors 141
regular expressions 193
removing
servers 59
removing objects 8
report
criteria 239
reports overview
overview 131
retaining
log files 225
roles
creating 34
field descriptions 35
managing 31
permissions 31
viewing or changing 35
roles listing 35
rule
criteria 239
rule sets
viewing by data visibility group 69
rules 72
creating 67
creating a calendar schedule 104
creating metadata 117
disabling 72
enabling 72

rules *(continued)*
field descriptions 70
overview 67
predefined 85, 169
using message IDs 173
viewing or modifying 70
Rules listing 69
rules template 13

S

SAN scenario
engine server and database server fail 233
saving listings of objects 7
schedule
creating an SLC duration 105
enabling or disabling 108
field descriptions 106
schedule properties
viewing or modifying 106
schedules
displaying schedules listing 106
overview 103
schedules listing 106
server
adding a 45
field descriptions 49
server group definition
viewing or changing 60
server groups
creating 59
managing 59
removing 60
servers
identifying for node discovery 123
license management 62
pushing licenses 64
removing 59
viewing or changing properties 47
services
field descriptions 140
Services setting 140
settings
application log 133
database 133
email 133
SNMP hosts 133
Settings
services 140
simple SLC group 99
viewing or modifying 100
simple SLC groupsimple SLC group
disabling 100
enabling 100
simple SLCs
about simple SLCs 98
Create Simple SLC Group wizard 99
SLC
criteria 239
SLC calendar schedule
creating 103
SLC duration
creating a schedule 105
SLC group
simple 81
standard 81
SLC group *(continued)*
types 81
wildcard 81
workflow 81
SLC group listing
displaying 83
SLCgroups
view by data visibility groups 83
SLCs
adding schedules 84
creating 82
creating a simple SLC group 99
creating a workflow SLC group 91
creating multiple 85
creating workflow SLC milestones 96
disabling 84
enabling 84
modifying workflow SLC message lists 95
modifying workflow SLC milestones 96
QuickFile considerations 81
removing schedules 84
using message IDs 173
viewing or modifying properties 84
viewing or modifying simple SLCs 100
workflow SLC message lists 94
workflow SLC milestone field definitions 97
SNMP host
adding 138
editing 139
removing 139
SNMP host settings 138
field definitions 139
SNMP hosts
settings 133
standard SLC
field descriptions 87
standard SLC group
creating 85
exporting information 89
importing information 88
Standard SLC groups template 13
standard SLCs
QuickFile considerations 81
standby engine
testing 235
Statistics viewer
Sterling File Gateway 260
Sterling B2B Integrator
accessing 145
collecting process data 256
message IDs 178
using collected process data 256
Sterling B2B Integrator cluster
monitoring through a load balancer 48
monitoring via an individual connection 47
Sterling B2B Integrator server
monitor 255
Sterling Connect:Direct
message IDs 173
Sterling Connect:Direct Browser User Interface
accessing 145
Sterling Connect:Enterprise
message IDs 173
Sterling Connect:Express
message IDs 176
Sterling Control Center buttons 1
Sterling Control Center console
setting preferences 141
Sterling Control Center objects 1
Sterling Control Center settings 133
Sterling File Gateway
accessing 146
mapping terms to Sterling Control Center terms 260
monitoring file transfers and activities 259
viewing activities 259
viewing source information 260
superuser role
restoring manually 36
system server groups
resolving naming conflict 61
system settings
changing 134, 141
System settings
engine connection 141

T

templates
calendar schedule 13
creating custom 16
duration schedule 13
e-mail schedule 13
operation system command 13
rules 13
standard SLC groups 13
wildcard SLC groups 13
testing standard wildcard and regular 91
troubleshooting system issues 165
tuning
additional reference information 156
DB2 databases 155
MS SQL servers 155
Oracle databases 154
performance 149
Sterling Control Center 149
tuning the engine 149

U

UNIX installations
copying configuration objects 20
user
field descriptions 39
viewing and changing information 38
users
adding 37
managing 37

V

variables 195
  by event type 212
  server type 195

W

wildcard SLC
  field descriptions 87
wildcard SLC group
  creating 90
Wildcard SLC groups template 13
wildcard SLCs
  QuickFile considerations 81
Workflow SLC
  field descriptions 92
workflow SLCs 96
  creating 91
  message lists 94
Workflow SLCs
  milestone field definitions 97
workflow SLCsmodifying a message
 list 95

Product Number: 5725-D02

Printed in USA