IBM® Connect:Direct File Agent 1.4.0.2

Documentation

This edition applies to Version 6 Release 1 of IBM® Connect:Direct and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Managing Files with Sterling Connect:Direct File Agent

Sterling Connect:Direct File Agent Overview

Sterling Connect:Direct® File Agent is the component of Sterling Connect:Direct that provides unattended file management. Before using Sterling Connect:Direct File Agent, you must plan how to configure it to automate file management for your site. After planning what you need to accomplish, configure Sterling Connect:Direct File Agent to connect to a Sterling Connect:Direct server, watch the directories that files of interest will be added to, and submit a specified Sterling Connect:Direct Process to the server when a file is detected.

Sterling Connect:Direct File Agent provides monitoring and detection capabilities that enhance the automation you accomplish with Sterling Connect:Direct Processes. You cannot create Processes with Sterling Connect:Direct File Agent; however, Sterling Connect:Direct File Agent variables can pass arguments to a Process. Sterling Connect:Direct File Agent does not delete, copy, or move files directly, but it helps you accomplish such tasks by submitting the Process you specify in the configuration to the Sterling Connect:Direct server. Before you configure Sterling Connect:Direct File Agent, you must create and test the Sterling Connect:Direct File Agent Process that you intend to specify as the default Process in the Sterling Connect:Direct File Agent configuration.

Using the Sterling Connect:Direct File Agent Configuration Interface and Help system, define the default configuration file (Default_Config.ser). This file defines the Sterling Connect:Direct server that Sterling Connect:Direct File Agent communicates with; the directory, or directories, that Sterling Connect:Direct File Agent monitors; and how a file added to a watched directory or a detected system event is processed.

You can configure Sterling Connect:Direct File Agent to operate in either of the following ways:

- Watch for any file to appear in one or more watched directories and submit the default Process after detecting the newly added file.
- Override the default Process specified and apply either watched file event rules (Submit Process rule) or system event rules enabled for the configuration. Sterling Connect:Direct File Agent applies a watched file event rule to a detected file by checking file properties to determine whether criteria specified by the rule are met. A system event rule checks whether a system event meets criteria specified by the rule. If all criteria for a rule are met, Sterling Connect:Direct File Agent submits Process associated with that rule.

You can create Sterling Connect:Direct File Agent rules based on the following properties:

- Full or partial name of the file detected in a watched directory
- Size of the file detected in a watched directory
- System event title
- System event contents (as included in a stack trace)

You can specify more than one rule in a Sterling Connect:Direct File Agent configuration; each rule can have Sterling Connect:Direct File Agent submit a different Process.

Although you can create multiple rules as part of a Sterling Connect:Direct File Agent configuration, Sterling Connect:Direct File Agent rules processing ends once all criteria for a rule are met. Therefore, you should specify rules so that those with more specific criteria (properties) are listed first in the configuration.

For optimum performance, you should configure Sterling Connect:Direct File Agent to communicate with the Sterling Connect:Direct node where it is installed. You can configure Sterling Connect:Direct File Agent to use continuous signon and remain connected to the API port for the Sterling Connect:Direct server at all times, or configure it to connect to the port only when it needs to. Sterling Connect:Direct File

Agent is available on UNIX, Microsoft Windows, and z/OS® operating systems. When you use Sterling Connect:Direct for UNIX or Microsoft Windows, the watched directory is a UNIX path name or a Microsoft Windows path to the directory. When you use Sterling Connect:Direct for z/OS, the watched directory can be a fully specified HFS path name for a file or a directory, a fully specified MVS data set name, a partial MVS data set name, or the name of a partitioned data set (PDS) or partitioned data set extended (PDSE). In addition, you can also watch Amazon S3 or S3 compatibles objects stores. Add the selected buckets and objects path to the watched directory list.

Sterling Connect:Direct File Agent can monitor multiple directories, including local and network directories. Sterling Connect:Direct File Agent scans the watched directories you specify in the configuration for newly added files (unless you specify a rule to force other operation). By default, Sterling Connect:Direct File Agent scans a watched directory once each minute. For example, if you start Sterling Connect:Direct File Agent at 1:00 p.m., a file added to that watched directory at 12:55 p.m. is not detected. If you start Sterling Connect:Direct File Agent at 1:00 p.m., and a file is placed in the watched directory at 1:01 p.m., then Sterling Connect:Direct File Agent detects this newly added file. Sterling Connect:Direct File Agent detects a file only one time, unless the file is accessed and saved with a later timestamp.

Using Sterling Connect:Direct File Agent requires an understanding of Sterling Connect:Direct Processes, operating systems, and scripting (for regular expression operator use with Sterling Connect:Direct File Agent rules).

Virtualization support

IBM cannot maintain all possible combinations of virtualized platforms. However, IBM generally supports all enterprise class virtualization mechanisms, such as VMware ESX, VMware ESXi, VMware vSphere, Citrix Xen Hypervisor, KVM (Kernel-based virtual machine), and Microsoft Hyper-V Server.

IBM investigates and troubleshoots a problem until it is determined that the problem is due to virtualization. The following guidelines apply:

- If a specific issue is happening because the system is virtualized and the problem cannot be reproduced on the non-virtualized environment, you can demonstrate the issue in a live meeting session. IBM can also require that further troubleshooting is done jointly on your test environment, as there is not all types and versions of VM software installed in-house.
- If the issue is not able to be reproduced in-house on a non-virtualized environment, and troubleshooting together on your environment indicates that the issue is with the VM software itself, you can open a support ticket with the VM software provider. IBM is happy to meet with the provider and you to share any information, which would help the provider further troubleshoot the issue on your behalf.
- If you chose to use virtualization, you must balance the virtualization benefits against its performance impacts. IBM does not provide advice that regards configuring, administering, or tuning virtualization platforms.

How to Run Sterling Connect:Direct File Agent

You can run Sterling Connect:Direct File Agent from a UNIX or MS-DOS command line, configure it to start automatically as a Microsoft Windows Service at system startup, or configure it to run from a Microsoft Windows shortcut. Use the command line to verify that Sterling Connect:Direct File Agent is working correctly or to specify an alternate configuration file. After you run Sterling Connect:Direct File Agent from the command line to verify that Sterling Connect:Direct File Agent is operating correctly, run it using the method that requires the least user intervention.

When Sterling Connect:Direct File Agent runs as a Microsoft Windows service, it is fully automated, requiring little user intervention. On UNIX, you can modify the initialization sequence of the computer to call the cdfa.sh script and run Sterling Connect:Direct File Agent whenever you restart the computer. On z/OS, you must run the appropriate job to start the Sterling Connect:Direct File Agent Configuration Interface, or to start or shut down Sterling Connect:Direct File Agent.

You can run more than one Sterling Connect:Direct File Agent on the same or different hosts. You can also monitor a directory with more than one file agent.

Sterling Connect:Direct File Agent Logging

Sterling Connect:Direct File Agent logs system information to the console and three separate log files. The level of information that is written to the logs is configurable.

Sterling Connect:Direct File Agent Monitoring

Sterling Connect:Direct File Agent can send SNMP traps to IBM® Sterling Control Center or other third-party software to monitor Sterling Connect:Direct File Agent activity. To use this feature, you must modify the Sterling Connect:Direct File Agent configuration.

Sterling Connect:Direct File Agent Configuration Interface and Help

Instructions for configuring Sterling Connect:Direct File Agent are available in the online Help system that you access from the configuration interface. Field-level Help is displayed in the bottom pane of the configuration interface. Clicking **Help** displays the online configuration procedures.

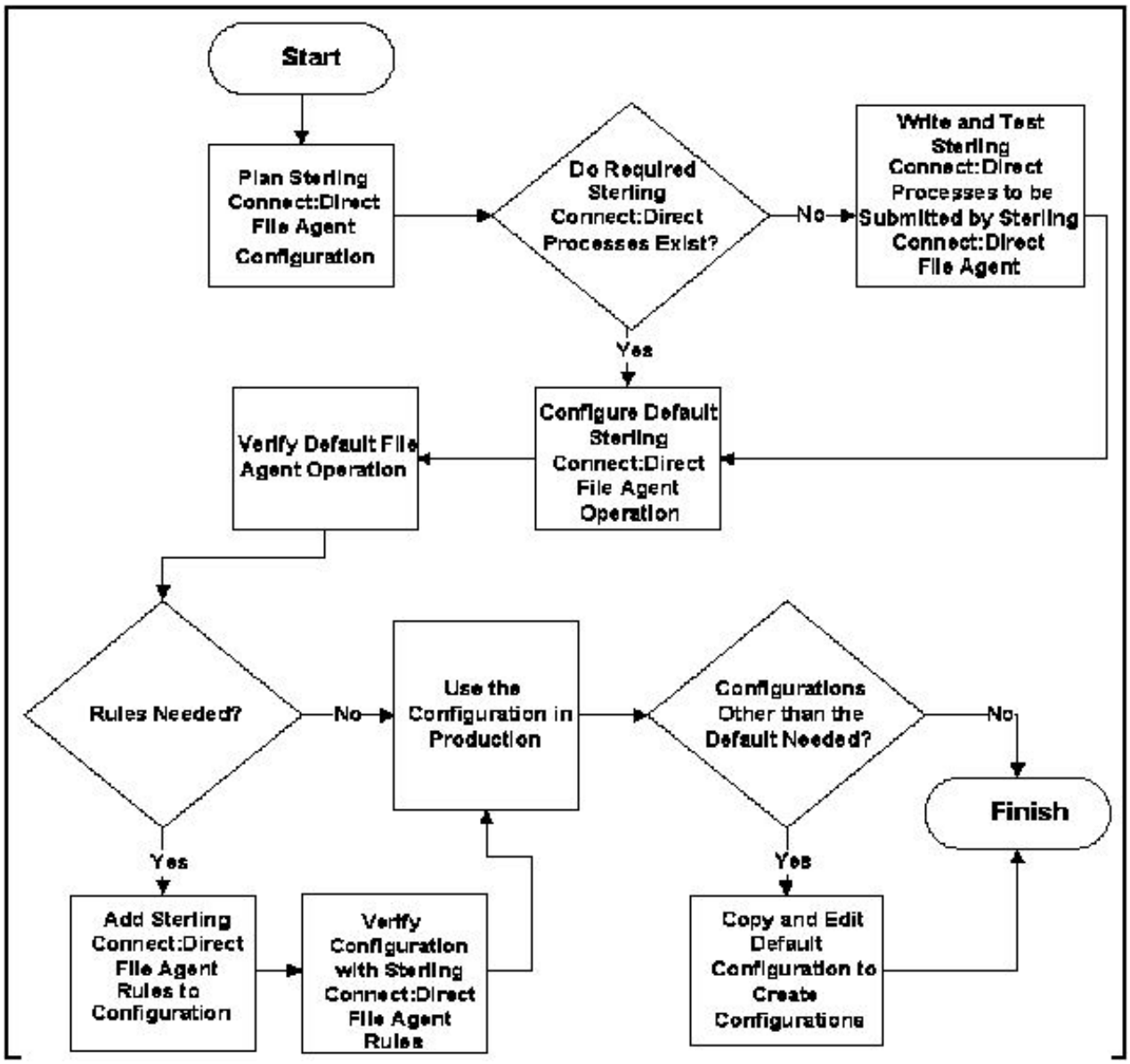
Sterling Connect:Direct File Agent Configuration Planning

Before you begin configuring Sterling Connect:Direct File Agent, you must choose or create the Sterling Connect:Direct File Agent Processes that perform the actions you want to automate. You configure Sterling Connect:Direct File Agent to connect to the Sterling Connect:Direct File Agent server and to monitor and detect conditions (such as a file addition to a directory). At detection, Sterling Connect:Direct File Agent submits the Process for executing actions that need to be performed in response to those conditions. Refer to the Sterling Connect:Direct File Agent Configuration Scenarios to review some configuration scenarios that can help you understand Sterling Connect:Direct File Agent configuration. The Sterling Connect:Direct File Agent Help documents the following incremental approach to configuration:

- Specify the server connection, a default Process, and the watched directory.
- Run a test from the command line and use the log to verify that the default Sterling Connect:Direct File Agent configuration is working correctly.
- After you verify the default configuration, you can create and validate Sterling Connect:Direct File Agent rules, one by one, by running Sterling Connect:Direct File Agent in verbose mode.
- After you successfully create a default configuration, you can use the file as the basis for other configuration files.

Use the Sterling Connect:Direct File Agent Worksheet to gather the information you need to configure Sterling Connect:Direct File Agent. Contact your system administrator for the site-specific information necessary to establish a connection to the Sterling Connect:Direct File Agent server. Make copies of this worksheet if you have to configure Sterling Connect:Direct File Agent on multiple Sterling Connect:Direct servers.

The following diagram illustrates the flow of steps for setting up Sterling Connect:Direct File Agent for use in a production environment.



Sterling Connect:Direct File Agent Worksheet

Sterling Connect:Direct Server Connection Information	Value to Assign
User ID for API (for connecting to the Sterling Connect:Direct server) **Required**Must match the user ID used to submit the default Process.	
Password for API (for connecting to the Sterling Connect:Direct server) **Required**Must match the password that submits the default Process.	
API host DSN name (name of the host on which the Sterling Connect:Direct server is located) **Required**	
API port (default =1363)1–5 digit port number that Sterling Connect:Direct File Agent uses to connect to the Sterling Connect:Direct server API. **Required**	
Gate Keeper port (default=65530) Port used to track directory monitoring and ensure that multiple file agents do not monitor a single directory. **Required**	

Sterling Connect:Direct Server Connection Information	Value to Assign
Gate keeper DNS name (optional) Default=127.0.0.1	
Default Process and Watched Directory Information	
Watched directories: **Required** For Microsoft Windows and UNIX, one or more valid specifications of paths (Microsoft Windows) or pathnames (UNIX). For z/OS, one or more fully specified HFS pathnames of a file or directory, or a full or partial MVS data set name. List one valid entry per line. For S3 Stores, a valid URI using the following syntax : `scheme://bucketname[/folders]`	
Monitor sub directories (default=Yes)	
Continuous signon (default=No)	
Default Process and Watched Directory Information	
Default Process: Microsoft Windows and UNIX: Valid path and filename that contains the default Process on the Sterling Connect:Direct server. z/OS: Member Name in DMPUBLIB **Note:** If you do not specify a default Process or create a rule, no processing is performed when a file or event is detected.	
Default arguments&FA_XXXX_XXX. Argument string to pass to the default Process in the following format: **Note:** The percent sign (&) and period (.) are required.	
Error Process:	
Error arguments	
Process class (default=1) **Required**	
Process priority (default=1)	
Watched file interval (default=1 minute)	
File completion delay (default=1 minute)	
Sterling Connect:Direct File Agent unique name (default=FileAgent) **Required** Unique name for each Sterling Connect:Direct File Agent instance to be monitored by Sterling Control Center.	
SNMP listener address Address of the SNMP trap receiver. Required when monitoring Sterling Connect:Direct File Agent with Sterling Control Center.	
SNMP listener port Listening port of the SNMP trap receiver. Required when monitoring Sterling Connect:Direct File Agent with Sterling Control Center.	

Sterling Connect:Direct Server Connection Information	Value to Assign
SNMP source port range Ports or port ranges used to pass through a firewall to the SNMP trap receiver, including Sterling Control Center, when Sterling Connect:Direct File Agent is behind a firewall. Type the ranges in the format nnnn-nnnn, separated by commas, for example, 5555-7777, 8888-8890, 9999.	
Refresh Configuration Whether configuration changes are in effect immediately (Yes) or after stopping and starting Sterling Connect:Direct File Agent (No).	

If you are using X Microsoft Windows, the X11 display variable connects to the GUI server for terminal emulation. The Sterling Connect:Direct File Agent Configuration Interface displays on the monitor specified for the X11 display variable. To display the Sterling Connect:Direct File Agent Configuration Interface on a Microsoft Windows computer, specify the network ID of the terminal to use to display the Sterling Connect:Direct File Agent Configuration Interface.

Considerations for a Large Number of Watch Directories

There are two considerations when watching a very large number of directories: scan time and log space. Sterling Connect:Direct File Agent scans each watch directory, then waits for the time specified in the watch interval, then repeats the cycle. With a large number of watch directories, each scan takes more time.

To keep each log file at a manageable size yet still keep enough current log data, the logging system uses a combination of MaxFileSize and MaxBackupIndex settings in the log4j.properties file to control logging. The MaxFileSize setting allows each file to grow only to a specified size, and the MaxBackupIndex setting specifies how many backup files are allowed. Multiplying these two settings will give you the maximum amount of disk space. Since there are three different logs, you would add the maximum disk space for each enabled log to get the maximum disk space for all Sterling Connect:Direct File Agent logging.

You can modify the MaxFileSize and MaxBackupIndex for each log to meet your requirements. The MaxFileSize recommended upper limit is 32MB. The MaxBackupIndex can be as large as you want and depends on how much log history to keep and the available disk space.

Modifying MaxFileSize

1. Open the log4j.properties file in the installation directory.
2. Modify one or more of the following log files:

Log File	Modify This Value
CDFA.log	log4j.appender.R.MaxFileSize=1000KB
CDFA_verbose.log	log4j.appender.V.MaxFileSize=1000KB
CDFA_stats.log	log4j.appender.S.MaxFileSize=1000KB

Modifying MaxBackupIndex

1. Open the log4j.properties file in the installation directory.
2. Modify one or more of the following log files:

Log File	Modify This Value
CDFA.log	log4j.appender.R.MaxBackupIndex=10
CDFA_verbose.log	log4j.appender.V.MaxBackupIndex=10

Log File	Modify This Value
CDFA_stats.log	log4j.appender.S.MaxBackupIndex=10

This product has been tested with 50,000 watch directories using MaxFileSize=32MB and MaxBackupIndex=10 with no adverse effects except the considerations noted above.

Considerations for a Large Number of Files in a Watch Directory

After Sterling Connect:Direct File Agent scans a watch directory, it submits a Sterling Connect:Direct Process for each available file that it finds. If it locates a large number of files in a watch directory, the time required to submit the Processes is larger than if it were handling a few files during each scan. Also, watch directories with a large number of files is not scanned as often because of the time required for a scan.

Also, consider that the Sterling Connect:Direct Server must be able to process the Processes that Sterling Connect:Direct File Agent submits. A limit may exist on how many Processes it runs concurrently. IBM tested with over 50,000 files in a watch directory with no adverse effects. The checkpoint file contained over 50,000 entries and files transferred appropriately. An upper limit to the files in a watch directory has not been determined, and depends on the amount of memory the system has available.

If the watch directory is a shared directory and the connection is lost, a log entry indicates that Sterling Connect:Direct File Agent does not have read/write access to the directory. When the connection is restored, the directory can be accessed on the next scan.

Sterling Connect:Direct File Agent Configuration Scenarios

The following examples illustrate typical scenarios for using Sterling Connect:Direct File Agent. Fields that are not required to be set for the operation demonstrated in the example are not included in the tables of configuration parameters. Required fields are indicated by an asterisk (*) in the Sterling Connect:Direct File Agent Configuration Interface, and all fields are described in field-level Help.

The sample scenarios have the following assumptions:

- You have configured the site-specific parameters required to establish a connection to the Sterling Connect:Direct File Agent server where Sterling Connect:Direct File Agent is installed (see the Sterling Connect:Direct File Agent Worksheet for a description of the parameters required to establish the connection).
- The Processes used in the Sterling Connect:Direct File Agent scenarios have been created.

Scenario:Detecting a File Added to a Watched Directory on a z/OS System

Some users need to access a report file that is expected to be transferred to a location that only administrators can access. The sample values in the table configure Sterling Connect:Direct File Agent to perform the following processing:

- Monitor the watched data set called EASTERN.Q1.REPTS.
- Submit a default Process called DEFPROC. The default Process is created to copy a file detected in the watched data set to a specified location for access by users.

Tab	Field	Sample or Description
File agent	Watched directories	Type EASTERN.Q1.REPTS to specify the fully qualified MVS data set name to monitor.
	Default Process	Type DEFPROC, the member name for the Process in DMPUBLIB. **Note:** If no default Process is specified and the file does not match a rule, then no processing occurs.

Scenario:Detecting a VSAM Data File Added to a Watched Directory on a z/OS System

Each month, users in the accounting department need to access a VSAM data file that contains their company's monthly payroll information. The name of the data file containing this information is VSAM.mm.yy.PAYCHECKS.DATA where mm is the month and yy is the year. The data file is expected to be transferred to a location that only administrators can access.

The Sterling Connect:Direct administrator configured Sterling Connect:Direct File Agent to watch for any file containing the string, VSAM.**.**.PAYCHECKS, and then to copy it to the directory location the accounting users could access. When the administrator tested Sterling Connect:Direct File Agent, she discovered that the Process had been submitted three times because Sterling Connect:Direct File Agent was triggered for the following VSAM files when the VSAM cluster was created:

- VSAM.mm.yy.PAYCHECKS
- VSAM.mm.yy.PAYCHECKS.INDEX
- VSAM.mm.yy.PAYCHECKS.DATA

To configure Sterling Connect:Direct File Agent to watch only for VSAM data files and not other VSAM-related files, the administrator modified the match string and specified VSAM.**.**.PAYCHECKS.DATA as the the VSAM data set to watch. She configured Sterling Connect:Direct File Agent to perform the following processing:

- Monitor the watched data set called VSAM.**.**.PAYCHECKS.DATA
- Submit a default Process called DEFPROC. The default Process has been created to copy a file detected in the watched data set to a specified location for access by users.

Tab	Field	Sample or Description
File agent	Watched directories	Type VSAM.**.**.PAYCHECKS.DATA to specify the fully qualified VSAM data set name to watch.
	Default Process	Type DEFPROC, the member name for the Process in DMPUBLIB. **Note:** If no default Process is specified and the file does not match a rule, then no processing occurs.

Scenario: Detecting a File by name on a S3 store

Accounting data files are regularly transferred into a S3 bucket under folder `AccountingData`. Files with name ending with “.dta” require special processing that will automatically be performed. The sample values in the table configure Sterling Connect:Direct File Agent to perform the following processing:

- Monitor the watched directory s3://onebucketname/AccountingData.
- Apply the rule titled "new dta file” to detect file name ending with “.dta”.
- Override the default Process and submit a Process that is associated with the name rule. This doondta.cdp Process will copy this file to local file for processing to a local directory for processing.
- Pass the path and file name of the file that meets the criteria for the "new dta file” rule to the Process doondta.cdp.

Tab	Field or Dialog Box	Actions and Sample Entry
File Agent	Watched directories field	Specify the directory to monitor. Type the path to the directory to monitor: `s3://onebucketname/AccountingData`

Tab	Field or Dialog Box	Actions and Sample Entry
Rules	Create a rule dialog box	1. Click **New** and type the name you want to give the rule in the **new dta file** field. 2. Click new dta file in the list or rules and click **Edit**.
	Match criteria list for rule “new dta file”	1. Click **Enabled** to enable the criteria you are about to specify. 2. Click name of the newly arrived file. 3. Click Matches to display the options for the comparison. 4. Select Matches. 5. Type */*.dta in the compare string field and click **OK**.
	Process name field	Scroll down to view the Submit Process information for watched file event rule “new dta file”. Type the directory path to doondta.cpd and file name of the Process that Sterling Connect:Direct File Agent submits when the new dta file rule detects a match. Click **Done** and then click **Save**.
	Process arguments	Type the Sterling Connect:Direct File Agent variable (&FAF=%FA_FILE_FOUND) for passing the S3 object URI, including the leading percent sign (%) and the ending period (.): In this example, &FAF is the variable to which Sterling Connect:Direct File Agent will pass the detected S3 object name. %FA_FILE_FOUND. is the Sterling Connect:Direct File Agent variable used to indicate the information to pass to the Sterling Connect:Direct Process.

Scenario:Detecting a File by File Size on a Microsoft Windows System

Customer transaction files are regularly transferred into the Microsoft Windows directory c:\monthend\datafile. Files larger than 1 MB require special processing that will automatically be performed on files in a certain directory.

The sample values in the table configure Sterling Connect:Direct File Agent to perform the following processing:

- Monitor the watched directory c:\monthend\datafile
- Apply the rule titled "find big file” to detect files larger than 1 MB.
- Override the default Process and submit a Process that is associated with the Check file size rule. This fixbigfile.cdp Process will copy a file larger than 1 MB from the c:\monthend\datafile directory to the c:\reprocess directory.
- Pass the path and file name of the file that meets the criteria for the "find big file” rule to the Process fixbigfile.cdp.

Tab	Field or Dialog Box	Actions and Sample Entry
File agent	Watched directories field	Specify the directory to monitor. Type the path of the directory to monitor: **c:\monthend\datafiles**
Rules	Create rule dialog box	Click **New** and type the name you want to give the rule in the field: **find big file** Click **find big file** in the list of rules and click Edit.
	Match criteria list for rule “find big file”	Specify the criterion to check for a detected file. Select the default criterion name, Not enabled: system event title matches “ ” and click Edit **match**.
	Edit match criterion for rule “find big file” dialog box	• Click **Enabled** to enable the criteria you are about to specify. • Click **Size of the newly arrived file** • Click **Matches** to display the options for the comparison. Click **Greater than** to define the how the file size should compare. • Type **1048576 in the Compare size field** and click **OK**.
	Process name field	Scroll down to view the Submit Process information for watched file event rule **“find big file”**. Type the directory path and file name of the Process that Sterling Connect:Direct File Agent submits when the Find big file rule detects a match: **c:\processes\fixbigfile.cdp** Click **Done** and then click **Save**.

Scenario:Detecting a System Event by Title on a Microsoft Windows System

IndexOutOfBoundsException is the title of an event that indicates a number is outside of an expected range. In the following example, Sterling Connect:Direct File Agent is used to detect an event with IndexOutOfBoundsException in the title, pass a string (the event title) to a Sterling Connect:Direct Process, and then submit a Process to the Sterling Connect:Direct server that will perform actions the environment requires for this type of event. In this scenario, the event IndexOutOfBoundsException could indicate activity that a network administrator should investigate. Because the site uses a Sterling Connect:Direct mailbox system, the configuration will include the administrator's account to be notified when Sterling Connect:Direct File Agent submits a Process for the IndexOutOfBounds rule.

The sample values in the table configure File to perform the following processing:

- Override the default Process and submit \processfolder\oo_boundserrproc.cdp
- Send a message to the mailbox system account for the administrator after submitting the oo_boundserrproc.cdp Process for the rule.

Tab	Dialog Box, Window, or Field	Description/Example
Rules	Create rule dialog box	Type index out of bounds as the rule to create.
	Match criteria list for rule “index out of bounds” window	Select the default criteria **Not enabled: System event title matches “ ”** and click **Edit match**.

Tab	Dialog Box, Window, or Field	Description/Example
	Edit match criterion for rule "index out of bounds" dialog box	• Click **Enabled** to enable the criteria to specify. • Click **System event title** as the criterion to match. • Click **Matches** on the drop-down field to see the options for comparison to a string. • Click **Contains** to specify how the compare string relates to a system event title detected. • Type **IndexOutofBounds** as the Compare String to indicate that the system event title should include this string. • Click **OK**.
	Submit Process information for system event rule "index out of bounds" window	Type information into the fields that will define the Process to submit and the mailbox user to notify after the Process is submitted.
	Process name field	Type **c:\processfolder\errproc.cdp** to specify the path and file name for the Process Sterling Connect:Direct File Agent submits when a file meets the rule criteria.
	Notification userid field	Type **adminjim@company.com** to specify the user to notify when the Process is submitted.

Scenario:Passing the UNIX Pathname for a Detected File to a Process

Because Sterling Connect:Direct File Agent can watch multiple directories for the appearance of a new file, the Sterling Connect:Direct Process that Sterling Connect:Direct File Agent is to submit to the server at the appearance of a new file might need to reference the Microsoft Windows path or UNIX path name for the detected file as part of commands and statements in the Process.

In the following example, a UNIX path name is passed to the default Process, copynewfile.cdp.

Tab	Dialog box, Window, or Field	Sample Entry
File agent	**Watched directories**	Type one UNIX path name per line for each location to monitor for the appearance of files: **user/bin/monthend/** **quartend/easterndiv/errorfiles** **managers/special/reports**
	Default Process	Type the UNIX path and file name for the Sterling Connect:Direct Process to run when a file is detected in any watched directory specified: **user/bin/admin/copynewfile.cdp** The path name where Sterling Connect:Direct File Agent detected a new file is passed to this Process.

Tab	Dialog box, Window, or Field	Sample Entry
	Default arguments	Type the Sterling Connect:Direct File Agent variable for passing the UNIX path name, including the leading percent sign (%) and the ending period (.): **&FAP=%FA_PATH_FOUND.** In this example, &FAP is the variable to which Sterling Connect:Direct File Agent will pass the UNIX path name where the file was detected. **%FA_PATH_FOUND. is the** Sterling Connect:Direct File Agent variable used to indicate the information to pass to the Sterling Connect:Direct Process.

Scenario:Configuring the Gate Keeper for Multiple Sterling Connect:Direct File Agent Instances

The Sterling Connect:Direct File Agent gate keeper keeps track of the directories that multiple file agents are configured to watch. If more than one file agent monitors the same directory, the gate keeper determines which Sterling Connect:Direct File Agent monitors that directory. This prevents more than one file agent from monitoring files in the same directory.

If you are using one instance of Sterling Connect:Direct File Agent or do not have multiple file agents monitoring the same directory, set the Gate keeper DNS name to blank for all of your Sterling Connect:Direct File Agent configurations. This will turn off the gate keeper and improve Sterling Connect:Direct File Agent performance.

If you have multiple file agents monitoring the same directory, use the same Gate keeper DNS name and Gate Keeper port for all Sterling Connect:Direct File Agent configurations. The Sterling Connect:Direct File Agent with the address that matches the configured gate keeper address becomes the Sterling Connect:Direct File Agent gate keeper. If you have Sterling Connect:Direct File Agent installed on different servers, decide which Sterling Connect:Direct File Agent to use as the gate keeper and use its Gate keeper DNS name and Gate Keeper port for all Sterling Connect:Direct File Agent configurations.

In the following example, multiple file agents installed on the same server are configured to monitor the C:\invoices directory. All Sterling Connect:Direct File Agent configurations use the same Gate Keeper port, Gate keeper DNS name, and Watched directory. When a file is detected in the C:\invoices directory, the default process, copynewfile.cdp, is submitted.

Tab	Dialog box, Window, or Field	Sample Entry
File agent	Gate Keeper port	Type the gate keeper port number Sterling Connect:Direct File Agent connects to. **65530** (default)
	Gate keeper DNS name	Type the host name of the Sterling Connect:Direct File Agent gate keeper. **10.10.10.10**
	Watched directories	Type one directory per line for each location monitored for files: **C:\invoices**
	Default Process	Type the Microsoft Windows path and file name for the Sterling Connect:Direct Process run when a file is detected in a watched directory: **C:\CDProcesses\copynewfile.cdp**

Tips for Using Sterling Connect:Direct File Agent

Review the following processing and operational guidelines before you use Sterling Connect:Direct File Agent in a production environment.

- You must monitor your standard output log files to detect problems or failures in Sterling Connect:Direct File Agent or configure Sterling Connect:Direct File Agent to send SNMP traps to Sterling Control Center or another SNMP monitoring application.
- The configuration interface is displayed when you attempt to start Sterling Connect:Direct File Agent if the .ser configuration file you are executing contains errors. Review your configuration file and correct the errors.
- You cannot configure e-mail alerts to notify you when errors occur unless you are using Sterling Control Center with Sterling Connect:Direct File Agent.
- Sterling Connect:Direct File Agent uses a checkpoint file (FA_*<API host><API port>*.ckpt) to keep track of files detected in the watched directories. The checkpoint file is created automatically when the first file is processed. If you start Sterling Connect:Direct File Agent and there is no checkpoint file, such as after a new installation, existing files in the watched directories are not detected for processing unless you do one of the following:
  - Specify the -f parameter when you start Sterling Connect:Direct File Agent.
  - Remove them and put them back with a new timestamp.
  - Use the UNIX touch command to alter their timestamp.
- Sterling Connect:Direct File Agent detects a file only once unless the file is accessed and saved with a new timestamp.
- To run Sterling Connect:Direct File Agent with a configuration file other than Default_Config.ser, you must stop and restart Sterling Connect:Direct File Agent manually from the command line and specify the name of the configuration file to use.
- For optimum performance, configure Sterling Connect:Direct File Agent to communicate with the Sterling Connect:Direct File Agent node on the same server.
- To determine the version of Sterling Connect:Direct File Agent that you are running, you must start Sterling Connect:Direct File Agent in verbose mode or check the CDFA.log.
- Obtain the latest version of Sterling Connect:Direct File Agent from the IBM Support Portal. See the Sterling Connect:Direct File Agent release notes for your platform for instructions.

Chapter 2. Configure the Default Settings

A Default Configuration

Before you start Sterling Connect:Direct File Agent in a production environment, you must create and validate the default configuration. The file defines the Sterling Connect:Direct server that Sterling Connect:Direct File Agent communicates with; the directory, or directories, that Sterling Connect:Direct File Agent monitors; and how a file added to a watched directory or a detected system event is processed.

Running Sterling Connect:Direct File Agent from the command line is practical only for testing and troubleshooting configurations, or for special processing other than that defined by the default configuration file, Default_Config.ser.

After you validate the default configuration, complete the procedures in Creating a New Configuration File to modify the default configuration as required for your enterprise, add a new configuration file, edit or delete existing configuration files, and, if necessary, define site-specific configuration files for mass distribution. Each time you modify a configuration, validate the changes before using Sterling Connect:Direct File Agent with that configuration in a production environment.

The default configuration file includes no Sterling Connect:Direct File Agent variables or rules. After you verify the default configuration, refer to Creating a New Configuration File to create a flexible configuration with rules.

Creating the Default Configuration File

To create the Default_Config.ser file:

1. Start the configuration interface:
   - On a Microsoft Windows system, select **Start>Programs >Sterling Connect Direct File Agent> Configure Connect Direct File Agent**. Sterling Connect:Direct File Agent starts and displays the configuration interface.
   - On a UNIX system, change to the directory where Sterling Connect:Direct File Agent is installed (/cdunix/file_agent/), and type **cdfa -C** at the command prompt. The **-C** parameter is case-sensitive. You must type a capital **C**.
   - On a z/OS system, submit and run the CDFACONF job to execute the Sterling Connect:Direct File Agent GUI.
2. Select **Default_Config** in the Configurations window and click **Edit** on the File Agent tab. Default_Config displays in red when you first start the Sterling Connect:Direct File Agent configuration interface because the file has not been saved. After you specify details for your network in the required fields and save the configuration, the default file displays in black to indicate that it is ready for use.
3. Identify the Sterling Connect:Direct server that Sterling Connect:Direct File Agent connects to and the default Process information. Type the information in fields on the **File Agent** tab as follows:
   - Userid for API
   - Password for API
   - API host DSN name
   - API port
   - Gate Keeper port
   - Watched directories
   - Process class

   The following table describes parameters for the default configuration file. An asterisk (*) before a field on the interface indicates a required parameter. Specify any other parameters required to configure Sterling Connect:Direct File Agent to operate on your site.

Parameter	Description
Comments	Type comments to describe the configuration. Comments are not used during the execution of Sterling Connect:Direct File Agent.
Userid for API	**Required**. Type the userid to use when connecting to the Sterling Connect:Direct server. This field is case-sensitive.
Password for API	**Required**. Type the associated password for the userid. This is the password that allows you to connect to the Sterling Connect:Direct server. This field is case-sensitive.
API host DNS name	**Required**. Type the DNS name of the host where the Sterling Connect:Direct server is located, or the IP address in the form nnn.nnn.nnn.nnn.
API port	**Required**. Type the 1–5 digit port number that Sterling Connect:Direct File Agent uses to connect to the Sterling Connect:Direct server API. If you do not specify a port number, the default port number, 1363, is used.
Gate Keeper port	**Required**. Type the 1–5 digit port number that Sterling Connect:Direct File Agent uses to connect to the gate keeper. Use any available port number higher than port 10000. If you do not specify a port number, the default port number, 65530, is used. The first instance of Sterling Connect:Direct File Agent to connect to the gate keeper port keeps track of watched directories to ensure that only one instance is monitoring a location.
Watched directories	Required. Type an operating system-specific, valid entry on a line to indicate a location to watch. Use multiple lines to specify multiple locations to watch. You can skip lines for readability; Sterling Connect:Direct File Agent ignores blank lines. For Microsoft Windows or UNIX, type the path to the directory to watch. For S3 object stores, type a bucket name and folder name in a valid URI format. (Scheme:// bucketname[/folder/]) For z/OS systems, specify any of the following types of entries to indicate the location to watch: A fully specified HFS pathname of a directory A fully specified MVS data set name, such as HLQ.MONTHLY.PAYROLL A partial MVS data set name, such as HLQ.MONTH%%.PAY** A partitioned data set (PDS) name or a partitioned data set extended (PDSE) name Sterling Connect:Direct File Agent uses the date to determine when a PDS member or dataset was modified. With a PDS member, the last modification date is used. For an executable file, Sterling Connect:Direct File Agent looks at members of a load module PDS to determine their binder link date. If no date is found, Sterling Connect:Direct File Agent uses the creation date of the PDS where it resides. When matching patterns in z/OS, the percent sign (%) matches a single character, the single asterisk (*) matches a single node level, and two asterisks (**) match all node levels from the point of placement. Refer to the appropriate operating system manuals for information about pattern matching rules. When a VSAM file is created on a z/OS system, three files are generated: the actual data file, an index file, and a cluster file. To prevent Sterling Connect:Direct File Agent from triggering a process for each of these files, be sure your naming rules specify on the data file. For an example of handling this behavior, refer to Scenario:Detecting a VSAM Data File Added to a Watched Directory on a z/OS System .
Monitor sub directories	Select Yes (the default) to monitor the Watched directories and sub-directories, or select No to monitor the Watched directories only.

Parameter	Description
Continuous signon	Select Yes to stay connected to the API port whenever Sterling Connect:Direct File Agent is active, or select No (the default) to have Sterling Connect:Direct File Agent disconnect and reconnect each time Processes are submitted after a directory scan. Sterling Connect:Direct File Agent scans the directories, then submits Processes for any files found during the scan. If Continuous signon is No, Sterling Connect:Direct File Agent will sign on to the Sterling Connect:Direct server the first time it submits a Process for a file found during the scan, and will close the connection to the Sterling Connect:Direct server when all Processes have been submitted for files found during the scan. When files are found during a subsequent scan, Sterling Connect:Direct File Agent will open a new connection to the Sterling Control Center server. Use this option if there are more than a few minutes between files being placed in the watched directories. If Continuous signon is Yes, Sterling Connect:Direct File Agent will open a new connection to the Sterling Connect:Direct Server the first time that a Process is submitted for a file found during the scan, and will leave that connection to the Sterling Connect:Direct server open until Sterling Connect:Direct File Agent is stopped. Use this option if files are placed in the watched directories more or less continuously.
Gate keeper DNS name	Type the name of the host for the Sterling Connect:Direct File Agent gate keeper, or the IP address in the format nnn.nnn.nnn.nnn. The gate keeper keeps track of watched directories so that the same directory is not watched by more than one instance of Sterling Connect:Direct File Agent. When multiple instances are running, the first instance to connect to the gate keeper port becomes the gate keeper. A gate keeper is not required if only one instance is running or if each watched directory is only listed in the configuration of one instance. To disable the gate keeper, set this parameter to blank: the gate keeper port is ignored. If multiple instances of Sterling Connect:Direct File Agent monitor the same network directory, a gate keeper DNS name must be provided.
Default Process	Type the name of the Process to submit when a file is detected by Sterling Connect:Direct File Agent. This default Process is submitted if there is not a rule defined for the file. **Note:** The userid and password used to submit the default Process must be the same as those used to connect to the Sterling Connect:Direct server. On z/OS systems, the default Process is specified as the Member Name in DMPUBLIB. On Microsoft Windows or UNIX, this includes directories in the path to the Process and the name of the Process file. Sterling Connect:Direct File Agent must have read access to the path and file on Microsoft Windows and UNIX. In addition, the userid and password used to submit the default Process must match the userid and password used to connect to the server.
Default arguments	Type the argument string that will be passed to the default Process. When arguments contain special characters, enclose the argument string in double quotes. See Sterling Connect:Direct File Agent Variables for a description of all variables Sterling Connect:Direct File Agent supports as default arguments. For example, in Microsoft Windows, type &ARG1="%FA_FILE_FOUND." to assign the path and filename of the file that Sterling Connect:Direct File Agent detected passed as the symbolic variable &ARG1 to the Process that Sterling Connect:Direct File Agent submits. The leading percent (%) and ending period (.) are required with all variables. See z/OS Process Arguments Example for examples of variable use.

Parameter	Description	
Error Process	Type the name of the Process to submit when an internal code error occurs in Sterling Connect:Direct File Agent, such as a java.lang.null pointer exception. On z/OS systems, this is specified as the Member Name in DMPUBLIB. On Microsoft Windows or UNIX, this is the pathname of the file that contains the Process. Sterling Connect:Direct File Agent must have read access to the path and file on Microsoft Windows or UNIX.	
Error Arguments	Type the argument string that will be passed to the error Process. Sterling Connect:Direct File Agent uses only the following variable. Using any other variable produces undefined results. The leading percent (%) character and the ending period (.) are required.	
	%FA_FILE_FOUND.	The default value is the full text of the Exception message.
Process Class	Required. Type the numeric class that the Process submitted to the Sterling Control Center server should use for execution. The Process class number is a value between 1-255 and is used to determine the order in which a Process is executed. Refer to Sterling Control Center documentation for more information.	
Process Priority	Type the numeric priority to use for execution of the Process Sterling Connect:Direct File Agent submits to the Sterling Control Center server. The Process priority is a number between 0-15 that determines the order of Process execution. Refer to the Sterling Control Center documentation for more information.	
Watch file interval	Type the number of minutes that you want Sterling Connect:Direct File Agent to wait before checking the watch directories for files. By default, Sterling Connect:Direct File Agent checks the watch directories for files once each minute. This field specifies how long Sterling Connect:Direct File Agent waits between directory scans. If you need to transfer files quickly after they are placed into the watched directories, specify a short Watch file interval. However, if there aren't many files placed into the watched directories, set a longer Watch file interval so that Sterling Connect:Direct File Agent is not scanning the watched directories as often. There is a trade-off between the processing time that Sterling Connect:Direct File Agent uses to scan the directories and the need to transfer the files quickly.	
File completion delay	Type the number of minutes that you want Sterling Connect:Direct File Agent to wait before a detected file is considered to be complete.This field is optional. The default time is 1 minute. This field only applies to UNIX systems. With many UNIX applications, different tasks can access the same file simultaneously. This may cause problems if Sterling Connect:Direct File Agent detects that a file is present in the watched directory and uses it before another application has closed it. Set this delay to allow an application to finish with the file before Sterling Connect:Direct File Agent accesses the file.	
File Agent unique name	**Required**. Provide a unique name for each Sterling Connect:Direct File Agent instance running on the same host or on a different host, while monitoring similar network drives, and configured to submit processes to the same Sterling Connect:Direct node. This ensures the unique identity of each Sterling Connect:Direct File Agent instance by Sterling Control Center. Failing to do so results in Sterling Control Center treating multiple instances of Sterling Connect:Direct File Agent as one.	
SNMP listener address	Type the address for the SNMP trap receiver, such as Sterling Control Center. Sterling Connect:Direct File Agent uses this address to send SNMP traps for statistics. This field is optional. You can obtain this information from your Sterling Control Center system administrator.	

Parameter	Description
SNMP listener port	Type the port used by the SNMP trap receiver, such as Sterling Control Center. Port 1163 is the default. This field is optional.
SNMP source port range	Type the ports or port ranges used to pass through a firewall to the SNMP trap receiver, such as Sterling Control Center, when Sterling Connect:Direct File Agent runs behind a firewall. You can specify a maximum of 5 port ranges. This field is optional. Type the ranges in the format nnnn-nnnn, separated by commas, for example, 5555-7777, 8888-8890, 9999. Contact the Sterling Control Center system administrator if you do not know this information.
Refresh Configuration	Select Yes to refresh the configuration after modifying the configuration without restarting Sterling Connect:Direct File Agent The default setting is No. **Note:** The Gate Keeper port setting will not be refreshed unless you restart Sterling Connect:Direct File Agent.

4. Click **Save**. If the file is complete, the listing changes from red to black to indicate that the configuration file is ready for use.

   If any required fields are blank, a dialog box lists those fields. Click **Cancel** to supply the information. Incomplete configuration files can be saved, but cannot be used for operation.

   Incomplete configuration files are saved as .inc files in the installation directory and are listed in red in the Configurations window.
5. If you have changes that have not been saved, a **save confirmation** dialog box appears. Click OK to save the changes.
6. Click **Exit**. If you have changes that have not been saved, an exit **confirmation** dialog box appears. Click OK to save the changes and exit the configuration interface.

The **Refresh Configuration** option is dynamic. You can select **Yes** or **No** and Sterling Connect:Direct File Agent will detect the option when you change the configuration. If you select **No**, you must restart Sterling Connect:Direct File Agent for the configuration changes to take effect.

Verifying the Default Configuration

To start Sterling Connect:Direct File Agent in verbose mode and verify that the configuration is working correctly:

1. Start Sterling Connect:Direct File Agent at a command prompt, with the Default_Config.ser file. The command parameters are case-sensitive.
   - On a Microsoft Windows computer, type **cdfa -v -c*default_config.ser***. To display the parameters on the title bar of the command window, type **cdfa1.bat -v -cdefault_config.ser**.
   - On a UNIX computer, type **cdfa -v -c*Default_Config.ser***.
   - On a z/OS computer, add the following parameters to the Execution job on the $FAJAVA line and submit the Execution job:

     ```
     $FAJAVA -Dsci.config=FAconfiguration -jar fasat.jar -cdefaultconfig.ser
     ```

     See Sterling Connect:Direct File Agent in a z/OS Environment for a sample Sterling Connect:Direct File Agent execution job.
2. Copy a file to the watched directory. The directory **C:\watch** is used in this example.
3. Verify that the log displays information similar to the following, depending on your operating system and the name of the watched directory and the file you copied to it.

   As the following sample from a Microsoft Windows log shows, Sterling Connect:Direct File Agent did not detect a file during the scan of the C:\watch directory at 11:22:33. However, the scan at 11:22:33 detected a file, C:\watch\newArrivedFile.txt, and one command was attempted and accepted.

```
2021-03-08 11:22:27,134 INFO  - Licensed Materials - Property of IBM
2021-03-08 11:22:27,137 INFO  - Connect:Direct File Agent, Version 1.4.0.2_iFix000
                                (c) Copyright IBM Corp. 2002, 2021,
                                All rights reserved.
                                Build 1.4.00.352, Date 2021/03/03
2021-03-08 11:22:27,137 INFO  - US Government Users Restricted Rights
                                Use, duplication or disclosure restricted
                                by GSA ADP Schedule Contract with IBM Corp.
2021-03-08 11:22:27,137 INFO  - Connect:Direct(tm) (c) Copyright 1982, 2021 IBM Corp.
2021-03-08    11:22:27,222    INFO         -    using    configuration    from:    C:\Program
Files\FileAgent\Default_Config.ser
2021-03-08 11:22:33,111 INFO  - Monitoring configuration file C:\Program Files \Default_Config.ser
2021-03-08 11:22:33,157 INFO  - ckpt file: C:\Program Files\FA_10.120.133.1101363.ckpt
2021-03-08 11:22:33,214 INFO  - Gate Server Started
2021-03-08 11:22:33,730 INFO  - Populating files from new watch directory c:\watch
2021-03-08 11:22:33,738 INFO  - Returning 0 ignored during this scan, 0 unchanged, 0 new, 0 changed,
0 removed file(s)
2021-03-08 11:22:33,739 INFO  - End populating files from new watch directory c:\watch
2021-03-08 11:24:33,196 INFO  - Configuration file is not modified
2021-03-08 11:24:34,737 INFO  - Processing directory: "c:\watch" with 1 minute(s) Completion Delay
2021-03-08 11:24:34,745 INFO  - New file c:\watch\newArrivedFile.txt [file date 20210308_112255,
size 0]
2021-03-08 11:24:34,745 INFO  - Returning 0 ignored during this scan, 0 unchanged, 1 new, 0 changed,
0 removed file(s)
2021-03-08 11:24:34,756 INFO  - New file found is: "c:\watch\newArrivedFile.txt [file date
20210308_112255, size 0]"
2021-03-08 11:24:36,907 INFO  - Directory scan ending, commands attempted 1, commands accepted 1
```

If the log does not validate the configuration, contact your system administrator to verify the information for the required parameters.

Sterling Connect:Direct File Agent Variables

To pass file details to the Process that Sterling Connect:Direct File Agent submits, you can specify the appropriate variable in the **Default arguments** field on the File Agent tab of the Sterling Connect:Direct File Agent configuration interface.

Observe the following rules when you specify variables:

- The starting percent sign (%) and the ending period (.) shown with variables are required.
- Enclose argument strings that contain special characters in double quotes.
- Enclose spaces and vertical bars in double quotation marks to avoid problems when variables are passed to a Sterling Connect:Direct File Agent Process.

Microsoft Windows or UNIX Process Arguments Example

The following example demonstrates the operation of Sterling Connect:Direct File Agent variables as Process arguments on a Sterling Connect:Direct server running UNIX.

The following arguments were specified in the **Default arguments** field of the configuration:

&F="%FA_FILE_FOUND."

The variable &F must be included in the default Process to perform the necessary tasks after the Sterling Connect:Direct File Agent detects a new file.

When the file payroll.txt appears in watched directory home/watch1/, then Sterling Connect:Direct File Agent passes the following argument string to the default Process: &F=/home/watch1/payroll.txt.

Usage	Variable	Description
All Operating Systems		

Usage	Variable	Description
Path and file	%FA_0. to %FA_99.	The number included in this variable represents a component of the name of the detected file, as delimited by the file delimiter, in sequence. For example, if the full file name is /usr/watch/test file.active.txt, then %FA_0 is usr, %FA_1 is watch, and so on.
	%FA_FILE_FOUND.	On Microsoft Windows and UNIX, the default value is the path and file name of the detected file. On z/OS systems, the default value is the entire name of the file that Sterling Connect:Direct File Agent detected, including any member name. This variable supports PDSE long member names. For example, when you specify this variable, Sterling Connect:Direct File Agent could pass the following member name: CUST.BENEFITS(PAYROLLPDSELONGNAME). On S3 object stores, the default value is the entire name of the object that Sterling Connect:Direct File Agent detected including the bucket name and scheme name. If a scheme name substitution occurred, this is the name after substitution. For the initial name see %FA_WATCHED_FILE_FOUND variable. For more details, refer Chapter 10, “Amazon S3 support,” on page 75.
	%FA_FSTYPE	The file or object file system type. Windows, Unix, OS390, AWSS3
Current® date and time	%FA_DATE.	The current date for the detected file. This value has 8 characters that represent the year, month, and day, for example, 20040903.
	%FA_DATE_DAY.	The current day, for example, 31.
	%FA_DATE_MONTH.	The current month, for example, 01.
	%FA_DATE_YEAR.	The current year, for example, 2004.
	%FA_NUM.	The millisecond timestamp. If multiple files are sent within the same second, they will get different millisecond values, for example, 13143512345, 13143512346, and 13143512347.
	%FA_TIME.	The current time. This value has 6 characters to represent the hour, minutes and seconds (format (hhmmss) using a 24-hour clock.
	%FA_TIME_HOUR.	The current hour, for example, 13.
	%FA_TIME_MINUTES.	The current minute, for example, 24.
	%FA_TIME_SECONDS.	The current second, for example, 35.

Usage	Variable	Description
Modification date and time	%FA_FDATE.	The date a detected file was last modified. This value has 8-characters representing year, month, and day, for example, 20040903.
	%FA_FDATE_DAY.	The day a file was last modified, for example, 21.
	%FA_FDATE_MONTH.	The month in which a file was last modified, for example, 09.
	%FA_FDATE_YEAR.	The year in which a file was last modified, for example, 2004.
	%FA_FTIME_HOUR.	The hour a file was last modified, for example, 22.
	%FA_FTIME_MINUTES.	The minute a file was last modified, for example, 24 will be passed for a file last modified at 6:24.
	%FA_FTIME_SECONDS.	The second a file was last modified, for example, 35.
	%FA_FTIME.	The time a file was last modified. This value has 6-characters representing hour, minutes, and seconds (hhmmss) using a 24-hour clock, for example, 153842.
UNIX and Microsoft Windows		
File name and path	%FA_EXT_FOUND.	On Microsoft Windows and UNIX, the file extension of the file that was added, for example, .txt.
	%FA_EXT_FOUND_NP.	On Microsoft Windows and UNIX, the file extension of the file that was added, but without the period before the file extension. For example, if the file added is file.txt, using the %FA_EXT_FOUND_NP variable will result in txt being passed (the extension with no period included).
	%FA_NAME_FOUND.	On Microsoft Windows and UNIX, the name of the file that was added, for example, myfile.
	%FA_NOT_PATH.	On Microsoft Windows and UNIX, the file name with the file extension, without any path. For example, if the full file name is /usr/watch/test file.active.txt, then %FA_NOT_PATH. is resolved as test file.active.txt.
	%FA_PATH_FOUND.	On Microsoft Windows and UNIX, the path of the file that was added, for example, on Microsoft Windows, C:\watch\, and on UNIX, /home/user/watch.
Microsoft Windows Only		
	%FA_DRIVE_FOUND.	On Microsoft Windows, the default value is the drive where the added file is located, for example, C:.
z/OS systems		
File and member	%FA_BASEFILE_FOUND.	The default value is the name of the file that was added, without the member name. This variable is only valid for PDS on z/OS operating systems, for example, CUST.BENEFITS.
	%FA_MEMBER_FOUND.	The default value is "." This variable is only valid for PDS on z/OS operating systems. PDSE long member names are supported. For example, the following member name is valid: PAYROLLPDSELONGNAME.

Usage	Variable	Description
S3 Object stores only		
	%FA_SCHEME	This is the object scheme when Connect:Direct File Agent discovered the object.
	%FA_OUTSCHEME	This is the object scheme if a scheme substitution occurred. Without substitution the value is same as %FA_SCHEME.
	%FA_WATCHED_FILE_FOUND	When a scheme substitution occurred value is the object name before substitution occurred, the object name Connect:Direct File Agent detected.

z/OS Process Arguments Example

For example, if you type the following Process arguments:

```
&BASEFILE="%FA_BASEFILE_FOUND. &MEMBER=%FA_MEMBER_FOUND.
&FILE=%FA_FILE_FOUND."
```

The following argument strings are submitted to the Process:

- The watched directory (a PDS) is CUST.PROCLIB and member PAYROLL changes. Sterling Connect:Direct File Agent passes the following to the associated Process:

  arg string= &BASEFILE="CUST.PROCLIB &MEMBER=PAYROLL &FILE=CUST.PROCLIB(PAYROLL)"
- The watched directory file is CUST.*, and member BENEFITS of PDS CUST.PARMFILE changes. Sterling Connect:Direct File Agent passes the following to the associated Process:

  arg string= &BASEFILE="CUST.PARMFILE &MEMBER=BENEFITS"
- The watched directory is CUST.GDGBASE.* and CUST.GDGBASE.G0223V00 is created. Sterling Connect:Direct File Agent passes the following to the associated Process:

  arg string= &BASEFILE="CUST.GDGBASE.G0223V00 &MEMBER="

The Default Configuration with Rules

Rules enable you to define conditions that override the operation defined by the default Sterling Connect:Direct File Agent configuration. When you specify rules for a configuration, Sterling Connect:Direct File Agent monitors one or more watched directories, but also performs some additional steps:

- Instead of only monitoring watched directories for file activity, Sterling Connect:Direct File Agent also checks for the criteria specified in a rule.
- Instead of submitting the default Process for the configuration after detecting activity in a watched directory, Sterling Connect:Direct File Agent submits the Process specified for the first rule for which all criteria match.

Rules are not required; they are an option available for overriding the default Process when you need to perform specific actions after Sterling Connect:Direct File Agent detects certain conditions. You must define the conditions as criteria for a Sterling Connect:Direct File Agent rule. Sterling Connect:Direct File Agent can check criteria for two types of rules: system event rules and submit Process rules (watched file event rules).

During internal processing, Sterling Connect:Direct File Agent detects significant system events, for example exception errors, which can be processed against rules. You can design a rule to test for an exception event and if the event is detected, submit a Process designed to perform appropriate actions in response to that exception event. See Creating a System Event Rule for more information. You can also create rules to test for events that are written to the system log.

When a configuration file rules specified and Sterling Connect:Direct File Agent detects a file in a watched directory, it submits the default Sterling Connect:Direct Process to the Sterling Connect:Direct server. Typically, the default Sterling Connect:Direct Process contains generic processing steps that can be applied to a variety of files. You can create a watched file event rule (Submit Process rule) to have Sterling Connect:Direct File Agent submit a specified Process after detecting a file that matches certain criteria. Watched file event rules enable more refined filtering of files in watched directories and submission of a Sterling Connect:Direct Process that performs actions required after detecting a particular type of file. See Creating a Watched File Rule for a sample watched file event rule.

Match Criteria and Operators

A Sterling Connect:Direct File Agent rule includes one or more match criteria and operators that specify how Sterling Connect:Direct File Agent evaluates a compare string against a detected file or system event. The Process specified for a rule is submitted to the Sterling Control Center server only when the evaluation results in a match.

Match criteria and compare string define the conditions that Sterling Connect:Direct File Agent checks for. For a submit Process rule, match criteria are based on the file name or file size of the file that Sterling Connect:Direct File Agentdetects in a watched directory. For a system event rule, match criteria are based on the title or the contents of a system event.

System event rules based on event contents are for use when Sterling Connect:Direct File Agent can analyze a stack trace for the event. Some system events may not qualify.

Operators define how Sterling Connect:Direct File Agent tests for the match criteria using the compare string to evaluate properties of a detected file (watched file event rule) or a system event (system event rule). Each rule can have one or more match criteria. If you define more than one criterion to match in a rule, all criteria must be met before the rule is processed.

Review the operator functions in the following definition list for how rules are processed and guidelines for creating rules.

Matches

To define a rule that instructs Sterling Connect:Direct File Agent to search only the directory specified by the path for the file name or the system event that match the specified compare string exactly.

The compare string can include the wildcard characters asterisk (*) and question mark (*?). For example, typing c:\devfiles'uality est* as the string to match causes Sterling Connect:Direct File Agent to process the rule after detecting any file name beginning with test in the c:\devfiles'uality directory.

The matches operator requires an exact match for any character except wildcards. This operator requires careful planning to filter files successfully.

Unless you match only on the end of a file name, you must include the path as part of the match string. For example, *.txt will correctly match any file in the watch directory ending in .txt. However, 09*.txt will not match on a file 09March.txt. Instead, use:

<watch directory pathname>/09*.txt

where <watch directory pathname> is the full path to the watch directory, such as c:\devfiles'uality\09*.txt.

Not matches

To define a rule based on characters to exclude. The path and file name or system event are checked against the compare string and Sterling Connect:Direct File Agent processes the rule when it detects any characters other than those specified in the string.

The compare string can include the wildcard characters asterisk (*) and question mark(?).

Contains

To define a rule in which Sterling Connect:Direct File Agent searches all directories in the watched directory for the file name or system event that contains the text specified as compare string. This

is the most versatile operator because it requires only that the compare string exist in any position within the string.

Equals

To define an exact match between the fully qualified path and file name, size of the detected file, title or contents of a system event, and the text string or size specified for comparison. This operator requires an exact match for every character position, so use it only when you know the entire file name.

Note: Do not use this operator to match 0-byte files.

Less than

The detected file must be smaller than the size specified for comparison.

Note: To match a 0-byte file, you must specify **1** in the **Compare size** field with the **Less than** operator.

Greater than

Requires that the detected file is larger than the size specified for comparison.

Rules Processing

Override the default Process specified in the default configuration by including one or more rules when you want to address specific file processing needs. Although you create rules to define conditions for Sterling Connect:Direct File Agent to detect, it is the Sterling Connect:Direct Processes associated with rules that perform actions to accomplish tasks. You can enable and disable rules by selecting or clearing the Enabled check box on the Rules tab of the configuration interface.

Defining rules can be challenging, and requires understanding of networks, operating systems, and Sterling Connect:Direct. The understanding of Sterling Connect:Direct Processes is essential because Sterling Connect:Direct File Agent simply monitors activity; Processes submitted to the Sterling Connect:Direct server accomplish the actions you want performed.

Sterling Connect:Direct File Agent processes rules as follows:

- Only enabled rules are searched. Rules are searched in the order that they are listed on the Rules tab.
- Only enabled match criteria are tested. When match criteria are met for a rule, that rule is processed and no further rules processing is performed.
- Sterling Connect:Direct File Agent executes a maximum of one rule for each file or system event detected.
- When a file matches a rule but the rule specifies no Process, nothing happens.

Guidelines for Defining Rules

When you create multiple rules of the same type, define the rule with the most specific criteria first. Rules are searched in the order that they are created. The rule hierarchy is displayed on the Rules tab. If the first rule listed is general, there will always be a match, and subsequent rules will never be processed.

For example, assume that you need to create the following two rules

- One rule tests for all files that start with the text string pay.
- Another rule test for all files that start with the text string pay and are larger than 2000 bytes.

Because the second rule has more specific criteria, create it first to list it first on the Submit Process rules tab; otherwise, it will never be processed.

Create and validate one rule at a time to verify that a rule produces expected result.

Creating a Watched File Rule

Complete the following procedure to create and validate a watched file rule that tests for a file name that contains a specified string:

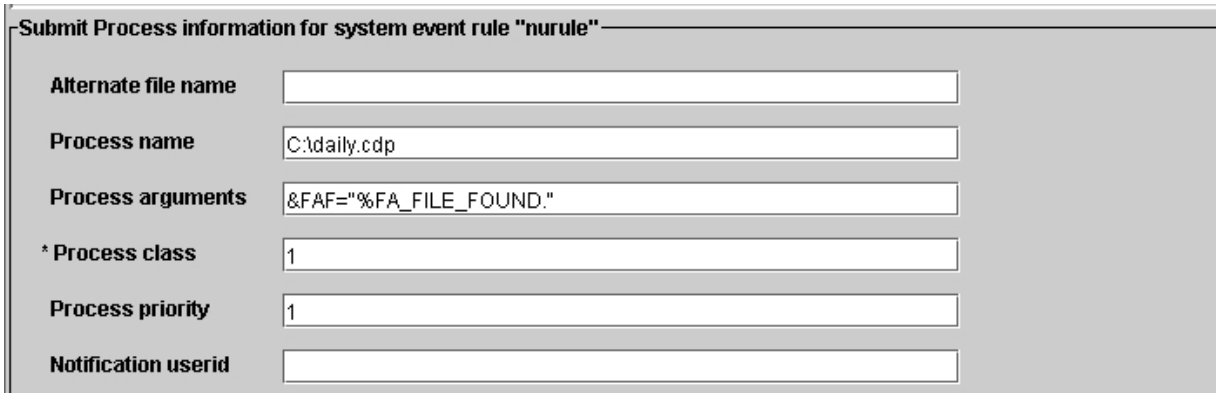
1. Select the Default_config file from the Configurations window.
2. Click the Rules tab.
3. Select the **Submit Process rules** tab and click **New**.
4. Type a name for the rule and click **OK**. The sample rule in this example is named *daily*. The rule is added to the list of rules.
5. Select the rule and click **Edit**.

   The Match criteria list (top) and the Submit Process information (bottom) display in the right pane of the GUI. These two areas must contain information as follows for the rule:

   - Match criteria list—A list of conditions that must be met before the rule is applied to the detected file or event.

   - Submit Process information—These parameters specify the Process that Sterling Connect:Direct File Agent submits to the Sterling Connect:Direct server. This Process is submitted only when there is a match for the associated rule.
6. Choose the first item in the Match criteria list and click Edit match. The Edit match criterion window is displayed.
7. Click Enabled to enable the match criterion.
8. Click the property of the file to test. Match either the name or the size of the new file. In this example, the option Name of the newly arrived file is selected.
9. Click the **Matches** arrow to display the drop down list of operators. In this example, **Contains** is selected as the operator for the match criterion.

   Using Contains as the operator searches all subdirectories in the watched directory and matches the name of the file in the compare string in any position (beginning, end, or middle). Characters other than those specified in the compare string can be included before and after the string and an exact match is not required. See Match Criteria and Operators for details about other operators.
10. Type the portion of the file name to detect in the Compare string field, for example, daily. Include the absolute path of the file. When the compare string is correct, click OK.
11. Define the Process information in **Submit Process information**.



In this example, the Process C:\daily.cdp is submitted to the Sterling Connect:Direct server. Specify the following Process arguments: **&FAF="%FA_FILE_FOUND**."

The path and file name for the detected file is sent the symbolic variable &FAF; this variable is included in the Sterling Connect:Direct Process (c:\daily.cdp) submitted.

Parameters allowed in the Submit Process information operate as described in the following table:

Parameter	Description	
Alternate file name	Name of an alternate file to process for this event. If you specify an alternate file name, the name of the alternate file is used instead of the file detected in a watched directory. Variables are evaluated against the alternate file name and the results of to the Process are submitted as arguments. For example, whe alt.txt is specified, the file q1sales.txt is detected in the watched directory c:\reports\ as a match for a rule. Although the argument string &F="%FA_FILE_FOUND." is specified as the Process arguments, the string alt.txt is sent to the Process it submits. With no alternate file name specified, c:\reports'1sales.txt is sent to the Process submitted after detection, based on the Sterling Connect:Direct File Agent variable (%FA_FILE_FOUND.).	
Process name	Process to submit. On z/OS systems, this is specified as the Member Name in DMPUBLIB. On Microsoft Windows and UNIX, this is the path and file name of the Process. Sterling Connect:Direct File Agent must have read access to the path and file on Microsoft Windows or UNIX. Type an asterisk in this field to copy the default Process name from the File Agent tab.	
Process arguments	Type the Process variable and argument string to send to the Process specified by the rule. For example, type: &F="%FA_DATE." to send the current date for the detected file as the symbolic variable &F to the Process that Sterling Connect:Direct File Agent submits. Sterling Connect:Direct File Agent allows the variables described in z/OS Process Arguments Example . The leading percent (%) character and the ending period (.) are required for all variables. When arguments contain special characters, enclose the argument string in double quotes.	
Process Class	Type the numeric class that the Process submitted to the Sterling Connect:Direct server should use for execution. This can be a value between 1-255 and is used to determine the order in which a Process is executed.	
Process Priority	Type the numeric priority that the Process submitted to the Sterling Connect:Direct server should use for execution. This can be a value between 0-15 and is used to determine the order in which a Process is executed. Refer to Sterling Connect:Direct documentation for more information.	

Parameter	Description	
Notification userid	Type the userid to notify when the Process completes if notification is supported. If this field is blank, no user is notified.	

12. After specifying parameters, click Done under the Match criteria list.
13. The **Rules** tab is displayed again, with the rule listed. Click Enabled on the right to enable the rule.
14. Click **Save**.

The **Refresh Configuration** option is dynamic. You can select **Yes** or **No** and the changes are recognized. If you select **No**, restart Sterling Connect:Direct File Agent to enable the changes

Validating a Watched File Rule

After you define a watched file rule, complete the following procedure to validate that it works correctly before you add more rules:

1. Start Sterling Connect:Direct File Agent from the command line with the Default Configuration file that contains a rule:
   - On a Microsoft Windows computer, type **cdfa -cdefault_config.ser** at a command prompt or to display the parameters on the title bar of the command window, type **cdfa1.bat -cdefault_config.ser** at a command prompt.
   - On a UNIX computer, type **cdfa -cDefault_Config.ser** at a command prompt.
   - On a z/OS computer, edit the script for the Execution job to specify which configuration file to use. Type the command parameter and the configuration file name on the $FAJAVA line and then submit the Execution job. The command parameters are case-sensitive.
2. Create a file with the word specified in the compare string (for example, *daily)* in the name and copy it to the watched directory you specified in Creating the Default Configuration File.
3. Confirm that the Process (for example, daily.cdp) to use for testing has been created on the Sterling Connect:Direct File Agent server.
4. Verify that the log displays information similar to the following sample. Some lines may differ because of operating system differences and the use of different parameter definitions.

```
...
November 22, 2010 3:51:33 PM CST  663 Thread[FADron1 /FILAGEN,5,main]
      Processing directory: "C:\watch"
November 22, 2010 3:51:33 PM CST  663 Thread[FADron1 /FILAGEN,5,main]
      Completed directory: "C:\watch"
November 22, 2010 3:51:33 PM CST  663 Thread[FADron1 /FILAGEN,5,main]
      directory scan ending, commands attempted 0, commands accepted 0
November 22, 2010 3:52:33 PM CST  671 Thread[FADron1 /FILAGEN,5,main]
      Processing directory: "C:\watch"
November 22, 2010 3:52:33 PM CST  691 Thread[FADron1 /FILAGEN,5,main]
      New file found is: "C:\watch\dailyreport 11/24/2003 16:58:58"
November 22, 2010 3:52:33 PM CST  771 Thread[FADron1 /FILAGEN,5,main]
      The matching rule criteria and actions are :
Rule (daily) type(watch_file)
 Match Criteria (Enabled: Name of the newly arrived file Contains  "daily"       )
       End Match Criteria
RuleAction type(watch_file) email(false) transfer(false) store(false)
      emailattachfile(false) emailID() emailSubject(An email notification from the
      IBM Sterling Connect:Direct Remote Agent) emailBody(A file event has occurred)
      xStoreFileName(null) xStoreEncoding(null) xStoreNewEncoding(null)
      xEmailFileName(null) xEmailEncoding(null) xEmailNewEncoding(null)
      xCDSnodeUid(null) xCDSnodeFileName(null) xCDPnodeFileName(null)
      xCDXferType(null) xCDMBCSCodePage(null) xCDMBCSNewCodePage(null)
      xCDMBCSLocalCodePage(null) xCDMBCSLocalNewCodePage(null) xCDCompress(null)\
      xCDCkpt(null) xCDDisp(null)
 priority(1) class(1) pnodeUid() pnodePwd(********) snodeUid() snodePwd(********)

      notifyUid() pnodeAcct() snodeAcct() procName(C:\daily.cdp) procArgs(&F=%FA_FILE_FOUND.)
       AltName() End Rule(daily)
November 22, 2010 3:52:33 PM CST  771 Thread[FADron1 /FILAGEN,5,main]
      Completed directory: "C:\watch"
November 22, 2010 3:52:34 PM CST   51 Thread[FADron1 /FILAGEN,5,main]
      directory scan ending, commands attempted 1, commands accepted 1
```

If the log does not validate the application of the rule, see “Troubleshooting” on page 63.

5. Repeat this procedure until you validate the rule.

   After you validate this rule, add more rules one at a time. Validate each rule before adding another one.

   Note: The Sterling Connect:Direct File Agent system log for Microsoft Windows may contain many lines of information, especially with multiple rule use. Instead of checking each line, use a line editor to search for key phrases related to details you need to check. For example, use Microsoft Windows Notepad to search for a rule name, directory path, or date.

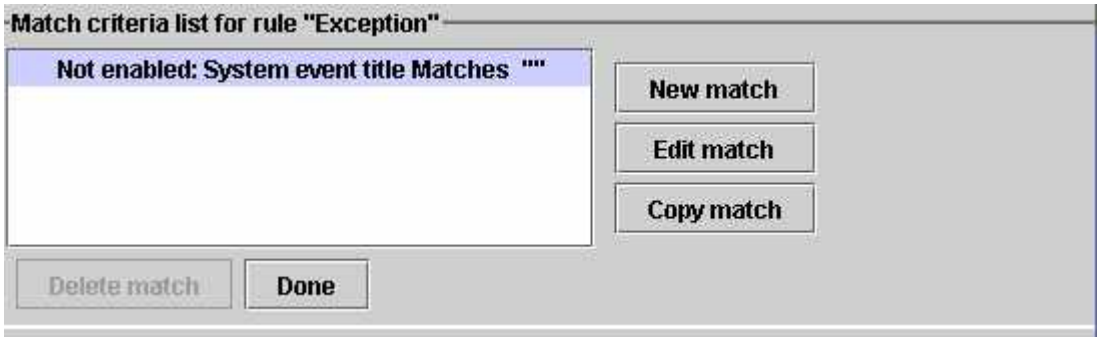
Creating a System Event Rule

With a system event rule, Sterling Connect:Direct File Agent compares a system event title or system event contents with the string you specify. An example of a system event title is RAAction for a remote agent action event. The contents of an event is something related to the event, such as a message. For example, the following message can be the contents of an event: Process submitted to Connect Direct: File_Test.

Use the following procedure to create a system event rule that tests for exception errors, submits a Process, and passes the text of the exception error to Sterling Connect:Direct.

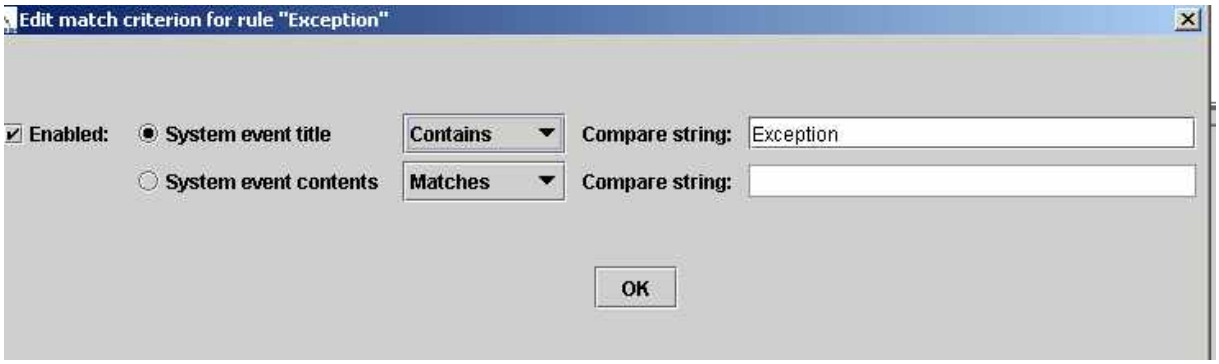
In this sample scenario, Sterling Connect:Direct File Agent submits a Process (ErrProc.cdp) to the Sterling Connect:Direct server when an Exception error event matches the rule named *Exception*.

1. Select the **Default_Config.ser** from the Configurations window.
2. Click the Rules tab.
3. Click System event rules.
4. Click New to create a new rule.
5. Type the rule in the **Create rule** dialog box and click OK. For this example, the rule is called Exception.
6. Select the new rule you created and click Edit.
7. Click Edit match to modify the criteria for this rule.



8. Select Enabled to enable your match criteria.
9. Select System event title and choose Contains as the operator.

   The Contains operator tests for the string in a system event title. The characters must be in exact order, but they can occur in any position (beginning, middle, or end).
10. In the Compare string field, type **Exception** to check for a system event title that includes these characters. Using Contains enables you to specify a portion of the event title without specifying all characters. The compare string is shorter and the rule is more likely to be processed because you have allowed for flexibility in the matching.

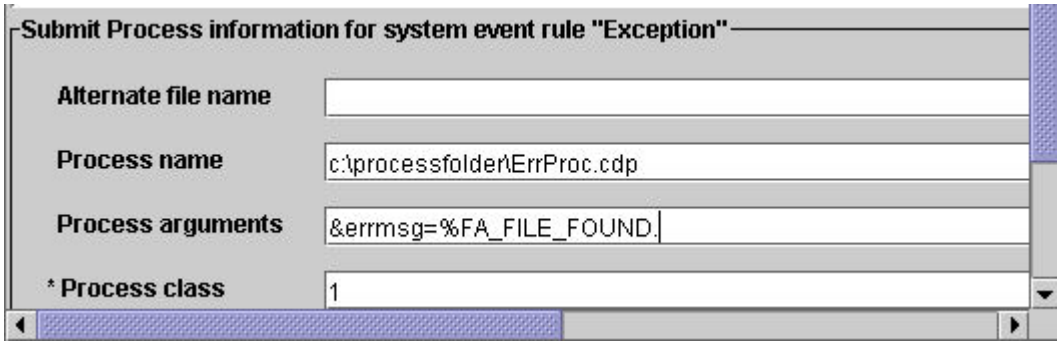


Note: You can use the following messages to compare system event titles and contents:

- Process submitted to Connect Direct: <process_name>
- unsupported product level: <CD Node Version>
- MsgException
- LogonException
- ConnectionException
- ParseException
- Unknown gatekeeper host - UnknownHostException
- InterruptedException
- SocketException
- IOException
- Exception
- Error finding service drone
- service <service name> has terminated in error

These exceptions will contain more information that just the text listed. For example, "MsgException" could be followed by "LAPP013I An invalid keyword value was found CCOD=8 FDBK=0 SBST="(|&line= : this ,error at line 8|)."

11. Click OK to return to the rule definition.
12. Scroll to **Submit Process information** and enter the Process information as shown in the following example. For system event rules, the only valid Process argument variable is %FA_FILE_FOUND.



The Sterling Connect:Direct error Process specified in this sample scenario, ErrProc.cdp, contains the following code that defines a default value for the argument &errMsg= so that when you specify the variable &errMsg="%FA_FILE_FOUND.", Sterling Connect:Direct File Agent passes the actual text of the error message to the Sterling Connect:Direct Process.

In the Process, a run task step calls a script that appends the message text to an Exceptions file; however, you can handle the exception text as necessary for your site:

```
/*BEGIN_REQUESTER_COMMENTS
    $PNODE$="EAST1_CHI" $PNODE_OS$="Microsoft Windows"
    $SNODE$="EAST1_CHI" $SNODE_OS$="Microsoft Windows"
    $OPTIONS$="WDOS"
  END_REQUESTER_COMMENTS*/
SYSLOG PROCESS
    &errMsg="'Default error message'"
    SNODE=EAST1_CHI
 RUN TASK PNODE (PGM=Microsoft Windows)
    SYSOPTS="pgm(c:    emp\syslog.bat) args(&errMsg)"
PEND
```

13. Click Done to return to the **Rules** tab.
14. Click Enabled to enable the rule.
15. Click Save to update your changes to the configuration.

The **Refresh Configuration** option is dynamic. You can select **Yes** or **No** and Sterling Connect:Direct File Agent will detect the option when you change the configuration. If you select **No**, you must restart Sterling Connect:Direct File Agent for the configuration changes to take effect.

Reordering Rules

To reorder Submit Process rules and System event rules:

1. On the **Rules** tab, select the rule you want to move.
2. To move the rule up one level, click **Up**.
3. To move the rule down one level, click **Down**.
4. Repeat steps 1 and 2 until the rules are in the desired order.
5. Click **Save**.
6. Click **OK** in the **Save confirmation** dialog box. The save confirmation dialog box only appears if there is unsaved data.

The **Refresh Configuration** option is dynamic. You can select **Yes** or **No** and Sterling Connect:Direct File Agent will detect the option when you change the configuration. If you select **No**, you must restart Sterling Connect:Direct File Agent for the configuration changes to take effect.

Configuration File Hierarchy

When Sterling Connect:Direct File Agent is running as a Microsoft Windows Service, it uses the Default_Config.ser configuration file. When started manually, it uses the following hierarchy to determine the configuration file to use:

- If you start from a command line with the **cdfa -c**configurationfilename command, the specified configuration file is used. For example, **cdfa -cmonthend.ser** starts with the configuration file named monthend.ser.
- If you do not specify **-c** with the **cdfa** command, it searches for a configuration file that matches the computer it is running on. For example, if Sterling Connect:Direct File Agent runs on a computer named Host1, and a configuration file named Host1.ser exists, it uses the Host1 configuration file.
- On a Microsoft Windows computer, view the computer name by selecting **Start>Settings>Control Panel>System** and select the **Computer Name** or **Network Identification** tab. For UNIX or Linux®, see operating system documentation for how to find the computer name.
- If you do not specify **-c** with the **cdfa** command and there is no configuration file that matches the computer name, the Default_Config.ser configuration file in the installation directory is used.

Chapter 3. Configuration Files

Creating a New Configuration File

You can add a new configuration file by copying, renaming, and changing the parameters for an existing configuration. You may need another configuration file to accommodate special-purpose processing, for example, for end-of-month processing or seasonal transaction activity. Using a different configuration file can also be helpful when you need to connect to a different Sterling Connect:Direct Server or submit Sterling Connect:Direct Processes with a different Process class and priority for execution. You can also create a new configuration so that you can test its operation without affecting the default configuration. New configuration files you create are saved with a .ser extension in the File Agent directory and are visible on the Configurations window of the Sterling Connect:Direct File Agent Configuration Interface.

To create a new configuration file:

1. Select the file that you want to copy from the Configurations window.
2. Click **Copy**.
3. Type the name of the new file in the **Copy configuration** dialog box and click **OK**.

   The configuration file is added to the Configurations window.
4. Select the new configuration file from the Configurations window. Click **Save** on the File Agent tab.
5. Click **Edit** on the File agent tab.
6. Change the **File Agent** tab settings as necessary. The following table describes the configuration file parameters. An asterisk (*) before a field name indicates a required parameter.

Parameter	Description
Comments	Type comments to describe the configuration. Comments are not used during the execution of Sterling Connect:Direct File Agent.
Userid for API	**Required**. Type the userid to use when connecting to the Sterling Connect:Direct server. This field is case-sensitive.
Password for API	**Required**. Type the password to use when connecting to the Sterling Connect:Direct server. This field is case-sensitive.
API host DNS name	**Required**. Type the name of the host where the Sterling Connect:Direct server is located, or the IP address in the form nnn.nnn.nnn.nnn.
API port	**Required**. Type the 1–5 digit port number that Sterling Connect:Direct File Agent uses to connect to the Sterling Connect:Direct server API. If you do not specify a port number, the default port number, 1363, is used.
Gate Keeper port	**Required**. Type the 1–5 digit port number that Sterling Connect:Direct for UNIX uses to connect to the gate keeper. Use any available port number higher than port 10000. If you do not specify a port number, the default port number, 65530, is used. The first instance of Sterling Connect:Direct File Agent to connect to the gate keeper port keeps track of watched directories to ensure that only one instance is monitoring a location.

Parameter	Description
Watched directories	**Required**. Type one or more directories or files. Type one fully qualified entry on each line. Blank lines are ignored to enhance readability. On Microsoft Windows and UNIX, an entry can be the pathname of a file or a directory. For S3 objects store, type a bucket name and folder name in a valid URI format. (Scheme://bucketname[/folder/]) On z/OS systems, an entry can be any of the following: • A fully specified HFS pathname of a file • A fully specified HFS pathname of a directory • A fully specified MVS data set name, such as HLQ.MONTHLY.PAYROLL • A partial MVS data set name, such as HLQ.MONTH%%.PAY** **Note:** When matching patterns in data set names, the % matches a single character, the single asterisk (*) matches a single node level, and the double asterisk (**) matches all node levels from the point of placement. Refer to the IBM document DFSMS: Managing Catalogs (SC26-7409-03) for information about using the catalog search interface with wildcards and other generic filter keys. You can specify a partitioned data set (PDS) or a partitioned data set extended (PDSE) in the watched directories field. Sterling Connect:Direct File Agent uses the date to determine when a PDS member or data set was modified. With a PDS member, the last modification date is used. For an executable file, Sterling Connect:Direct File Agent checks members of a load module PDS to determine their binder link date. If no date is found, Sterling Connect:Direct File Agent uses the creation date of the PDS where it resides. When a VSAM file is created on a z/OS system, three files are generated: the actual data file, an index file, and a cluster file. To prevent Sterling Connect:Direct File Agent from triggering a process for each of these files, be sure your naming rules specify on the data file. For an example of handling this behavior, refer to Scenario:Detecting a VSAM Data File Added to a Watched Directory on a z/OS System.
Monitor sub directories	Select Yes (the default) to monitor the Watched directories, or No to monitor the Watched directories only.

Parameter	Description
Continuous signon	Select Yes to stay connected to the API port whenever Sterling Connect:Direct File Agent is active, or No (the default) disconnect and reconnect each time Processes are submitted after a directory scan. Sterling Connect:Direct File Agent scans the directories, then submits Processes for any files found during the scan. If Continuous signon is No, Sterling Connect:Direct File Agent will sign on to the Sterling Connect:Direct server the first time it submits a Process for a file found during the scan, and will close the connection to the Sterling Connect:Direct server when all Processes have been submitted for files found during the scan. When files are found during a subsequent scan, Sterling Connect:Direct File Agent will open a new connection to the Sterling Connect:Direct server. Use this option if there are more than a few minutes between files being placed in the watched directories. If Continuous signon is Yes, Sterling Connect:Direct File Agent will open a new connection to the Sterling Connect:Direct server the first time that a Process is submitted for a file found during the scan, and will leave that connection to the Sterling Connect:Direct server open until Sterling Connect:Direct File Agentis stopped. Use this option if files are placed in the watched directories more or less continuously.
Gate keeper DNS name	Type the name of the host for the Sterling Connect:Direct File Agent gate keeper, or the IP address in the format nnn.nnn.nnn.nnn. The gate keeper keeps track of watched directories so that the same directory is not watched by more than one instance of Sterling Connect:Direct File Agent. When multiple instances are running, the first instance to connect to the gate keeper port becomes the gate keeper. A gate keeper is not required if only one instance is running or if each watched directory is only listed in the configuration of one instance. To disable the gate keeper, set this parameter to blank: the gate keeper port is ignored. If multiple instances of Sterling Connect:Direct File Agent monitor the same network directory, a gate keeper DNS name must be provided.
Default Process	Type the name of the Process to submit when a file is detected by Sterling Connect:Direct File Agent. This default Process is submitted if there is not a rule defined for the file. On z/OS systems, this is specified as the Member Name in DMPUBLIB. On Microsoft Windows or UNIX, this is the pathname of the file that contains the Process. Sterling Connect:Direct File Agent must have read access to the path and file on Microsoft Windows or UNIX.
Default arguments	Type the argument string that will be passed to the default Process. Sterling Connect:Direct File Agent uses the variables described in z/OS Process Arguments Example . The leading % character and the ending "." are required for variables.
Error Process	Type the name of the Process to submit when an internal code error occurs in Sterling Connect:Direct File Agent, such as a java.lang.null pointer exception. On z/OS systems, this is specified as the Member Name in DMPUBLIB. On Microsoft Windows or UNIX, this is the pathname of the file that contains the Process. Sterling Connect:Direct File Agent must have read access to the path and file on Microsoft Windows or UNIX.

Parameter	Description
Error Arguments	Type the argument string that will be passed to the error Process. Sterling Connect:Direct File Agent uses only the following variable. Using any other variable produces undefined results. The leading % character and the ending "." are required. %FA_FILE_FOUND. - The default value is the full text of the Exception message.
Process Class	Type the numeric class that the Process submitted to the Sterling Connect:Direct server should use for execution. This can be a value between 1-255 and is used to determine the order in which a Process is executed. Refer to Sterling Connect:Direct documentation for more information.
Process Priority	Type the numeric priority that the Process submitted to the Sterling Connect:Direct server should use for execution. This can be a value between 0-15 and is used to determine the order in which a Process is executed. Refer to Sterling Connect:Direct documentation for more information.
Watch file interval	Type the number of minutes that you want Sterling Connect:Direct File Agent to wait before checking the watch directories for files. By default, Sterling Connect:Direct File Agent checks the watch directories for files once each minute. This field specifies how long Sterling Connect:Direct File Agent waits between directory scans. If you need to transfer files quickly after they are placed into the watched directories, specify a short Watch file interval. However, if there aren't many files placed into the watched directories, set a longer Watch file interval so that Sterling Connect:Direct File Agent is not scanning the watched directories as often. There is a trade-off between the processing time that Sterling Connect:Direct File Agent uses to scan the directories and the need to transfer the files quickly.
File completion delay	Type the number of minutes that you want Sterling Connect:Direct File Agent to wait before a detected file is considered to be complete.This field is optional. The default time is 1 minute. This field only applies to UNIX systems. With many UNIX applications, different tasks can access the same file simultaneously. This may cause problems if Sterling Connect:Direct File Agent detects that a file is present in the watched directory and uses it before another application has closed it. Set this delay to allow an application to finish with the file before Sterling Connect:Direct File Agent accesses the file.
File Agent unique name	**Required**. Provide a unique name for each Sterling Connect:Direct File Agent instance running on the same host or on a different host, while monitoring similar network drives, and configured to submit processes to the same Sterling Connect:Direct node. This ensures the unique identity of each Sterling Connect:Direct File Agent instance by Sterling Control Center. Failing to do so results in Sterling Control Center treating multiple instances of Sterling Connect:Direct File Agent as one.
SNMP listener address	Type the address for the SNMP trap receiver, such as Sterling Control Center Sterling Connect:Direct File Agent uses this address to send SNMP traps for statistics. This field is optional. You can obtain this information from your Sterling Control Center system administrator.
SNMP listener port	Type the port used by the SNMP trap receiver, such as Sterling Control Center. Port 1163 is the default. This field is optional.

Parameter	Description
SNMP source port range	Type the ports or port ranges used to pass through a firewall to the SNMP trap receiver, such as Sterling Control Center, when Sterling Connect:Direct File Agent runs behind a firewall. You can specify a maximum of 5 port ranges. This field is optional. Type the ranges in the format nnnn-nnnn, separated by commas, for example, 5555-7777, 8888-8890, 9999. Contact the Sterling Control Center system administrator if you do not know this information.
Refresh Configuration	Select Yes to refresh the configuration after modifying the configuration without restarting Sterling Connect:Direct File Agent. The default setting is No. **Note:** The gate keeper port setting will not be refreshed unless you restart Sterling Connect:Direct File Agent.

7. Click the **Rules** tab to override the default behavior. When you copy a configuration file, any rules for the original configuration file are copied to the new configuration file. See Guidelines for Defining Rules for information about setting up rules.
8. Click **Save**.

   If you left any required fields blank, a window is displayed listing the fields. Click **Cancel** and supply the missing information or click **Save** to save an incomplete file. Incomplete files are saved with an .inc extension and are displayed in red. A file must be completed before it can be used in production.
9. Click **OK** in the **Save confirmation** dialog box.
10. Click **Exit**.
11. Start Sterling Connect:Direct File Agent.
    - On a Microsoft Windows computer, type **cdfa -**cconfigfile**.ser** at a command prompt, where configfile is the configuration file to use.
    - On a UNIX computer, type **cdfa -**cconfigfile**.ser** at a command prompt, where configfile is the file to use.
    - On a z/OS system, edit the script for the Execution job if you want to specify which configuration file to use. Type the command parameter and the configuration file name on the $FAJAVA line. Then you can submit the Execution job. The command parameters are case-sensitive.

      If Sterling Connect:Direct File Agent cannot connect to the Sterling Connect:Direct server, see “Troubleshooting” on page 63.

Editing a Configuration File

1. Select the file that you want to edit from the Configurations window.
2. Click the tab that you want to change (**File Agent** or **Rules**).
3. Click **Edit**.
4. Change the settings as necessary.
5. Click **Save** to save the updated configuration file.

   If you left any required fields blank, a window is displayed listing the fields. You can either:
   - Click **Cancel**, then supply the missing information.
   - Click **OK** to save an incomplete configuration for future editing. Incomplete configurations are saved with .inc file extensions, and are displayed in red in the Configurations window. Sterling Connect:Direct File Agent cannot use an incomplete configuration.
6. Click **OK** in the **Save confirmation** dialog box.

7. Click **Exit**. An exit confirmation dialog box is displayed if there is unsaved data.

The **Refresh Configuration** option is dynamic. Select **Yes** or **No** and the option is detected when you change the configuration. If you select **No**, restart Sterling Connect:Direct File Agent to enable the configuration changes.

Deleting a Configuration File

1. Select the configuration file that you want to delete from the Configurations window.
2. Click **Delete**.
3. Click **OK** in the **Delete confirmation** dialog box.

   To restart the configuration interface with default values, delete all configurations, exit the Configuration window, and restart the configuration interface. The configuration is regenerated with the default values.

Creating Multiple Configurations with the Copy Function

You can create multiple configuration files by copying an existing configuration file, naming the new configuration file, and changing the configuration information.

Rather than have the client sites create their own configurations, a Sterling Connect:Direct server site can create configuration files and distribute them to Sterling Connect:Direct File Agent client sites. This reduces the possibility of typing errors and ensures consistent configurations throughout the Sterling Connect:Direct File Agent network.

In the following procedure, assume that you create three new configuration files named FA1, FA2, and FA3 for distribution.

1. Select the file to copy from the Configurations window.
2. Click **Copy**.
3. Type the new file name(**FA1**) in the Copy configuration dialog box and click **OK**.
4. Select the **FA1** configuration file from the Configurations window.
5. Click **Edit**.
6. On the **File Agent** tab, change the following fields.

Parameter	Description
Comments	Type comments to describe the configuration. Comments are not used during execution
Userid for API	Required. Type the userid to use when connecting to the Sterling Connect:Direct server. This field is case-sensitive.
Password for API	Required. Type the password to connect to the Sterling Connect:Direct server. This field is case-sensitive.
API host DNS name	Required. Type the host where the Sterling Connect:Direct server is located, or the IP address in the form nnn.nnn.nnn.nnn.
API port	Required. Type the 1–5 digit port number that Sterling Connect:Direct File Agent uses to connect to the Sterling Connect:Direct server API. If you do not specify a port number, 1363 is used.

Parameter	Description
Gate Keeper port	**Required**. Type the 1–5 digit port number that Sterling Connect:Direct File Agent uses to connect to the gate keeper. Use any available port number higher than port 10000. If you do not specify a port number, the default port number, 65530, is used. The first Sterling Connect:Direct File Agent to connect to the gate keeper port keeps track of watched directories to ensure that only one Sterling Connect:Direct File Agent is monitoring a location.
Watched directories	Required. Type a path (Microsoft Windows), pathname (UNIX) to specify a Microsoft Windows or UNIX directory. Type one valid entry on each line. Blank lines are ignored to enhance readability. For S3 objects store, type a bucket name and folder name in a valid URI format. (Scheme://bucketname[/folder/]) For z/OS systems, specify any of the following types of entries: • A fully specified HFS pathname of a file • A fully specified HFS pathname of a directory • A fully specified MVS data set name, such as HLQ.MONTHLY.PAYROLL • A partial MVS data set name, such as HLQ.MONTH%%.PAY** **Note:** When matching patterns in data set names, the % matches a single character, the single asterisk (*) matches a single node level, and the double asterisk (**) matches all node levels from the point of placement. Refer to the IBM document DFSMS: Managing Catalogs (SC26-7409-03) for information about using the catalog search interface with wildcards and generic filter keys. For z/OS systems, you can also specify a partitioned data set (PDS) or a partitioned data set extended (PDSE) in the watched directories field. Sterling Connect:Direct File Agent uses the date to determine when a PDS member or data set was modified. With a PDS member, the last modification date is used. For an executable file, Sterling Connect:Direct File Agent looks at members of a load module PDS to determine their binder link date. If no date is found, Sterling Connect:Direct File Agent uses the creation date of the PDS where it resides. When a VSAM file is created on a z/OS system, three files are generated: the actual data file, an index file, and a cluster file. To prevent Sterling Connect:Direct File Agent from triggering a process for each of these files, be sure your naming rules specify on the data file.
Monitor sub directories	Select Yes (the default) to monitor the Watched directories or select No to monitor the Watched directories only.

Parameter	Description
Continuous signon	Select Yes to stay connected to the API port when Sterling Connect:Direct File Agent is active, or No (the default) to have Sterling Connect:Direct File Agent disconnect and reconnect each time Processes are submitted after a directory scan. Sterling Connect:Direct File Agent scans the directories, then submits Processes for any files found during the scan. If Continuous signon is set to No, Sterling Connect:Direct File Agent will sign on to the Sterling Connect:Direct server the first time it submits a Process for a file found during the scan, and will close the connection to the Sterling Connect:Direct server when all Processes have been submitted for files found during the scan. When files are found during a subsequent scan, Sterling Connect:Direct File Agent opens a new connection to the Sterling Connect:Direct Server. Use this option if more than a few minutes elapses between files placed in the watched directories. If Continuous signon is Yes, Sterling Connect:Direct File Agent opens a new connection to the Sterling Connect:Direct Server the first time that a Process is submitted for a file found during the scan, and will leave that connection to the Sterling Connect:Direct server open until Sterling Connect:Direct File Agent is stopped. Use this option if files are placed in the watched directories more or less continuously.
Gate keeper DNS name	Type the name of the host for the Sterling Connect:Direct File Agent gate keeper, or the IP address in the format nnn.nnn.nnn.nnn. The gate keeper keeps track of watched directories so that the same directory is not watched by more than one instance of Sterling Connect:Direct File Agent. When multiple instances are running, the first instance to connect to the gate keeper port becomes the gate keeper. A gate keeper is not required if only one instance is running or if each watched directory is only listed in the configuration of one instance. To disable the gate keeper, set this parameter to blank: the gate keeper port is ignored. If multiple instances of Sterling Connect:Direct File Agent monitor the same network directory, a gate keeper DNS name must be provided.
Default Process	Type the name of the Process to submit when a file is detected by Sterling Connect:Direct File Agent. This default Process is submitted if there is not a rule defined for the file. On z/OS systems, this is specified as the Member Name in DMPUBLIB. On Microsoft Windows or UNIX, this is the pathname of the file that contains the Process. Sterling Connect:Direct File Agent must have read access to the path and file on Microsoft Windows or UNIX.
Default arguments	Type the argument string that will be passed to the default Process. Sterling Connect:Direct File Agent uses the variables described in z/OS Process Arguments Example. The leading % character and the ending "." are required.
Error Process	Type the name of the Process to submit when an internal code error occurs in Sterling Connect:Direct File Agent, such as a java.lang.null pointer exception. On z/OS systems, this is specified as the Member Name in DMPUBLIB. On Microsoft Windows or UNIX, this is the pathname of the file that contains the Process. Sterling Connect:Direct File Agent must have read access to the path and file on Microsoft Windows or UNIX.

Parameter	Description	
Error Arguments	Type the argument string that will be passed to the error Process. Sterling Connect:Direct File Agent uses only the following variable. Using any other variable produces undefined results.The leading % character and the ending "." are required.	
	%FA_FILE_FOUND.	The default value is the full text of the Exception message.
Process Class	Required. Type the numeric class that the Process submitted to the Sterling Connect:Direct server should use for execution. This can be a value between 1-255 and is used to determine the order in which a Process is executed. Refer to Sterling Connect:Direct documentation for more information.	
Process Priority	Type the numeric priority that the Process submitted to the Sterling Connect:Direct server should use for execution. This can be a value between 0-15 and is used to determine the order in which a Process is executed. Refer to Sterling Connect:Direct documentation for more information.	
Watch file interval	Type the number of minutes for Sterling Connect:Direct File Agent to wait before checking the watch directories for files. By default, the watch directories are checked for files once each minute. This field specifies how long Sterling Connect:Direct File Agent waits between directory scans. If you need to transfer files quickly after they are placed into the watched directories, specify a short Watch file interval. However, if there aren't many files placed into the watched directories, set a longer Watch file interval so that Sterling Connect:Direct File Agent is not scanning the watched directories as often. There is a trade-off between the processing time that Sterling Connect:Direct File Agent uses to scan the directories and the need to transfer the files quickly.	
File completion delay	Type the number of minutes that you want Sterling Connect:Direct File Agent to wait before a detected file is considered to be complete.This field is optional. The default time is 1 minute. This field only applies to UNIX systems. With many UNIX applications, different tasks can access the same file simultaneously. This may cause problems if Sterling Connect:Direct File Agent detects that a file is present in the watched directory and uses it before another application has closed it. Set this delay to allow an application to finish with the file before Sterling Connect:Direct File Agent accesses the file.	
File Agent unique name	**Required**. Provide a unique name for each Sterling Connect:Direct File Agent instance running on the same host or on a different host, while monitoring similar network drives, and configured to submit processes to the same Sterling Connect:Direct node. This ensures the unique identity of each Sterling Connect:Direct File Agent instance by Sterling Control Center. Failing to do so results in Sterling Control Center treating multiple instances as one instance.	
SNMP listener address	Type the address for the SNMP trap receiver, such as Sterling Connect:Direct. Sterling Connect:Direct File Agent uses this address to send SNMP traps for statistics. This field is optional. Obtain this information from your Sterling Control Centersystem administrator.	
SNMP listener port	Type the port used by the SNMP trap receiver, such as Sterling Control Center. Port 1163 is the default. This field is optional.	

Parameter	Description
SNMP source port range	Ports or port ranges used to pass through a firewall to the SNMP trap receiver, such as Sterling Control Center, when Sterling Connect:Direct File Agent runs behind a firewall. Specify a maximum of 5 port ranges. This field is optional. Type the ranges in the format nnnn-nnnn, separated by commas, for example, 5555-7777, 8888-8890, 9999. Contact the Sterling Control Center system administrator if you do not know this information.
Refresh Configuration	Select Yes to refresh the configuration after modifying it and without restarting Sterling Connect:Direct File Agent. The default is No. **Note:** The gate keeper port setting will not be refreshed unless you restart.

7. Click **Save**.
8. Repeat this procedure for the FA2 and FA3 sites, changing information and renaming the configuration file for each site. You should now the following configuration files in the Sterling Connect:Direct File Agent directory:
   - Default_Config.ser
   - FA1.ser
   - FA2.ser
   - FA3.ser

Creating Multiple Configurations

The **cdfa -g** command creates multiple configuration files for implementations with a large number of Sterling Connect:Direct File Agent sites. This command uses a configuration template and a text-based build file to create the configuration files, which can then be sent through e-mail to client sites. This reduces the amount of configuration that the Sterling Connect:Direct File Agent site must perform.

In the following procedure, assume that you want to create three new configuration files for distribution named FA1, FA2, and FA3.

1. Use the configuration interface to create a configuration named Template. (Name it whatever you want.)
2. Modify the Template configuration settings as necessary for your site. However, type variables into the following fields:

Tab	Field	Variable
File Agent	Password for API	&passwd.
	API host DNS name	&netmap.

   Variables are user-defined. See Configuration Template Variable Rules for more information about variables.
3. Save the Template configuration file.
4. Use a text editor to create a configuration build file named build.cfg. (Give the file any name you want.)
5. Insert the following text into the build.cfg file. Bold text indicates the values to change for each client.

```
#FA1's unique configuration
copy Template
&passwd=PROCEED1
&netmap=CDFA1
save FA1
#FA2's unique configuration
copy Template
&passwd=FORWARD23
&netmap=CDFA2
save FA2
#FA3's unique configuration
copy Template
&passwd=MUSTER43
&netmap=CDFA3
save FA3
```

See Configuration Build File Variable Rules for build file syntax.

6. Save the build.cfg file in any directory. In this example, it is saved in the c:\ directory.
7. Change your directory to the Sterling Connect:Direct for UNIX installation directory.
8. Type **cdfa -g c:\build.cfg** at a command prompt. Be sure to specify the complete path to the build.cfg file. This command is case-sensitive.

   Using this example, Sterling Connect:Direct File Agent builds three new configuration files based on the values in the template and the build.cfg file. You should now have five configuration files in the File Agent directory:

   - Default_Config.ser
   - FA1.ser
   - FA2.ser
   - FA3.ser
   - Template.ser
9. E-mail the FA1.ser, FA2.ser, and FA3.ser configuration files to the appropriate Sterling Connect:Direct File Agent client site, with the following instructions:
   - Copy the configuration file into the File Agent directory.
   - Rename the configuration file to Default_Config.ser.

Configuration Template Variable Rules

When you create multiple configuration files from the command line, observe the rules for using variables in the configuration template file.

- All variable statements in the configuration template consist of an ampersand (&), a user-defined variable name, and a period. For example:
  - &userid.
  - &netmap.
- The variable name is case-sensitive. For example, &userid and &USERID are considered two different variables.
- Variables can be used for any text field. You cannot use a variable for a numeric field.
- Be careful when specifying a variable as part of a file name. For example, assuming that the &userid. value is user1, c:\&userid.txt results in c:\user1txt, with no period separating user1 and txt. In this case, the variable definition should have two periods. For example, c:\&userid..txt, which results in c:\user1.txt.

Configuration Build File Variable Rules

When you create build file variable rules, observe the rules for using variables in the configuration template file.

- All variables in the configuration build file consist of an ampersand (&), a variable name, an equals sign (=), and a substitution value. The trailing period is not included in the configuration build file. For example:
  - &userid=client1
  - &netmap=WIN.CLIENT2
- The variable name is case-sensitive. For example, &userid and &USERID are considered two different variables.
- Sterling Connect:Direct File Agent removes all leading and trailing spaces from the substitution value.
- The build file can also have comments, which must be on a separate line and begin with a number sign (#), for example #FA1's unique configuration.

Locking a Configuration File for Distribution

You can lock a configuration file to prevent changes to it. This ensures that any configurations that you distribute remain static.

To lock a configuration file, add the following command to the build.cfg file you created in Creating Multiple Configurations.

```
lock configurationfilename
```

This command saves the configuration file specified in configurationfilename and locks it against any additional changes.

In the following example, a configuration file named Eastern43 is created and locked:

```
#Eastern43 configuration
copy Template
&passwd=Prescott5
&netmap=CDEast1
lock Eastern43
```

When a configuration file is locked, no one, not even the configuration creator, can unlock or change it. However, you can replace a locked configuration file with a new file that has the same file name, if necessary.

Locked configuration files appear in the configuration list on the configuration interface. However, you cannot select them. To start Sterling Connect:Direct File Agent with a locked configuration file, do one of the following:

- Start Sterling Connect:Direct File Agent with the **cdfa -c**configurationfilename command, where configurationfilename is the name of the locked configuration. For example, **cdfa -cregion5.ser**. On a z/OS system, you must edit the script for the Execution job and type this information on the $FAJAVA line. On a Microsoft Windows or UNIX system, you can edit the .lax file to always start Sterling Connect:Direct File Agent with this parameter. Refer to Running Sterling Connect:Direct File Agent from the UNIX Command Line with a Specific Configuration File for information about editing this file.
- If you do not use the **cdfa** command to start Sterling Connect:Direct File Agent, assign the locked configuration file a name that matches the name of the computer where Sterling Connect:Direct File Agent is running. For example, if Sterling Connect:Direct File Agent runs on a computer named Host1, name the locked configuration file **Host1.ser**.
- Saved the locked file as **Default_Config.ser** (the default configuration file).

Copying a Rule

You can copy an existing rule to create a new rule. Complete the following steps to copy a rule.

1. Select the configuration file that you want to work with from the Configurations window.
2. Click the Rules tab.
3. Click the tab that contains the rule that you want to copy.
4. Select the rule that you want to copy, then click Copy.
5. Type the name of the new rule that you are creating, then click OK.
6. Edit the rule to modify match criteria, Process information, or both.
7. Click **Done**.

Deleting a Rule

You can delete a rule that is no longer needed. Complete the following steps to delete a rule.

1. Select the configuration file that you want to edit from the Configurations window.
2. Click the Rules tab.
3. Click the tab that contains the rule that you want to delete.
4. Select the rule that you want to delete, then click Delete.
5. Click **Yes** in the Delete rule confirmation dialog box.

Enabling and Disabling a Rule

When you create a rule, it is disabled. You must enable a rule to activate it.

1. Select the configuration file to edit from the Configurations window.
2. Click the Rules tab.
3. Click the tab that contains the rule that you want to enable or disable.
4. Click Enabled to activate or deactivate the rule.

Editing a Rule

After you define a rule, you can edit match criteria and Process information. Copy match criteria to create new criteria, delete or edit match criteria, and enable or disable match criteria. You can modify or delete Process information. When a rule contains no Process information and a file with the rule criteria matches, nothing happens.

1. Select the configuration file to edit from the Configurations window.
2. Click the Rules tab.
3. Click the tab for the type of rule to edit. Click the **System event rules** tab to edit a rule based on system events or click the **Submit Process rules** tab to edit a rule based on a detected file.
4. Select the name of the rule to modify.
5. To modify match criteria:
   - Select an item from the match criteria list and click the button for the operation that you want to perform. You can create a new match criteria or edit or copy the selected match criteria.
   - From the Match criteria window, select the property to change, define the criteria and operators as necessary, enable the criteria, and click **OK** to return to the match criteria list. The additional criteria or changed criteria is displayed in the Match criteria list.
6. To modify Process information, scroll to the field to edit and define Process information.
7. Click Done to return to the **Rules** tab.

Variables in Rules

Specify variables to substitute text in any field of a rule. Sterling Connect:Direct File Agent uses the following variables. The leading percent (%) and the ending period (.) are required. For system event rules, the only valid variable is %FA_FILE_FOUND.

Usage	Variable	Description
All Operating Systems		
Path and file	%FA_0. to %FA_99.	The number included in this variable represents a component of the name of the detected file, as delimited by the file delimiter, in sequence. For example, if the full file name is /usr/watch/test file.active.txt, then %FA_0 is usr, %FA_1 is watch, and so on.
	%FA_FILE_FOUND.	On Microsoft Windows and UNIX, the default value is the path and file name of the detected file. On z/OS systems, the default value is the entire name of the file that Sterling Connect:Direct File Agent detected, including any member name. This variable supports PDSE long member names. For example, when you specify this variable, Sterling Connect:Direct File Agent could pass the following member name: CUST.BENEFITS(PAYROLLPDSELONGNAME). On S3 object stores, the default value is the entire name of the object that Sterling Connect;Direct File Agent detected including the bucket name and scheme name. If a scheme name substitution occurred, this is the name after substitution. For the initial name see %FA_WATCHED_FILE_FOUND variable. For more details, refer Chapter 10, “Amazon S3 support,” on page 75.
	%FA_FSTYPE	The file or object file system type. Windows, Unix, OS390, AWSS3
Current date and time	%FA_DATE.	The current date for the detected file. This value has 8 characters that represent the year, month, and day, for example, 20040903.
	%FA_DATE_DAY.	The current day, for example, 31.
	%FA_DATE_MONTH.	The current month, for example, 01.
	%FA_DATE_YEAR.	The current year, for example, 2004.
	%FA_NUM.	The millisecond timestamp. If multiple files are sent within the same second, they will get different millisecond values, for example, 13143512345, 13143512346, and 13143512347.
	%FA_TIME.	The current time. This value has 6 characters to represent the hour, minutes and seconds (format (hhmmss) using a 24-hour clock.
	%FA_TIME_HOUR.	The current hour, for example, 13.
	%FA_TIME_MINUTES.	The current minute, for example, 24.
	%FA_TIME_SECONDS.	The current second, for example, 35.

Usage	Variable	Description
Modification date and time	%FA_FDATE.	Date a detected file was modified. 8-characters representing year, month, and day, for example, 20040903.
	%FA_DATE_DAY.	The day a file was last modified, for example, 21.
	%FA_FDATE_MONTH.	The month in which a file was last modified, for example, 09.
	%FA_FDATE_YEAR.	Year in which a file was last modified, for example, 2004.
	%FA_FTIME_HOUR.	The hour a file was last modified, for example, 22.
	%FA_FTIME_MINUTES.	The minute a file was last modified, for example, 24 will be passed for a file last modified at 6:24.
	%FA_FTIME_SECONDS.	The second a file was last modified, for example, 35.
	%FA_FDATE_TIME.	The time a file was last modified. This value has 6-characters representing hour, minutes, and seconds (hhmmss) using a 24-hour clock, for example, 153842.
UNIX and Microsoft Windows only		
File name and path	%FA_EXT_FOUND.	On Microsoft Windows and UNIX, the file extension of the file that was added, for example, .txt.
	%FA_EXT_FOUND_NP.	On Microsoft Windows and UNIX, the file extension of the file that was added, but without the period before the file extension. For example, if the file added is file.txt, using the %FA_EXT_FOUND_NP variable will result in txt being passed (the extension with no period included).
	%FA_NAME_FOUND.	On Microsoft Windows and UNIX, the name of the file that was added, for example, myfile.
	%FA_NOT_PATH.	On Microsoft Windows and UNIX, the file name with the file extension, without any path. For example, if the full file name is /usr/watch/test file.active.txt, then %FA_NOT_PATH. is test file.active.txt.
	%FA_PATH_FOUND.	On Microsoft Windows and UNIX, the path of the file that was added, for example, on Microsoft Windows, C:\watch\, and on UNIX, /home/user/watch.
Microsoft Windows only		
	%FA_DRIVE_FOUND.	On Microsoft Windows, the default value is the drive of the file that was added, for example, C:.
z/OS systems only		
File and member	%FA_BASEFILE_FOUND.	The default value is the name of the file that was added, without the member name. This variable is only valid for PDS on z/OS operating systems, for example, CUST.BENEFITS
	%FA_MEMBER_FOUND.	The default value is "." This variable is only valid for PDS on z/OS operating systems. PDSE long member names are supported, for example, PAYROLLPDSELONGNAME.
S3 Object stores only		

Usage	Variable	Description
	%FA_SCHEME	This is the object scheme when Connect:Direct File Agent discovered the object.
	%FA_OUTSCHEME	This is the object scheme if a scheme substitution occurred. Without substitution the value is same as %FA_SCHEME.
	%FA_WATCHED_FILE_FOUND	When a scheme substitution occurred value is the object name before substitution occurred, the object name Connect:Direct File Agent detected. For more details, refer Chapter 10, “Amazon S3 support,” on page 75.

Microsoft Windows/UNIX Example

If you configure Process arguments as:

```
&FAF=%FA_FILE_FOUND.
```

When the watched directory is /home/watch1/ and the file payroll appears in the watched directory, the following argument string is submitted to the Process. &FAF=/home/watch1/payroll

z/OS Examples

If you configure Process arguments as:

```
&FA=%FA_BASEFILE_FOUND. &LM=%FA_MEMBER_FOUND. &BC=”%FA_FILE_FOUND.”
```

The following argument strings are submitted to the Process for each scenario:

- The watched directory PDS is CUST.PROCLIB and member PAYROLL changed.

```
arg string= &FA=CUST.PROCLIB &LM=PAYROLL &BC="CUST.PROCLIB(PAYROLL)"
```

- The watched directory file is CUST.*, and member BENEFITS of PDS CUST.PARMFILE changed.

```
arg string= &FA=CUST.PARMFILE &LM=BENEFITS
```

- The watched directory is CUST.GDGBASE.* and CUST.GDGBASE.G0223V00 is created.

```
arg string= &FA=CUST.GDGBASE.G0223V00 &LM=.
```

Saving a Configuration in a Text File

You can create a text file that contains all of the configuration details and rules for a configuration. The password for the API connection is written as asterisks.

1. Select the configuration file to save as a text file from the **Configurations** window.

   If you imported the configuration .ser file, click **Edit**, make any changes to the configuration, and click **Save**.
2. Click **Save to a text file** from the **File agent** tab.

   The text file is written to the installation directory as configuration_name.txt. When you update the file and click **Save**, you update both the configuration .ser file and the configuration text file.

   Verify that the text file displays information similar to the following sample. Some lines may differ because of operating system differences and different parameter definitions.

```
************************************************************
    Configuration Details for Default_Config
************************************************************
Comments:
Userid for API: user01
Password for API: ****
API host DNS name: prodhost
API port: 1363
Gate Keeper port: 65530
Watched directories: C:\Output\Binary
Monitor sub directories: true
Continuous sign-on: false
Gate Keeper DNS name:
Default Process:
Default arguments:
Error Process:
Error arguments:
Process class: 1
Process priority: 1
Watch file interval: 1
File completion delay: 0
File Agent unique name: FileAgent
SNMP listener address: controlcenter.prod.domain.com
SNMP listener port: 1163
SNMP source port range:
Refresh Configuration: false
************************************************************
 Submit process rules:
************************************************************
Rule Name: S-1
Enabled: true
Match Criteria (Enabled: Size of the newly arrived file Greater than  "1")
Alternate file name:
Process Name: C:\Process\FileAgent.cdp
Process Arguments: &F=%FA_FILE_FOUND. &dir=%FA_0.\%FA_1. &D=%FA_DRIVE_FOUND.
   &P=%FA_PATH_FOUND. &N=%FA_NAME_FOUND. &E=%FA_EXT_FOUND. &G=%FA_FDATE.
   &R=%FA_FTIME. &A=%FA_FDATE_MONTH.
   &AS=%FA_DATE_MONTH. &DE=%FA_DATE_YEAR. &TT=%FA_NOT_PATH. &PP=%FA_TIME_HOUR.
   &OP=%FA_TIME_MINUTES.
   &IO=%FA_TIME_SECONDS. &FN=%FA_NUM.
Process Class: 1
Process Priority: 1
Notification userid:
Rule Name: S-2
Enabled: false
Match Criteria (Enabled: Size of the newly arrived file Greater than  "1")
Alternate file name:
Process Name: C:\Process\FileAgent.cdp
Process Arguments: &F=%FA_FILE_FOUND. &N=%FA_NAME_FOUND. &E=%FA_EXT_FOUND.
Process Class: 1
Process Priority: 1
Notification userid:
************************************************************
 System event rules:
************************************************************
Rule Name: System
Enabled: true
Match Criteria (Enabled: System event contents Contains  "java"
     Not enabled: System event title Matches  ""
     Not enabled: System event title Matches  "")
Alternate file name:
Process Name:
Process Arguments:
Process Class: 1
Process Priority: 1
Notification userid:
```

Chapter 4. Operating Sterling Connect:Direct File Agent

Running Sterling Connect:Direct File Agent as a Microsoft Windows Service

When you run Sterling Connect:Direct File Agent as a Microsoft Windows service, the application runs automatically when Microsoft Windows starts.

You must use the command line instead of running Sterling Connect:Direct File Agent as a Microsoft Windows service if you need to verify operation, run in verbose logging mode, or use an alternate configuration file.

To configure Sterling Connect:Direct File Agent to start automatically when you restart a Microsoft Windows computer:

1. Configure Sterling Connect:Direct File Agent.
2. Select **Start>Control Panel>Administrative Tools>Services**.
3. Right-click **Connect Direct File Agent** in the list of services and select **Properties**.
4. On the **General** tab, Select **Automatic** as the **Startup Type**.
5. Click **OK**.

   The service will not start without a valid configuration. If you try to start the service without a valid configuration and the service is set up to **Allow service to interact with desktop**, Sterling Connect:Direct File Agent will launch the configurator and the service appears to start in the Microsoft Windows Services dialog box.

Starting Sterling Connect:Direct File Agent Automatically on a UNIX Computer

To configure Sterling Connect:Direct File Agent to start automatically whenever you restart your UNIX computer, modify the computer's initialization sequence to call the cdfa.sh script.

Starting Sterling Connect:Direct File Agent from a Microsoft Windows Shortcut

You can start Sterling Connect:Direct File Agent from a Microsoft Windows shortcut. This can be helpful if you want to run Sterling Connect:Direct File Agent with a different configuration file. To start Sterling Connect:Direct File Agent from a shortcut, complete the following procedure to place command line parameters in the shortcut.

To place the parameters in a shortcut:

1. Create a Microsoft Windows shortcut to the cdfa file (usually located in C:\Program Files\FileAgent).
2. Right-click on the shortcut and select **Properties.**
3. Add the desired parameter after the cdfa command, outside of the quotation marks. For example, to add a parameter starting Sterling Connect:Direct File Agent with the configuration file monthend.ser, the command string is:

   ```
   "C:\Program Files\FileAgent\cdfa" -cmonthend.ser
   ```

4. To display the parameters on the title bar of the command window, use **cdfa1.bat**.
5. Click **OK**.

Running Sterling Connect:Direct File Agent from the UNIX Command Line with a Specific Configuration File

When you run Sterling Connect:Direct File Agent in a Microsoft Windows or UNIX environment, you can run the program from a command line and use command line parameters. Refer to “Specifying Command Line Parameters” on page 67for a list of parameters.

Microsoft Windows Command

To run Sterling Connect:Direct File Agent and always specify a parameter, edit the .lax file. A .lax file is an installation file that sets runtime properties for an application. For example, to run Sterling Connect:Direct File Agent and always use a specific configuration file edit the .lax file and add the parameter -cabc.ser. The .lax files are described in the following table:

File	Description
cdfa$.lax	Runs Sterling Connect:Direct File Agentas a Microsoft Windows service.
cdfac.lax	Runs Sterling Connect:Direct File Agent as a GUI configurator.
cdfa.lax	Runs Sterling Connect:Direct File Agent from a command window.

When you edit the appropriate .lax file, scroll to the command line arguments field and enter the parameters, as shown in the following example:

```
# LAX.COMMAND.LINE.ARGS

#   ---------------------
#  what will be passed to the main method -- be sure to quote
#  arguments with spaces in them lax.command.line.args=\-cabc.ser\
```

Using UNIX Commands to Start

To run in a UNIX environment, use the following command line prompts:

Command	Description
cdfa -C	Runs Sterling Connect:Direct File Agent as a GUI configurator.
cdfa	Runs Sterling Connect:Direct File Agent from a command window.

Shutting Down Sterling Connect:Direct File Agent as a Microsoft Windows Service

To shut down Sterling Connect:Direct File Agent running as a Microsoft Windows Service:

1. From the **Start** menu, select **Settings**>**Control Panel>Administrative Tools>Services.**
2. Find Sterling Connect:Direct File Agent and stop the Service.

Shutting Down Connect:Direct File Agent in a Windows or UNIX Environment

To safely shut down Connect:Direct File Agent in a Windows or UNIX environment, you can create an empty file named “shut” in the File Agent installation directory. File Agent will detect the empty file and delete it before shutting down. The following commands create a shut file in a File Agent installation directory:

```
cd <installation directory>
echo "" > shut
```

To shut down Connect:Direct File Agent running as a Windows Service:

1. Open the Services management console in Windows.
2. Stop the "IBM Sterling Connect Direct File Agent" service.

Sterling Connect:Direct File Agent in a z/OS Environment

When you run Sterling Connect:Direct File Agent in a z/OS environment, you run jobs to start the configuration interface, and to start or shutdown Sterling Connect:Direct File Agent. This section describes Sterling Connect:Direct File Agent information that applies to the z/OS environment only.

Using Installation Variables

If you are running Sterling Connect:Direct File Agent on a z/OS computer, you create and name a Sterling Connect:Direct File Agent JCL data set during the installation process. All installation variables are saved in this JCL. Refer to Installing Sterling Connect:Direct File Agent for z/OS, in the Sterling Connect:Direct File Agent for z/OS Installation Guide for more information.

Using Command Line Parameters

On a z/OS system, you start Sterling Connect:Direct File Agent with the Execution job. Therefore, if you want to use command line parameters, such as -v or -g, you must edit the script for the Execution job and include these parameters in the script. The following screen shows a sample execution job script.

```
//PS010   EXEC PGM=IKJEFT01
//STDIN     DD PATH='&A&B&C&D./FAEXEC.in',
//             PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//             PATHMODE=(SIRWXU,SIRGRP,SIROTH)
//STDOUT    DD PATH='&A&B&C&D./FAEXEC.out',
//             PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//             PATHMODE=(SIRWXU,SIRGRP,SIROTH)
//STDERR    DD PATH='&A&B&C&D./FAEXEC.err',
//             PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//             PATHMODE=(SIRWXU,SIRGRP,SIROTH)
//SYSTSPRT   DD SYSOUT=*
//SYSPRINT   DD SYSOUT=*
//CMD1       DD *
 export DISPLAY=amo-dev2:0.0
 export RUN_DIR=/u/kstic1/bubba/yum
 export RUN_DIR=$RUN_DIR''
 export RUN_DIR=$RUN_DIR''
 export RUN_DIR=$RUN_DIR''
 export JV1='/ZOS12/usr/lpp/java130/IBM/J1.3/bin/java'
 export JV2=''
 export JV3=''
 export JV4=''
 export FAJAVA=$JV1$JV2$JV3$JV4
 export PATH=$PATH:$RUN_DIR
 export LIBPATH=$LIBPATH:$RUN_DIR
 echo "Lib path is.." $LIBPATH
 echo "path is.." $PATH
 echo "Execution directory is..." $RUN_DIR
 echo "JAVA executable is" $FAJAVA
 echo "DISPLAY variable is" $DISPLAY
 cd $RUN_DIR
 sizeCheck
 abc=$?
 if [  $abc -lt 180 ]; then
   echo " insufficent region size:" $abc
   exit 9
 fi
 $FAJAVA -Dsci.config=FAConfiguration -jar fasat.jar -cabc.ser
```

You can edit the line that begins with $FAJAVA (shown in bold) to add the command line parameters.

Using Data Sets

On z/OS systems, you can configure Sterling Connect:Direct File Agent to watch data sets that can include different file types and have differences in data set organization. Be sure to consider the relevant file characteristics of the generation data group (GDG), partitioned data set (PDS), or partitioned data set extended (PDSE) when one is a Sterling Connect:Direct File Agent watched directory.

Sterling Connect:Direct File Agent with SMS-Managed GDGs

When you run Sterling Connect:Direct File Agent on z/OS, it scans catalogs and captures details that describe files, such as data set organization, catalog type, and volume. Sterling Connect:Direct File Agent uses this metadata to detect file changes and distinguish between files as required for operation. For example, Sterling Connect:Direct File Agent uses metadata from the data set to distinguish between sequential (DSORG=PS) and partitioned (DSORG=PO) data sets.

If Sterling Connect:Direct File Agent is watching for changes in a GDG (Generation Data Group) that is SMS-managed, roll in can be deferred. If roll in is deferred, the timing of changes to file details that Sterling Connect:Direct File Agent uses for operation can cause unexpected performance. For example, Sterling Connect:Direct File Agent can detect a previously detected file as newly added, or detect a file type in error. A file that Sterling Connect:Direct File Agent originally detects as non-VSAM, after a second cataloging, can be detected as GDG. To prevent unpredictable operation when you use Sterling Connect:Direct File Agent to watch GDGs that can have SMS-deferred roll in, you can force Sterling Connect:Direct File Agent to operate without evaluating the file metadata that can change.

Sterling Connect:Direct File Agent for SMS-Deferred Roll In Configuration

Configuring Sterling Connect:Direct File Agent to watch the trigger file for the GDG instead of the actual file can prevent operational issues caused by SMS-deferred roll in for GDGs. Alternatively, you can configure Sterling Connect:Direct File Agent to use command line options for ignoring certain details for files. To use the command line options that change how Sterling Connect:Direct File Agent captures details when watching a GDG, you must edit the script for the Sterling Connect:Direct File Agent execution job to modify Sterling Connect:Direct File Agent Java™ parameters ($FAJAVA line) and specify the command line options to use.

The following command line options enable Sterling Connect:Direct File Agent to log events and ignore certain file metadata:

–verbosevents
Enables event logging to STDOUT. With event logging on, you can view event details in a log file.

--ignoreos390catalogtype

Replaces the catalog type (for example, A, H, or G) of the detected file with dashes (-).

--ignoreos390volumes

Replaces the volume serial list for the detected file with dashes.

--ignoreos390filetype

Replaces the PDS or DSN characters of the detected file with dashes.

Modifying the Script for the Sterling Connect:Direct File Agent Execution Job

To use the command line options, modify the Sterling Connect:Direct File Agent job execution script.

The following example shows the lines that enable the command line options and modify the Sterling Connect:Direct File Agent Java parameters in bold:

```
...
 export JV1='/ZOS12/usr/lpp/java130/IBM/J1.3/bin/java'
 export JV2=''
 export JV3=''
 export JV4=''
 export FAJAVA=$JV1$JV2$JV3$JV4
 export PATH=$PATH:$RUN_DIR
 export LIBPATH=$LIBPATH:$RUN_DIR
 echo "Lib path is.." $LIBPATH
 echo "path is.." $PATH
 echo "Execution directory is..." $RUN_DIR
 echo "JAVA executable is" $FAJAVA
 echo "DISPLAY variable is" $DISPLAY
 export f1='--ignoreos390catalogtype'
 export f2='--ignoreos390volumes'
 export f3='--ignoreos390filetype'
 export f4='--verboseevents'
  cd $RUN_DIR
  sizeCheck
  abc=$?
    if [  $abc -lt 180 ]; then
    echo " insufficent region size:" $abc
    exit 9
 fi
$FAJAVA -Dsci.config=FAConfiguration -jar fasat.jar -cabc.ser $f1 $f2 $f3 $f4
```

Enabling the command line options as shown above changes how Sterling Connect:Direct File Agent captures the file metadata. In following sample metadata, pds is the data set organization, A is the catalog type, and USER15 is the volume:

(LOs390/pds;A;USER15;)

The following information illustrates how Sterling Connect:Direct File Agent detects the metadata shown above after command line options are implemented:

Header	Header
--ignoreos390catalogtype	(LOs390/pds;-;USER15;)
--ignoreos390volumes	(LOs390/pds;A;------;)
--ignoreos390filetype	(LOs390/---;A;USER15;)

Shutting Down Sterling Connect:Direct File Agent on z/OS

To shut down Sterling Connect:Direct File Agent in the z/OS environment, you run the Shutdown job. If you cancel the Execution job, two data sets are created in the installation directory called ceedu and hpitrace. Delete these periodically to save space.

Ending a Sterling Connect:Direct File Agent Configuration Session

To end a session using the configuration interface:

1. Click **Exit** to close the configuration interface.
2. Click **Yes** on the **Exit confirmation prompt**.

Sterling Connect:Direct File Agent Log Files

Sterling Connect:Direct File Agent logs system information to the console and three separate log files. The following logs are available:

Console Log

Contains information at the INFO levels which includes error messages generated by Sterling Connect:Direct File Agent and basic information about the files found and what action was taken on the file. The console log is enabled by default.

CDFA.log

Contains information at the INFO level which includes error messages generated by Sterling Connect:Direct File Agent and basic information about the files found and what action was taken on the file. This log file is enabled by default.

CDFA_verbose.log

Contains information at the DEBUG level which includes all system activity. This file is not enabled by default and is only written when Sterling Connect:Direct File Agent is running in verbose mode.

CDFA_stats.log

Contains only one line per file with process submission (successful or not) information. This log file is enabled by default. Information in this file is only available at the INFO level. Do not modify the setting for this log file.

You can change the level of information generated for each log (except the CDFA_stats.log) by modifying the log4j.properties file in the installation directory. The following log levels are available:

WARN

Writes error messages generated by Sterling Connect:Direct File Agent.

INFO

Writes error messages and basic information that you may want to reference on a daily basis regarding files and actions. Information is written to CDFA.log and CDFA_verbose.log.

DEBUG

Writes all information related to Sterling Connect:Direct File Agent activity. Information is written to CDFA_verbose.log.

Changing Console Logging Level to WARN

To change the level setting for a log to WARN so that only error messages are displayed:

1. Open the log4j.properties file, located in the installation directory.
2. Change the appropriate setting to WARN, as follows:

   For the console log

   log4j.appender.C.threshold=WARN

   For CDFA.log

   log4j.appender.R.threshold=WARN

   For CDFA_verbose.log

   log4j.appender.V.threshold=WARN

Changing Console Logging Level to DEBUG

To change the level setting for a log to DEBUG so that only error messages are displayed:

1. Open the log4j.properties file, located in the installation directory.
2. Change the appropriate setting to DEBUG, as follows:

   For the console log

   log4j.appender.C.threshold=DEBUG

   For CDFA.log

   log4j.appender.R.threshold=DEBUG

For CDFA_verbose.log

log4j.appender.V.threshold=DEBUG

Configuring to Run in Verbose Mode

1. Open the log4j.properties file, located in the installation directory.
2. Add V to the log4j.rootLogger= line as follows: log4j.rootLogger=DEBUG, R, C, V.

Chapter 5. Status and Monitoring

Sterling Connect:Direct File Agent Status Information

when you verify configurations or troubleshoot operation, you may need to review status information. On Microsoft Windows, Sterling Connect:Direct File Agent creates a snaps subdirectory in the installation directory and directs log files there.

No logs are created for Linux and UNIX, but you can use your Sterling Connect:Direct commands to monitor Process activity. On Sterling Connect:Direct for UNIX and Sterling Connect:Direct for z/OS systems, the DEBUG parameter of the SUBMIT command can monitor and trace execution of Processes submitted by Sterling Connect:Direct File Agent. No logging occurs when you run Sterling Connect:Direct File Agent as a service, unless an error occurs. Sterling Connect:Direct

File Agent provides several levels of status information:

- System log–A log of all system activity. A system log is only created if you run verbose, or if an error occurs. If you are not running verbose, the system log appears in the snaps subdirectory of the installation directory when an error occurs. The snaps subdirectory is created when the first event occurs.

  If you are using Sterling Connect:Direct File Agent rules in your configuration or if you have more than a few watched directories, the Sterling Connect:Direct File Agent system log may contain many lines of information. After you become familiar with the phrases that the log uses for status details, you can use the Find command of a line editor such as Microsoft Windows Notepad to locate those phrases and quickly check status.

  Sterling Connect:Direct File Agent system log files provide detailed information about Sterling Connect:Direct File Agent operation. Among the details provided are the following:

  – Sterling Connect:Direct File Agent version
  – Application status and the number of services
  – Date, time, and other details for each directory scan
  – Number of commands attempted and accepted for a directory scan
  – Rule and match criteria details from the configuration interface

- First Failing Status (FFS) log–One or more logs created when an error occurs.View the snaps subdirectory of the Sterling Connect:Direct File Agent installation directory to obtain FFS statuses. The snaps directory is created as needed, and contains the FFS logs for any errors encountered by Sterling Connect:Direct File Agent. The following screen shows the contents of the snaps subdirectory.

```
,, File, Directory, Special_file, Commands, Help,
,sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
,                  Directory List ,
,
,Select one or more files with / or action codes. If / is used also select an,,
,action from the action bar otherwise your default action will be used. Select,
,with S to use your default action. Cursor select can also be used for quick, ,
,navigation. See help for details., ,
,EUID=10040008 /u/fileagent/100/snaps/
, Type Filename Row 1 of 3
,_,Dir ,.
,_,Dir ,..
,_,File ,java.util.NoSuchElementException.txt
```

Sterling Connect:Direct File Agent Configuration Guidelines

To configure Sterling Connect:Direct File Agent to be monitored by Sterling Control Center or other SNMP monitoring software, configure the following parameters in the configurator:

- Sterling Connect:Direct File Agent unique name—Type a unique name, in order for Sterling Control Center to distinguish between multiple instances of Sterling Connect:Direct File Agent running from the same IP address. Configure this parameter only if you want to monitor Sterling Connect:Direct File Agent with Sterling Control Center.
- SNMP listener address—Type the address for the SNMP trap receiver (such as Sterling Control Center). Sterling Control Center uses this address to send SNMP traps for statistics. This field is optional.

  You can obtain this information from your Sterling Control Center system administrator.
- SNMP listener port—Type the port used by the SNMP trap receiver (such as Sterling Control Center). Port 1163 is the default. This field is optional.
- SNMP source port range—When Sterling Connect:Direct File Agent runs behind a firewall, type the ports or port ranges used to pass through a firewall to the SNMP trap receiver (such as Sterling Control Center). You can specify a maximum of 5 port ranges. This field is optional.

  Type the ranges in the format nnnn-nnnn, separated by commas. For example, 5555-7777, 8888-8890, 9999. You can obtain this information from your Sterling Control Center system administrator.

Sterling Control Center Monitoring Guidelines

Put your short description here; used for first paragraph and abstract.

To configure Sterling Control Center to monitor Sterling Connect:Direct File Agent, configure the following parameters:

- Server Address—Type the Sterling Connect:Direct File Agent server address.
- SNMP Listener Address—Type the address of the Sterling Control Center SNMP listener. This must match the SNMP listener address value configured in Sterling Connect:Direct File Agent.
- SNMP Listener Port—Type the port of the Sterling Control Center SNMP listener. This value must match the SNMP listener port value configured in Sterling Connect:Direct File Agent.

SNMP Trap Information

When the Sterling Connect:Direct File Agent SNMP parameters are properly configured, the following information is sent from Sterling Connect:Direct File Agent using the SNMP traps:

- Sterling Connect:Direct File Agent is active (heartbeat)—Sent at startup and every scan interval Sterling Connect:Direct File Agent has submitted a process
- For all submit attempts, SNMP trap includes Sterling Connect:Direct server name, filename, rule name (or default), and message ID from submit (success or failure)
- If the process submit is successful, SNMP trap includes process name and process number Sterling Connect:Direct File Agent configuration has changed

  The first 25 characters of the Sterling Connect:Direct File Agent unique name and the first 100 characters of the rule name are sent in the SNMP trap. Sterling Connect:Direct File Agent also sends time zone difference, connect type, and local node (Sterling Connect:Direct File Agent unique name) with every trap.

Error Reporting

Any errors that occur during the SNMP trap processing are sent to the Sterling Connect:Direct File Agent log files. Error messages are as follows:

- Could not register an SNMP listener
- SNMP Cannot get source port
- SNMP Cannot get source port in range
- SNMPBadValueException caught
- SNMP UnknownHostException caught

- SNMP IOException caught

Chapter 6. Troubleshooting

Troubleshooting

To troubleshoot Sterling Connect:Direct File Agent, check the following details to identify and resolve issues:

- Format Sterling Connect:Direct File Agent variables as described in z/OS Process Arguments Example
- Set appropriate permissions for watched directories
- Specify valid Sterling Connect:Direct server parameters in the Sterling Connect:Direct File Agent configuration
- Check for inactivity from files arriving in watched directories before Sterling Connect:Direct File Agent starts
- Check that required Sterling Connect:Direct File Agent rules are enabled
- Confirm that the most specific rule is in first position
- Confirm that all Sterling Connect:Direct File Agent rules specify a Process to perform actions
- Correct syntax errors in Processes

Refer to the problems and solutions that follow to identify and resolve other issues that occur when you use Sterling Connect:Direct File Agent.

Sterling Connect:Direct File Agent does not start and displays a Cannot run without a valid configuration message.

The configuration (.ser) file is missing. See A Default Configuration to create a configuration file.

Unable to determine the version of Sterling Connect:Direct File Agent running on Microsoft Windows.

Click the Start Menu. Click **Programs>Accessories>Command Prompt**. At the MS-DOS prompt, use the **cd** command to change to the Sterling Connect:Direct File Agent installation directory. Type **cdfa -v -cdefault_config.ser** and press **Enter**. A message including the Sterling Connect:Direct File Agent version is displayed.

Arguments on entry:

Arguments listing complete

November 22,2010 :16:32 PM CDT 783 Thread[Thread-0,5,main] Product IBM Sterling Connect:Direct File Agent Version 1.3.01 Copyright IBM Corp. 2003, 2010, GA fix 00000000 Date 2010/10/27

Sterling Connect:Direct File Agent runs with the wrong configuration file.

Sterling Connect:Direct File Agent uses the following hierarchy when determining what configuration file to use:

- If you specify the cdfa command with the -c option, Sterling Connect:Direct File Agent uses the specified configuration file. For example, **cdfa -cmonthend.ser** starts Sterling Connect:Direct File Agent with the configuration file named monthend.ser.
- If you do not specify the -c option at startup, Sterling Connect:Direct File Agent looks for a configuration file that matches the name of the computer it is running on. For example, if Sterling Connect:Direct File Agent runs on a computer named Host1, and a configuration file named Host1.ser exists in the cdfa directory, Sterling Connect:Direct File Agent uses the Host1 configuration file.

  On a Microsoft Windows computer, you can determine the computer name by selecting **Start<Settings>Control Panel>System** and selecting the **Network Identification** tab.

On a UNIX or Linux computer, see the operating system documentation to determine how to find the computer name.

- If you do not specify the -c option and no configuration file exists that matches the computer name, Sterling Connect:Direct File Agent uses the Default_Config configuration file.

Sterling Connect:Direct File Agent starts, but no activity occurs.

- Type **cdfa -v** to start Sterling Connect:Direct File Agent in verbose mode to obtain more details.
- Verify with the Sterling Connect:Direct system administrator that the Sterling Connect:Direct server is active.
- Run the Sterling Connect:Direct File Agent Configuration Interface to check that you have specified watched directories in the Sterling Connect:Direct File Agent configuration.
- Check that no other application is accessing a file that Sterling Connect:Direct File Agent should detect. Sterling Connect:Direct File Agent cannot process files that are in use by other applications.
- Verify that the Sterling Connect:Direct File Agent is running with exclusive access to the specified gate keeper port number.
- The Sterling Connect:Direct system administrator should verify that the Sterling Connect:Direct server is properly configured for a connection with Sterling Connect:Direct File Agent. See the Installation Guide for your platform for information about configuring the Sterling Connect:Direct server for Sterling Connect:Direct File Agent.

Sterling Connect:Direct File Agent compares the Compare String for a rule against the fully qualified path of the file found, not just against the file name

- Sterling Connect:Direct File Agent is designed to compare the Compare String against the fully qualified path of the file found, but if necessary, you can redefine your match criteria to have it match against the file name, for example:

  In UNIX, specify: '*/abc*' or '/my_watchdir/abc*' Microsoft Windows: '*\abc*' or 'C:\My_Watchdir\abc*'

  This forces pattern matching at the file name level only.

A rule should produce a match, but does not occur.

This could be caused by several conditions:

- Sterling Connect:Direct File Agent supports multiple rules in a configuration. If more than one rule applies, only the first rule encountered produces a match. When a match occurs, rules processing ends.

  The first rule should always contain the most specific criterion because rules are searched in the order listed on the Rules tab. If the first rule is too general, then it will always match and subsequent rules will never be processed.
- Match criteria are case-sensitive. For example, USER1 will not match User1 or user1.
- Verify that the match criteria and the rule are enabled.
- If the rule has multiple match criteria, all match criteria must match for the rule to apply.

Security properties not found, using default message is displayed when Sterling Connect:Direct File Agent starts.

This message is produced by the Java Virtual Machine (JVM), not Sterling Connect:Direct File Agent. It may be caused by having more than one JVM installed on your computer. It does not affect Sterling Connect:Direct File Agent operation and can be ignored.

When monitoring a watched directory, Sterling Connect:Direct File Agent scans the subdirectories of the watched directory, although this is not required.

Edit the rule to use the Matches operator to force Sterling Connect:Direct File Agent to detect only the directory specified in the path and ignore the subdirectories. To prevent unpredictable operation, be sure to specify this rule first.

Sterling Connect:Direct File Agent causes a parser error instead of operating as configured.

Early versions of Sterling Connect:Direct File Agent experienced parser errors when filenames or directory names specified in the configuration contained embedded spaces.

You can download Sterling Connect:Direct File Agent from the IBM Support Portal.

On z/OS, SCBC085I is received during an attempt to resolve a symbolic in a Sterling Connect:Direct File Agent rule.

This error occurs when a symbolic is enclosed in double quotes in the Sterling Connect:Direct File Agent rule. To remove the double quotes from the symbolic, run the Sterling Connect:Direct File Agent Configuration Interface and access the Sterling Connect:Direct File Agent rules fields as described in Editing a Rule .

On z/OS, Sterling Connect:Direct File Agent scans GDG files that are managed by SMS, and causes two destination files to be written for one source file.

You will need to apply software fixes to resolve this problem. For V4R4, apply fix T035471 (PUT4402). For V4R5, apply fix T035648 (PUT4501).

Sterling Connect:Direct File Agent is detecting files and submitting a Process, but no other action occurs.

Sterling Connect:Direct File Agent works with the Sterling Connect:Direct Processes you create, but this Sterling Connect:Direct component performs no actions other than detecting files in a specified location and submitting the specified Process. The actions you need to perform in response to file detection are performed by your Sterling Connect:Direct Processes. Refer to IBM Sterling Connect:Direct Process Lanuage Web site at http://www.sterlingcommerce.com/Documentation/processes/processhome.html.

After restarting Sterling Connect:Direct File Agent, files in the watched directory are not processed, even though processing was interrupted before it was completed.

Sterling Connect:Direct File Agent detects a file in a watched directory only one time. If processing is interrupted, files must be removed and replaced with a new timestamp, or in the case of UNIX systems, you can use the touch command to alter the timestamp so that Sterling Connect:Direct File Agent will detect the files.

Some files moved into the watched directory are not processed according to the Sterling Connect:Direct File Agent configuration, although other files are processed as expected.

Confirm that no other application is accessing the files that Sterling Connect:Direct File Agent should detect in the watched directory.

Test the files in the watched directory for file corruption.

Determine whether a synchronization problem is occurring because files are copied into the watched directory before Sterling Connect:Direct File Agent starts. For Sterling Connect:Direct File Agent to detect files in a watched directory, files must be transferred into the watched directory after Sterling Connect:Direct File Agent starts. Sterling Connect:Direct File Agent starts and assumes that any files already in watched directories were sent previously and should not be detected as a change in the watched directory.

To determine whether synchronization of the agent and the transfer of the files in question is the issue:

Stop Sterling Connect:Direct File Agent and remove all files from the monitored directory (or directories).

Start Sterling Connect:Direct File Agent from the command prompt. (For example, in Microsoft Windows, from the \Program Files\Sterling Connect:Direct File Agent directory, type: cdfa -v > cdfa.log to turn on verbose logging and send the output to a file.)

Place the files that were not processed according to the configuration into the monitored directory (or directories) and let Sterling Connect:Direct File Agent run for a few minutes.

Check to see if Sterling Connect:Direct File Agent processed the files according to the configuration and check the logging details output to the file.

If the files that were not processed according to the configuration are now processed, the issue was caused by certain files being copied into the watched directory before Sterling Connect:Direct File Agent started monitoring.

Sterling Connect:Direct File Agent is detecting files, but Sterling Connect:Direct File Agent is not submitting the Process that it should submit after detecting a file.

Check the user identification and password information. The user ID and password used to Submit the Process must be the same as the user ID and password used when Sterling Connect:Direct File Agent connected to the Sterling Connect:Direct server.

After disabling a rule in the configuration, Sterling Connect:Direct File Agent is still processing files as if the rule is enabled.

You must restart Sterling Connect:Direct File Agent before it can recognize that the rule has been disabled.

Spaces in the graphical interface display as boxes when Sterling Connect:Direct File Agent runs in an X Microsoft Windows emulator.

This is due to X Microsoft Windows configuration and behavior. Contact the X Microsoft Windows emulator vendor for a solution.

Receive the following error during a z/OS batch configuration job:Can't connect to X11 window server using 'hostname:0.0' as the value of the DISPLAY variable.

Please make sure that your setup environment variable DISPLAY correctly or issue xhost command on X server to include this host. Then restart the configurator.

Verify that the Alias provide in the DISPLAY is accessible to both the Sterling Connect:Direct File Agent mainframe and PC platforms. Use NSLOOKUP command on the mainframe or Microsoft Windows PC and Sterling Connect:Direct IUI NM gethostname function on the mainframe to look up the alias name.

Receive the following error during a z/OS batch configuration job:Can't connect to X11 window server using 'hostname:0.0' as the value of the DISPLAY variable.

Please make sure that your setup environment variable DISPLAY correctly or issue xhost command on X server to include this host. Then restart the configurator.

Verify the following:

- Mainframe to PC connection is passing through Firewall. Exceed uses ports 6000 - 6063. These ports must be allowed to come through the firewall.
- Exceed is allowing the Mainframe host access because of Exceed Security setting. Use Exceed Xconfig utility to set Security to allow DISPLAY host access or allow all hosts access.

Chapter 7. Command Line Parameters

Specifying Command Line Parameters

You can specify the following parameters when you start Sterling Connect:Direct File Agent. These parameters are case sensitive.

cdfa

Starts Sterling Connect:Direct File Agent.

cdfa1.bat

On Microsoft Windows systems, starts Sterling Connect:Direct File Agent and displays parameters on the command window. Use in place of **cdfa**.

-cconfigfile.ser

Specifies the Sterling Connect:Direct File Agent configuration file (specified in configfile.ser) to use instead of any other configuration file. For example, **cdfa -cmonthend.ser** starts Sterling Connect:Direct File Agent with the configuration file named monthend.ser.

-C

Starts the configuration interface, for example, **cdfa -C**.

-g configbuild

Specifies that Sterling Connect:Direct File Agent create one or more configuration files from the configuration template and the text file specified in configbuild.

See Creating Multiple Configurations for more information about this command.

-f

Force processing of existing files in the watched directories when starting Sterling Connect:Direct File Agent.

-uxx

Specifies the country code that Sterling Connect:Direct File Agent should use in place of the default country code. For example, **cdfa -ufr** starts Sterling Connect:Direct File Agent using France as the country code.

-lxx

Specifies the language code (xx) that Sterling Connect:Direct File Agent should use in place of the default language. For example, **cdfa -lfr** starts Sterling Connect:Direct File Agent using French.

-v

Runs in verbose mode. No internal log is kept and all actions are displayed on the monitor. For example, **cdfa -v**.

Chapter 8. Setting up TLS and Certificate-Based User Authentication in File Agent

Setting up TLS and Certificate-Based User Authentication in File Agent

File Agent 1.4.0.1 and later supports certificate-based user authentication and secure API connections to the Connect:Direct server. The required configuration to setup File Agent and the Connect:Direct server is explained in this section.

Enabling Secure API Connections in File Agent

1. Run the Java Connection Utility (JCU) to create the external login file (`cddef.jcu`) in the File Agent directory.
2. Enter the appropriate information for the Connect:Direct server and set the protocol to TLS12.

   Note: The loopback address shown in the illustration below is only for example. Enter the correct address and port for client connections to your server.

   If certificate-based authentication will be used, you can specify a dummy userid and password here, because the real user name will be determined by the Common Name of the certificate.

   Windows:

   ```
   jre\bin\java.exe -classpath CDJAI.jar com.sterlingcommerce.cd.sdk.JCU -fcddef.jcu
   ```

   UNIX:

   ```
   jre/bin/java -classpath CDJAI.jar com.sterlingcommerce.cd.sdk.JCU -fcddef.jcu
   ```

   ```
   IBM Sterling Connect:Direct Java Client Connection Utility, Version 1.1.00
   ? Copyright IBM Corp. [2001, 2011] All Rights Reserved.

   US Government Users Restricted Rights - Use, duplication or
   disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
   ============================================================
   Node:     <Enter> = 'VOLKER.600'
   >
   Address:  <Enter> = '127.0.0.1'
   >
   Port:     <Enter> = '1363'
   >
   UserId:   <Enter> = 'dummy'
   >
   Password:
   >dummy123
   Protocol:  <Enter> = 'TLS12'
   >
   ```

3. If certificate-based authentication will be used, the password must be empty. Since the JCU currently does not allow entering an empty password, it has to be removed manually. So as a workaround, open `cddef.jcu` in a text editor and remove all characters after "2=" from the line starting with User, for example

   ```
   User;NAME.600;dummy;2=
   ```

Later versions of the JCU may not require this workaround anymore. Check File Agent `fixlist` for the latest updates.

4. To enable the JCU login file, open the File Agent configuration and set the **Userid for API** to jcu. The settings for **Password for API**, **API host DNS name** and **API port** will be ignored. At runtime, File Agent will load the connection information from the specified JCU login file instead.

Creating Certificate and Key Store for File Agent

This step is only required when using certificate-based authentication. The Common Name of the certificate specifies the userid that File Agent will use to submit processes to the Connect:Direct server.

Note: This userid must be a real local user on the Connect:Direct server.

1. Create a new key store (`keystore.jks`) in the File Agent directory and add the user's key certificate.

   Note: The userid certuser shown in the illustration below is only for example. Enter a real local user name to be used for submitting processes on the Connect:Direct server.

   If you do not already have a user certificate, you can simply run the following command to create a self-signed certificate and a new keystore. Replace `certuser` with the userid that File Agent should use to submit processes to the Connect:Direct server.

   Windows:

   ```
   jre\bin\keytool.exe -genkey -alias certuser -keyalg RSA -keystore keystore.jks
   ```

   UNIX:

   ```
   jre/bin/keytool -genkey -alias certuser -keyalg RSA -keystore keystore.jks
   ```

   Export the certificate to a file and use it as the CA root certificate in later steps.

   Windows:

   ```
   jre\bin\keytool.exe -exportcert -alias certuser -keystore keystore.jks -file ca_certuser.pem
   -rfc
   ```

   UNIX:

   ```
   jre/bin/keytool -exportcert -alias certuser -keystore keystore.jks -file ca_certuser.pem -rfc
   ```

Creating Trust Store for File Agent

Create a new trust store (`truststore.jks`) in the File Agent directory and import the CA root and intermediate certificates for the Connect:Direct server into it.

Windows:

```
jre\bin\keytool.exe -importcert -file ca_cdserver.pem -keystore truststore.jks
```

UNIX:

```
jre/bin/keytool -importcert -file ca_cdserver.pem -keystore truststore.jks
```

Setting up Secure+ in Connect:Direct

Open the Secure+ configuration in CD Secure+ Admin Tool (spadmin), CD Secure+ CLI (spcli) or any other configuration client.

1. Import the **CA root and any intermediate certificates** into the keystore, which are required to validate your user certificate. If you had created a self-signed certificate in the above illustration, import the `ca_certuser.pem` file here.

2. Configure the **.Client** record for **TLS 1.2** and, if using certificate-based authentication, **Enable Client Authentication**. If you have not configured **Key Certificate Label** and **Cipher Suites** on the `.Local` record, do so here.

Setting up the User Account in Connect:Direct

This step is only required when using certificate-based authentication.

1. Create a local user named after the Common Name of the certificate with which File Agent will connect. In the above illustration, a Common Name of certuser was used.

   For **Connect:Direct for UNIX**, set `client.cert_auth=y` for this user.

   For **Connect:Direct for Windows**, enable the options to **Allow Client Certificate Authentication** and **Allow Process to run using Service Account** for this user.

Launching File Agent

Specify the key and trustStore settings as java system properties (-D) on the java command when launching File Agent. See the java command for details.

```
-Djavax.net.ssl.keyStore=keystore.jks
-Djavax.net.ssl.keyStorePassword=changeit
-Djavax.net.ssl.trustStore=truststore.jks
-Djavax.net.ssl.trustStorePassword=changeit
```

Note: It is not possible to hide passwords from the settings.

UNIX:

Edit the cdfa script in the FileAgent directory and add the settings to the java command line.

```
"jre/bin/java" -Djavax.net.ssl.keyStore=keystore.jks -Djavax.net.ssl.keyStorePassword=changeit
-Djavax.net.ssl.trustStore=truststore.jks -Djavax.net.ssl.trustStorePassword=changeit ...
```

Windows:

Edit the cdfa.lax and cdfa$.lax files in the FileAgent directory and add these settings to the lax.nl.java.option.additional property in each file.

```
lax.nl.java.option.additional=-Djavax.net.ssl.keyStore=keystore.jks
-Djavax.net.ssl.keyStorePassword=changeit -Djavax.net.ssl.trustStore=truststore.jks
-Djavax.net.ssl.trustStorePassword=changeit ...
```

Alternatively, for either platform, specify these settings in an environment variable named IBM_JAVA_OPTIONS.

Chapter 9. High Availability Support

High Availability in File Agent

The new high availability support is enabled by specifying a shared work directory on the command line. The shared work directory allows File Agent instances running on different computers to synchronize work and determine who is active or standby.

Command	Description
-w	Specifies the shared work directory when running multiple Sterling Connect:Direct File Agents in a high availability environment. The directory must exist before starting Sterling Connect:Direct File Agent. It is highly recommended that the shared work directory does not overlap with any watch directory as this can cause high availability to fail on some systems.

File Agent supports High Availability in both UNIX and Windows environments. The following steps are for a Linux environment, but enabling High Availability in other environments is similar.

1. Install two or more File Agent instances on different Linux systems using the provided version.
2. Create a new work directory on a shared network drive and grant access permission to the account(s) that will be running File Agent.
3. Create a common File Agent configuration to be used by all instances. Store the configuration file with the default name `Default_Config.ser` in the shared work directory or copy it to all local File Agent directories.
4. Start your File Agent instances specifying the shared work directory on the command line (-w), for example

```
cdfa -w /opt/shared/FASharedWorkDir
```

The 1st File Agent instance will become active and begin monitoring watch directories, as usual. CDFA.log indicates this with a “Lock acquired successfully” message.

```
2019-12-30 19:20:15,433 INFO  - using configuration from: /home/fauser/work/shared/
Default_Config.ser
2019-12-30 19:20:15,434 INFO  - Shared work path: /home/fauser/work/shared
2019-12-30 19:20:15,445 INFO  - Lock acquired successfully: /home/fauser/work/shared/
FA_Shared.lck
2019-12-30 19:20:16,207 INFO  - Monitoring configuration file /home/fauser/work/shared/
Default_Config.ser
2019-12-30 19:20:16,208 INFO  - ckpt file: /home/fauser/work/shared/FA_Shared.ckpt
```

The 2nd and later File Agent instances will remain in standby and check every 10 seconds. CDFA.log indicates this with “Waiting to acquire lock” message.

```
2019-12-30 19:20:26,441 INFO  - using configuration from: /home/fauser/work/shared/
Default_Config.ser
2019-12-30 19:20:26,443 INFO  - Shared work path: /home/fauser/work/shared
2019-12-30 19:20:26,448 WARN  - Standby - Waiting to acquire lock: /home/fauser/work/shared/
FA_Shared.lck
2019-12-30 19:20:36,449 WARN  - Standby - Waiting to acquire lock: /home/fauser/work/shared/
FA_Shared.lck
```

```
2019-12-30 19:20:46,451 WARN  - Standby - Waiting to acquire lock: /home/fauser/work/shared/
FA_Shared.lck
```

Once the active File Agent instance terminates, another standby File Agent instance will become active and resume its work.

Chapter 10. Amazon S3 support

File Agent supports Amazon S3 or S3 compatible object stores. A default configuration is provided to access S3 objects using the default Amazon S3 credential mechanisms. Depending on where File Agent is executing the following credential mechanisms apply.

Credential Mechanism	On EC2	Outside EC2 or S3 compatible providers
Environment variables AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY	Yes	Yes
Java system properties aws.accessKeyId and aws.secretKey	Yes	Yes
Web Identity Token credentials from the environment or container.	Yes	No
The credential profiles file typically located at ~/.aws/credentials	Yes	Yes
Amazon ECS container credentials loaded from the Amazon ECS if the environment variable *AWS_CONTAINER_CRED ENTIALS_RELATIVE_URI* is set.	Yes	No
Instance profile credentials used on EC2 instances and delivered through the Amazon EC2 metadata service.	Yes	Yes

Amazon S3 default configuration

A property file located in the File Agent directory is dedicated to S3 configuration if some particular configuration properties should be changed from the default values or created for another S3 provider. A default set of properties is already available to connect to Amazon S3. This configuration will enable Fie Agent to connect and Amazon S3 using the credentials mechanisms described above.

```
# AWS S3 provider - default
cdfa.provider.1=scheme=S3://
cdfa.provider.1=provider=aws-s3
```

S3 configuration

A set of provider properties is declared by using the following syntax: *cdfa.provider.n=property=value* with n the set name. All properties declared on this set will rely on the same provider. A scheme property identifies and link the scheme name in File Agent watched directory and a provider.

Credential Mechanism	Scheme in providers.properties	Scheme in watched directories
cdfa.provider.1=scheme= S3://	S3://abucketname/afolder	This watched directory will be linked to provider 1.

Credential Mechanism	Scheme in providers.properties	Scheme in watched directories
cdfa.provider.2=scheme=OS3://	OS3://otherbucketname/otherfolder	This watched directory will be linked to provider 2.
Instance profile credentials used on EC2 instances and delivered through the Amazon EC2 metadata service.	X4://bucket/f	This watched directory will be rejected. There is no provider definition available.

Additional S3 configuration

The following additional properties can be selected:

Property name	Scheme in providers.properties	Mandatory	Default value	Example
cdfa.provider.n=provider=ProviderName	This is the Store provider name. The only valid value is aws-s3.	Yes	No	cdfa.provider.2=provider=aws-s3
cdfa.provider.n=aws.region=regionName	The AWS region to work with.	No	No	cdfa.provider.3=aws.region=US-EAST-1
cdfa.provider.n=aws.identity=aws_access_key_id	This is the aws_access_key_id value when using the credential provider. This property must be set in conjunction with aws.credentials	No	No	cdfa.provider.1=aws.identity=<key_id>
cdfa.provider.n=aws.credential=aws_secret_access_key	This is the aws_secret_access_key value when using the credential provider. This property must be set in conjunction with aws.identity.	No	No	cdfa.provider.1=aws.credential=<secret_access_key>

Property name	Scheme in providers.properties	Mandatory	Default value	Example
cdfa.provider.n=aws.profile =ProfileName	When the credential file provider is used, [default] profile will be replaced by this profile name. This profile name must exist in credentials file. This property has no effect when aws.identity and aws.credetential are set. When this property is set, only the credential file credential mechanism is executed.	No	Default	cdfa.provider.2= aws.profile =PProduction
cdfa.provider.n= aws.credentialspath =PathToCredentialsFile	Locate the credentials file when on a different location than the default. Default is typically located at ~/.aws/credentials. When this property is set, only the credential file credential mechanism is executed.	No	No	cdfa.provider.2= aws.credentialspath= /home/CDFA/credentials
cdfa.provider.n= aws.endpoint =http/https://endpoint:port	Defines the endpoint for a compatible AWS S3 provider	No	No	cdfa.provider.3= aws.endpoint =https:// my.s3.provider:8080
cdfa.provider.n= outscheme=scheme://	If scheme property must be replaced when generating S3 object URI for Connect Direct Process.	No	Scheme property value	
cdfa.provider.n= maxobjectsretrieved=n	Maximum number of objects retrieved per batch request to S3. All objects are retrieved but each batch request to S3 will be limited to this number of objects.	No	100	cdfa.provider.3= maxobjectsretrieved=50
cdfa.provider.n= aws.virtual-host-buckets=true/false	Some S3 compatible providers can't work with virtual host URI syntax. Set this value to false to work with path style syntax.	No	True	cdfa.provider.1= aws.virtual-host-buckets=false

Out scheme property

When Connect Direct is configured to work with S3 schemes but not the same than File Agent, use outscheme property to define what scheme will be used when generating %FA_FILE_FOUND. variable. %FA_WATCHED_FILE_FOUND content is the original name.

Scheme	Outscheme	Discovered File	%FA_FILE_FOUND	%FA_WATCHED_FILE_FOUND
S3://	Not provided	S3://bucket/folder/name	S3://bucket/folder/name	S3://bucket/folder/name
S3://	OS3://	S3://bucket/folder/name	OS3://bucket/folder/name	S3://bucket/folder/name

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBMproducts. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as shown in the next column.

© 2015.
Portions of this code are derived from IBM Corp. Sample Programs.
© Copyright IBM Corp. 2015.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Connect Control Center®, Connect:Direct®, Connect:Enterprise®, Gentran®, Gentran®:Basic®, Gentran:Control®, Gentran:Director®, Gentran:Plus®, Gentran:Realtime®, Gentran:Server®, Gentran:Viewpoint®, Commerce™, Information Broker®, and Integrator® are trademarks, Inc., an IBM Company.

Other company, product, and service names may be trademarks or service marks of others.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED,

INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Part Number:
Product Number: 5655-X01

(1P) P/N: