Sterling Control Center™

Reports Guide

Version 5.2

Sterling Commerce
An IBM Company

Sterling Control Center Reports Guide
Version 5.2

First Edition

Contents

Chapter 3   Display the Log Files   83

Chapter 4   Sample Reports in Crystal Reports Format   85

Chapter 5   Data for Third-Party Reporting Tools   109

Chapter 1

Reports Overview

There are four main types of Sterling Control Center reports:

✦ Standard Sterling Control Center reports are produced from the 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 e-mail (**Reports** > **Automate**).

The Audit Log is a standard report of changes made to 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 Control Center databases if you already have Crystal Reports. You can also use these samples as templates to design your own reports. Chapter 5, *Data for Third-Party Reporting Tools* provides details of database schemas, including database tables and field definitions.

✦ Log file printouts are helpful for troubleshooting installation problems and other support-related issues. The log files are stored in the ..\log subdirectory of the Sterling Control Center installation directory. They can be accessed easily from the Tools menu on the Control Center console (by selecting **Tools** > **Trace Logs**).

✦ The SLC Debug Report is useful for troubleshooting an SLC. This report includes the SLC definition, definition of all schedules referenced by the SLC, related SLC events produced for the SLC, definition of rules triggered by the SLC events generated, definition of actions taken by triggered rules, and the email system settings for the engine. This report is initiated from the Control Center Console (by selecting **Tools > Run SLC Debug Report**).

Standard Reports

This chapter discusses the following subjects and procedures:

◆ About Standard Reports
◆ Create Reports
◆ Run Reports on Demand
◆ View or Modify Report Details
◆ Automate Reports
◆ Standard Reports: Configuration Management
◆ Standard Reports: Monitoring
◆ Standard Reports: Node Discovery
◆ Standard Reports: System

About Standard Reports

Sterling Control Center includes a number of standard reports which you can create on demand or via automation. Grouped into four categories, the report types include:

Report Category	Report Name	
Configuration Management	◆ Functional Authorities Report	◆ Secure+ Cipher Suites Report
	◆ Initialization Parameters Report	◆ Secure+ Key Certificates Report
	◆ Netmap Communication Paths Report	◆ Secure+ Nodes Report
	◆ Netmap Modes Report	◆ Secure+ Trusted Certifications Report
	◆ Netmap Nodes Report	◆ User Proxies Report
Monitoring	◆ Connect:Direct Process Statistics Details	◆ Sterling File Gateway Route Detail by Producer
	◆ Connect:Direct Process Statistics Summary	◆ Sterling File Gateway Route Detail by Consumer
	◆ Connect:Direct Statistics Log Report	◆ Sterling Integrator Business Process Details
	◆ Connect:Enterprise Batch Statistics Details	◆ Sterling Integrator Business Process Summary
	◆ Connect:Enterprise Batch Statistics Summary	◆ Sterling Integrator File Transfer Report
	◆ Connect:Enterprise Statistics Log Report	◆ High Watermark Report
	◆ FTP File Transfer Report	◆ File Agent Process Submission Report
Node Discovery	◆ Potentially Inactive Netmap Entries Report	◆ Netmap Connections Summary Report
	◆ Potentially Missing Netmap Entries Report	◆ Node Discovery Topology Report
System	◆ Alerts Report	◆ Server Inventory Report
	◆ Audit Log Report	◆ Server Status Report
	◆ Control Center License Report	◆ Service Level Criteria Summary Report
	◆ Database Events Report	◆ Users-Roles Summary Report
	◆ Monthly File Transfer Activity Report	

Create Reports

To generate a Control Center report:

1. Select **Tools > Reports > Define/Run** to display the **Report Listing**.

2. Click + to display the **Create Report** dialog.

3. Select the report category and type you want to create.

4. For Configuration Management reports, to include non-current versions of configuration objects in reporting, check Allow Selection of Non-current Versions. If you do not click this option, only current versions of configuration objects are included.

5. Click **Next**.

6. To limit a report to certain criteria, specify those criteria and click **Next**.

Note: Specifying the same Key value more than once is treated as an AND condition. **Example:** To narrow an Alerts report to a date/time range, specify report criteria similar to the following:

Alert Date/Time - Greater Than - Sept 30, 2010 00:00:00 America/Chicago
Alert Date/Time - Less Than -Today 00:00:00 America/Chicago

For more, see *About Report Criteria* on page 12 and *Define Report Criteria* on page 12.

Note: Not all reports allow you to specify criteria to narrow the report or to specify parameters.

---

7. In the **Available Columns** window, highlight the columns you want to appear in the report and click >.

8. In the **Selected Columns** window, change the sort order of columns by selecting the column name and clicking **Move Up** or **Move Down**.

9. The default sort order within columns is ascending. To sort a column in descending order, highlight the column name and select ⬇.

10. If you want to limit the report to a maximum number of records, type a value (up to 5000) in the **Max Records Returned** field.

11. Click **Next**.

12. Click **Run Report** to generate the report. The report is displayed in a separate window called the **Reports Viewer**. Familiar standard icons allow you to print or reload the report, navigate through its pages, or change the report magnification percentage.

13. To save the report output as displayed in the Report Viewer, click 🖫, type a **File Name**, click **File Type** to choose a different export format (if needed), and click **Save**.

14. Click ❌ to close the report output. The Save Report panel of the Create Report wizard is displayed.

15. To save the report, type a **Name** and optional **Description** and click **Save**.

16. Click **Close** to close the Run Report window.

About Report Criteria

When you create or modify a report, the output may be limited by one or more filter criteria. At least one criterion is required. The available criteria depend on the report type selected. For many reports, the list of filter criteria is equivalent to the report's available columns. See individual report descriptions for details.

When filtering on Server or Server Group, you select from a list of managed servers/groups. For Date and Time you select Relative to identify a date/time relative to report generation time, or Absolute to select a specific date and time.

Wildcard characters can be used in the selection criteria for some reports. Wildcard characters are as follows:

Wildcard Character	Meaning
*	From this point to the end of the value the characters can be any combination. **Example 1**: 'C*' represents any value that begins with the letter C. **Example 2**: 'proc*' represents any value that begins with the letters 'proc'.
?	The individual character in this exact position can be any character.

Define Report Criteria

To limit report output based on one or more criteria:

1. From the **Report Listing** window, double-click the report to modify or click **Create** to create a new report.
2. Do one of the following:
   ◆ If you are modifying an existing report, click the **Filter** tab and select the criteria used to limit the report output in the **Key** field.
   ◆ If you are creating a new report, follow the prompts. When prompted for Filters, select a filter criterion to use in the **Key** field.
3. Select the operator to use to further define the criteria. Choices of operator depend on type of data. For example, numeric-based keys typically take an operator of "equal to," 'not equal to," "greater than," or "less than," while character-based keys take operators of "matches," "doesn't match," and "contains."

   Note: Some reports also allow the use of wildcard characters in the selection criteria. See *About Report Criteria* on page 12.

4. Click the cell in the **Value** column and enter or select an argument to finish defining the filter criterion.
5. Repeat steps 2 through 4 to define multiple selection criteria. Multiple criteria must all be true for a record to be selected (they result in a logical AND condition).

6. Do one of the following:

    ◆ If you are modifying an existing report, click **Update**.

    ◆ If you are creating a new report, follow the prompts to complete the report. Refer to *Create Reports* on page 11.

View or Modify Report Details

To view or change report output:

1. Select **Tools > Reports > Define/Run**.

2. Double-click the report to view or modify.

3. Modify fields as necessary.

4. Click **OK**.

Run Reports on Demand

To run a report:

1. From the Sterling Control Center menu, select **Tools > Reports > Define/Run** to display the **Report Listing** window.

2. Select the report you want to run and click **Run Report**, or, to define a new report, click **+**, and follow the prompts (see *Create Reports* on page 11). The **Report Output** window is displayed. Icons in the report task bar allow you to save, print, or reload the report, navigate through its pages, or change the degree of magnification.

3. To save the report, click 🖫. Type a **File Name**, click **File Type** to choose a different export format, and click **Save**. File types to which you can export a report include the following:

   ◆ PDF

   ◆ RTF* ODT (Open Document Text)

   ◆ HTML

   ◆ Excel XLS (single sheet or multiple sheets)

   ◆ Comma-separated file (CSV)

   ◆ XML

   ◆ Embedded images XML

4. Click ❎ to close the report, then click **Close** to close the **Report Listing** window.

Customize a Report

Once you create and save a report definition, you can run it any time. A report definition identifies the criteria used to create the report output. Use the customize option to modify a report definition.

To customize a report:

1. Select **Tools > Reports > Define/Run**.

2. Highlight the report you want to customize and click 📝.

3. Make changes as necessary to the existing filter criteria and click **Update**.

4. Click **Run Report** 📄 to generate the report. Report output is displayed in a separate window.

5. To print the report, click 🖨, select print properties, and click **OK**.

6. To close the report output window, select ❎.

7. To save the report, type a report name and description and click **Save**.

8. Click **Close** to close the **Report Listing** window.

Print a Report

To print a report:

1. Select **Tools > Reports > Define/Run**.

2. Highlight the report you want to print.

3. Click **Run Report** to generate the report. The report is displayed in a separate window.

4. To print the report, click , select print properties, and click **OK**.

Remove a Saved Report

To remove a saved report:

1. Select **Tools > Reports > Define/Run**.

2. Highlight the report you want to remove and click **-**.

3. Click **OK** to remove the report.

4. Click to close the **Report Listing** window.

Note: You cannot delete a report that is referenced by an automated report.

Automate Reports

You can automate standard Control Center reports to run according to a defined schedule and be sent to a list of email recipients.

Note: For UNIX systems, you must have an X11 graphics package on the UNIX host where the Control Center engine is installed and a video card for graphics.

To automate a report:

1. Click **Tools** > **Reports > Automate**. The Automated Report listing displays.

2. Click **+**. The **Add Automated Report** wizard displays.

3. Supply a **Name** and **Description** for the automated report and check **Enabled** to enable it. Name is required. See *Automated Reports Field Definitions* on page 17 for detailed field descriptions.

4. To schedule an existing report, highlight the report in the Reports list and click **>**. To create a new report to schedule, click **+**. (See *Create Reports* on page 11 for more.) To create a new report to schedule using an existing report as a starting point, select the report and click 🗈 . Click Next.

5. Select a **Report Schedule** and click **>**. Then click Next. Or, create a new schedule (click **+** under the schedule list) or duplicate an existing one (click 🗈 under the schedule list).

6. Select a list of email recipients and click **+**. Then click Next. (You can also add or duplicate an email list). See *Maintain Automated Reports Email Lists* on page 18.

7. Select a **Report Format** and report **Attachment Extension**. You can leave off the extension or modify it to circumvent email attachment restrictions. Add a **From** email address and a **Subject** line and click Next.

8. Review your entries and click **Finish** to create the automated report.

Automated Reports Field Definitions

Following are descriptions of automated reports fields.

Field	Description
Name	Automated report name.
Description	A description of the automated report.
Report Schedule	The schedule attached to the automated report. The schedule determines when the automated report is generated and sent.
(List of recipients)	The name of the list or lists of email recipients for the automated report.

Field	Description
Report Format	Format of the automated report. Options are comma-separated (CSV), portable document format (PDF), or Excel spreadsheet (XLS).
Attachment Extension	The file type or extension of the report file. You can specify no file type or an alternative type which can later be changed by the recipient to circumvent firewall restrictions.
From	The "from" address to be specified in the email.
Subject	The subject line of the email.

Maintain Automated Reports Email Lists

Automated reports are generated and sent via email to lists of addressees. You can maintain these lists of email addressees. Because you can specify more than one email list for an automated report, you can maintain a list specifically for a given report or construct the list from multiple email lists.

To create an email list:

1. Click **Manage** > **Email Lists**.

2. Click +.

3. Add a **Name** (required) and **Description** for the new email list and click Next.

4. In the Email wizard panel, add email addresses to whom you want to send one or more generated reports, separating the addresses with commas. You can click **Import** to import a text file of email addresses. You can also click **Export** to export an email list to an external text file. Click Next when finished adding addresses.

5. Limit the roles to grant permission to see and use this email list by selecting a role in the list of All Roles and clicking **>**. Filter the list of roles by typing a filter criterion in Filter. Click Next.

6. Click **Finish** to finish creating the email list.

Later, when you create or modify an automated report, you can add this email list to the list of addressees to receive the report.

Automated Reports Frequently Asked Questions

Following are solutions to issues that might arise with automated reports.

What could cause an automated report not to be delivered?

If an automated report fails to be delivered as expected, check for these conditions:

✦ The email server could be down. Make sure it is up.

✦ The output attachment size could exceed the limit allowed by the email server.

✦ Email servers may strip attachments with certain extensions. To prevent this from happening, double-click the report in the Automated Reports listing, click the Parameters tab, and change the Attachment Extension. Inform recipients to change the file's extension back after receiving it via email to reflect the report's format.

✦ Email settings may not have been set up. Check on the Email tab of System Settings (on the Manage menu).

✦ Make sure that the report schedule is correct.

If you are still having problems, look in the engine log file for errors.

Are there best practices to follow for automated reports?

It is a good idea to schedule automated reports to run when less activity is occurring on managed servers. This reduces the impact of report generation on normal monitoring activity.

Standard Reports: Configuration Management

Sterling Control Center features reports that describe aspects of Control Center server configuration management. These reports include:

◆ Functional Authorities Report	◆ Secure+ Cipher Suites Report
◆ Initialization Parameters Report	◆ Secure+ Key Certificates Report
◆ Netmap Communication Path Report	◆ Secure+ Nodes Report
◆ Netmap Modes Report	◆ Secure+ Trusted Certificates Report
◆ Netmap Nodes Report	◆ User Proxies Report

The following sections describe the available standard report types related to configuration management. Sample reports are shown.

Functional Authorities Report

The Functional Authorities Report lists details about the functional authorities that have been set up for Connect:Direct servers added to Control Center.

The following table describes the report columns:

Column	Description
Server Name	Name of the selected server.
Functional Authority Name	The name of the functional authority.
Version	Version of the functional authority.
Parameter	The functional authorities parameters selected for this report.
Value	Parameter value.

Parameters you can choose to report on in the Parameter column can be found in the "Functional Authorities" chapter of the *Sterling Control Center Configuration Management Guide*.

Following is a sample report:

Functional Authority Report

Server Name	Functional Authority Name	Version	Parameter	Value
ccdev02_44_0	*admin	2008/08/12 16:58:18	Admin	Y
			User Authority	Y
			User ID	*admin
			User Proxy	Y
ccdev02_44_0	*GENUSR	2008/08/12 16:58:18	Admin	N
			User Authority	N
			User ID	*GENUSR
			User Proxy	N
ccdev02_44_0	cduser	2008/08/12 16:58:18	Admin	
			User Authority	Y
			User ID	cduser
			User Proxy	Y
ccdev02_44_0	pgounder	2008/08/12 16:58:18	Admin	Y
			User Authority	Y
			User ID	pgounder
			User Proxy	Y

Page 2 of 2

Tue Aug 12 17:09:33 CDT

Initialization Parameters Report

The Initialization Parameters Report lists initialization parameter (initparm) values for selected servers. The listing is broken down by server and initialization parameter version.

The following table describes the report columns:

Column	Description
Server Name	Name of the selected server.
Initialization Parameters Name	This column simply reflects that the object being reported upon is initialization parameters.
Version	Version of the initialization parameters. Version indicates the date and time that the initialization parameters were last changed.
Parameter	The specific initialization parameters that were selected for the report.
Value	Parameter value.

The set of parameters you can choose to report on in the Parameter column vary depending on server operating system. Definitions of the parameters can be found in the console in the form of tooltips. When you hover the cursor over an initialization parameter its definition displays. You can find further detail on initialization parameters in the Connect:Direct documentation set for the relevant platform (z/OS, UNIX, or Windows).

Following is a sample report:

Initialization Parameters Report

Server Name	Initialization Parameters Name	Version	Parameter	Value
CDW44.W2003.VM	Initialization Parameters	2008/09/23 11:34:08	active.directory.enabled	N
			ckpt.interval	10240K
			comm.bufsize	65535
			conn.retry.ltattempts	10
			conn.retry.ltwait	00:03:00
			conn.retry.stattempts	10
			conn.retry.stwait	00:00:10
			contact.name	not specified
			contact.phone	not specified
			continue.on.exception	N
			descrip	no description specified
			disable.cache	N
			download.dir	C:\Program Files\Sterling Commerce\Connect Direct v4.4.00\Server\DOWNLOAD\"
			ecz.memlevel	4
			ecz.windowsize	13
			event.log	All
			exec.prio.default	7
			file.exit	<None>
			license.management.key	C:\Program Files\Sterling Commerce\Connect Direct v4.4.00\Server\directLMkey2008.txt
			log.commands	Y
			log.select	N
			max.api.connects	10
			name	CDW44.W2003.VM
			netmap.check	N
			node.check	B
			notify.level	A
			outgoing.address	<None>

Page 1 of 8

Tue Sep 23 11:34:20 CDT

Netmap Nodes Report

The Netmap Nodes Report lists all nodes in the netmap of selected servers.

The following table describes the report columns:

Column	Description
Server Name	Name of the selected server.
Netmap Node Name	The name of the netmap node.
Version	Version of the netmap node.
Parameter	The netmap node parameters selected for this report.
Value	Parameter value.

Parameters you can choose to report on in the Parameter column can be found in "Managing Netmap Nodes" in the *Sterling Control Center Configuration Management Guide*.

Following is a sample report:

Netmap Node Report

Server Name	Netmap Node Name	Version	Parameter	Value
u_phoenix	b3800	2008/08/12 13:10:21	Contact Name	<None>
			Contact Phone	<None>
			LU62 Profile Name	phoenix
			Max PNODE Sessions	255
			Max SNODE Sessions	255
			Node Name	b3800
			Session Type	
			Short Term Retries	3
			Short Term Retry Interval	00:00:30
			TCP Address	phoenix
			TCP Port	3814
u_phoenix	c38	2008/08/12 13:10:21	Contact Name	
			Contact Phone	
			LU62 Profile Name	phoenix
			Max PNODE Sessions	255
			Max SNODE Sessions	255
			Node Name	c38
			Session Type	
			Short Term Retries	3
			Short Term Retry Interval	00:00:30
			TCP Address	phoenix
			TCP Port	3824
u_phoenix	c3800	2008/08/12 13:10:21	Contact Name	
			Contact Phone	
			LU62 Profile Name	phoenix
			Max PNODE Sessions	255
			Max SNODE Sessions	255

Page 2 of 4   Tue Aug 12 17:22:43 CDT

Netmap Modes Report

The Netmap Modes Report lists the netmap modes associated with selected servers.

The following table describes the report columns:

Column	Description
Server Name	Name of the selected server.
Netmap Mode Name	The name of the netmap mode associated with the server.
Version	Version of the netmap mode.
Parameter	The netmap mode parameters selected for this report.
Value	Parameter value.

Parameters you can choose for the Parameter column can be found in "Managing Netmap Modes" in the *Sterling Control Center Configuration Management Guide*.

Following is a sample report:

Netmap Mode Report

Server Name	Netmap Mode Name	Version	Parameter	Value
w_winbody44	Mode1	2008/08/12 17:17:41	Buffer Size	65535
			CRC	
			Max Pacing Size	0
			Max RU Size	65535
			Max Sessions	0
			Mode Name	Mode1
			Pacing Send Count	0
			Pacing Send Delay	0
			Protocol	TCP/IP

Page 2 of 2

Tue Aug 12 17:19:28 CDT

Netmap Communication Path Report

The Netmap Communication Path Report lists communication paths (comm paths) associated with the nodes in a server's netmap.

The following table describes the report columns:

Column	Description
Server Name	Name of the selected server.
Netmap Communication Path Name	The name of the communication path.
Version	Version of the communication path.
Parameter	The communication path parameters selected for this report.
Value	Parameter value.

Parameters you can choose to report on in the Parameter column can be found in "Managing Netmap Communication Paths" in the *Sterling Control Center Configuration Management Guide*.

Following is a sample report:

Netmap Communication Path Report

Server Name	Netmap Communication Path Name	Version	Parameter	Value
			Netmap Communication Path Name	TCPCommPath
			Protocol	TCP/IP
			Remote Address	000000000000
jlegel-DT4400	TCPPath2	2008/09/22 17:37:51	Adapter Number	Primary
			Local SNA Network	
			LU Name	
			Mode	Mode2
			Netmap Communication Path Name	TCPPath2
			Protocol	TCP/IP
			Remote Address	000000000000

Page 2 of 3

Mon Sep 22 17:37:51 CDT

Secure+ Nodes Report

The Secure+ Nodes Report lists details about the Secure+ Nodes used by selected servers to move data securely.

Following are the columns included in this report:

Column	Description
Server Name	Name of the server.
Secure+ Node Name	Name of the key certificate.
Version	Version of key certificate.
Parameter	Parameters to include in the report.
Value	Value of the parameter in question.

Possible parameters to include in this report are defined in "Managing Secure+ Nodes" in the *Sterling Control Center Configuration Management Guide*.

Following is a sample report:

Secure+ Node Report

Server Name	Secure+ Node Name	Version	Parameter	Value
hpag4000sp	.Client	2008/09/22 14:18:14	Certificate Label	/svshare/CDSP/certs/openssl/cdwopsxp01_1024_keycert.txt
			Certificate Validation Definition	
			Client Authentication	N
			Enabled Protocol	SSL
			Host Name	
			Node Name	.Client
			Port Number	
			Trusted Cert Label	/svshare/CDSP/certs/openssl/OpenSSLCAcert.txt
			Use External Authentication	
hpag4000sp	.Local	2008/09/22 14:18:14	Certificate Label	/svshare/splus/certs/selfsigned/nokeyext/1024NESSkeycert.txt
			Certificate Validation Definition	
			Client Authentication	N
			Enabled Protocol	TLS
			Host Name	
			Node Name	.Local
			Port Number	
			Trusted Cert Label	/svshare/splus/certs/selfsigned/nokeyext/1024NESScert.txt
			Use External Authentication	N
hpag4000sp	.SEAServer	2008/09/22 14:18:14	Certificate Label	
			Certificate Validation Definition	
			Client Authentication	
			Enabled Protocol	DefaultToLN
			Host Name	
			Node Name	.SEAServer
			Port Number	61366
			Trusted Cert Label	

Page 1 of   161   Mon Sep 22 14:18:26 CDT

Secure+ Key Certificates Report

The Secure+ Certificates Report lists Secure+ key certificates (certs).

The following table describes the report columns:

Column	Description
Server Name	Name of the server.
Secure+ Key Certificate Name	Name of the key certificate.
Version	Version of key certificate.
Parameter	Parameters to include in the report. These include Data, Label Name, and Passphrase.
Value	The data contained in the certificate.

Parameters you can choose to report on in the Parameter column can be found in "Managing Secure+ Nodes" in the *Sterling Control Center Configuration Management Guide*.

Following is a sample report:

Secure+ Key Certificate Report

Server Name	Secure+ Key Certificate Name	Version	Parameter	Value
hpag4000sp	/svshare/CDSP/certs/openssl/cdwopsxp0 1_1024_keycert.txt	2008/09/22 14:14:43	Data	-----BEGIN ENCRYPTED PRIVATE KEY----- MIICoTAbBgkqhkiG9w0BBQMwDgQI5QMkMDZwLSsCAggABIICgO7wVA CCxP4FgFzg AepU65D2FqRY/U25C+Cex5TNcutoFAUy3q831a5YzhNIUZAdIF9X1H4d8 2YwAVOO gQ5t8WyWGBEZo6hMY4a0sy4TX8df5U4LbhbmthLGNjU6Hk0Ox0vH2Hg Gcz6KN1SG MQYNqjwKaWDFnw4kOwwoJHCAKW0NCzYui3dTPfSbM6eR4cT7y56rS4 p7n0uXxEoV Eq0hZVJI+swEWDysEs226owonOy+tkbyn3V03Bu9Ez2aEMbWnNCsElaan g5dL4WC z7gMqXfEClTybrQTMD1z6HVh82cRf5f4yO4vyzq+if7muCtZOke6xRhOrTV O1rN2 qYT4KjUxrkk8jwK0kMJDYEgFrznF4AuRkT4POXvufvuBgBolbyGoH2eJAR cHqDRP iPMuGLd+FSDSV8/nCfSPy1paYDsmqPxMjTRhyVJ06marduTmVw8bXdA Gi6T4TeJM TblMkFodHS9mSp9c6C+jMc1lBGgNpu8XzpWkiqjgTYYNHgIzJoKKARQZdl bvu2+p 94ONLjVhCuGecCWgIKRpbaehGqrad+k4y2abJeru4A/z0J5g1BeY/gQSpC/ PVvSC AwxYgLsbNuiJ7mRNUwlBW++p8egeZ7tj4hQD2nBoQmmHT/hh+Td+wkfZ 5iJY5T2d n1f6u6yranK+Gd0ntdqXHSuW2VeXdua3Kcsv6Q+SMXPSy5l/fVnV9I5CBz dREVc2 TUr2pPM14J3wRsa5V6Gl9zmg+zjA4OHIxU+PWXncCZZ0wkencNHdr0ah 0yr/yl8A k/HQjni8eeqN7qOWhY/Xe+7uf0BU0qWhqfIzvTzA9B8gdPTw44V3QQ/bsY hdb/i1 E4PeuD0= -----END ENCRYPTED PRIVATE KEY----- -----BEGIN CERTIFICATE----- MIIDvjCCAyegAwIBAgIBezANBgkqhkiG9w0BAQQFADA8MQwwCgYDVQ QKEwNTQ0kx DzANBgNVBAcTBklydmluZzEOMAwGA1UECBMFVGV4YXMxCzAJBgNV BAYTAiVTMB4X DTA2MDYyMDE2MDAxOFoXDTE2MDYxNzE2MDAxOFowgYcxCzAJBgN VBAYTAiVTMQ4w DAYDVQQIEwVUZXhhczEMMAoGA1UEChMDU0NJMQswCQYDVQQLE wJTVjEkMCIGA1UE

Secure+ Trusted Certificates Report

The Secure+ Trusted Certificates Report lists available trusted certificates.

The following table describes the report columns:

Column	Description
Server Name	Name of the server.
Secure+ Trusted Certificate Name	Trusted certificate name.
Version	Version of trusted certificate.
Parameter	Trusted certificate parameter. Possible parameters include Data and Label. Data is the trusted certificate data itself. Label name is the name by which to identify the trusted certificate when it is imported.
Value	Parameter value.

Following is a sample report:

Secure+ Trusted Certificate Report

Server Name	Secure+ Trusted Certificate Name	Version	Parameter	Value
hpag4000sp	/svshare/CDSP/certs/openssl/OpenSSL CAcert.txt	2008/09/22 14:20:44	Data	-----BEGIN CERTIFICATE----- MIIClTCCAf6gAwIBAgIBADANBgkqhkiG9w0BAQQFADA8MQwwCgYDVQQKEwNTQ0kx DzANBgNVBAcTBklydmluZzEOMAwGA1UECBMFVGV4YXMxCzAJBgNVBAYTAlVTMB4X DTA1MDkxOTE2NTUxMFoXDTE1MDkxNzE2NTUxMFowPDEMMAoGA1UEChMDU0NJMQ8w DQYDVQQHEwZJcnZpbmcxDjAMBgNVBAgTBVRleGFzMQswCQYDVQQGEwJVUzCBnzAN BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAq39oHgKTG+VsrufLi/sKAAVxrWkyUQp+ L8Z55iO8KwNmP8VMlkfQCk+4fryu0OSimOMleS/b8owk154gLwNcjJKDHWsxPAFL VONZKhh9gbiVzM/PttBpsh2YMMg3sNjPLVj4ce1aMP2cw+TQkJITFDO9QDFwqx0C x+JqMi7T9JMCAwEAAaOBpjCBozAPBgNVHRMBAf8EBTADAQH/MAsGA1UdDwQEAwIB hjAdBgNVHQ4EFgQUGdgWBpZe/PkDiCaFmHTz5erN46gwZAYDVR0jBF0wW4AUGdgW BpZe/PkDiCaFmHTz5erN46ihQKQ+MDwxDDAKBgNVBAoTA1NDSTEPMA0GA1UEBxMG SXJ2aW5nMQ4wDAYDVQQIEwVUZXhhczELMAkGA1UEBhMCVVOCAQAwDQYJKoZIhvcN AQEEBQADgYEAp4MQopUhOdKDQTAtUEm8+2Q43QXwxSfFfgN1KW435qLqmR2wg8a7 h/lvZpxMoP7i3LNRZH9y3iNMgpIh8oyLnydnaWwUmUVV9YJueO+Ajlsfn6wTgHOv oduPCJLxK9ZIECmJqGfY1W1tsApypQHNo/kD+eGTleyjFvT9bvCKxzM= -----END CERTIFICATE-----
			Label Name	/svshare/CDSP/certs/openssl/OpenSSLCAcert.txt
hpag4000sp	/svshare/certs/CDTestCert.txt	2008/09/22 14:20:44	Data	-----BEGIN CERTIFICATE----- MIICsTCCAhqgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBkzELMAkGA1UEBhMCVVMx DjAMBgNVBAgMBVRleGFzMQ8wDQYDVQQHDAZJcnZpbmcxCzAJBgNVBAoMAlNDMQsw CQYDVQQLDAJRQTEgMB4GA1UEAwwXbGJua2vyLmNzZy5zdGVyY29tbS5jb20xJzAl BgkqhkiG9w0BCQEWGExhcnJ5X0Jha2VyQHN0ZXJjb21tLmNvbTAeFw0w

Page 1 of 89

Mon Sep 22 14:20:49 CDT

Secure+ Cipher Suites Report

The Secure+ Cipher Suites Report lists the cipher suites associated with Secure+ nodes.

The following table describes the report columns:

Column	Description
Server Name	Name of the server.
Secure+ Cipher Suite Name	Name of the cipher suite.
Version	Cipher suite version.
Parameter	Cipher suite parameter. These include SSL (Secure Sockets Layer) and TLS (Transport Layer Security).
Value	The possible values for the two parameters are true or false.

Following is a sample report:

Secure+ Cipher Suite Report

Server Name	Secure+ Cipher Suite Name	Version	Parameter	Value
hpag4000sp	SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	2008/09/22 14:11:50	Name	SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
			SSL	true
			TLS	true
hpag4000sp	SSL_DHE_RSA_WITH_DES_CBC_SHA	2008/09/22 14:11:50	Name	SSL_DHE_RSA_WITH_DES_CBC_SHA
			SSL	true
			TLS	true
hpag4000sp	SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	2008/09/22 14:11:50	Name	SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
			SSL	true
			TLS	true
hpag4000sp	SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5	2008/09/22 14:11:50	Name	SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
			SSL	true
			TLS	true
hpag4000sp	SSL_RSA_EXPORT_WITH_RC4_40_MD5	2008/09/22 14:11:50	Name	SSL_RSA_EXPORT_WITH_RC4_40_MD5
			SSL	true
			TLS	true
hpag4000sp	SSL_RSA_WITH_3DES_EDE_CBC_SHA	2008/09/22 14:11:50	Name	SSL_RSA_WITH_3DES_EDE_CBC_SHA
			SSL	true
			TLS	true
hpag4000sp	SSL_RSA_WITH_DES_CBC_SHA	2008/09/22 14:11:50	Name	SSL_RSA_WITH_DES_CBC_SHA
			SSL	true

Page 1 of 8

Mon Sep 22 14:12:01 CDT

User Proxies Report

The User Proxies Report lists the user proxies associated with selected servers.

The following table describes the report columns:

Column	Description
Server Name	Name of the selected server.
User Proxy Name	The name of the user proxy.
Version	Version of the user proxy.
Parameter	The user proxy parameters selected for this report.
Value	Parameter value.

Parameters you can choose to report on in the Parameter column can be found in the "Managing User Proxies" chapter of the *Sterling Control Center Configuration Management Guide*.

Following is a sample report:

User Proxy Report

Server Name	User Proxy Name	Version	Parameter	Value
u_phoenix	arajput@b3800	2008/08/12 17:22:44	Copy	
			Description	
			Download	yes
			Download Directory	
			Local User ID	pgoun1
			Process Directory	
			Program Directory	
			Remote Node	b3800
			Remote User ID	arajput
			Run Job	
			Run Task	
			Submit	
			Upload	yes
			Upload Directory	
u_phoenix	dande1@b3800	2008/08/12 17:22:44	Copy	
			Description	
			Download	yes
			Download Directory	
			Local User ID	dande1
			Process Directory	
			Program Directory	
			Remote Node	b3800
			Remote User ID	dande1
			Run Job	
			Run Task	
			Submit	
			Upload	yes
			Upload Directory	

Page 2 of 3   Tue Aug 12 17:24:36 CDT

Standard Reports: Monitoring

Sterling Control Center features reports that present details on the monitoring of Control Center managed servers. These reports include:

◆ Connect:Direct Process Statistics Details Report	◆ Sterling File Gateway Route Detail by Producer Report
◆ Connect:Direct Process Statistics Summary Report	◆ Sterling File Gateway Route Detail by Consumer Report
◆ Connect:Direct Statistics Log Report	◆ Sterling Integrator Business Process Details Report
◆ Connect:Enterprise Batch Statistics Details Report	◆ Sterling Integrator Business Process Summary Report
◆ Connect:Enterprise Batch Statistics Summary Report	◆ Sterling Integrator File Transfer Report
◆ Connect:Enterprise Statistics Log Report	◆ High Watermark Report
◆ FTP File Transfer Report	◆ File Agent Process Submission Report

The following sections describe the available standard report types related to server monitoring. Sample reports are shown.

Connect:Direct Process Statistics Details

The Connect:Direct Process Statistics Details report contains detailed statistics information about Processes occurring on managed Connect:Direct servers during a specified time period.The following table describes the report columns:

Column	Description
Bytes Sent	The number of bytes sent by the sending node.
Date Time	Date and time that the statistics records were generated.
Record ID	Record identifier (also known as statistic ID). See Event Type Descriptions in the *Sterling Control Center System Administration Guide* for a list of statistic IDs.
Server Name	Name of the managed server that generated the statistic record.
Remote Server	Name of other server involved in the Process.
Process Name	Connect:Direct Process name.
Process Number	Identification number assigned to the Process.
Return Code	Numeric code returned from a completed Process that indicates failure or success. The following are the standard return codes: ◆ 0 indicates successful completion ◆ 4 indicates a warning ◆ 8 indicates an error ◆ 16 indicates a catastrophic error
Message ID	Connect:Direct message identification number. See the appropriate product and platform documentation for a description of message IDs.
Message Text	Short message text associated with the message ID.
Destination File Name	Path and file name for the file received.

Following is a sample report:

Connect:Direct Process Statistics Details Report

Date / Time	Record ID	Server Name	Remote Server	Process Name	Process Number	Return Code	Message ID	Bytes Sent
2008/09/23 11:03:09.880	PI	Q1A47M1	L2GISW2K3.GIS43	PSHCDSA1	1	0		0
Destination File Name								
Message Text:								
2008/09/23 11:03:10.610	CI	Q1A47M1	L2GISW2K3.GIS43	PSHCDSA1	1	0		0
Destination File Name		/mailbox/CDUSER/pshcdsa1.out						
Message Text:								
2008/09/23 11:03:11.700	CT	Q1A47M1	L2GISW2K3.GIS43	PSHCDSA1	1	0	SCPA000I	56700
Destination File Name		/mailbox/CDUSER/pshcdsa1.out						
Message Text:		Copy step successful.						
2008/09/23 11:03:11.720	PT	Q1A47M1	L2GISW2K3.GIS43	PSHCDSA1	1	0	SVTM100I	0
Destination File Name								
Message Text:		PROCESS TERMINATED.						
2008/09/23 12:12:52.410	PI	Q1A47M1	UNIX.	PSHUNIX1	2	0		0
Destination File Name								
Message Text:								
2008/09/23 12:12:52.850	CI	Q1A47M1	UNIX.	PSHUNIX1	2	0		0
Destination File Name		/home/nis01/monty/cdstuff/testfiles/output/pshunix1.out						
Message Text:								

Connect:Direct Process Statistics Summary

The Connect:Direct Process Statistics Summary report contains summary statistics information about Processes occurring on managed Connect:Direct servers during the specified time period.

The following table describes the report columns:

Column	Description
Date Time	Date and time that the statistics record was generated.
Server Name	Name of the managed server that generated the status record.
Process Name	Connect:Direct Process name.
Process Number	Identification number assigned to each Process.
Submitter	User ID of the user who submitted the Process.
Return Code	Numeric code returned from a completed Process that indicates failure or success. The following are the standard return codes: 0 indicates successful completion 4 indicates a warning 8 indicates an error 16 indicates a catastrophic error
Msg ID	Sterling Control Center or Connect:Direct message identification number. See the appropriate product documentation for a description of message IDs.
Message Text	Short message text associated with the message ID.

Following is a sample report:

Connect:Direct Process Statistics Summary Report

Date / Time	Server Name	Process Name	Process Number	Submitter	Return Code	Message ID
2008/09/19 07:15:47.570	A1B.ZOS.AT46	LOAD081	40223	QATEST	0	
Message Text:						
2008/09/19 07:15:47.830	A1B.ZOS.AT46	LOAD066	40218	QATEST	0	SVTM100I
Message Text: PROCESS TERMINATED.						
2008/09/19 07:15:49.060	A1B.ZOS.AT46	LOAD062	40217	QATEST	0	
Message Text:						
2008/09/19 07:15:51.400	A1B.ZOS.AT46	LOAD084	40228	QATEST	0	
Message Text:						
2008/09/19 07:15:52.350	A1B.ZOS.AT46	LOAD081	40223	QATEST	0	SVTM100I
Message Text: PROCESS TERMINATED.						
2008/09/19 07:15:54.810	A1B.ZOS.AT46	LOAD062	40217	QATEST	0	SVTM100I
Message Text: PROCESS TERMINATED.						
2008/09/19 07:15:54.890	A1B.ZOS.AT46	LOAD087	40238	QATEST	0	
Message Text:						
2008/09/19 07:15:55.340	A1B.ZOS.AT46	LOAD082	40241	QATEST	0	
Message Text:						
2008/09/19 07:15:55.760	A1B.ZOS.AT46	LOAD084	40228	QATEST	0	SVTM100I
Message Text: PROCESS TERMINATED.						
2008/09/19 07:15:57.850	A1B.ZOS.AT46	LOAD088	40247	QATEST	0	
Message Text:						
2008/09/19 07:15:59.390	A1B.ZOS.AT46	LOAD088	40247	QATEST	0	SVTM100I
Message Text: PROCESS TERMINATED.						
2008/09/19 07:15:59.800	A1B.ZOS.AT46	LOAD085	40250	QATEST	0	
Message Text:						

Page 1 of   419

Fri Sep 19 16:48:02 CDT

Connect:Direct Statistics Log Report

The Database Connect:Direct Statistics Log Report allows you to compose a report of database statistical data based on the information that is important to you. You choose the database fields to display and their sort order. You can also state filter criteria to limit the records to include in the report. Filter criteria include any of the database statistics fields except for CC Name.

The database statistics fields you can choose from are listed and described in . An example follows of the Connect:Direct Statistics Log Report.

CD Stats Report

Date Time	Event ID	Msg ID	Msg Short Txt	Node ID	Node Type	Process Name	Return Code
2008/10/03 00:01:15.000	80153343933418470	LSMG402I	A user RUNTASK step completed. Exit code = &ECOD.	w_winbody44	1	PROC44	0
2008/10/03 00:01:15.000	80153343933418471			w_winbody44	1	PROC44	0
2008/10/03 00:01:15.000	80153343933418472	LSMG407I	SUBMIT within a process step completed successfully.	w_winbody44	1	PROC44	0
2008/10/03 00:01:15.000	80153343933418473	LSMG252I	A user process has completed successfully.	w_winbody44	1	PROC44	0
2008/10/03 00:01:15.000	80153343933418474	LSMG252I	A user process has completed successfully.	w_winbody44	1	PROC44	0
2008/10/03 00:01:15.000	80153343933418475			w_winbody44	1	PROC44	0
2008/10/03 00:01:15.000	80153343933418476	LSMG200I	Process number 261 (name PROC44, SNODE WINBODY44) executing	w_winbody44	1	PROC44	0
2008/10/03 00:01:15.000	80153343933418477	LSMG200I	Process number 261 (name PROC44, SNODE WINBODY44) executing	w_winbody44	1	PROC44	0
2008/10/03 00:01:15.000	80153343933418478			w_winbody44	1	PROC44	0
2008/10/03 00:01:15.000	80153343933418479			w_winbody44	1	PROC44	0

Page 1 of 468   Fri Oct 03 10:01:58 CDT

Connect:Enterprise Batch Statistics Details Report

The Connect:Enterprise Batch Statistics Details Report contains detailed information about batches on managed Connect:Enterprise servers during the specified time period.

The following table describes the report columns:

Column	Description
Start Date Time	Date and time that start-of-batch transmission information is received by the Sterling Control Center engine.
End Date Time	Date and time that end-of-batch transmission information is received by the Sterling Control Center engine.
Server Name	The server involved in the batch transmission.
Message ID	Message ID resulting from the batch Process.
Status	Batch status.
Mailbox ID	Repository associated with the Connect:Enterprise batch
Batch ID	User-assigned description of a Connect:Enterprise batch.
Batch Number	System-assigned number for each batch in a Connect:Enterprise repository.
Size	Size of the batch file.
Flags	Connect:Enterprise batch status flag. See the appropriate Connect:Enterprise documentation for a list of batch status flags.
Function	Function performed on the batch. See the Connect:Enterprise documentation for a description of functions.

Following is a sample report:

Connect:Enterprise Batch Statistics Details Report

Start Date / Time	End Date / Time	Server Name	Message ID	Status	Mailbox ID	Batch ID	Batch Number	Size	Flags	Function
2008/08/20 13:13:07.000	2008/08/20 13:13:07.000	QAAIX160	CNCE015I	0	CEU0302	CEU0302	105	0		ERA
2008/08/20 13:13:07.000	2008/08/20 13:13:07.000	QAAIX160	CNCE015I	0	CEU0302	CEU0302L	31	0		ERA
2008/08/20 13:13:43.000	2008/08/20 13:13:49.000	QAAIX160	CNCE013I	0	CEU0303	CEU0303	31	0		C
2008/08/20 13:13:49.000	2008/08/20 13:13:49.000	QAAIX160	CNCE011I	0	CEU0303	CEU0303	31	0		EXT
2008/08/20 13:13:58.000	2008/08/20 13:13:58.000	QAAIX160	CNCE015I	0	CEU0303	CEU0303	31	0		ERA
2008/08/20 13:13:23.000	2008/08/20 13:13:32.000	QAAIX160	CNCE012I	0	CEU0303	CEU0303L	105	52428800		ADD
2008/08/20 13:13:33.000	2008/08/20 13:13:38.000	QAAIX160	CNCE014I	0	CEU0303	CEU0303L	105	52428800		T
2008/08/20 13:13:58.000	2008/08/20 13:13:58.000	QAAIX160	CNCE015I	0	CEU0303	CEU0303L	105	0		ERA

Page 1 of 3

Tue Sep 23 15:09:18 CDT

Sterling Control Center Reports Guide

Connect:Enterprise Batch Statistics Summary Report

The Connect:Enterprise Batch Statistics Summary report contains summary information about batches on managed Connect:Enterprise servers during the specified time period.

The following table describes the report columns:

Column	Description
Start Date Time	Date and time that start-of-batch transmission information is received by the Sterling Control Center engine.
End Date Time	Date and time that end-of-batch transmission information is received by the Sterling Control Center engine.
Server Name	The server involved in the batch transmission.
Message ID	Message ID resulting from the batch Process.
Status	Batch status.
Mailbox ID	Repository associated with the Connect:Enterprise batch.
Batch ID	User-assigned description of a Connect:Enterprise batch.
Function	Function performed on the batch. See the Connect:Enterprise documentation for a description of functions.
Batch Number	System-assigned number for each batch in a Connect:Enterprise repository.

Following is a sample report:

Connect:Enterprise Batch Statistics Summary Report

Start Date / Time	End Date / Time	Server Name	Message ID	Status	Mailbox ID	Batch ID	Batch Number	Function
2008/08/20 13:13:07.000	2008/08/20 13:13:07.000	QAAIX160	CNCE015I	0	CEU0302	CEU0302	105	ERA
2008/08/20 13:13:07.000	2008/08/20 13:13:07.000	QAAIX160	CNCE015I	0	CEU0302	CEU0302L	31	ERA
2008/08/20 13:13:43.000	2008/08/20 13:13:49.000	QAAIX160	CNCE013I	0	CEU0303	CEU0303	31	C
2008/08/20 13:13:49.000	2008/08/20 13:13:49.000	QAAIX160	CNCE011I	0	CEU0303	CEU0303	31	EXT
2008/08/20 13:13:58.000	2008/08/20 13:13:58.000	QAAIX160	CNCE015I	0	CEU0303	CEU0303	31	ERA
2008/08/20 13:13:23.000	2008/08/20 13:13:32.000	QAAIX160	CNCE012I	0	CEU0303	CEU0303L	105	ADD
2008/08/20 13:13:33.000	2008/08/20 13:13:38.000	QAAIX160	CNCE014I	0	CEU0303	CEU0303L	105	T
2008/08/20 13:13:58.000	2008/08/20 13:13:58.000	QAAIX160	CNCE015I	0	CEU0303	CEU0303L	105	ERA

Page 1 of 3

Tue Sep 23 15:10:52 CDT

Sterling Control Center Reports Guide

Connect:Enterprise Statistics Log Report

The Database Connect:Enterprise Statistics Log Report allows you to compose a report of database statistical data based on the information that is important to you. You choose the database fields to display and their sort order. You can also state filter criteria to limit the records to include in the report. Filter criteria include any of the database fields except for CC Name. For definitions of these fields, see *Connect:Enterprise Statistics Table (CE_STATS_LOG)* on page 128.

An example follows of a Connect:Enterprise Statistics Log Report.

CE Stats Report

Bytes Read	Bytes Written	Node ID	Node Type	Event ID	Msg ID
0	0	qasles8	2	75969471413748207	CNCE009I
0	0	qasles8	2	75969471413748208	CNCE006I
0	3010	qasles8	2	75969471413748214	CNCE003I
0	0	qasles8	2	75969471413748218	CNCE006I
3010	0	qasles8	2	75969471413748220	CNCE011I
0	0	qasles8	2	75969471413748265	CNCE010I

Mon Sep 25 14:41:52 CDT

FTP File Transfer Report

The FTP File Transfer Report presents information on file transfer activity for FTP servers managed by Control Center.

The following table describes the columns included in this report.

Column	Description
Event Date/Time	Date and time of the transfer.
Process ID	Process identifier for the Process used to transfer the file.
Return Code	Return code returned for the file transfer.
Direction	Direction of the file transfer with respect to the FTP server.
File Size	Size of the file transferred, in bytes.
Submitter	User ID of the user who submitted the Process.
Source	Server from which the file was transferred (submitter for FTP PUTs).
Destination	Server to which the file was transferred (submitter for FTP GETs).

A sample FTP File Transfer Report follows.

FTP File Transfer Report

Event Date / Time	Process ID	Return Code	Direction	File Size	Submitter	Source	Destination
						palani	/chpst.log
2008/09/24 10:51:47.000	80102651756821492	0	inBound	90	palani	palani	/chpst.log
2008/09/24 10:51:51.000	80102651756821499	0	inBound	90	palani	palani	/notepad.cdp
2008/09/24 10:51:56.000	80102651756821503	0	inBound	363	palani	palani	/sedinst2.log
2008/09/24 10:52:23.000	80102651756821763	0	inBound	200	palani	palani	/syntp.log
2008/09/24 10:52:23.000	80102651756821767	0	inBound	191	palani	palani	/setup.log
2008/09/24 10:52:23.000	80102651756821771	0	inBound	163	palani	palani	/sedinst.log
2008/09/24 10:52:24.000	80102651756821775	0	inBound	161	palani	palani	/chpst.log
2008/09/24 10:52:25.000	80102651756821779	0	inBound	90	palani	palani	/ticrdbus.log
2008/09/24 10:52:26.000	80102651756821783	0	inBound	32	palani		

Page 1 of 2

Wed Sep 24 10:52:59 CDT

Sterling File Gateway Route Detail by Producer Report

The Sterling File Gateway Route Detail by Producer report presents detailed information on route activity by producer for Sterling File Gateway servers.

The fields that make up this report are described in the following table.

Field	Description
Producer	The name of the partner who created and sent the arrived file involved in the File Gateway file transfer.
Server	The name of the Sterling File Gateway server being monitored.
Arr File Name	The name of the arrived file involved in the File Gateway file transfer.
Status	The status of the arrived file involved in the File Gateway file transfer. Arrived Failed Ignore
Consumer	The name of the partner who received the arrived file involved in the File Gateway file transfer.
Consumer File	The name of the file the consumer expects in their mailbox when delivery is completed.
File Size	Size of file transferred, in bytes.
Start Time	The date and time the file transfer started.
End Time	The date and time the file transfer ended.

A sample Sterling File Gateway Route Detail by Producer report follows.

Sterling File Gateway Route Detail Report (by Producer)

Producer	Server	Arr File Name	Status	Consumer	Consumer File	File Size	Start Time	End Time
Palani1	neith-filegateway	producer_file.zip	Routed			511	2009/07/22 15:29:34.000	2009/07/22 15:29:38.000
			Route Complete	RQ103PGPConsumerF			2009/07/22 15:29:36.000	2009/07/22 15:29:37.000
			Delivery Complete		from_Palani1_20090722.txt	9	2009/07/22 15:29:37.000	2009/07/22 15:29:37.000
			Message: Consumer destination mailbox is /RQ103PGPConsumerF/Inbox.					
			Route Complete	RQ103PGPConsumerE			2009/07/22 15:29:37.000	2009/07/22 15:29:37.000
			Delivery Complete		from_Palani1_20090722.txt	9	2009/07/22 15:29:38.000	2009/07/22 15:29:37.000
			Message: Consumer destination mailbox is /RQ103PGPConsumerE/Inbox.					
			Route Complete	RQ103PGPConsumer D			2009/07/22 15:29:38.000	2009/07/22 15:29:38.000
			Delivery Complete		from_Palani1_20090722.txt	9	2009/07/22 15:29:39.000	2009/07/22 15:29:38.000
			Message: Consumer destination mailbox is /RQ103PGPConsumerD/Inbox.					
		producer_file.zip	Routed			511	2009/07/20 13:02:03.000	2009/07/20 13:02:06.000
			Route Complete	RQ103PGPConsumer D			2009/07/20 13:02:05.000	2009/07/20 13:02:05.000
			Delivery Complete		from_Palani1_20090720.txt	9	2009/07/20 13:02:05.000	2009/07/20 13:02:05.000
			Message: Consumer destination mailbox is /RQ103PGPConsumerD/Inbox.					

Thu Jul 23 16:11:33 CDT

Sterling Control Center Reports Guide

Sterling File Gateway Route Detail by Consumer Report

The Sterling File Gateway Route Detail by Consumer report presents detailed information on route activity by consumer for Sterling File Gateway servers.

The fields that make up this report are described in the following table.

Field	Description
Consumer	The name of the partner who received the arrived file involved in the File Gateway file transfer.
Consumer File	
File Size	Size of file transferred, in bytes.
Status	The status of the arrived file involved in the File Gateway file transfer. Arrived Failed Ignored
Producer	The name of the partner who created and sent the arrived file involved in the File Gateway file transfer.
Arr File Name	The name of the arrived file involved in the File Gateway file transfer.
Start Time	The date and time the file transfer started.
End Time	The date and time the file transfer ended.

A sample Sterling File Gateway Route Detail by Consumer report follows.

Sterling File Gateway Route Detail Report (by Consumer)

Consumer	Consumer File	File Size	Status	Producer	Arr File Name	Start Time	End Time
Multi_Delivery2	multi_delivery_test.txt	1610	Delivery Failed	Multi_Delivery	multi_delivery_test.txt	2009/03/19 08:55:03.000	2009/03/19 08:55:10.000
	Message: Delivery is now failed while Delivering with error message: Delivery failed. Cause: Unable to access or verify mandatory service parameter.						
	multi_delivery_test.txt	1610	Delivery Failed	Multi_Delivery	multi_delivery_test.txt	2009/03/19 08:55:04.000	2009/03/19 08:55:10.000
	Message: Delivery is now failed while Delivering with error message: Delivery failed. Cause: Unable to access or verify mandatory service parameter.						
	multi_delivery_test.txt	1610	Delivery Failed	Multi_Delivery	multi_delivery_test.txt	2009/03/18 17:14:50.000	2009/03/18 17:14:58.000
	Message: Delivery is now failed while Delivering with error message: Delivery failed. Cause: Unable to access or verify mandatory service parameter.						
	multi_delivery_test.txt	1610	Delivery Failed	Multi_Delivery	multi_delivery_test.txt	2009/03/18 17:14:52.000	2009/03/18 17:14:58.000
	Message: Delivery is now failed while Delivering with error message: Delivery failed. Cause: Unable to access or verify mandatory service parameter.						
	jpro.txt		Delivery Failed	Multi_Delivery	jpro.txt	2009/04/06 10:54:38.000	2009/04/06 10:54:43.000
	Message: Delivery is now failed while Delivering with error message: Delivery failed. Cause: Mailbox Repository Error.						
	jpro.txt	55	Delivery Failed	Multi_Delivery	jpro.txt	2009/04/06 10:54:38.000	2009/04/06 10:54:43.000
	Message: Delivery is now failed while Delivering with error message: Delivery failed. Cause: Unable to access or verify mandatory service parameter.						
RQ103PGPConsumerD	from_Palani1_20090317.txt	9	Delivery Complete	Palani1	producer_file.zip	2009/03/17 15:53:01.000	2009/03/17 15:53:01.000
	Message: Consumer destination mailbox is /RQ103PGPConsumerD/Inbox.						
	from_Palani1_20090326.txt	9	Delivery Complete	Palani1	producer_file.zip	2009/03/26 16:39:34.000	2009/03/26 16:39:30.000
	Message: Consumer destination mailbox is /RQ103PGPConsumerD/Inbox.						
	from_Palani1_20090330.txt	9	Delivery Complete	Palani1	producer_file.zip	2009/03/30 08:52:50.000	2009/03/30 08:52:51.000
	Message: Consumer destination mailbox is /RQ103PGPConsumerD/Inbox.						

Page 1 of 10

Wed Apr 08 10:39:10 CDT

Sterling Control Center Reports Guide

Sterling Integrator Business Process Details Report

The Sterling Integrator Business Process Details Report presents detailed information on business process activity for Sterling Integrator servers.

The fields that make up this report are described in the following table.

Field	Description
Event Date/Time	Date and time that the event was generated.
Event Type	The type of event generated.
Node ID	The identifier for the node that generated the business process.
Node Name	The name of the node that generated the business process.
Process Name	The name of the process.
Process ID	The process identifier.
Event Return Code	The code returned by the process.
Message ID	The identifier for the message associated with the event.
Step Name	The step name associated with the event.
Step ID	The identifier for the step associated with the event.
Advanced Status	Service-specific details about any errors that occurred for a step in this instance.
	For list of advanced status messages, see the Sterling Integrator product documentation.

A sample of this report follows:

Sterling Integrator Business Process Details Report

Event Date / Time	Event Type	Node Id	Node Name	Process Name	Process ID	Event Return Code	Message ID	Step Name	Step Id
2009/04/09 06:34:49.000	Process step started	pgounder-l	node1	CCC_Xfer_From_Winbody_	199517	0	0	AssignService	4
Advanced Status:									
2009/04/09 06:34:49.000	Process step started	pgounder-l	node1	CCC_Xfer_From_Winbody_	199517	0	0	CDServerPrimitiveBeginSession	5
Advanced Status:									
2009/04/09 06:34:49.000	Process step started	pgounder-l	node1	CCC_Xfer_From_Winbody_	199517	0	0	AssignService	6
Advanced Status:									
2009/04/09 06:34:49.000	Process step started	pgounder-l	node1	CCC_Xfer_From_Winbody_	199517	0	0	AssignService	7
Advanced Status:									
2009/04/09 06:34:49.000	Process step started	pgounder-l	node1	CCC_Xfer_From_Winbody_	199517	0	0	DecisionEngineService	8
Advanced Status: 1									
2009/04/09 06:34:49.000	Process step started	pgounder-l	node1	CCC_Xfer_From_Winbody_	199517	0	0	ReleaseService	9
Advanced Status:									
2009/04/09 06:34:49.000	Process step started	pgounder-l	node1	CCC_Xfer_From_Winbody_	199517	0	0	CDServerBeginSession	10
Advanced Status: Inline End									
2009/04/09 06:34:49.000	Process step started	pgounder-l	node1	CCC_Xfer_From_Winbody_	199517	0	0	CDServerCopyFrom	11
Advanced Status: Inline Begin CDInterop_CopyFromWithLoop									
2009/04/09 06:34:49.000	Process step started	pgounder-l	node1	CCC_Xfer_From_Winbody_	199517	0	0	EchoService	12
Advanced Status:									
2009/04/09 06:34:49.000	Process step started	pgounder-l	node1	CCC_Xfer_From_Winbody_	199517	0	0	AssignService	13
Advanced Status:									

Page 1 of 2

Fri Apr 10 10:42:58 CDT

Sterling Control Center Reports Guide

Sterling Integrator Business Process Summary Report

The Sterling Integrator Business Process Summary Report presents summary information on business process activity for Sterling Integrator servers.

The fields that make up this report are described in the following table.

Field	Description
Event Date/Time	Date and time that the event was generated.
Event Type	The type of event generated.
Node ID	The identifier for the node that generated the business process.
Node Name	The name of the node that generated the business process.
Process ID	The Process identifier.
Process Name	The name of the Process.
Event Return Code	The code returned by the Process.
Message ID	The identifier for the message associated with the event.
Advanced Status	Service-specific details about any errors that occurred for a step in this instance. For list of advanced status messages, see the Sterling Integrator product documentation.

A sample of this report follows:

Sterling Integrator Business Process Summary Report

Event Date / Time	Event Type	Node Id	Node Name	Process Name	Process ID	Event Return Code	Message ID
2009/04/10 04:00:00.000	Process started	pgounder-l	node1	AFTPurgeArchiveMailboxes	201641	0	0
Advanced Status:							
2009/04/10 04:15:04.000	Process started	pgounder-l	node1	CCC_FTP_Get_From_Phoenix	201658	0	0
Advanced Status:							
2009/04/10 04:24:44.000	Process started	pgounder-l	node1	CCC_Xfer_From_Winbody_CD_To_GIS	201669	0	0
Advanced Status:							
2009/04/10 03:44:44.000	Process started	pgounder-l	node1	CCC_Xfer_From_Winbody_CD_To_GIS	201622	0	0
Advanced Status:							
2009/04/10 03:45:04.000	Process started	pgounder-l	node1	CCC_FTP_Get_From_Phoenix	201624	0	0
Advanced Status:							
2009/04/10 03:14:53.000	Process started	pgounder-l	node1	CCC_FTP_Get_From_Phoenix	201590	0	0
Advanced Status:							
2009/04/10 03:04:44.000	Process started	pgounder-l	node1	CCC_Xfer_From_Winbody_CD_To_GIS	201579	0	0
Advanced Status:							
2009/04/10 02:44:53.000	Process started	pgounder-l	node1	CCC_FTP_Get_From_Phoenix	201557	0	0
Advanced Status:							
2009/04/10 10:24:44.000	Process started	pgounder-l	node1	CCC_Xfer_From_Winbody_CD_To_GIS	202068	0	0
Advanced Status:							
2009/04/10 10:16:07.000	Process started	pgounder-l	node1	CCC_FTP_Get_From_Phoenix	202058	0	0
Advanced Status:							

Page 1 of 2

Fri Apr 10 10:43:43 CDT

Sterling Integrator File Transfer Report

The Sterling Integrator File Transfer Report presents summary information on communications activity for Sterling Integrator servers.

The fields that make up this report are described in the following table.

Field	Description
Event Date/Time	Date and time that the event was generated.
Adapter Name	Name of the Sterling Integrator adapter that generated the event.
Process Name	The name of the process.
Process ID	The process identifier.
Return Code	The code returned by the process.
Message ID	The identifier for the message associated with the event.
Orig Node	The originating node for the process.
Remote Node	The receiving node for the process.
Direction	The direction of the transfer
File Size	The size of file transferred.
Submitter ID	The identifier for the process submitter.
Protocol	The protocol used for the transfer.
Secure Mode	A flag indicating whether the transfer was accomplished via a secure connection.

A sample of this report follows:

Sterling Integrator File Transfer Report

Event Date / Time	Adapter Name:	Process Name	Process ID	Return Code	Message ID	Orig Node	Remote Node	Direction	File Size	Submitter Id	Protocol	Secure Mode
2009/04/10 00:16:49.000	FTPClientAdapter	CCC_FTP_Get_From_Phoenix	201389	0		node1	10.20.42.130:	inBound	1607715	admin	FTP	none
Destination File: CCCTest							**Message Text:**					
2009/04/10 00:34:54.000	CDServerforCCC	CCC_Xfer_From_Winbody_CD_To_GIS	201402	0	0	node1	WINBODY420	inBound	30	admin	Connect:	none
Destination File: pgoun1-l.txt							**Message Text:**					
2009/04/10 00:47:02.000	FTPClientAdapter	CCC_FTP_Get_From_Phoenix	201424	0		node1	10.20.42.130:	inBound	1607715	admin	FTP	none
Destination File: CCCTest							**Message Text:**					
2009/04/10 01:15:11.000	CDServerforCCC	CCC_Xfer_From_Winbody_CD_To_GIS	201446	0	0	node1	WINBODY420	inBound	30	admin	Connect:	none
Destination File: pgoun1-l.txt							**Message Text:**					
2009/04/10 01:17:11.000	FTPClientAdapter	CCC_FTP_Get_From_Phoenix	201458	0		node1	10.20.42.130:	inBound	1607715	admin	FTP	none
Destination File: CCCTest							**Message Text:**					
2009/04/10 01:46:54.000	FTPClientAdapter	CCC_FTP_Get_From_Phoenix	201491	0		node1	10.20.42.130:	inBound	1607715	admin	FTP	none
Destination File: CCCTest							**Message Text:**					
2009/04/10 01:55:01.000	CDServerforCCC	CCC_Xfer_From_Winbody_CD_To_GIS	201492	0	0	node1	WINBODY420	inBound	30	admin	Connect:	none
Destination File: pgoun1-l.txt							**Message Text:**					
2009/04/10 02:17:21.000	FTPClientAdapter	CCC_FTP_Get_From_Phoenix	201525	0		node1	10.20.42.130:	inBound	1607715	admin	FTP	none
Destination File: CCCTest							**Message Text:**					

Page 1 of 6

Fri Apr 10 10:44:24 CDT

High Watermark Report

Server licenses often stipulate a maximum number of simultaneous sessions that can run on a server. The High Watermark Report provides information to help manage Connect:Direct licenses or node usage, perform audits of usage, or meet other reporting needs.

For example, you can use the report to determine whether the number of sessions a Connect:Direct node is licensed for are ever reached and, if so, how often and for what periods. Do this by setting the report limit equal to the license limit.

The High Watermark Report can also be used to see how many times sessions would be queued if the number of concurrent sessions allowed were reduced. To do this, set the report session limit to a value lower than the license limit.

In some cases Connect:Direct licenses specify an overall limit on the number of simultaneous sessions, as opposed to a limit for each server. You can use the report in these cases as well, to see whether you are violating your license agreement. Or use the report to determine what would happen if the limit on simultaneous sessions were raised or reduced. The # Times sessions exceeded limit column tells how many processes would have been queued to run later if the session limit were enforced.

> **Note:** The more times processes are queued instead of run immediately, the more times your processing window for file transfers may be missed.

The start time of the longest period over limit—in conjunction with the Last time max reached —can serve as an indicator of when the most Connect:Direct processing is occurring on your systems.

Max Concurrent Sessions indicates the maximum number of processes that ran at the same time. The # Times max reached column can indicate whether or not the maximum number of processes running at one time was an aberration or whether it happens frequently. By reducing the report limit, you can determine the typical number of processes running simultaneously by watching for an increase in the # Times max reached value.

You can restrict High Watermark Report output to a range of dates and times, to specific servers or server groups, and to a session limit. Default filter criteria preset for this report include Limit, Max Process Duration, Data/Time, and Servers. You can change the presets at the time of creation. Servers is the only one required.

After you confirm your choices and run the report, a status window displays the time elapsed since the report was initiated, along with start date/time and end date/time criteria. A progress bar depicts report generation progress and shows the date of the last statistics record processed.

> **Note:** High Watermark reports may require an extended time to run. Press **Background** to perform other Control Center tasks. You can stop the report by pressing **Stop**. When the report is complete, press **Show Report**.

The report includes detailed statistics for each selected server or server group as well as summary statistics across all selected servers.

The following table describes the columns of the High Watermark Report.

Column	Description
*	An asterisk next to a server ID indicates that a process on this server has exceeded the maximum duration.
Server Name	The server ID.
Max Concurrent Sessions	The peak number of sessions reached during the selected period.
# Times Max Reached	The number of occurrences within the selected period that Max Concurrent Sessions was reached.
Last Time Max Reached	The date and time of the last point when Max Concurrent Sessions was reached.
# Times Above Limit	The number of times the specified session limit was exceeded.
# Times Sessions Exceeded Limit	The number of sessions initiated while the session concurrency count was at or above the session limit.
Last Time Limit Exceeded	The date and time of the point when the limit was last exceeded (not the point when concurrent sessions returned below the threshold).
Start Time of Longest Period Over Limit	The date and time when the longest over limit period began.
Longest Period Over Limit	The amount of time in the longest over limit period.
% Time Over Limit	The percent of the total date/time range that the server or servers spent over the limit.
# Processes Exceeding Max Duration	The number of processes that have exceeded the maximum process duration.
Longest Process Exceeding Max Duration	The running time for the process that has furthest exceeded the maximum process duration.

Following is a sample High Watermark Report.

High Watermark Report

Note: * indicates Server with Process exceeding Maximum Process Duration found during specified Report Range

Server Name	Max Concurrent Sessions	Number of Times Max Reached	Last Time Max Reached	Number of Times Above Limit	Number of Times Session Exceeded Limit	Last Time Limit Exceeded	Start Time of Longest Period Over Limit	Longest Period Over Limit	Percentage of Time Over Limit
All Servers	2	1	Wed Sep 24 10:26:35 CDT	1	2	Wed Sep 24 10:26:35 CDT	Wed Sep 24 10:26:35 CDT	0:00:00	0
jrandall297	2	1	Wed Sep 24 10:26:35 CDT	1	2	Wed Sep 24 10:26:35 CDT	Wed Sep 24 10:26:35 CDT	0:00:00	0
qa160aix	0	1	Wed Sep 24 00:00:00 CDT	0	0			0:00:00	0
qa160sol	0	1	Wed Sep 24 00:00:00 CDT	0	0			0:00:00	0
qasles10	0	1	Wed Sep 24 00:00:00 CDT	0	0			0:00:00	0
qasles11	0	1	Wed Sep 24 00:00:00 CDT	0	0			0:00:00	0
qasles8	0	1	Wed Sep 24 00:00:00 CDT	0	0			0:00:00	0
qasol10	0	1	Wed Sep 24 00:00:00 CDT	0	0			0:00:00	0
svhppag	0	1	Wed Sep 24 00:00:00 CDT	0	0			0:00:00	0

Wed Sep 24 10:34:03 CDT

Sterling Control Center Reports Guide

High Watermark Report Considerations

The statistics featured in the High Watermark Report may prove easier to understand by viewing a series of graphics that show sessions starting and ending over a time span. In the examples, the time span covers 19 generic units. The report is based on the following series of events, which occurred on a managed server.

Time	Event	Time	Event
1	Process Start	9	Process End
2	Process Start	10	Process Start
2	Process Start	11	Process Start
3	Process End	12	Process Start
3	Process End	14	Process End
4	Process Start	15	Process Start
4	Process Start	16	Process End
6	Process Start	17	Process End
7	Process End	18	Process End
8	Process End		

maximum concurrent sessions = 4

times max reached = 3

times above limit = 3

last time limit exceeded = 11

(OL = over limit)

OL period A = 1 time unit
OL period B = 4 time units
OL period C = 6 time units
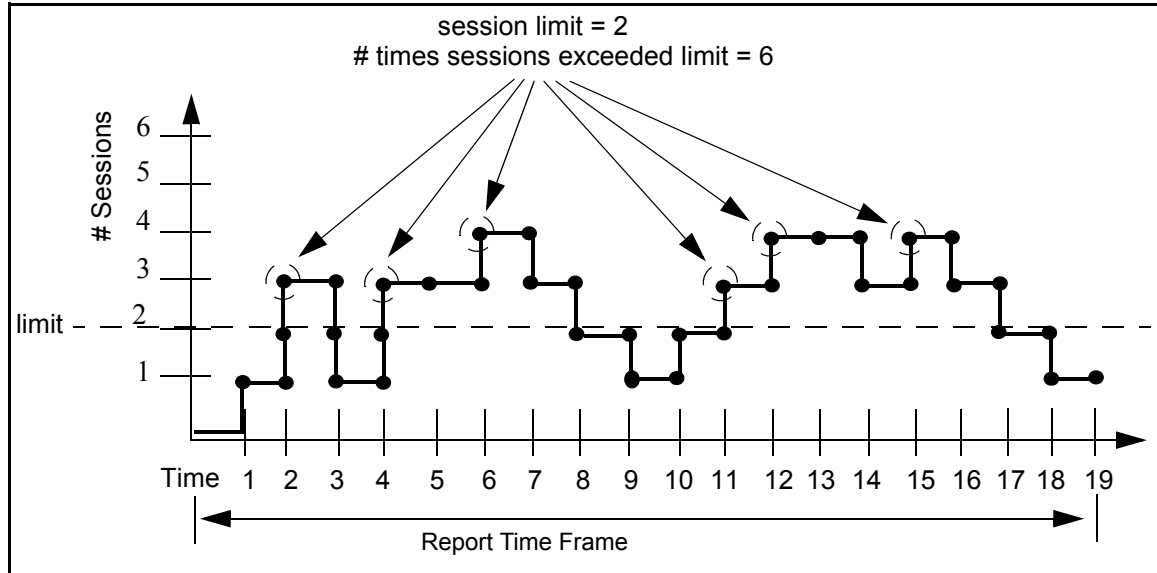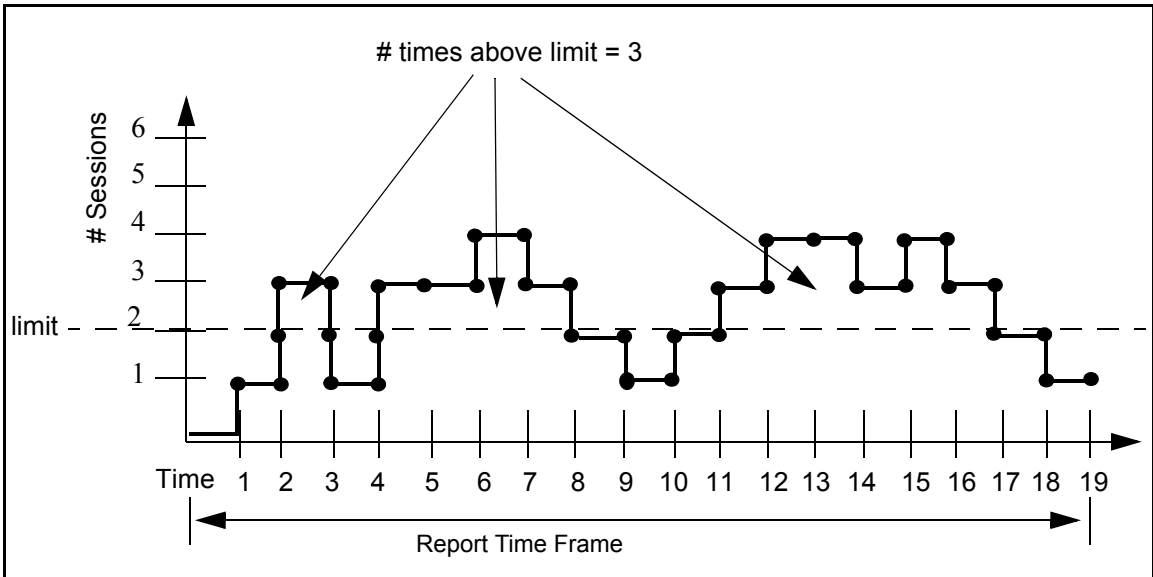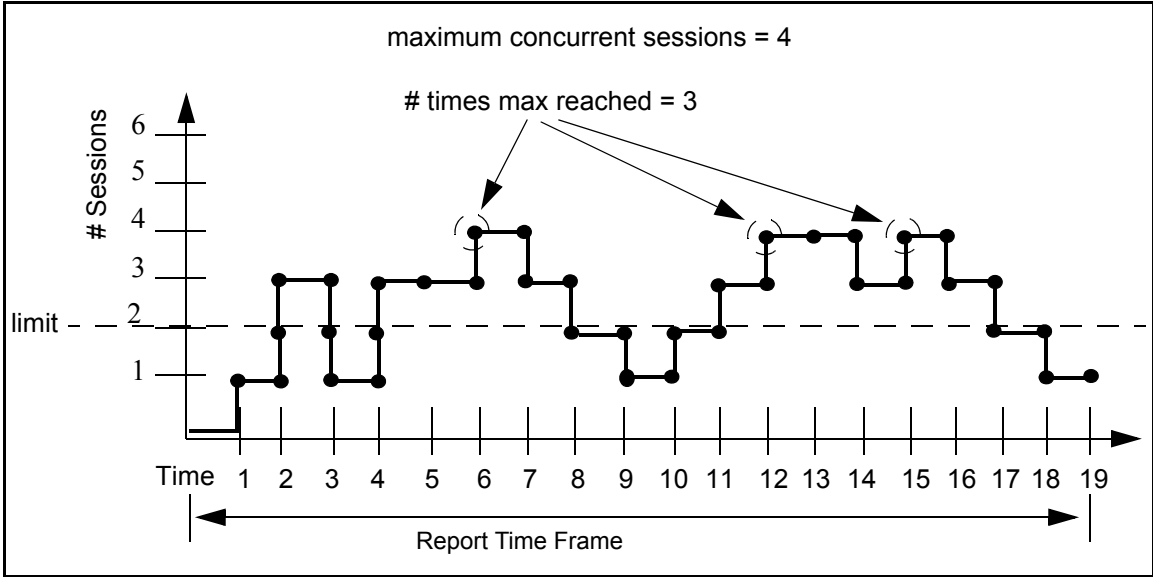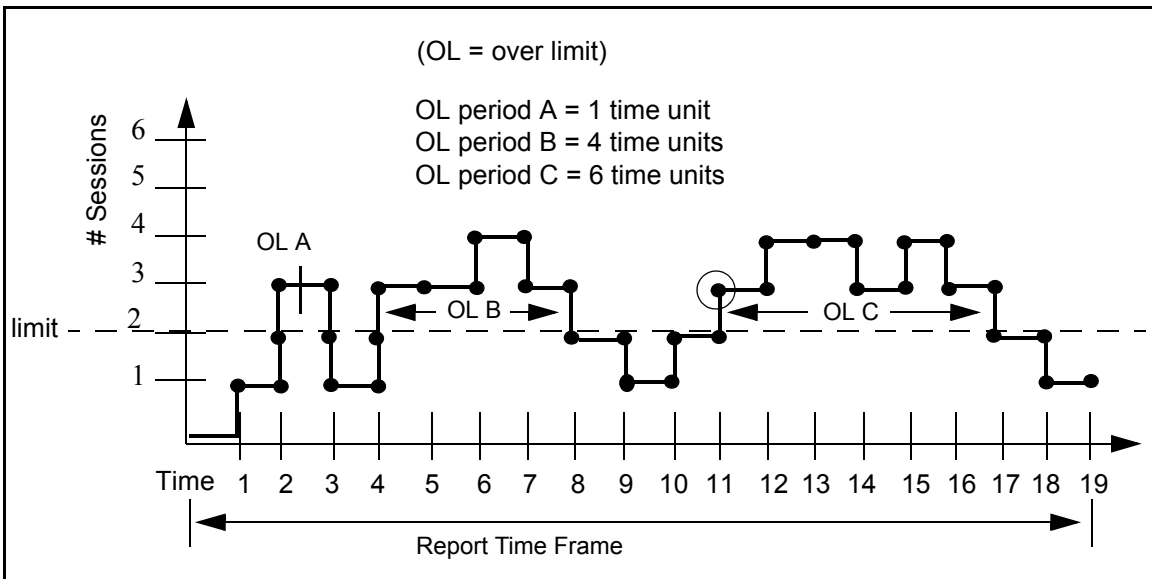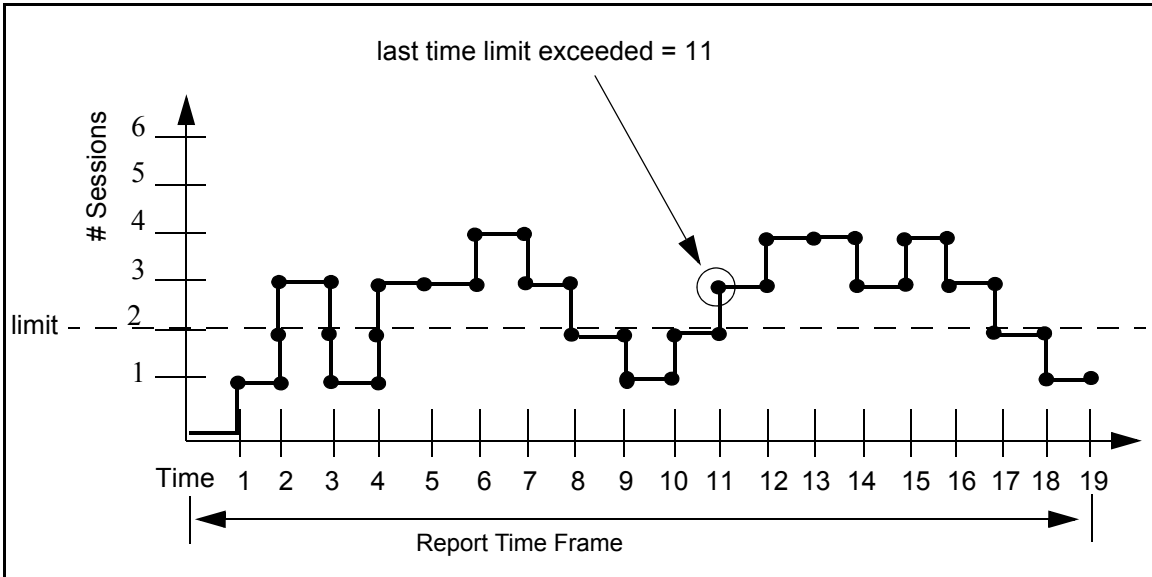
In the above illustration:

✦ Start Time of Longest Period Over Limit = 11

✦ Longest Period Over Limit = 6 time units

✦ Percent Time Over Limit = (1+4+6 units) / 19 units = 57.89%

All Servers Statistics. On the High Watermark Report, the results detailed for All Servers may not make intuitive sense at first glance. The source of the confusion has to do with the nature of what is being quantified.

For example, take a High Watermark Report run against two nodes, A and B, each with a session limit of 1. If the two nodes behave identically, as in the following graphic, each will have a number of sessions over the limit equal to two.
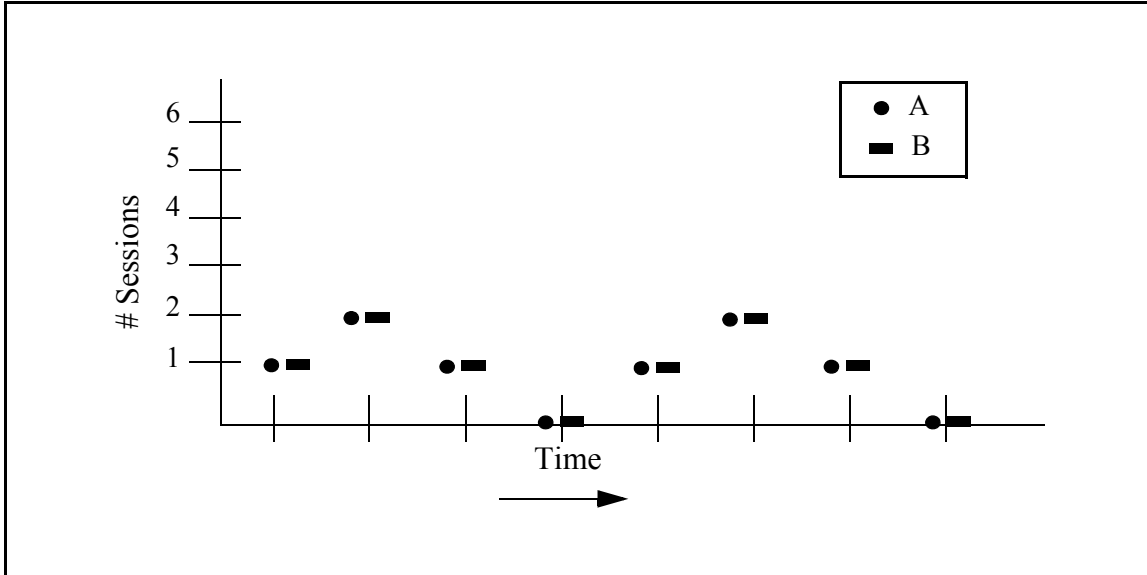
However, the number of sessions in which the two combined are over the limit is six, as shown in the next graphic. Therefore, the report column # Times Sessions Exceeded Limit will show a value of 6 for All Servers.
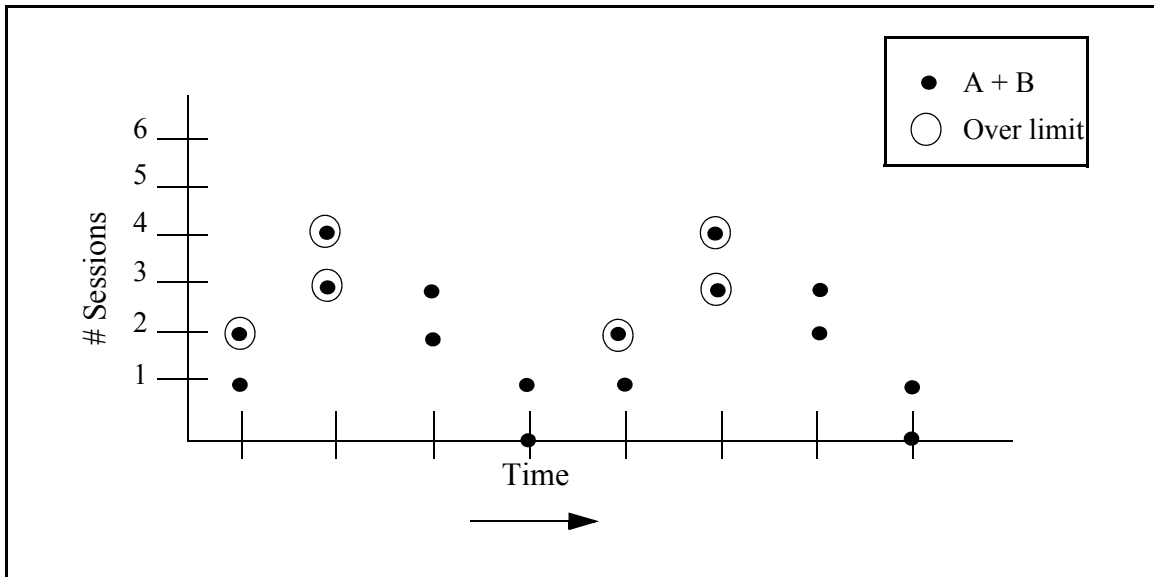
Caveats. Keep in mind these caveats in using and interpreting the High Watermark Report.

✦ If the clocks are not accurate for all managed servers included in the report, the values for All Servers may not be accurate.

✦ For Connect:Direct for Windows version 4.2, *in the absence of the fix for SR1343840,* whenever Processes are put on the wait, hold, or timer queues, they are treated as still running. This may affect the accuracy of the report. No fix is needed with later versions of Connect:Direct for Windows.

During the report's specified time frame, if one or more Processes exceed the Max Process Duration value specified, the report's accuracy will be affected.

File Agent Process Submission Report

The File Agent Process Submission Report presents information on Processes submitted by file agents associated with a managed Connect:Direct server.

The fields that make up this report are described in the following table.

Field	Description
Date / Time	Date and time that the event was generated.
Server Name	ID of the server the file agent submitted the process to.
File Agent Name	The identifier of the file agent.
Process Name	The name of the submitted Process.
Process Number	Number of the submitted Process.
Return Code	The code returned by the Process.
Trigger File	The name of the file that triggered the File Agent to submit a Process.
Rule Name	The name of the File Agent rule that triggered the event.

A sample of this report follows:

File Agent Process Submission Report

Date / Time	Server Name	File Agent Name	Process Name	Process Number	Return Code	Rule Name	Trigger File
2010/08/23 09:06:59.000	dvarnell	FileAgent	TESTDMV	1	0	default	c:\program files\fileagent1300C\watch\FileAgent_InstallLog.log
2010/08/23 09:07:00.000	dvarnell	FileAgent	TESTDMV	2	0	default	c:\program files\fileagent1300C\watch\output.txt
2010/08/23 09:07:01.000	dvarnell	FileAgent	TESTDMV	5	0	default	c:\program files\fileagent1300C\watch\CDFA.log
2010/08/23 09:07:01.000	dvarnell	FileAgent	TESTDMV	3	0	default	c:\program files\fileagent1300C\watch\CDFA_stats.log
2010/08/23 09:07:01.000	dvarnell	FileAgent	TESTDMV	4	0	default	c:\program files\fileagent1300C\watch\CDFAConfigGuide.pdf
2010/08/23 09:08:59.000	dvarnell	FileAgent	TESTDMV	6	0	default	c:\program files\fileagent1300C\watch\OGNL-LICENSE.txt
2010/08/23 09:08:59.000	dvarnell	FileAgent	TESTDMV	7	0	default	c:\program files\fileagent1300C\watch\OVAL-LICENSE.txt
2010/08/23 11:17:04.058	dvarnell	FileAgent			8	default	c:\program files\fileagent1300C\watch\cvslist.txt
2010/08/23 11:18:03.000	dvarnell	FileAgent	TESTDMV	1	0	default	c:\program files\fileagent1300C\watch\cvslist.txt

Page 1 of 3

Mon Aug 23 11:19:07 CDT

Standard Reports: Node Discovery

Sterling Control Center features reports that give details on aspects of Control Center node discovery. These reports include:

◆ Potentially Missing Netmap Entries Report	◆ Netmap Connections Summary Report
◆ Node Discovery Topology Report	◆ Potentially Inactive Netmap Entries Report

The following sections describe the available standard report types related to node discovery. Sample reports are shown.

Potentially Inactive Netmap Entries Report

The Potentially Inactive Netmap Entries Report lists nodes identified during Node Discovery that were found in the network map file of an Explorer node but on which no statistics records were found. Use this information to determine if you need to remove these node definitions from the network map of the corresponding Explorer node after validating that the connections to these nodes are no longer required.

The following table describes the report columns:

Column	Description
Server	Name of the Connect:Direct server.
Potentially Inactive Netmap Entry for Node(s)	The network map entry that may be inactive.

Following is a sample report:

Node Discovery Potentially Inactive Netmap Entries Report

Server	Potentially Inactive Netmap Entry for Node(s)
JRANDALL	CCDEV02
JRANDALL	JRANDALL4400
JRANDALL	MYNODE
JRANDALL	TEST3

Page 1 of 2

Wed Sep 24 10:20:06 CDT

Potentially Missing Netmap Entries Report

The Potentially Missing Netmap Entries report identifies the nodes that were found in the statistics records of the Explorer node but were not defined in the network map file. Use this information to determine if you need to add these node definitions to the network map of the corresponding server.

The following table describes the report columns:

Column	Description
Server	Name of the Connect:Direct server.
Potentially Missing Netmap Entry for Node(s)	The nodes found in statistics records that were not defined in the network map.

Following is a sample report:

Node Discovery Potentially Missing Netmap Entries Report

Server	Potentially Missing Netmap Entry for Node(s)
JRANDALL	MYNODE

Page 1 of 2

Wed Sep 24 10:28:53 CDT

Netmap Connections Summary Report

The Netmap Connections Summary Report contains a summary of all connection information collected during Node Discovery.

The following table describes the report columns:

Column	Description
Server Name	Name of the Connect:Direct servers.
Netmap Entries	The number of network map entries defined.
Last Used Date/Time	The last time the server connected with another node.
API Address	The TCP/IP address and port used by Sterling Control Center to establish a session with the Connect:Direct server.
DTF Address	The TCP/IP address and port of the server that a remote Connect:Direct server uses to establish a connection.
Platform	The platform on which the server is running.
Number of Partner Nodes	The number of partner nodes defined in the network map and the statistics records of the server.
Explorer/Discovered	The type of node. E = nodes defined in the Explorer List and D = nodes located in the Discovery List.

Following is a sample report:

Netmap Connection Summary Report

Server Name	Netmap Entries	Last Used Date / Time	API Address	DTF Address	Platform	Number of Partner_Nodes	Explorer / Discovered
N/A	0		10.20.246.36:3313			1	E
N/A	0		WINBODY:4363			1	E
N/A	0		CCDEV01.CSG.STERCOMM.COM:			1	E
N/A	0		10.20.4.222:1363			1	E
N/A	0		10.20.9.56:3383			1	E
N/A	0		JRANDALLXP.CSG.STERCOMM.			1	E

Page 1 of   1   Fri Oct 20 11:13:03 CDT

Node Discovery Topology Report

The Node Discovery Topology report contains information about the partners associated with the specified Explorer node.

The following table describes the report columns:

Column	Description
Explorer Node Name	The name of the server defined in the Explorer List.
API Address	The TCP/IP address and port used by Sterling Control Center to establish a session with the Connect:Direct server.
DTF Address	The TCP/IP address and port of the server that a remote Connect:Direct server uses to establish a connection.
Platform	The platform on which the server is running.
License Key Expiration Date	The date the license key expires for the node.
Last Explored Date Range	The date range used to search the last time that Node Discovery was run.
Last Explored Date/Time	The date and time that Node Discovery was last run.
# Partners	The number of partner nodes defined in the network map and found in statistics records for the server.
# Processes	The number of Processes found in the statistics records during Node Discovery.
Discovered Node Name	The name of a server found during Node Discovery.
Found in Netmap/Stats/Both	Identifies where the discovered node was found: either defined in the network map, in a statistics record, or identified in both the network map and a statistics record.
IP Address/APPL ID	The IP address or the APPL ID for SNA-enabled nodes.
Data Transfer Port	The port used for data transfer.
Platform	The platform on which the discovered node is running.
Last Used Date/Time	The time stamp of the communications between server pair under consideration.
# Explorer Partners	The number of Explorer nodes that this node communicates with.
# Processes	The number of Processes found in the statistics record for the server pair under consideration.

Following is a sample report:

Node Discovery Topology Report

Explorer Node Name	API Address	DTF Address	Platform	License Key Expiration Date	Last Explored Date Range	Last Explored Date/Time	# Partners	# Processes
Q1B.ZOS.V4600	10.20.129.8:8225	10.20.129.8:8224	OS390 4600	2009/10/30 14:47:28.101			0	0

Discovered Node Name	Found in Netmap/Stats/Both	IP Address/APPL ID	Data Transfer Port	Platform	Last Used Date/Time	# Explorer Partners	# Processes	

Explorer Node Name	API Address	DTF Address	Platform	License Key Expiration Date	Last Explored Date Range	Last Explored Date/Time	# Partners	# Processes
CDW44.W2003.VM	10.20.234.43:1363	10.20.234.43:1364	WINDOWS 4450	2008/12/26 15:47:11.333			0	0

Discovered Node Name	Found in Netmap/Stats/Both	IP Address/APPL ID	Data Transfer Port	Platform	Last Used Date/Time	# Explorer Partners	# Processes	

Explorer Node Name	API Address	DTF Address	Platform	License Key Expiration Date	Last Explored Date Range	Last Explored Date/Time	# Partners	# Processes
JLEGEL-DT4400	10.20.4.247:1363	10.20.4.247:1364	WINDOWS 4451	2008/12/26 15:47:24.250			0	0

Discovered Node Name	Found in Netmap/Stats/Both	IP Address/APPL ID	Data Transfer Port	Platform	Last Used Date/Time	# Explorer Partners	# Processes	

Sterling Control Center Reports Guide

Standard Reports: System

Sterling Control Center features reports that detail aspects of overall system functioning. These reports include.

◆ Alerts Report	◆ Server Inventory Report
◆ Audit Log Report	◆ Server Status Report
◆ Control Center License Report	◆ Service Level Criteria Summary Report
◆ Database Events Report	◆ Users and Roles Summary Report
◆ Monthly File Transfer Activity Report	

The following sections describe the available system standard report types. Sample reports are shown.

Alerts Report

The Alerts Report contains information about alerts generated by Sterling Control Center on managed servers during a specified time period. The report includes any comments that may have been entered for an alert. For more on alert comments, see "Updating Alerts" in the *Sterling Control Center User Guide*.

The following table describes the report columns:

Column	Description
Alert Date Time	Date and time that the alert was generated.
Severity	Alert severity level. (0–3)
Server Name	Name of the managed server on which the alert was generated.
Proc/Batch Name	Process name or Batch ID that generated the alert.
Proc Number	Process or batch number that generated the alert.
Rule Name	Rule that triggered the alert.
User Data 1–4	User-definable metadata fields. See Managing Metadata in the *System Administration Guide* or the Help system.
Handled Time	Time that the alert was handled.
Alert Handled	A flag indicating whether the alert was handled (Y/N).
Handled By	User ID of the Sterling Control Center user who handled the alert.
Comments	User comments supplied when the alert was handled.

Following is a sample report:

Alerts Summary Report

Alert Date / Time	Severity	Server Name	Process / Batch Name	Process Number	Rule Name	Handled Time	Alert Handled	Handled By
2007/09/25 10:14:39.000	1	sv160dell3	CCWINRT	13088	Bad Return Code			
2007/09/27 12:56:45.000	1	sv160dell3	FILESLC	13122	Bad Return Code			
2007/09/27 13:13:26.000	1	sv160dell3	FILESLC	13123	Bad Return Code			
2007/09/27 17:39:39.000	1	sv160dell3	FILESLC	13145	Bad Return Code			
2007/09/28 09:59:32.000	1	sv160dell3	FILESLC	13147	Bad Return Code			
2007/09/28 13:11:40.663	2	qasles8			Linked rule 1			
2007/09/28 13:12:04.217	2	winbody			Linked rule 1			

Page 1 of   1

Tue Oct 02 14:00:38 CDT

Audit Log Report

The Audit Log Report lists changes that have been made to the configuration of one or more Connect:Direct servers managed by Sterling Control Center.

The following table describes the report columns.

Column	Description
Date Time	Date and time of the change.
User	User ID of the user who made the change.
Server	The server the change affected.
Object ID	The identifier of the object that was changed.
Object Type	The type of object changed.
Property	The specific property of the object that was changed.
Type	Type of property change: Added, Modified, or Deleted.
Value Before	The value of the property before the change.
Value After	The value of the property after the change.

Following is a sample report.

Audit Log Report

Date Time	User	Server	Object ID	Object Type	Property	Type	Value Before	Value After
2008/09/22 13:58:07.011	admin	Q1B.ZOS.V 4600	Q1B.ZOS.V4600,A LLUSER	Functional Authority	Confirm Delete	Added		Y
2008/09/22 13:58:07.011	admin	Q1B.ZOS.V 4600	Q1B.ZOS.V4600,A LLUSER	Functional Authority	Reset Signon	Added		Y
2008/09/22 13:58:07.011	admin	Q1B.ZOS.V 4600	Q1B.ZOS.V4600,A LLUSER	Functional Authority	Confirm Delete	Added		Y
2008/09/22 13:58:07.011	admin	Q1B.ZOS.V 4600	Q1B.ZOS.V4600,A LLUSER	Functional Authority	Secure+ Admin	Added		Y
2008/09/22 13:58:07.011	admin	Q1B.ZOS.V 4600	Q1B.ZOS.V4600,A LLUSER	Functional Authority	update_user	Deleted	Y	
2008/09/22 13:58:07.011	admin	Q1B.ZOS.V 4600	Q1B.ZOS.V4600,A LLUSER	Functional Authority	Flush	Deleted	A	
2008/09/22 13:58:07.011	admin	Q1B.ZOS.V 4600	Q1B.ZOS.V4600,A LLUSER	Functional Authority	Refresh	Deleted	Y	
2008/09/22 13:58:07.011	admin	Q1B.ZOS.V 4600	Q1B.ZOS.V4600,A LLUSER	Functional Authority	Security ID	Modified	***	***
2008/09/22 13:58:07.011	admin	Q1B.ZOS.V 4600	Q1B.ZOS.V4600,A LLUSER	Functional Authority	Password	Modified	***	***
2008/09/22 13:58:07.011	admin	Q1B.ZOS.V 4600	Q1B.ZOS.V4600,A LLUSER	Functional Authority	Security ID	Modified	***	***
2008/09/22 13:58:07.011	admin	Q1B.ZOS.V 4600	Q1B.ZOS.V4600,A LLUSER	Functional Authority	Password	Modified	***	***
2008/09/22 13:58:45.661	admin	Q1B.ZOS.V 4600	Q1B.ZOS.V4600,A LLUSER	Functional Authority	Reset Signon	Added		N
2008/09/22 13:58:45.661	admin	Q1B.ZOS.V 4600	Q1B.ZOS.V4600,A LLUSER	Functional Authority	Update APKEY	Added		Y
2008/09/22 13:58:45.661	admin	Q1B.ZOS.V 4600	Q1B.ZOS.V4600,A LLUSER	Functional Authority	Confirm Delete	Added		Y
2008/09/22 13:58:45.661	admin	Q1B.ZOS.V 4600	Q1B.ZOS.V4600,A LLUSER	Functional Authority	Update Initialization Parameters	Added		Y
2008/09/22 13:58:45.661	admin	Q1B.ZOS.V 4600	Q1B.ZOS.V4600,A LLUSER	Functional Authority	Confirm Delete	Added		Y
2008/09/22 13:58:45.661	admin	Q1B.ZOS.V 4600	Q1B.ZOS.V4600,A LLUSER	Functional Authority	Secure+ Admin	Added		Y
2008/09/22 13:58:45.661	admin	Q1B.ZOS.V 4600	Q1B.ZOS.V4600,A LLUSER	Functional Authority	update_user	Deleted	Y	
2008/09/22 13:58:45.661	admin	Q1B.ZOS.V 4600	Q1B.ZOS.V4600,A LLUSER	Functional Authority	Flush	Deleted	A	
2008/09/22 13:58:45.661	admin	Q1B.ZOS.V 4600	Q1B.ZOS.V4600,A LLUSER	Functional Authority	Refresh	Deleted	Y	

Page 2 of 6

Mon Sep 22 14:56:21 CDT

Server Status Report

The Server Status report contains system status information about selected managed servers.

The following table describes the report columns:

Column	Description
Server Name	Name of the managed server.
Alerts	Number of active high, medium, and low severity alerts on the server.
Server Version	Version of the server.
License Expire Date	Date that the managed server's software license expires.
License Type	Type of product license on the server.
License Notification	How many days before a server license expiration date that Sterling Control Center begins generating license expiration events.
Sessions/ Accounts	Number of concurrent sessions or accounts permitted by the server license.
Max Processes Permitted/Time Max Reached	Maximum number of concurrent sessions that have occurred on the server / Number of times the maximum number of concurrent sessions was reached.
Processes Exec	Number of executing Processes on the server. This is shown for Connect:Direct servers only.
Processes Non-Exec	Number of non-executing Processes on the server. This is shown for Connect:Direct servers only.

Following is a sample report:

Server Status Report

Server Name	Alerts (H,M,L)	Server Version	License Expire Date	License Type	License Notification	Sessions / Accounts	Max Process / Times Reached	Process EXEC	Process NON-EXEC
ccdev02_44_0	0 0 0	WINDOWS 4451	01-01-2010	EMERGENCY-KEY	30			0	1
w_winbody44	0 0 0	WINDOWS 4451	01-01-2010	EMERGENCY-KEY	30		1 / 1	1	0

Page 1 of 2

Mon Oct 20 10:12:34 CDT

Server Inventory Report

The Server Inventory Report prints an inventory of the servers monitored and managed by Sterling Control Center.

Following is a description of the columns that make up the report.

Column	Description
Server Name	The name of the server.
Server Type	Type of server (Connect:Direct, Connect:Enterprise, Sterling Integrator, File Transfer Protocol).
Description	Server description.
Server Version	Server platform.
Current Status	The current status of the server.
Monitor	This server is monitored by Control Center. X indicates Yes, blank indicates No.
Configure	This server is configurable by Control Center. X indicates Yes, blank indicates No.
License Push	This server supports license push by Control Center. X indicates Yes, blank indicates No.
Secure+	This server supports Secure+. X indicates Yes, blank indicates No.
License Expiration	Expiration date for this server's current license.
License Type	Type of current license.
License PSP	Software product ID, which uniquely identifies a specific licensed copy of software.

Following is a sample report:

Server Inventory Report

Server Name	Server Type	Description	Server Version	Current Status	Monitor	Configure	License Push	Secure+	License Expiration	License Type	License PSP
James-FG	Sterling Integrator		Unknown	Unknown	X						
pgl-SI_R2	Sterling Integrator		Unknown	Unknown	X						
qa-ce-unix	Connect:Enterprise		UNIX 2.4.02	Running	X					PROD	
XLIGHT ftp server 1	File Transfer Protocol		Windows 2003	Running	X						
ccbuild2-cdwin42	Connect:Direct		WINDOWS 4234	Running	X	X			01-01-2010	EMERGENCY-KEY	
augusta	Connect:Direct		UNIX 400090423	Running	X	X	X		11-21-2009 HALT	PROD	888888

Page 1 of 2

Thu Jul 23 14:29:40 CDT

Sterling Control Center Reports Guide

Service Level Criteria Summary Report

The SLC Summary Report lists details regarding each Control Center SLC.

The following table describes SLC Summary Report columns:

Column	Description
SLC Type	Standard, Wildcard, or Workflow
ID	The name of the SLC.
Enabled	Whether or not the SLC is enabled.
Monitoring Window	The SLC's monitoring window parameters.
Matching Properties	The matching criteria for items being monitored.
Cal. Sched.	The calendar schedule used in setting up the SLC.
Enabled	Whether or not the calendar schedule is enabled.
Dur Schedule	Duration schedule.
Milestone ID	Identifier of the workflow SLC milestone.

Following is a sample report.

<table>
<tr><td colspan="9" align="center">SLC Summary Report</td></tr>
<tr><td>Standard</td><td></td><td>Monitoring</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>ID</td><td>Enabled</td><td>Window</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>example</td><td>true</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Matching Properties:</td><td>nodeId</td><td>destFile</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>-</td><td>ccdev01</td><td>bob.txt</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Cal.Sched</td><td>Enabled</td><td>NSR Start</td><td>NSR End</td><td>NER Start</td><td>NER End</td><td>NER Day</td><td>Calendar ID</td><td>TimeZone</td></tr>
<tr><td>Tuesdays</td><td>true</td><td>06:00</td><td>08:00</td><td>07:00</td><td>09:00</td><td>0</td><td>Tuesday</td><td>America/Chicago</td></tr>
<tr><td>Wildcard</td><td></td><td>Monitoring</td><td>Missing</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>ID</td><td>Enabled</td><td>Window</td><td>Events</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>wc example</td><td>true</td><td></td><td>true</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Matching Properties:</td><td>Name</td><td>Match Type</td><td>Value</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>-</td><td>nodeId</td><td>Wildcard</td><td>*</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>-</td><td>destFile</td><td>Wildcard</td><td>bob*.txt</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Cal.Sched</td><td>Enabled</td><td>NSR Start</td><td>NSR End</td><td>NER Start</td><td>NER End</td><td>NER Day</td><td>Calendar ID</td><td>TimeZone</td></tr>
<tr><td>Tuesdays</td><td>true</td><td>06:00</td><td>08:00</td><td>07:00</td><td>09:00</td><td>0</td><td>Tuesday</td><td>America/Chicago</td></tr>
<tr><td>Workflow</td><td>Concurrence</td><td>Relative</td><td>Monitoring</td><td>Monitoring</td><td></td><td>Suppress</td><td></td><td></td></tr>
<tr><td>ID</td><td>Count</td><td>MS Sched</td><td>Win.Start</td><td>Win.End</td><td>Missing Events</td><td>MS Messages</td><td></td><td></td></tr>
<tr><td>Bobolink</td><td>1</td><td>true</td><td>6</td><td>6</td><td>true</td><td>false</td><td></td><td></td></tr>
<tr><td>Milestone ID</td><td>NSR Start</td><td>NSR End</td><td>NER Start</td><td>NER End</td><td>DMin</td><td>DMAX</td><td></td><td></td></tr>
<tr><td>Milestone A</td><td></td><td></td><td></td><td></td><td>000:15:00</td><td>000:30:00</td><td></td><td></td></tr>
<tr><td>Matching Properties:</td><td>Name</td><td>Match Type</td><td>Value</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>-</td><td>nodeId</td><td>Wildcard</td><td>Srvr1</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Page 1 of 3</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Thu Oct 19 15:34:29 CDT</td></tr>
</table>

Monthly File Transfer Activity Report

The Monthly File Transfer Activity Report lists details regarding monthly file transfer activity on selected servers.

Following are the columns that make up the Monthly File Transfer Activity Report.

Column	Description
Server Name	Name of server.
Date	Date of file transfer.
Files Sent	Number of files sent.
Files Received	Number of files received.
File Bytes	Number of bytes in files involved in the transfer.
Transmitted Bytes	Number of bytes transmitted in the transfer.

Following is a sample report:

Monthly File Transfer Activity Report
2008/01 - 2008/12

Server Name	Date	Files Sent	Files Received	File Bytes	Transmitted Bytes
qasles10	2008/09	22	22	36,035,121	21,414,195
qasles10	**Totals**	**22**	**22**	**36,035,121**	**21,414,195**
qasol10	2008/09	4	4	40,500,000	40,504,800
qasol10	**Totals**	**4**	**4**	**40,500,000**	**40,504,800**
svhppag	2008/09	4	4	40,500,000	40,504,800
svhppag	**Totals**	**4**	**4**	**40,500,000**	**40,504,800**
All Servers	**Totals**	**30**	**30**	**117,035,121**	**102,423,795**

Page 1 of 2

Wed Sep 24 10:31:08 CDT

Database Events Report

The Database Events Report allows you to compose a report of database event data based on the information that is important to you. You choose the database fields to display and their sort order. You can also state filter criteria to limit the records to include in the report. Filter criteria include any of the database fields except for CC Name.

The database fields you can choose from are listed in *Events Table (EVENTS)* on page 110.

An example follows of a Database Events Report.

Date Time	Event ID	Event Type	From Node	MSG ID	Node ID	Node Type
2008/09/23 00:54:25.556	80094354718600658	5		CCNS005E	jlegel-DT4400	1
2008/09/23 00:54:25.736	80094354718600659	5		CCNS005E	CDW44.W2003.VM	1
2008/09/23 00:54:25.968	80094354718600660	5		CCNS005E	Q1B.ZOS.V4600	1
2008/09/23 00:54:26.265	80094354718600661	5		CCNS005E	Q1G.ZOS.V4700	1
2008/09/23 00:54:26.508	80094354718600662	5		CCNS005E	hpag4000sp	1
2008/09/23 00:54:26.511	80094354718600663	5		CCNS010I	hpag4000sp	1
2008/09/23 00:54:26.691	80094354718600664	5		CCNS005E	hpig4000sp	1
2008/09/23 00:54:26.694	80094354718600665	5		CCNS010I	hpig4000sp	1
2008/09/23 00:54:26.818	80094354718600666	5		CCNS005E	rhel504000sp	1
2008/09/23 00:54:26.821	80094354718600667	5		CCNS010I	rhel504000sp	1
2008/09/23 00:54:27.064	80094354718600668	10		CCTR046E	CCEngineService	0
2008/09/23 01:54:25.565	80094354718607269	5		CCNS005E	jlegel-DT4400	1

Events Report

Page 1 of 15

Tue Sep 23 11:08:01 CDT

Control Center License Report

The Control Center License Report contains Sterling Control Center license information.

The following table describes the report columns.

Column	Description
Total Licensed Servers	Total number of servers that your Sterling Control Center permits you to manage.
Defined Servers	Number of managed servers defined to Sterling Control Center.
Licensed Console Connections	Number of consoles that the Sterling Control Center license allows to connect to the engine.
Current Console Connections	Current number of consoles connected to the Sterling Control Center engine.
License Type	Server platform and the license types for that platform.
Licensed Managed Servers Per License Type	Number of servers permitted by license type.
Servers Accounted for in Each License Slot	Actual number of managed servers per license type.

Following is a sample report:

Control Center License Report

Total Licensed Servers	Defined Servers	Licensed GUI Connections	Current GUI Connections	License Type	Monitored Servers Per License Type	Servers Accounted For in Each License Slot
100 Licensed to Monitor	24	10	1			
100 Licensed to Configure	11					
				CD-LOWRANGE	100	0
				CD-LOWRANGE-PROD	100	0
				CD-LOWRANGE-TEST	100	0
				CD-MIDRANGE	100	10
				CD-MIDRANGE-PROD	100	4
				CD-MIDRANGE-TEST	100	0
				CD-NONSTOP	100	0
				CD-NONSTOP-PROD	100	0
				CD-NONSTOP-TEST	100	0
				CD-OS390	100	1
				CD-OS390-PROD	100	1
				CD-OS390-TEST	100	0
				CD-OS400	100	0
				CD-OS400-PROD	100	0
				CD-OS400-TEST	100	0
				CE-OS390	100	0
				CE-OS390-PROD	100	0
				CE-OS390-TEST	100	0

Page 1 of 2   Fri Sep 19 17:08:53 CDT

Users and Roles Summary Report

The Users and Roles Summary report is a three-part report that lists the following information:

✦ All Sterling Control Center users and their associated roles

✦ All Sterling Control Center roles and the users assigned to them

✦ All Sterling Control Center roles and their associated permissions

The following table describes the report columns:

Column	Description
Part 1	
User ID	Sterling Control Center user.
User Role	Role assigned to the user.
Description	Description text provided for the user ID.
Last Login Time	Date and time that the user last logged into Sterling Control Center.
Host	The host through which the user last logged in.
IP Address	The IP address of the computer on which user last logged in.
Domain	The domain of the computer on which user logged in.
Active	Whether the user was active when the report was run (Y/N).
Part 2	
User Role	Roles defined in Sterling Control Center.
Assigned User IDs	User IDs assigned to the role.
Part 3	
User Role	Roles defined in Sterling Control Center.
Role Authority	Server groups and permissions assigned to the role.

Following is a sample report:

		Users and Roles Summary Report					
User ID	**User Role**	**Description**	**Last Login Time**	**Host**	**IP Address**	**Domain**	**Active**
admin	superuser	Admin User with Super user Role	10/19/06 2:57 PM	GWHITE.sci.local	10.251.65.136	SCI	Yes

User Role	**Assigned User IDs**
superuser	admin

User Role	**Role Authority**
Flunky	rules=none
	reports=view
	actions=view
	alerts=view
	processes=view
	systemSettings=none
	slcs=none
	roles=none
	webAccess=view
	users=none
	servers=view
superuser	rules=manage
	reports=manage
	actions=manage
	alerts=manage
	processes=manage
	systemSettings=man
	slcs=manage

Page 1 of 2   Thu Oct 19 15:18:19 CDT

Display the Log Files

You can easily display Sterling Control Center engine trace log files to aid in troubleshooting installation or other technical support issues.

To display engine trace log files:

1. Select **Tools** > **Trace Logs**.

   A list of links displays in your default Internet browser.

2. Select a .log file whose name begins with "CCEngine."

   The log file is displayed in your default text editor application.

Note:	To view engine trace logs through this tool, a user's role in Role Properties must have View Engine Logs permission level set to View.

Note:	If the engine resides on UNIX but you are viewing the trace logs from a Windows system, it is recommended that you right-click, save each log file, and open it using Wordpad.

To display the audit log:

Select **Tools** > **Audit Log**.

The Audit Log window displays all objects that have changed. The listing includes the properties of the object that have changed and when, as well as the values before and after the change. You can filter this list or save it to disk.

Sample Reports in Crystal Reports Format

Sterling Control Center provides the following sample reports in Crystal Reports format.

- ✦ Connect:Direct Events
- ✦ Connect:Direct Exception Trends
- ✦ Connect:Direct Exception Trends Chart
- ✦ Connect:Direct Usage Report
- ✦ Connect:Direct Usage Report Chart
- ✦ Connect:Direct Usage by Server Pair Report
- ✦ Connect:Direct Usage by Server Pair Report Chart
- ✦ Connect:Direct Usage by Server Pair Detail/Summary Report

---

Note: Sterling Commerce does not provide assistance for implementing report solutions in all environments using all possible third-party tools, including Crystal Reports Viewer. The sample reports provided in the Sterling Control Center package are designed to act as a starting point for designing your own reports using the tools of your choice.

Configuring ODBC DSN for the Sample Reports

To use the sample Crystal Reports, you must configure an ODBC DSN as described here.

To perform this procedure, you must already have installed Sterling Control Center with a database.

To configure your computer before using the sample Sterling Control Center reports:

1. Download and install the ODBC driver for your database type.
2. After the driver is installed, select **Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)** to display the **ODBC Data Source Administrator** window.
3. Select the **System DSN** tab.
4. Click **Add**.
5. Select the appropriate driver from the driver list and click **Finish**.

A configuration window is displayed.

6. Type the following information and click **OK**.

Field	Description
Data Source Name	SterlingCommerce Type the name in the exact case shown above. Do not type a space between Sterling and Commerce.
Host/Server Name (or IP)	IP address of the Sterling Control Center database (production or staging).
Database name	Name of the Sterling Control Center database (production or staging).
User	User name to access the Sterling Control Center database (production or staging).
Password	Password to access the Sterling Control Center database (production or staging).
Port	Port number to access the Sterling Control Center database (production or staging).

Note: The configuration parameters may vary depending on the database type.

Using a Later Version of Crystal Reports for the Sample Reports

Sterling Control Center reports are created using Crystal Reports version 9.0. If you use a later version of Crystal Reports to generate Sterling Control Center reports, perform the following procedure to convert the sample reports.

Note: The following procedure is not a substitute for the actual product documentation for Crystal Reports.

This procedure assumes that you have already connected to the database.

To convert the sample reports using a version of Crystal Reports later than 9.0:

1. Open a report.
2. Select **Database**.
3. Select **Show SQL Query**.
4. Click **OK** on the **Enter Parameter Values** window.
5. Click **OK** on the Verify Database message.
6. Click **OK** on the database is up to date message.
7. Click **Reset**, then click **OK** on the **Show SQL Query** window.
8. Save the report under a new name.

The report is saved in the later version of Crystal Reports. Use this report in the future.

9. Repeat this procedure for each report.

Running the Sterling Control Center Sample Reports

To run the sample reports included with Sterling Control Center:

1. Copy the SampleReports folder from the Sterling Control Center DVD to the desired directory on your desktop.

2. Start Crystal Reports.

3. Select **File > Log On/Off Server**. The **Data Explorer** window is displayed.

4. Expand the ODBC folder.

5. Select the SterlingCommerce ODBC and click **Log On**.

> **Note:** You must log on to the SterlingCommerce ODBC every time you start Crystal Reports before you run a report.

6. Open a sample report from the SampleReports directory and run it.

7. Select the report criteria and click **OK**. The report is displayed on your monitor.

Troubleshooting Sterling Control Center Sample Reports

When running the Sterling Control Center sample reports, you may receive a database ODBC error similar to the following message.

If you receive such a message, do the following:

1. Select **Database > Show SQL Query** from the Crystal Reports menu bar.

2. Select the **Show SQL Query** tab.

3. Click **Reset**.

4. Generate the report again.

Sample Reports

The following pages describe the sample reports created by Crystal Reports for Sterling Control Center. All Crystal Reports Sterling Control Center sample reports must be printed on 14-inch wide paper.

Connect:Direct Events

The Connect:Direct Event report contains information about events occurring on managed servers during the specified time period.

The file name for this report is CD_Select_Events.rpt.

The following table lists selection criteria for this report:

Criteria	Description
Event Type	Sterling Control Center event to show on the report. See the *Sterling Control Center System Administration Guide* for a description of event types. To include an event, select the event from the list box and click **Add**. You can select multiple events for the report.
Start Date	Start date of the data range.
End Date	End date of the data range.
Start Time	Start time of the data range. The default is 00:00:00 (midnight).
End Time	End time of the data range. The default is 23:59:59.

The following table describes the report columns:

Column	Description
Date/Time	Date and time that the event was generated.
Node ID	Server alias.
Event Type	Type of event. See the *Sterling Control Center System Administration Guide* for a description of event types.
Alert	Indicates if an alert was triggered. The values are: Blank=No alert 0-3=Alert severity
Alert Deleted By	Sterling Control Center user name of the person who removed the alert.
Rule ID	Name of the rule triggered by the event.
Action ID	Name of the action called by the rule.
Msg ID	Server or Sterling Control Center message ID issued with the event.
Msg Short Text	Message short text for the message ID.

Following is a sample report:

Connect:Direct Events

From: **2003/06/02 00:00:00**   To: **2003/06/11 23:59:59**

Selected Event Types: 6, 3, 4

Date/Time	Node ID	Event Type	Alert	Alert Deleted By	Rule ID	Action ID	Msg ID	Msg Short Text
2003/06/02 20:38:54.000	SV160DELL3	3 Process started					LSMG200I	Process number 5 (name ASCII001, SNODE SVDELL3WPVM) executing
2003/06/02 20:38:54.000	SV160DELL3B	3 Process started					LSMG200I	Process number 5 (name ASCII001, SNODE SVDELL3WPVM) executing
2003/06/02 20:39:10.000	SV160DELL3B	3 Process started					LSMG200I	Process number 6 (name ASCII001, SNODE SVDELL3WPVM) executing
2003/06/02 20:39:10.000	SV160DELL3	4 Process ended					LSMG252I	A user process has completed successfully.
2003/06/02 20:39:10.000	SV160DELL3B	4 Process ended					LSMG252I	A user process has completed successfully.
2003/06/02 20:39:10.000	SV160DELL3	3 Process started					LSMG200I	Process number 6 (name ASCII001, SNODE SVDELL3WPVM) executing
2003/06/02 20:39:40.000	SV160DELL3	3 Process started					LSMG200I	Process number 7 (name ASCII001, SNODE SVDELL3WPVM) executing
2003/06/02 20:39:40.000	SV160DELL3B	3 Process started					LSMG200I	Process number 7 (name ASCII001, SNODE SVDELL3WPVM) executing
2003/06/02 20:39:40.000	SV160DELL3	4 Process ended					LSMG252I	A user process has completed successfully.
2003/06/02 20:39:40.000	SV160DELL3B	4 Process ended					LSMG252I	A user process has completed successfully.
2003/06/02 20:40:37.000	SV160DELL3	3 Process started					LSMG200I	Process number 8 (name ASCII001, SNODE SVDELL3WPVM) executing
2003/06/02 20:40:37.000	SV160DELL3B	3 Process started					LSMG200I	Process number 8 (name ASCII001, SNODE SVDELL3WPVM) executing
2003/06/02 20:41:06.000	SV160DELL3B	4 Process ended					LSMG252I	A user process has completed successfully.
2003/06/02 20:41:06.000	SV160DELL3	4 Process ended					LSMG252I	A user process has completed successfully.
2003/06/02 20:43:14.000	SV160DELL3B	3 Process started					LSMG200I	Process number 9 (name ASCII001, SNODE SVDELL3WPVM) executing
2003/06/02 20:43:14.000	SV160DELL3	3 Process started					LSMG200I	Process number 9 (name ASCII001, SNODE SVDELL3WPVM) executing
2003/06/02 20:43:42.000	SV160DELL3	4 Process ended					LSMG252I	A user process has completed successfully.

Printed: 06/11/2003   10:01:23AM

Sterling Control Center Reports Guide

Connect:Direct Exception Trends

The Connect:Direct Exception Trends report lists exception counts by category (such as failed Process steps or Copy steps) during a specified time period. You can specify the report by month, week, day, or hour. This report is in date/time order.

The file name for this report is CD_Exception_Trends_By_Period.rpt.

The following table lists selection criteria for this report:

Criteria	Description
Period	Time period that the data is summarized by: monthly, weekly, daily, and hourly.
Start Date	Start date of the data range.
End Date	End date of the data range.
Start Time	Start time of the data range. The default is 00:00:00 (midnight).
End Time	End time of the data range. The default is 23:59:59.

The following table describes the report columns:

Column	Description
Processes Total	Total number of Processes (failed and successful) for the specified time period.
Processes Failed	Number of Processes for the specified time period that completed with completion code greater than 0.
Processes % Failed	Percentage of Processes for the specified time period that completed with completion code greater than 0.
Copy Steps Total	Total number of Copy steps (failed and successful) for the specified time period.
Copy Steps Failed	Number of Copy steps for the specified time period that completed with completion code greater than 0.
Copy Steps % Failed	Percentage of Copy steps for the specified time period that completed with completion code greater than 0.
Run Tasks Total	Total number of Run Task steps (failed and successful) for the specified time period.
Run Tasks Failed	Number of Run Task steps for the specified time period that completed with completion code greater than 0.
Run Tasks % Failed	Percentage of Run Task steps for the specified time period that completed with completion code greater than 0.
Run Jobs Total	Total number of Run Job steps (failed and successful) for the specified time period.
Run Jobs Failed	Number of Run Job steps for the specified time period that completed with completion code greater than 0.

Column	Description
Run Jobs % Failed	Percentage of Run Job steps for the specified time period that completed with completion code greater than 0.
Submit Steps Total	Total number of Submit steps (failed and successful) for the specified time period.
Submit Steps Failed	Number of Submit steps for the specified time period that completed with completion code greater than 0.
Submit Steps % Failed	Percentage of Submit steps for the specified time period that completed with completion code greater than 0.

Following is a report sample:

Connect:Direct Exception Trends

From: 2003/06/02 00:00:00   To: 2003/06/11 23:59:59   Period: Daily

	Processes			Copy Steps			Run Tasks			Run Jobs			Submit Steps		
	Total	Failed	% Failed	Total	Failed	% Failed	Total	Failed	% Failed	Total	Failed	% Failed	Total	Failed	% Failed
2003/06/02	13	1	7.69%	15	3	20.00%	0	0	0.00%	0	0	0.00%	0	0	0.00%
2003/06/03	6	0	0.00%	6	0	0.00%	0	0	0.00%	0	0	0.00%	0	0	0.00%
2003/06/05	6	0	0.00%	6	0	0.00%	0	0	0.00%	0	0	0.00%	0	0	0.00%
2003/06/06	77	2	2.60%	81	6	7.41%	0	0	0.00%	0	0	0.00%	0	0	0.00%
2003/06/09	51	0	0.00%	51	0	0.00%	0	0	0.00%	0	0	0.00%	0	0	0.00%
2003/06/10	16	4	25.00%	16	4	25.00%	0	0	0.00%	0	0	0.00%	0	0	0.00%
2003/06/11	68	0	0.00%	68	0	0.00%	0	0	0.00%	0	0	0.00%	0	0	0.00%

Printed: 06/11/2003   9:58:57AM

Page 1 of 1

Connect:Direct Exception Trends Chart

The Connect:Direct Exception Trends Chart is nearly identical to *Connect:Direct Exception Trends* on page 91. The only difference is that this report displays the following graphs on the first page:

✦ Daily total Copy steps (successful and failed)

✦ Daily percentage of failed Copy steps

The file name for this report is CD_Charts_Bar_Copy and PctFail_ByDay.rpt.

The selection criteria and report columns for this report are the same as the Connect:Direct Exception Trends report.

Following is a sample report:

Copy Total Steps Per Day

Legend: 2003/05/11, 2003/05/10, 2003/05/09, 2003/05/06, 2003/05/05, 2003/05/03, 2003/05/02

Copy Steps Pct Failed per Day

Legend: 2003/06/02, 2003/06/03, 2003/06/05, 2003/06/06, 2003/06/09, 2003/06/10, 2003/06/11
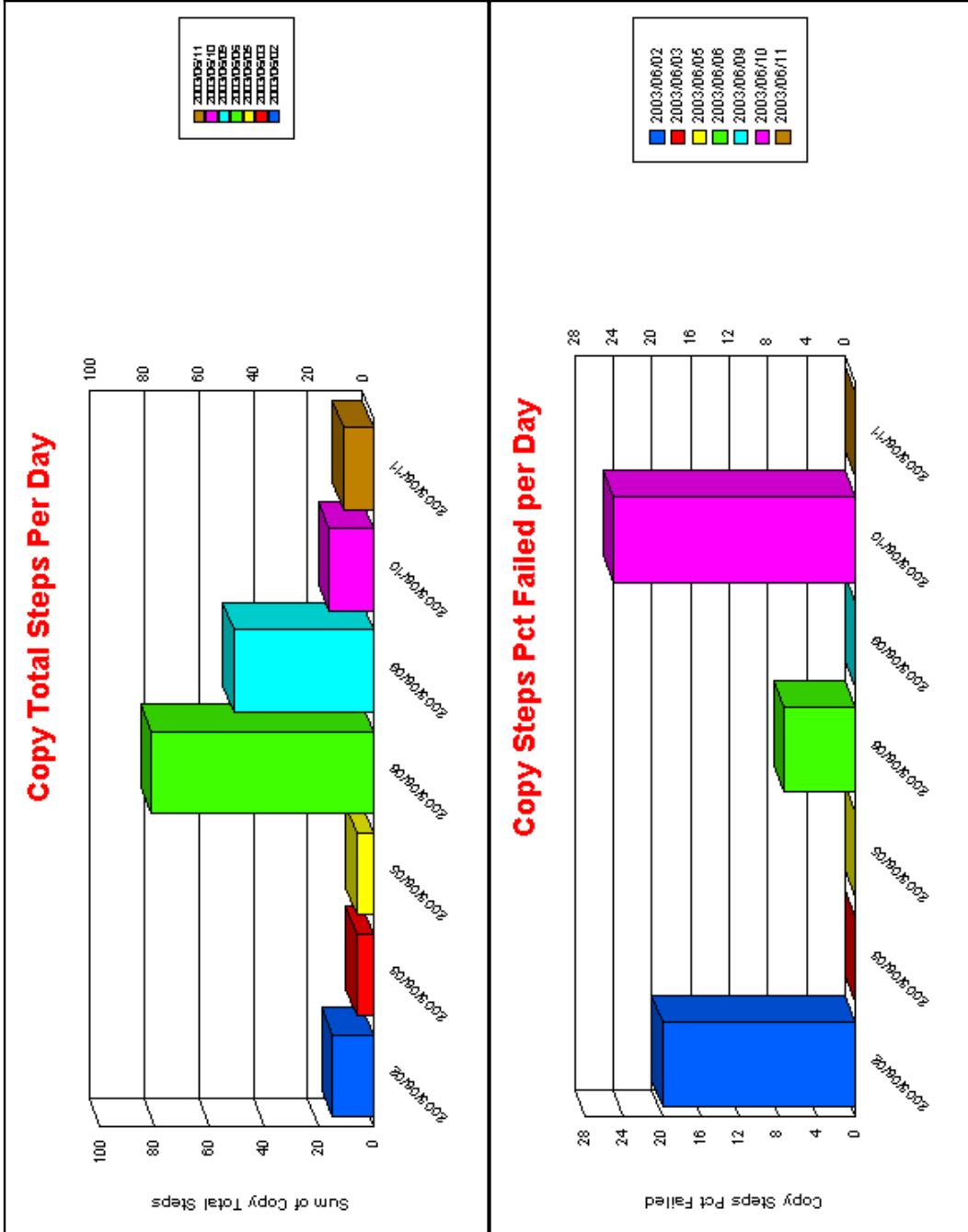
Connect:Direct Usage Report

The Connect:Direct Usage Report details Process activity during a specified time period. You can select to show all Connect:Direct activity or exception processing only. This report is in date/time order.

The last page of the report summarizes totals and average run time for Processes, Copy steps, Run Jobs, Run Tasks, and Submit steps, and file transfer information for the report.

The file name for this report is CD_Usage_and_Exceptions.rpt.

The following table lists selection criteria for this report:

Criteria	Description
Exceptions Only (Y/N)	Indicates if the report shows all Connect:Direct activity or exception processing only.
Start Date	Start date of the data range.
End Date	End date of the data range.
Start Time	Start time of the data range. The default is 00:00:00 (midnight).
End Time	End time of the data range. The default is 23:59:59.

The following table describes the report columns:

Column	Description
Log Date Time	Date and time that the statistics record was written to the log file. Format yyyy/mm/dd hh:mm:ss.msmsms.
Rec Type	Type of statistics record generated. See the *Event Type Descriptions* topic in the Help for a list of record IDs.
PNODE	Primary node name.
Dir	Data transfer or command direction. ==> indicates from the PNODE to the SNODE. <== indicates from the SNODE to the PNODE.
SNODE	Secondary node name.
Proc Name	Connect:Direct Process name.
Proc Nbr	Connect:Direct Process number.
Step Name	Process step.
Duration	Amount of time the step took. Format hh:mm:ss.

Column	Description
CC	Condition code associated with step termination. Typical codes are: 0=Successful execution. 4=A warning level error was encountered. The statement probably finished normally, but you should verify the execution results. 8=An error occurred during execution. 16=A catastrophic error occurred during execution.
Msg ID	Server or Sterling Control Center message ID issued with the event.
File Name	Name of the transferred file. Depending on the step, this can be either the source or destination file name.
The following columns are displayed on the summary page.	
Total	Total number (successful and failed) of Processes, Copy steps, Run Job Steps, Run Task steps, and Submit steps for the specified time period.
Successful	Number of Processes, Copy steps, Run Job Steps, Run Task steps, and Submit steps that completed with a condition code of 0 for the specified time period.
Failed	Number of Processes, Copy steps, Run Job Steps that completed with a condition code greater than 0 for the specified time period.
% Failed	Percent of Processes, Copy steps, Run Job Steps that completed with a condition code greater than 0 for the specified time period.
Average Time	Average time for a Process, Copy step, Run Job Step, Run Task step, and Submit step for the specified time period. This average includes all successful and failed Processes and steps.
Bytes Sent	Total number of bytes read from source files for the specified time period for all Copy Steps.
Bytes Received	Total number of bytes received by destination files for the specified time period for all Copy Steps.
Avg Send Rate (Bytes/Sec)	Average send rate in bytes/second for all Copy Steps.
Avg Receive Rate (Bytes/Sec)	Average receive rate in bytes/second for all Copy Steps.

Following is a sample report:

Connect:Direct Usage Report

From: 2003/06/01 00:00:00   To: 2003/06/11 23:59:59

LOG DATE TIME	REC TYPE	PNODE	DIR	SNODE	PROC NAME	PROC NBR	STEP NAME	DURATION	CC	MSG ID	FILE NAME
2003/06/02 20:39:10.000	Copy Step	SV160DELL3	==>	SVDELL3WPVM	ASCII001	5	STEP0001	00:00:16	0	SCPA000I	\\Svdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:39:10.000	Process	SV160DELL3	<==	SVDELL3WPVM	ASCII001	5		00:00:16	0	LSMG252I	
2003/06/02 20:39:10.000	Copy Step	SV160DELL3	==>	SVDELL3WPVM	ASCII001	5	STEP0001	00:00:16	0	SCPA000I	\\Svdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:39:10.000	Process	SV160DELL3	<==	SVDELL3WPVM	ASCII001	5		00:00:16	0	LSMG252I	
2003/06/02 20:39:39.000	Copy Step	SV160DELL3	==>	SVDELL3WPVM	ASCII001	6	STEP0001	00:00:28	0	SCPA000I	\\Svdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:39:39.000	Copy Step	SV160DELL3	==>	SVDELL3WPVM	ASCII001	6	STEP0001	00:00:28	0	SCPA000I	\\Svdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:39:40.000	Process	SV160DELL3	<==	SVDELL3WPVM	ASCII001	6		00:00:29	0	LSMG252I	
2003/06/02 20:39:40.000	Process	SV160DELL3	<==	SVDELL3WPVM	ASCII001	6		00:00:29	0	LSMG252I	
2003/06/02 20:40:06.000	Copy Step	SV160DELL3	==>	SVDELL3WPVM	ASCII001	7	STEP0001	00:00:26	8	LSMG250I	\\Svdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:40:06.000	Copy Step	SV160DELL3	==>	SVDELL3WPVM	ASCII001	7	STEP0001	00:00:26	8	LSMG250I	\\Svdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:41:06.000	Copy Step	SV160DELL3	==>	SVDELL3WPVM	ASCII001	8	STEP0001	00:00:28	0	SCPA000I	\\Svdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:41:06.000	Process	SV160DELL3	<==	SVDELL3WPVM	ASCII001	8		00:00:28	0	LSMG252I	
2003/06/02 20:41:06.000	Copy Step	SV160DELL3	==>	SVDELL3WPVM	ASCII001	8	STEP0001	00:00:28	0	SCPA000I	\\Svdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:41:06.000	Process	SV160DELL3	<==	SVDELL3WPVM	ASCII001	8		00:00:28	0	LSMG252I	
2003/06/02 20:43:42.000	Process	SV160DELL3	<==	SVDELL3WPVM	ASCII001	9		00:00:28	0	LSMG252I	
2003/06/02 20:43:42.000	Copy Step	SV160DELL3	==>	SVDELL3WPVM	ASCII001	9	STEP0001	00:00:28	0	SCPA000I	\\Svdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:43:42.000	Process	SV160DELL3	<==	SVDELL3WPVM	ASCII001	9		00:00:28	0	LSMG252I	
2003/06/02 20:43:42.000	Copy Step	SV160DELL3	==>	SVDELL3WPVM	ASCII001	9	STEP0001	00:00:28	0	SCPA000I	\\Svdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:49:02.000	Copy Step	SV160DELL3	==>	SVDELL3WPVM	ASCII001	5	STEP0001	00:00:17	0	SCPA000I	\\Svdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:49:02.000	Process	SV160DELL3	<==	SVDELL3WPVM	ASCII001	5		00:00:17	0	LSMG252I	
2003/06/02 20:49:02.000	Copy Step	SV160DELL3	==>	SVDELL3WPVM	ASCII001	6	STEP0001	00:00:29	0	SCPA000I	\\Svdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:49:31.000	Process	SV160DELL3	<==	SVDELL3WPVM	ASCII001	6		00:00:29	0	LSMG252I	
2003/06/02 20:49:58.000	Process	SV160DELL3	<==	SVDELL3WPVM	ASCII001	7		00:00:26	8	LSMG250I	

Printed: 06/11/2003   10:08:42AM

Connect:Direct Usage Report Chart

The Connect:Direct Usage Report Chart is nearly identical to the *Connect:Direct Usage Report* on page 96. The only difference is that the last page of this report displays two pie charts categorizing usage by step type and failed step type.

You can select to show all Connect:Direct activity or exception processing only. This report is in date/time order.

The next-to-last page of the report summarizes totals and average run time for Processes, Copy steps, Run Jobs, Run Tasks, and Submit steps, and file transfer information for the report.

The file name for this report is CD_Charts_Pie _Usage_and_Exceptions.rpt.

The selection criteria and report columns for this report are the same as for the Connect:Direct Usage Report.

Following is a sample report:

Connect:Direct Usage Report

From: 2003/06/01 00:00:00   **To:** 2003/06/11 23:59:59

Percentages by Step Type

50.

8.33%

Sum of @#CopyTotalSteps	50.7%
Sum of @#ProcessesTotal	49.3%
Sum of @#RunJobsTotal	0.0%
Sum of @#RunTasksTotal	0.0%
Sum of @#SubmitStepsTotal	0.0%
Total:	100.0%
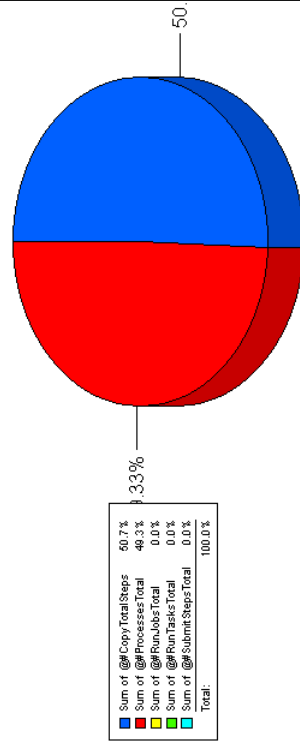
Percentages by Bad Step Type

35.00%

Sum of @#ProcessesBad	35.0%
Sum of @#CopyBadSteps	65.0%
Sum of @#RunJobsBad	0.0%
Sum of @#RunTasksBad	0.0%
Sum of @#SubmitStepsBad	0.0%
Total:	100.0%

Printed: 06/11/2003   9:57:05AM
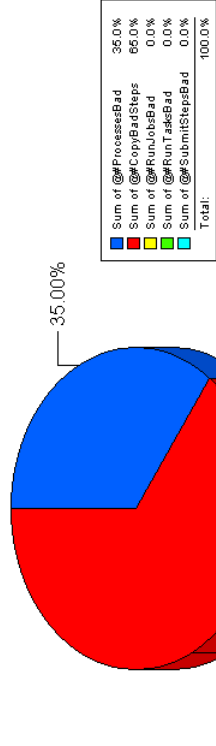
Connect:Direct Usage by Server Pair Report

The Connect:Direct Usage by Server Pair Report summarizes by PNODE-SNODE the type of activity occurring during a specified time period. This report is in alphabetic PNODE-SNODE pair order.

You can select to show all Connect:Direct activity or exception processing only.

You can see the detail for any summary item by double-clicking the item. The detail is identical to the *Connect:Direct Usage Report* on page 96.

The file name for this report is CD_Usage_By_ServerPair_and_Exceptions.rpt.

The following table lists selection criteria for this report:

Criteria	Description
Exceptions Only (Y/N)	Indicates if the report shows all Connect:Direct activity or exception processing only.
Start Date	Start date of the data range.
End Date	End date of the data range.
Start Time	Start time of the data range. The default is 00:00:00 (midnight).
End Time	End time of the data range. The default is 23:59:59.

The following table describes the report columns:

Column	Description
Total	Total number (successful and failed) of Processes, Copy steps, Run Job steps, Run Task steps, and Submit steps for the indicated PNODE-SNODE combination during the specified time period.
Failed	Number of Processes, Copy steps, Run Job steps, Run Task steps, and Submit steps that completed with a condition code greater than 0 for the indicated PNODE-SNODE combination during the specified time period.
% Failed	Percentage of Processes, Copy steps, Run Job steps, Run Task steps, and Submit steps that completed with a condition code greater than 0 for the indicated PNODE-SNODE combination during the specified time period.
Average Time	Average time for a Process, Copy step, Run Job step, Run Task step, and Submit step for the indicated PNODE-SNODE combination during the specified time period.
Bytes Sent	Total number of bytes read from source files for all Copy Steps on the indicated PNODE-SNODE combination.
Bytes Received	Total number of bytes received by destination files for all Copy Steps on the indicated PNODE-SNODE combination.
Avg Send Rate (Bytes/Sec)	Average send rate in bytes/second for all Copy Steps on the indicated PNODE-SNODE combination.
Avg Receive Rate (Bytes/Sec)	Average receive rate in bytes/second for all Copy Steps on the indicated PNODE-SNODE combination.

Column	Description
The following columns are displayed on the summary page.	
Successful	Number of Processes, Copy steps, Run Job Steps, Run Task steps, and Submit steps that completed with a condition code of 0 for the specified time period. This information is not displayed on the exceptions only report.
Failed	Number of Processes, Copy steps, Run Job Steps that completed with a condition code greater than 0 for the specified time period.
Total	Total number (successful and failed) of Processes, Copy steps, Run Job Steps, Run Task steps, and Submit steps for the specified time period. This information is not displayed on the exceptions only report.
Average Time	Average time for a Process, Copy step, Run Job Step, Run Task step, and Submit step for the specified time period. This average includes all successful and failed Processes and steps. This information is not displayed on the exceptions only report.
Bytes Sent	Total number of bytes read from source files for the specified time period for all Processes and Copy Steps. This information is not displayed on the exceptions only report.
Bytes Received	Total number of bytes received by destination files for the specified time period for all Processes and Copy Steps. This information is not displayed on the exceptions only report.
Avg Send Rate (Bytes/Sec)	Average send rate in bytes/second for all Processes and Copy Steps. This information is not displayed on the exceptions only report.
Avg Receive Rate (Bytes/Sec)	Average receive rate in bytes/second for all Processes and Copy Steps. This information is not displayed on the exceptions only report.

Following is a sample report:

Connect:Direct Usage By Server Pair - Report

From: 2003/06/01 00:00:00   To: 2003/06/11 23:59:59

SV160DELL3 <==> SV160DELL3

| | 2003/06/01 00:00:00 | | 2003/06/11 23:59:59 |
	PROCESSES	COPY STEPS	RUN JOBS	RUN TASKS	SUBMIT STEPS
Total:	4	4	0	0	0
Failed:	4	4	0	0	0
% Failed:	100.00%	100.00%	0.00%	0.00%	0.00%
Average Time:	00:00:00.00	00:00:00.00	00:00:00.00	00:00:00.00	00:00:00.00
Bytes Sent:		0			
Bytes Received:		0			
Avg Send Rate: (Bytes/Sec)		0.00			
Avg Receive Rate: (Bytes/Sec)		0.00			

Printed: 06/11/2003   10:11:48AM

Connect:Direct Usage by Server Pair Report Chart

The Connect:Direct Usage by Server Pair Report Chart is nearly identical to the *Connect:Direct Usage by Server Pair Report* on page 101. The only difference is that this report displays the following three usage graphs for each server pair:

✦ Daily Process and Copy steps

✦ Daily failed Process and Copy steps

✦ Daily Copy bytes sent and received

You can select to show all Connect:Direct activity or exception processing only. This report is in alphabetic PNODE-SNODE pair order.

The last page of the report summarizes totals and average run time for Processes, Copy steps, Run Jobs, Run Tasks, and Submit steps, and file transfer information for the report.

The file name for this report is CD_Charts_Line _ServerPair_ByDay.rpt.

The selection criteria and report columns for this report are the same as the Connect:Direct Usage by Server Pair Report.

Following is a sample:

Connect:Direct Usage By Server Pair - Report

From: 2003/04/30 00:00:00   **To:** 2003/06/11 23:59:59

LOG DATE TIME	DIR	REC TYPE	PROC NAME	PROC NBR	STEP NAME	DURATION	CC	MSG ID	FILE NAME

Processes and Copy Steps - by the Day
For SV160DELL3 <==> SVDELL3WPVM
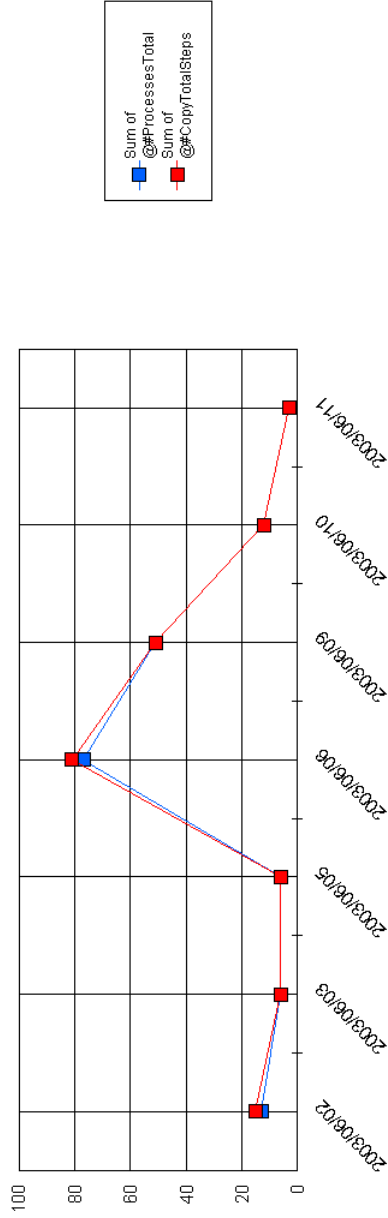
Sum of @#ProcessesTotal
Sum of @#CopyTotalSteps

Connect:Direct Usage by Server Pair Detail/Summary Report

The Connect:Direct Usage by Server Pair report shows Process activity occurring during a specified time period by PNODE-SNODE. This report is in alphabetic PNODE-SNODE pair order.

You can specify this report to show detail and summary information or summary information only. You can also select to show all Connect:Direct activity or exception processing only.

The last page of the report displays summary report data.

The file name for this report is CD_Usage_By_ServerPair_and_Exceptions_Summary_Detail.rpt.

The following table lists selection criteria for this report:

Criteria	Description
Exceptions Only (Y/N)	Indicates if the report shows all Connect:Direct activity or exception processing only.
Summary_Detail (S/D)	Indicates if the report shows detail and summary information or only summary information.
Start Date	Start date of the data range.
End Date	End date of the data range.
Start Time	Start time of the data range. The default is 00:00:00 (midnight).
End Time	End time of the data range. The default is 23:59:59.

The following table describes the report columns:

Column	Description
The following information is shown only on the detail report.	
Log Date Time	Date and time that the statistics record was written to the log file. Format yyyy/mm/dd hh:mm:ss.msmsms.
Dir	Data transfer or command direction. ==> indicates from the PNODE to the SNODE. <== indicates from the SNODE to the PNODE.
Rec Type	Type of statistics record generated. See the documentation for the appropriate Connect:Direct platform for a list of record IDs.
Proc Name	Connect:Direct Process name.
Proc Nbr	Connect:Direct Process number.
Step Name	Process step.
Duration	Amount of time the step took. Format hh:mm:ss.

Column	Description
CC	Condition code associated with step termination. Typical codes are: 0=Successful execution. 4=A warning level error was encountered. The statement probably finished normally, but you should verify the execution results. 8=An error occurred during execution. 16=A catastrophic error occurred during execution. This report only shows condition codes greater than 0.
Msg ID	Server or Sterling Control Center message ID issued with the event.
File Name	Name of the transferred file. Depending on the step, this can be either the source or destination file name.
The following columns are displayed on the summary report and the last page of the detail report.	
Successful	Number of Processes, Copy steps, Run Job Steps, Run Task steps, and Submit steps that completed with a condition code of 0 for the specified time period. This information is not displayed on the exceptions only report.
Failed	Number of Processes, Copy steps, Run Job Steps that completed with a condition code greater than 0 for the specified time period.
Total	Total number (successful and failed) of Processes, Copy steps, Run Job Steps, Run Task steps, and Submit steps for the specified time period. This information is not displayed on the exceptions only report.
Average Time	Average time for a Process, Copy step, Run Job Step, Run Task step, and Submit step for the specified time period. This average includes all successful and failed Processes and steps. This information is not displayed on the exceptions only report.
Bytes Sent	Total number of bytes read from source files for the specified time period for all Processes and Copy Steps. This information is not displayed on the exceptions only report.
Bytes Received	Total number of bytes received by destination files for the specified time period for all Processes and Copy Steps. This information is not displayed on the exceptions only report.
Avg Send Rate (Bytes/Sec)	Average send rate in bytes/second for all Processes and Copy Steps. This information is not displayed on the exceptions only report.
Avg Receive Rate (Bytes/Sec)	Average receive rate in bytes/second for all Processes and Copy Steps. This information is not displayed on the exceptions only report.

Following is a sample report:

Connect:Direct Usage By Server Pair - Detail Report

From: 2003/06/01 00:00:00   To: 2003/06/11 23:59:59

SV160DELL3 <==> SVDELL3WPVM

LOG DATE TIME	DIR	REC TYPE	PROC NAME	PROC NBR	STEP NAME	DURATION	CC	MSG ID	FILE NAME
2003/06/02 20:39:10.000	==>	Copy Step	ASCII001	5		00:00:16	0	SCPA000I	\\S\vdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:39:10.000	<==	Process	ASCII001	5		00:00:16	0	LSMG252I	
2003/06/02 20:39:10.000	==>	Copy Step	ASCII001	5		00:00:16	0	SCPA000I	\\S\vdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:39:10.000	<==	Process	ASCII001	5		00:00:16	0	LSMG252I	
2003/06/02 20:39:39.000	==>	Copy Step	ASCII001	6		00:00:28	0	SCPA000I	\\S\vdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:39:39.000	<==	Copy Step	ASCII001	6		00:00:28	0	SCPA000I	\\S\vdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:39:40.000	<==	Process	ASCII001	6		00:00:29	0	LSMG252I	
2003/06/02 20:39:40.000	<==	Process	ASCII001	6		00:00:29	0	LSMG252I	
2003/06/02 20:40:06.000	==>	Copy Step	ASCII001	7		00:00:26	8	LSMG252I	\\S\vdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:40:06.000	==>	Copy Step	ASCII001	7		00:00:26	8	LSMG250I	\\S\vdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:41:06.000	<==	Copy Step	ASCII001	8		00:00:28	0	SCPA000I	\\S\vdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:41:06.000	<==	Process	ASCII001	8		00:00:28	0	LSMG252I	
2003/06/02 20:41:06.000	==>	Copy Step	ASCII001	8		00:00:28	0	SCPA000I	\\S\vdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:41:06.000	<==	Process	ASCII001	9		00:00:28	0	LSMG252I	
2003/06/02 20:43:42.000	<==	Process	ASCII001	9		00:00:28	0	LSMG252I	
2003/06/02 20:43:42.000	==>	Copy Step	ASCII001	9		00:00:28	0	SCPA000I	\\S\vdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:43:42.000	<==	Process	ASCII001	9		00:00:28	0	LSMG252I	
2003/06/02 20:43:42.000	==>	Copy Step	ASCII001	9		00:00:28	0	SCPA000I	\\S\vdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:49:02.000	==>	Copy Step	ASCII001	5		00:00:17	0	SCPA000I	\\S\vdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:49:02.000	<==	Process	ASCII001	6		00:00:17	0	LSMG252I	
2003/06/02 20:49:31.000	==>	Copy Step	ASCII001	6		00:00:29	0	SCPA000I	\\S\vdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:49:31.000	<==	Process	ASCII001	7		00:00:29	0	LSMG252I	
2003/06/02 20:49:58.000	==>	Copy Step	ASCII001	7		00:00:26	8	LSMG250I	\\S\vdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:49:58.000	==>	Copy Step	ASCII001	8		00:00:26	8	LSMG250I	\\S\vdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:50:58.000	==>	Copy Step	ASCII001	8		00:00:28	0	SCPA000I	\\S\vdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:50:58.000	<==	Process	ASCII001	9		00:00:28	0	LSMG252I	
2003/06/02 20:53:34.000	==>	Copy Step	ASCII001	9		00:00:28	0	SCPA000I	\\S\vdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/02 20:53:35.000	<==	Process	ASCII001	9		00:00:29	0	LSMG252I	
2003/06/03 13:13:19.000	<==	Process	ASCII001	10		00:00:31	0	LSMG252I	
2003/06/03 13:13:19.000	==>	Copy Step	ASCII001	10		00:00:31	0	SCPA000I	\\S\vdell3wpvm\c_drive\Output\Binary\ascii.001
2003/06/03 13:13:19.000	<==	Process	ASCII001	10		00:00:31	0	LSMG252I	

Data for Third-Party Reporting Tools

Data for third-party reporting tools is contained in Sterling Control Center tables. The following tables are discussed here:

✦ Events Table (EVENTS)

✦ Events Extension Table (EVENTS_EXT)

✦ Event Comments Table (EVENT_COMMENTS)

✦ Connect:Direct Statistics Table (CD_STATS_LOG)

✦ Connect:Direct Statistics Table By Record ID

✦ Connect:Enterprise Statistics Table (CE_STATS_LOG)

✦ Event Type Table (EVENT_TYPE)

✦ Node Type Table (NODE_TYPE)

✦ Pair Connections Table (PAIR_CONN)

✦ Discovery Node Table (DISCOVERY_NODE)

✦ Metadata Labels Table (META_DATA_LABELS)

✦ Sterling Control Center Internal Tables

> **Note:** Some fields use a Java epoch timestamp as a unique value. This timestamp is the number of milliseconds that have elapsed since January 1, 1970.

Events Table (EVENTS)

The following table describes the data fields available from the Events table for Sterling Control Center reports.

Element	Type	Description
ACTION_ID	varchar	Name of an action called by a rule.
ACTIONS_COMPLETED	bigint	Indicates if the Sterling Control Center actions are completed. The values are: Null=Actions not completed Timestamp=Actions completed This element is used for restarts.
ALERT	char	Indicates if an alert was triggered. The values are: Null=No alert 0-3=Alert severity
ALERT_DELETED	char	Indicates if the alert was deleted. The values are: Null=Alert not deleted Y=Alert deleted
ALERT_DELETED_BY	varchar	Sterling Control Center user name of the person who removed the alert. If the alert was deleted by a rule, this field will contain "unknown."
ALERT_DESC	varchar	Comments entered by the user when the alert was deleted.
ALERT_UPD_TIME	bigint	Time that the alert was updated, in Java epoch timestamp format (that is, the number of milliseconds that have elapsed since January 1, 1970).
DATE_TIME	varchar	Date and time that the event was generated. Format yyyy/mm/dd hh:mm:ss.msmsms.
DEST_FILE	varchar	Destination file name in a copy operation.
EMAIL_FLAG	bigint	This field is used by Control Center for recover purposes. When a rule matches an event, the associated action is executed. If the action includes sending an e-mail, this flag updates after the e-mail is sent. Reporting on this field is not recommended. The values are: 0=No e-mail sent >0=E-mail sent The value is set to zero if nothing was done, but is set to the Timestamp if something was done.
EVENT_ID	bigint	ID number assigned by the system to each event.

Element	Type	Description
EVENT_TYPE	bigint	Code indicating the type of event. See *Event Type Table (EVENT_TYPE)* on page 131 for a listing of event types and descriptions.
FILE_SIZE	bigint	Size of the file transferred by the Connect:Direct Process or Connect:Enterprise batch.
FROM_NODE	varchar	Server that sent the file. P=Pnode was sending server. S=Snode was sending server.
MSG_ID	varchar	Server or Sterling Control Center message ID issued with the event.
NODE_ID	varchar	Server name of alias.
NODE_TYPE	varchar	Code indicating the type of server. The server types are: 0=Sterling Control Center 1=Connect:Direct 2=Connect:Enterprise 3=Sterling Integrator 4=FTP Server
ORIG_NODE	varchar	The server that initiated the Process.
PART_KEY	date	The date the event was generated. The format is yyyy-mm-dd.
PERCENT_COMPLETE	bigint	Percentage of a Connect:Direct Copy Process that is complete.
PROC_ID	varchar	Connect:Direct Process or Connect:Enterprise batch number.
PROC_NAME	varchar	Connect:Direct Process name or Connect:Enterprise batch name.
REMOTE_NODE	varchar	Name of the remote server involved in the Process or file transfer.
RET_CODE	varchar	Specifies a numeric code returned from a completed Process or file transfer that indicates failure or success. The standard return codes are: 0=Successful completion 4=Warning 8=Error 16=Catastrophic error
RULE_ID	varchar	Name of the rule triggered by the event.
RULE_INSTANCE_ID	bigint	Unique identifier for rule matching instances
SEQ_NUM	bigint	A number used to uniquely identify events generated at the same time.
SHORT_MSG	varchar	Message text associated with the Message ID.

Element	Type	Description
SLC_FLAG	bigint	Internally used by Control Center for recovery purposes. When an event is generated, it is sent to the SLC subsystem. This flag indicates whether or not the event has been sent to that subsystem. Reporting on this field is not recommended. The values are: 0=Event was not sent >0=Event was sent
SLC_ID	text	System-assigned name for each SLC window.
SLC_INSTANCE_ID	bigint	Unique identifier for each SLC window.
SLC_SOURCE_1	text	Internal field used for SLC recovery.
SLC_SOURCE_2	text	Internal field used for SLC recovery.
SLC_SRC_EVENT_ID	bigint	EVENT_ID of the event that triggered the SLC.
SOURCE_FILE	varchar	Source file name in a copy.
STEP_NAME	varchar	Name of the Connect:Direct Process step.
SUBMITTER	varchar	User ID of the Process submitter.
TRAP_FLAG	bigint	Internally used by Control Center for recovery purposes. When a rule matches an event, the associated action is executed. If the action includes sending an SNMP trap, this flag updates after the SNMP trap is sent. Reporting on this field is not recommended. The values are: 0=No trap generated >0=Trap generated The value is set to zero if nothing was done, but is set to the Timestamp if something was done.
USER_DATA_1	varchar	User metadata field 1.
USER_DATA_2	varchar	User metadata field 2.
USER_DATA_3	varchar	User metadata field 3.
USER_DATA_4	varchar	User metadata field 4.
SERVER_DATA_1	varchar	Server metadata field 1.
SERVER_DATA_2	varchar	Server metadata field 2.
SERVER_DATA_3	varchar	Server metadata field 3.
SERVER_DATA_4	varchar	Server metadata field 4.
SERVER_DATA_5	varchar	Server metadata field 5.
SERVER_DATA_6	varchar	Server metadata field 6.
SERVER_DATA_7	varchar	Server metadata field 7.
SERVER_DATA_8	varchar	Server metadata field 8.

Element	Type	Description
SERVER_DATA_9	varchar	Server metadata field 9.
SERVER_DATA_10	varchar	Server metadata field 10.
USER_OP_FLAG	bigint	Internally used by Control Center for recovery purposes. When a rule matches an event, the associated action is executed. If the action includes invoking an OS command script, this flag is updated after invoking the OS command script. Reporting on this field is not recommended. The values are: 0=No OS command invoked >0=OS command invoked The value is set to zero if nothing was done, but is set to the Timestamp if something was done.
XML_STRING	text	An XML representation of the event.

Events Extension Table (EVENTS_EXT)

The Events Extension (EVENTS_EXT) database table is used when an event triggers one or more Data Visibility Group (DVG) rules. For each DVG rule an event triggers, a supplemental entry, or row, is inserted into the EVENTS_EXT table and the EVENT_ID value is used to join the information in the two tables.

The following table describes the data fields available from the EVENTS_EXT table for Sterling Control Center reports.

Element	Type	Description
ACTION_ID	varchar	Name of an action called by a rule.
ACTIONS_COMPLETED	bigint	Indicates if the Sterling Control Center actions are completed. The values are: Null=Actions not completed Timestamp=Actions completed This element is used for restarts.
ALERT	char	Indicates if an alert was triggered. The values are: Null=No alert 0-3=Alert severity
ALERT_DELETED	char	Indicates if the alert was deleted. The values are: Null=Alert not deleted Y=Alert deleted
ALERT_DELETED_BY	varchar	Sterling Control Center user name of the person who removed the alert. If the alert was deleted by a rule, this field will contain "unknown."
ALERT_UPD_TIME	bigint	Time that the alert was updated, in Java epoch timestamp format (that is, the number of milliseconds that have elapsed since January 1, 1970).
DATE_TIME	varchar	Date and time that the event was generated. Format yyyy/mm/dd hh:mm:ss.msmsms.
DVG	varchar	Data visibility group for this event.
EMAIL_FLAG	bigint	This field is used by Control Center for recovery purposes. When a rule matches an event, the associated action is executed. If the action includes sending an e-mail, this flag updates after the e-mail is sent. Reporting on this field is not recommended. The values are: 0=No e-mail sent >0=E-mail sent The value is set to zero if nothing was done, but is set to the Timestamp if something was done.

Element	Type	Description
EVENT_ID	bigint	ID number assigned by the system to each event. The EVENT_ID value can be used to find additional information associated with this event in the Events database table.
PART_KEY	date	The date the event was generated. The format is yyyy-mm-dd.
RULE_ID	varchar	Name of the rule triggered by the event.
RULE_INSTANCE_ID	bigint	Unique identifier for rule matching instances
TRAP_FLAG	bigint	Internally used by Control Center for recovery purposes. When a rule matches an event, the associated action is executed. If the action includes sending an SNMP trap, this flag updates after the SNMP trap is sent. Reporting on this field is not recommended. The values are: 0=No trap generated >0=Trap generated The value is set to zero if nothing was done, but is set to the Timestamp if something was done.
USER_OP_FLAG	bigint	Internally used by Control Center for recovery purposes. When a rule matches an event, the associated action is executed. If the action includes invoking an OS command script, this flag is updated after invoking the OS command script. Reporting on this field is not recommended. The values are: 0=No OS command invoked >0=OS command invoked The value is set to zero if nothing was done, but is set to the Timestamp if something was done.

Event Comments Table (EVENT_COMMENTS)

The Event Comments Table stores comment information on alerts when those alerts are deleted. In earlier versions of Sterling Control Center these comments were part of the Events table.

The following table describes the data fields in the Event Comments table for Sterling Control Center reports:

Element	Type	Description
DATE_TIME	varchar	The event date and time.
EVENT_COMMENT	text	Textual comment describing the event's deletion.
EVENT_ID	bigint	The identifier for the specific event.
PART_KEY	date	The date the event was generated. The format is yyyy-mm-dd.
USER_ID	varchar	The identifier of the Control Center user entering the comment and deleting the event.

Connect:Direct Statistics Table (CD_STATS_LOG)

The following table describes the data fields available from the Connect:Direct Statistics (CD_STATS_LOG) table for Sterling Control Center reports:

Element	Type	Description
ALIAS_MEMBER_NAME	varchar	PDS alias member name.
BYTES_READ	bigint	Number of bytes read from the source file.
BYTES_RECEIVED	bigint	Number of bytes received by the destination file.
BYTES_SENT	bigint	Number of bytes sent to the destination file.
BYTES_WRITTEN	bigint	Number of bytes written to the destination file.
CB_ENC_ALG	varchar	Specifies the name of the encryption algorithm.
CERT_ISSUER	text	Issuer value from certificate used.
CERT_SUBJECT	text	Subject name value from certificate used.
CHECK_POINT	varchar	Indicates if Checkpoint is activated for this Process. Y=Checkpoint is activated N=Checkpoint is not activated
CIPHER_SUITE	text	Name of cipher suite used.
CLASS	varchar	Determines the server-to-server session on which a Process can be executed.
COND_CODE	varchar	Return code associated with step termination. Typical codes are: 0=Successful execution. 4=A warning level error was encountered. The statement probably finished normally, but you should verify the execution results. 8=An error occurred during execution. 16=A catastrophic error occurred during execution. **Note:** This column is not populated in this table since it is duplicated in the Events table.
DEBUG	varchar	For Connect:Direct OS/390, the DEBUG setting within the Process.

Element	Type	Description
DEST_DISP_1	varchar	What to do with the destination file after a copy is complete. The values are:
		NEW=Creates a new file on the destination node.
		RPL=Creates a new file on the destination node or, if the file already exists, replaces the named file on the destination node.
		MOD=Appends data to the end of an existing file for which you have exclusive rights.
DEST_DISP_2	varchar	Disposition of the destination file after a normal Process step termination. The values are:
		C=Catalog
		K=Keep
DEST_DISP_3	varchar	Disposition of the destination file after an abnormal Process step termination.
		C=Catalog
		D=Delete
		K=Keep
DEST_FILE	varchar	Destination file name.
		Note: This column is not populated in this table since it is duplicated in the Events table.
EVENT_ID	bigint	ID number assigned by the system to each event.
EXEC_PRIORITY	varchar	Priority under which the operating system thread that executes Connect:Direct runs. Applies to Windows only.
EXT_COMPRESSION	varchar	Extended compression option.
		Y=Extended compression is activated
		N=Extended compression is not activated
FEED_BACK	varchar	Feedback code for the module. The value depends on the module that creates it. Your Connect:Direct Customer Support representative may ask you for this value.
FROM_NODE	varchar	Node that sent the file. The values are:
		S=SNODE
		P=PNODE
		Note: This column is not populated in this table since it is duplicated in the Events table.
FUNCTION_INFO	varchar	Specifies the function being performed.

Element	Type	Description
HOLD	varchar	Hold status of a Process. The Hold statuses are:
		No=The Process is not placed in the Hold queue. It is executed as soon as resources are available.
		Yes=The Process is held in the Hold queue in Held Initially (HI) status until it is explicitly released.
		Call=The Process is held until the SNODE, as specified in the Process SNODE parameter, connects to the PNODE. The Process is then released for execution. The Process is also released when another Process on the PNODE connects to the SNODE.
LINK_FAIL	varchar	Indicated whether a link failure occurred during transmission.
		◆ Link fail occurred
		◆ Link fail did not occur
LOCAL_COND_CODE	varchar	Condition (return) code produced by the local server. See *COND_CODE* on page 117 for typical return codes.
LOCAL_MSG_ID	varchar	Specifies the message ID produced by the local server.
LOCAL_NODE	varchar	Server that processed the file.
		S=SNODE
		P=PNODE
LOG_DATE_TIME	varchar	Date and time that the statistics record was written to the log file. Format yyyy/mm/dd hh:mm:ss.msmsms.
MEMBER_NAME	varchar	Name of the member copied.
MERGE_EA	varchar	Specifies the merged data encryption algorithm resulting from the merger of the PNODE and SNODE encryption algorithms.
MERGE_SIGN	varchar	Specifies the merged results from the digital signature settings for the PNODE and SNODE. If digital signature is enabled for either the PNODE or the SNODE, then digital signatures are used for the session. If digital signatures are not enabled for both the PNODE and SNODE, digital signatures are not used.
MSG_ID	varchar	Server or Sterling Control Center message ID issued with the event.
		Note: This column is not populated in this table since it is duplicated in the Events table.
MSG_SHORT_TXT	varchar	Message short text.
		Note: This column is not populated in this table since it is duplicated in the Events table.
NODE_ID	varchar	Server alias.
		Note: This column is not populated in this table since it is duplicated in the Events table.
NODE_NAME	varchar	Name of the Connect:Direct server.

Element	Type	Description
NODE_TYPE	varchar	Code indicating the type of server.
		Note: This column is not populated in this table since it is duplicated in the Events table.
OTHER_COND_CODE	varchar	Condition (return) code produced by the other (remote) server. See *COND_CODE* on page 117 for typical return codes.
OTHER_MSG_ID	varchar	Specifies the message ID produced by the other (remote) server.
PART_KEY	date	The date the statistics record was written to the log file. The format is yyyy-mm-dd.
PNODE	varchar	Primary node name.
		Note: This column is not populated in this table since it is duplicated in the Events table.
PNODE_ACCT_INFO	varchar	PNODE accounting information.
PNODE_ENC_ALG_LIST	varchar	Data encryption algorithm used on the PNODE.
PNODE_ENC_DATA	varchar	PNODE encryption data.
PNODE_PLEX_CLASS	varchar	PLEXCLASS of the PNODE.
PNODE_SIGN	varchar	Specifies if digital signatures are enabled for the PNODE.
PREV_SIGN_VERIFIED	varchar	Specifies if the previous encryption key was used for verifying the digital signature.
PRIORITY	varchar	Specifies the priority assigned to the Process. The lower the number the higher the priority.
PROC_NAME	varchar	Connect:Direct Process name.
		Note: This column is not populated in this table since it is duplicated in the Events table.
PROC_NUMBER	varchar	Connect:Direct Process number.
		Note: This column is not populated in this table since it is duplicated in the Events table.
QUEUE	varchar	Specifies the queue containing the Process. The queues are:
		Execution=Processes currently being executed.
		Hold=Processes that are either held by the user or operator or held due to execution errors.
		Timer=Processes that are scheduled to be executed later, or Processes in time retry due to session errors.
		Wait=Processes that are eligible for execution and are awaiting selection.

Element	Type	Description
RECORD_CATEGORY	varchar	Specifies whether the record is related to an event or to a Process. The values are: CAEV=The record is related to a Connect:Direct event, such as a CONNECT:Direct shutdown. CAPR=The record is related to a Connect:Direct Process.
RECORD_ID	varchar	Type of statistics record generated. See the *Event Type Descriptions* Help topic for a list of record IDs.
RECORDS_READ	bigint	Specifies the number of records read from the source file.
RECORDS_WRITTEN	bigint	Specifies the number of records written to the destination file.
RESTART	varchar	Indicates if Restart is activated for the Process. Y=Restart was activated N=Restart was not activated
RETAIN	varchar	Indicates whether Connect:Direct retains a copy of a Process after it is executed. The Retain options are: Initial=Specifies to retain the Process in the Hold queue for execution every time that Connect:Direct initializes. No=Specifies not to retain the Process after it is executed. Yes=Specifies to retain the Process in the Hold queue after it is executed. You can release the Process for execution later or delete it.
RU_SIZE	varchar	Specifies the size of buffers received by the destination file.
RUS_RECEIVED	bigint	Specifies the number of buffers received by the destination file.
RUS_SENT	bigint	Specifies the number of buffers sent to the destination file.
SCH_DATE_TIME	varchar	Specifies the date and time that a Process is scheduled to execute. Format yyyy/mm/dd hh:mm:ss.msmsms.
SECURE_ENABLED	varchar	Indicates that Secure+ is activated for the Process.
SECURE_PROTOCOL	text	Name of protocol used for secure connection.
SEQ_NUM	bigint	System-assigned sequence number. **Note:** This column is not populated in this table since it is duplicated in the Events table.
SERVER_NAME	varchar	Connect:Direct/Plex server name.
SNODE	varchar	Secondary node name. **Note:** This column is not populated in this table since it is duplicated in the Events table.
SNODE_ACCT_INFO	varchar	Specifies SNODE accounting information.
SNODE_ENC_ALG_LIST	varchar	Data encryption algorithm used on the SNODE.
SNODE_ENC_DATA	varchar	SNODE encryption data.

Element	Type	Description
SNODE_PLEX_CLASS	varchar	PLEXCLASS of the SNODE.
SNODE_SIGN	varchar	Specifies if digital signatures are enabled for the SNODE.
SOURCE_MEMBER_NAME	varchar	Source file member name.
SRC_DISP_1	varchar	Specifies access to the source file during a copy operation. The source disposition values are: SHR=The file can be opened by another Process for read-only access while it is being copied. OLD=The file cannot be opened by another Process during the transfer.
SRC_DISP_2	varchar	Disposition of the source file after a successful Process step termination.
SRC_DISP_3	varchar	Disposition of the source file after an abnormal Process step termination.
SRC_FILE	varchar	Source file name. **Note:** This column is not populated in this table since it is duplicated in the Events table.
START_TIME	varchar	Process start time.

Element	Type	Description
STATUS	varchar	Specifies the Process status. The statuses are:
		Execution (EX)=The Process is executing.
		Pending Execution (PE)=The Process is selected for execution and startup is in progress.
		Waiting Connection (WC)=The Process is ready to execute, but all available connections to the SNODE are in use.
		Waiting Start Time (WS)=The Process is waiting in the Timer queue because it was submitted with a start time or date that has not expired. When the start time is reached, the Process is placed into the Wait queue for scheduling for execution.
		Held Suspension (HS)=The operator issued a delete Process request with Hold set to Yes.
		Timer Retry (RE)=A Process error occurred and the Process was moved to the Timer queue in RE status with short-term and long-term wait times beginning.
		Held for Call (HC)=The Process was submitted with the Hold parameter set to Call. A session started from either node moves the Process to the Wait queue in WC status. The Process is placed in the Execution queue when it is selected for execution.
		Held Due to Error (HE)=A session error or other abnormal condition occurred.
		Held Initially (HI)=The Process was submitted with the Hold option set to Yes.
		Held By Operator (HO)=A change Process request with Hold set to Yes was issued.
		Held By Retain (HR)=The Process was submitted with retain after execution set to Yes or Initial.
STD_COMPRESSION	varchar	Standard compression option.
		Y=Standard compression is activated
		N=Standard compression is not activated
STEP_NAME	varchar	Process step name.
		Note: This column is not populated in this table since it is duplicated in the Events table.
STOP_TIME	varchar	Process stop time.
SUB_DATE_TIME	varchar	Date and time that the Process was submitted. Format yyyy/mm/dd hh:mm:ss.msmsms.
SUBMIT_NODE	varchar	Server where the submit operation was performed.
SUBMITER	varchar	User ID that submitted the Process.
		Note: This column is not populated in this table since it is duplicated in the Events table.
SUBMITTER_NODE	varchar	Server that submitted the Process.

Element	Type	Description
SUR_SIGN_VERIFIED	varchar	Specifies if the current encryption key was used for verifying the digital signature.
SYS_OPTS	varchar	Specifies the platform-specific system operations.
TARGET_MEMBER_NAME	varchar	Destination target member name.
TRANSLATION	varchar	Specifies if the data was translated. Y=Data was translated N=Data was not translated
USER_DATA_1	varchar	Metadata field 1. **Note:** This column is not populated in this table since it is duplicated in the Events table.
USER_DATA_2	varchar	Metadata field 2. **Note:** This column is not populated in this table since it is duplicated in the Events table.
USER_DATA_3	varchar	Metadata field 3. **Note:** This column is not populated in this table since it is duplicated in the Events table.
USER_DATA_4	varchar	Metadata field 4. **Note:** This column is not populated in this table since it is duplicated in the Events table.

Connect:Direct Statistics Table By Record ID

The following table shows the columns filled in for each Record ID in the Virtual Connect:Direct Statistics Table (V_CD_STATS_LOG). These record IDs are for Connect:Direct z/OS only.

Record ID	SI	CH	QE	SB	PI	ZI	CI	CT	PT	ZT	MC
ALIAS_MEMBER_NAME											X
BYTES_READ								X			
BYTES_SENT								X			
CERT_ISSUER				X				X			
CERT_SUBJECT				X				X			
CHECK_POINT								X			
CIPHER_SUITE				X				X			
COND_CODE	X	X		X	X	X	X	X	X	X	
DEST_DISP_1								X			
DEST_DISP_2								X			
DEST_DISP_3								X			
DEST_FILE								X			
EVENT_ID	X	X	X	X	X	X	X	X	X	X	
FEED_BACK								X			
FROM_NODE							X	X			
LOCAL_NODE								X			X
LOG_DATE_TIME	X	X	X	X	X	X	X	X	X	X	
MEMBER_NAME							X	X			X
MSG_ID	X	X						X	X	X	
MSG_SHORT_TXT	X	X						X	X	X	
NODE_ID	X	X	X	X	X	X	X	X	X	X	
NODE_NAME	X	X	X	X	X	X	X	X	X	X	
NODE_TYPE	X	X	X	X	X	X	X	X	X	X	
OTHER_COND_CODE								X			
OTHER_MSG_ID								X			

Record ID	SI	CH	QE	SB	PI	ZI	CI	CT	PT	ZT	MC
PNODE			X	X	X	X	X	X	X	X	
PNODE_ACCT_INFO								X			
PNODE_ENC_ALG_LIST				X							
PNODE_PLEX_CLASS								X			
PNODE_SIGN				X							
PRIORITY		X									
PROC_NAME		X	X	X	X	X	X	X	X	X	
PROC_NUMBER		X	X	X	X	X	X	X	X	X	
QUEUE			X								
RECORD_ID	X	X	X	X	X	X	X	X	X	X	X
RECORDS_READ								X			
RESTART								X			
RETAIN			X	X	X	X	X	X	X	X	
RU_SIZE								X			
RUS_RECEIVED								X			
RUS_SENT								X			
SCH_DATE_TIME					X				X		
SECURE_ENABLED				X				X			
SECURE_PROTOCOL				X				X			
SEQ_NUM	X	X	X	X	X	X	X	X	X	X	
SERVER_NAME			X	X	X	X	X	X			X
SNODE			X	X	X	X	X	X	X	X	
SNODE_ACCT_INFO								X			
SNODE_ENC_ALG_LIST				X							
SNODE_PLEX_CLASS								X			
SNODE_SIGN				X							
SOURCE_MEMBER_NAME											X
SRC_DISP_1								X			
SRC_DISP_2								X			
SRC_DISP_3								X			
SRC_FILE							X	X			

Record ID	SI	CH	QE	SB	PI	ZI	CI	CT	PT	ZT	MC
START_TIME		X	X	X	X	X	X	X	X	X	
STATUS			X								
STD_COMPRESSION								X			
STEP_NAME				X			X	X			
STOP_TIME								X	X		
SUB_DATE_TIME					X	X			X	X	
SUBMIT_NODE	X	X		X	X	X	X	X	X	X	
SUBMITER	X	X		X	X	X	X	X	X	X	
TARGET_MEMBER_NAME							X	X			X
USER_DATA_1	X	X	X	X	X	X	X	X	X	X	X
USER_DATA_2	X	X	X	X	X	X	X	X	X	X	X
USER_DATA_3	X	X	X	X	X	X	X	X	X	X	X
USER_DATA_4	X	X	X	X	X	X	X	X	X	X	X

Connect:Enterprise Statistics Table (CE_STATS_LOG)

The following table describes the data fields available from the Connect:Enterprise Statistics (CE_STATS_LOG) table for Sterling Control Center reports:

Element	Type	Description
APPL_AGENT_TYPE	varchar	Specifies one of the following application agent types: ◆ Console ◆ End Of Batch ◆ Logging ◆ Scheduler ◆ Wake Up Terminate
BATCH_ID	varchar	User-assigned description of a Connect:Enterprise batch. **Note:** This column is not populated in this table since it is duplicated in the Events table.
BATCH_NUMBER	varchar	System-assigned number for each batch in a Connect:Enterprise repository. **Note:** This column is not populated in this table since it is duplicated in the Events table.
BYTES_READ	bigint	Number of bytes read from the source file.
BYTES_WRITTEN	bigint	Number of bytes written to the destination file.
DEST_FILE	varchar	Destination file name. **Note:** This column is not populated in this table since it is duplicated in the Events table.
EVENT_ID	bigint	ID number assigned by the system to each event.
JOB_ID	varchar	Batch job identifier.
JOB_NAME	varchar	Name of the job that added the batch.
LINE_NAME	varchar	Line accessed during Auto and Remote Connects.
LIST_NAME	varchar	Connect:Enterprise Auto Connect List Name. The Auto Connect List defines the remote sites that the Connect:Enterprise server automatically connects to and transmits batches to.
LOG_DATE_TIME	varchar	Date and time that the statistics record was written to the log file. Format yyyy/mm/dd hh:mm:ss.msmsms.
MAILBOX_FLAGS	varchar	Connect:Enterprise batch status flag. See the appropriate Connect:Enterprise documentation for a list of batch status flags.

Element	Type	Description
MAILBOX_ID	varchar	Specifies the repository associated with the Connect:Enterprise batch
MSG_ID	varchar	Server or Sterling Control Center message ID issued with the event. **Note:** This column is not populated in this table since it is duplicated in the Events table.
MSG_SHORT_TXT	varchar	Message short text. **Note:** This column is not populated in this table since it is duplicated in the Events table.
NODE_ID	varchar	Server alias. **Note:** This column is not populated in this table since it is duplicated in the Events table.
NODE_NAME	varchar	Name of the Connect:Direct server.
NODE_TYPE	varchar	Code indicating the type of server. **Note:** This column is not populated in this table since it is duplicated in the Events table.
OID	varchar	Object identifier that identifies the Connect:Enterprise SNMP trap received by the engine.
PART_KEY	date	The date the statistics record was written to the log file. The format is yyyy-mm-dd.
PROTOCOL	varchar	Protocol used for the file transfer.
RECIP_MAILBOX_ID	varchar	Connect:Enterprise Mailbox ID of the repository that received the batch.
RECORD_CATEGORY	varchar	One of the following connection types: AC=Auto Connect RC=Remote Connect
RECORD_ID	varchar	Type of statistics record generated. See the *Event Type Descriptions* Help topic for a list of record IDs.
REL_SELECT_STMT	varchar	Position of the Connect:Enterprise SELECT statement that executed the rule which caused an SNMP trap to be generated.
REMOTE_NAME	varchar	Name of the remote server involved in the file transfer.
RULE_MEMBER_NAME	varchar	Data set member name that contains the application agent rules.
RULE_NAME	varchar	Name of the Connect:Enterprise application agent rule.
SEQ_NUM	bigint	System-assigned sequence number. **Note:** This column is not populated in this table since it is duplicated in the Events table.
SESSION_ID	varchar	System-assigned ID identifying a connection between a Connect:Enterprise host and a remote site.

Element	Type	Description
SRC_FILE	varchar	Source file name. **Note:** This column is not populated in this table since it is duplicated in the Events table.
START_TIME	varchar	Time that start-of-batch transmission information is received by the Sterling Control Center engine.
STATUS	varchar	FTP session status (active or inactive). **Note:** This column is not populated in this table since it is duplicated in the Events table.
STOP_TIME	varchar	Time that end-of-batch transmission information is received by the Sterling Control Center engine.
TIME_UP	varchar	Length of time that the Connect:Enterprise server has been running.
USER_DATA_1	varchar	Metadata field 1. **Note:** This column is not populated in this table since it is duplicated in the Events table.
USER_DATA_2	varchar	Metadata field 2. **Note:** This column is not populated in this table since it is duplicated in the Events table.
USER_DATA_3	varchar	Metadata field 3. **Note:** This column is not populated in this table since it is duplicated in the Events table.
USER_DATA_4	varchar	Metadata field 4. **Note:** This column is not populated in this table since it is duplicated in the Events table.
WKFLOW_ID	varchar	Sterling Integrator ID, if Sterling Integrator requested a file transfer from a Connect:Enterprise UNIX server.
WRKFLOW_URL	varchar	Sterling Integrator URL, if Sterling Integrator requested a file transfer from a Connect:Enterprise UNIX server.

Event Type Table (EVENT_TYPE)

The Event Type table contains a listing of Sterling Control Center event types and descriptions.

Element	Type	Description
EVENT_TYPE	bigint	Code indicating the type of event.
EVENT_TYPE_DESCR	varchar	Description of the event type codes. The codes and descriptions are: 1=Process Step Started 2=Process Step Ended 3=Process Started 4=Process Ended 5=Server Status 6=SLC Notification 7=Server Shutdown Started (for future use) 8=Server Shutdown (for future use) 9=Process Status 10=Server license 11=Server Error 12=Server Command 13=Connection Started 14=Connection Shutdown Started (for future use) 15=Sterling Control Center Status (for future use) 16=Process Queue 17=Process Interrupted 66=Suppressed SLC Notification

Node Type Table (NODE_TYPE)

The Node Type table contains a listing of node (server) types monitored by Sterling Control Center.

Element	Type	Description
NODE_TYPE	bigint	Code indicating the type of event.
NODE_TYPE_DESCR	varchar	Type of server. The server types are: 0=Sterling Control Center 1=Connect:Direct 2=Connect:Enterprise 3=Sterling Integrator 4=FTP

Pair Connections Table (PAIR_CONN)

The following table describes the data fields available from the Node Discovery Pair Connections Table for Sterling Control Center reports.

Element	Type	Description
DISCOVERED_ID	bigint	Reference to Discovery Node table.
DISCOVERY_START_TM	varchar	Discovery start date range value.
DISCOVERY_STOP_TM	varchar	Discovery end date range value.
EXPLORER_ID	bigint	Reference to Discovery Node table.
FROM_NETMAP	smallint	1=Found in Netmap 0=Not found in Netmap
FROM_STATS	smallint	1=Found in statistics 0=Not found in statistics
LAST_CONN_D2E	varchar	Last connection time found from Discovered to Explorer node.
LAST_CONN_E2D	varchar	Last connection time found from Explorer to Discovered node.
TIMES_CONN_D2E	bigint	Number of connections initiated by Discovered node to Explorer node.
TIMES_CONN_E2D	bigint	Number of connections initiated by Explorer node to Discovered node.

Discovery Node Table (DISCOVERY_NODE)

The following table describes the data fields in the Discovery Node Table.

Element	Type	Description
ANOS400	smallint	0=Node is not OS/400. 1=Node is OS/400.
API_PORT	varchar	API port value.
COMMENTS	text	User description for node.
CONNECTION_TIMEOUT	bigint	Internal field used for Node Discovery.
DB_LIBRARY	varchar	Connect:Direct OS/400 database library name.
DISCOVERED_TIME	varchar	Time node was discovered.
DISCOVERY_START_TM	varchar	Discovery start date range value.
DISCOVERY_STOP_TM	varchar	Discovery end date range value.
DTF_ADDRESS	varchar	Server host address.
DTF_PORT	varchar	Server port value.
ENABLED	smallint	0=Disabled 1=Enabled
FROM_NETMAP	smallint	0=Not found in Netmap. 1=Found in Netmap.
FROM_STATS	smallint	0=Not found in statistics. 1=Found in statistics.
HOST_NAME	varchar	Host name for server.
ID	bigint	For internal use.
IGNORED	smallint	For discovered nodes: 1=Found in Mylist. 0=Found in Discovered list.
LAST_DSCVRY_ATTEMPT	varchar	Time of last discovery attempt.
LST_SCCSSFL_DSCVRY	varchar	Time of last successful discovery attempt.
MESSAGE_KEY	varchar	Message.
MESSAGE_PARAMETERS	text	Values used to construct message text.

Element	Type	Description
MESSAGE_PRIORITY	bigint	Priority of message
NET_MAP_ENTRIES	bigint	Number of Netmap entries found.
NODE_NAME	varchar	Name of server.
OPERATING_SYSTEM	varchar	Server operating system.
PARTNERS	bigint	Number of partner nodes found.
PASSWORD	text	Password for API connection.
PROCESSES	bigint	Number of Processes found to have run during Discovery.
PROTOCOL	varchar	Internal field for Node Discovery.
RETURN_CODE	bigint	Return code for Discovery.
SERVER_LICENSE	text	Server license text.
SERVICE_ID	varchar	Node or alias name.
SOURCE_PORT	varchar	Source port range to use for API connection.
SRVR_LCNS_EXPRTN_D	varchar	Server license expiration date.
TYPE	varchar	Type of node. E=Explorer node D=Discovered node
USER_ID	varchar	User ID for API connection.

Metadata Labels Table (META_DATA_LABELS)

The following table describes the data fields available from the META_DATA_LABELS database table for reports. It holds the user-provided labels for the metadata fields.

There are four rows in this table, one for each of the four metadata fields.

Element	Type	Description
USER_DATA_TITLE	varchar	Name of the metadata field.
USER_DATA_FIELD	varchar	User-provided label for the metadata field. The default is User Data *x*, where *x* ranges from one to four, or SERVER_DATA_*x* where *x* ranges from one to ten.

Default table contents are as follows:

USER_DATA_TITLE	USER_DATA_FIELD
userData1Title	User Data 1
userData2Title	User Data 2
userData3Title	User Data 3
userData4Title	User Data 4
serverMetaData1Title	Server Data 1
serverMetaData2Title	Server Data 2
serverMetaData3Title	Server Data 3
serverMetaData4Title	Server Data 4
serverMetaData5Title	Server Data 5
serverMetaData6Title	Server Data 6
serverMetaData7Title	Server Data 7
serverMetaData8Title	Server Data 8
serverMetaData9Title	Server Data 9
serverMetaData10Title	Server Data 10

Sterling Control Center Internal Tables

The following tables are used internally by Sterling Control Center. They are not available for third-party reporting.

- ✦ DURATION_MONITORS (No longer used)
- ✦ TIME_MONITORS
- ✦ LICENSES
- ✦ CCC_INFO
- ✦ CONFIG_JOBS
- ✦ CONFIG_OBJECTS
- ✦ CONFIG_SERVER_IDS
- ✦ CONFIG_VERSIONS
- ✦ AUDIT_LOG
- ✦ FILE_COUNTS

Index