IBM® Connect:Direct File Agent 6.2

Documentation

This edition applies to Version 6 Release 2 of IBM® Connect:Direct and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright International Business Machines Corporation 1993, 2021.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

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

What's New..1

Known Restrictions...1

Sterling Connect:Direct Integrated File Agent Overview...1

Configuring Sterling Connect:Direct Integrated File Agent..2

How to Run Sterling Connect:Direct Integrated File Agent...3

Sterling Connect:Direct Integrated File Agent Monitoring..3

Sterling Connect:Direct Integrated File Agent Configuration Planning.......................3

Tips for Using Sterling Connect:Direct Integrated File Agent.....................................3

Chapter 2. Converting a Standalone File Agent configuration file to an Integrated File Agent configuration file.. 5

Chapter 3. Basic Configuration...7

Configure General Settings..7

Configure Monitoring through Sterling Control Center..8

SNMP Trap Information...9

Error Reporting...9

Chapter 4. Watch Directories... 11

Chapter 5. Rules...13

Rules...13

Evaluating Rules...13

Prioritizing Rules...13

General Parameters..13

Match Criteria...14

Match Operators...14

Process Information...15

Sterling Connect:Direct Integrated File Agent Variables..16

Microsoft Windows/UNIX Example...19

z/OS Examples...19

Chapter 6. Logging..21

Logging.. 21

Chapter 7. Best Practices and Troubleshooting... 23

Best Practices... 23

Considerations for a Large Number of Watch Directories...................................23

Considerations for a Large Number of Files in a Watch Directory....................... 23

Considerations for Watch Directory Scans.. 24

Troubleshooting... 24

Chapter 8. Object Stores support.. 27

Notices...29

Trademarks.. 30

Terms and conditions for product documentation... 31

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

What's New

IBM Sterling Connect:Direct® Integrated File Agent version 6.2 and its related software have the following features and enhancements:

Base Release (v6.2)

New Features and Enhancements

To install this software, you should go to the Passport Advantage website, and follow instructions described to complete the download.

- IBM Sterling Connect:Direct 6.2 adds an Integrated File Agent as an installation option. Integrated File Agent provides users with these benefits:
  - Since it is a component of Connect:Direct, Integrated File Agent's deployment - new deployment, maintenance, upgrade and decommission- is included in Connect:Direct's deployment, and hence, involves no additional work. This is true if Connect:Direct is deployed directly or through IBM Sterling Control Center Director.
  - Integrated File Agent's User Interface is integrated with Connect:Direct's Web Services UI, giving File Agent a modern UI and making Integrated File Agent configuration intuitive.
  - Integrated File Agent includes significant enhancements to “Rules” on page 13, that make Rules more flexible and powerful. These include
    - The watch directories to which a rule is applied are configurable
    - Whether a watch directory includes its sub-directories or not is configurable
    - Process class and priority are optional
  - Integrated File Agent comes with a simple process library hosted by Connect:Direct, supporting process organization and control. For more information refer Connect:Direct for UNIX and Microsoft Windows.

Known Restrictions

Sterling Connect:Direct Integrated File Agent and its related software have the following known restrictions:

- IBM Sterling Connect:Direct Web Services is required to configure Integrated File Agent.
- Integrated File Agent is supported in a container deployment of CD UNIX from CDU 6.2.0.1 IFix029.
- The self-signed certificate automatically generated during new installation, although suitable for production Integrated File Agent to Connect:Direct connections, is unsuitable for production Connect:Direct to Connect:Direct and remote-API-client to Connect:Direct connections. Customers who wish to secure these connections must replace the key certificate in the .Local node record with a certificate suitable for production, such as a CA certificate issued by an internal or public CA.
- Match Criteria against File Size are not supported on z/OS systems.

Sterling Connect:Direct Integrated File Agent Overview

Sterling Connect:Direct Integrated File Agent is a component of IBM Sterling Connect:Direct that provides unattended file management. It is an installation option of IBM Sterling Connect:Direct for UNIX,

© Copyright IBM Corp. 1993, 2021

Windows and z/OS. Integrated File Agent can only be configured using IBM Sterling Connect:Direct Web Services.

IBM Sterling Connect:Direct File Agent provides monitoring and detection capabilities that enhance the automation you accomplish with IBM Sterling Connect:Direct Processes. It can pass a variety of Sterling Connect:Direct File Agent variables as arguments to a Process. IBM 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 IBM Sterling Connect:Direct server. Before you configure IBM Sterling Connect:Direct File Agent, you must create and test the IBM Sterling Connect:Direct File Agent Process that you intend to specify with a Rule in the IBM Sterling Connect:Direct File Agent configuration.

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

- Watch for any file to appear or being updated in any watched directory and submit the Process defined in the default Rule after detecting the file.
- Create one or more Rules to take different actions based on the location or properties of the detected files. IBM Sterling Connect:Direct File Agent checks file location and properties to determine whether criteria specified by the rule are met. If criteria for a rule are met, IBM Sterling Connect:Direct File Agent submits the Process associated with that rule. The processes that Integrated File Agent submits are stored in a Process Library that is part of IBM Sterling Connect:Direct. The Process Library is managed with IBM Sterling Connect:Direct Web Services.

You can create Sterling Connect:Direct Integrated File Agent rules based on the following match criteria:

- Watch directory where the file was detected
- Full or partial name of the file detected in a watched directory
- Size of the file detected in a watched directory

You can specify more than one rule in a IBM Sterling Connect:Direct File Agent configuration; each rule can have IBM Sterling Connect:Direct File Agent submit a different Process. Although, you can create multiple rules as part of a IBM Sterling Connect:Direct File Agent configuration, its rules' processing ends once match criteria for a rule is met. Therefore, you should specify rules so that those with more specific criteria (properties) are listed first in the configuration.

Sterling Connect:Direct Integrated File Agent can monitor multiple directories. When you use IBM 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 IBM 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, on Linux, you can also watch Amazon S3 or S3-compatible objects stores. Add the selected buckets and objects path to the watched directory list.

Sterling Connect:Direct Integrated File Agent can monitor multiple directories, including local and network directories. It scans the watched directories you specify in the configuration for newly added files. By default, Sterling Connect:Direct Integrated File Agent scans a watched directory once every minute.

For example, if you start IBM 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 IBM 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 IBM Sterling Connect:Direct File Agent detects this newly added file. IBM Sterling Connect:Direct File Agent detects a file only one time, unless the file is accessed and saved with a later timestamp. Using IBM Sterling Connect:Direct File Agent requires an understanding of IBM Sterling Connect:Direct Processes, operating systems, and scripting (for regular expression operator use with IBM Sterling Connect:Direct File Agent rules).

Configuring Sterling Connect:Direct Integrated File Agent

Use the Sterling Connect:Direct Web Services User Interface, to configure File Agent, including basic configuration, one or more watch directories, that Sterling Connect:Direct File Agent monitors and one or more rules that specify how a file found in watched directory is processed. Sterling Connect:Direct Web Services User Interface and Sterling Connect:Direct Integrated File Agent will perform a validation before a new configuration gets be applied. If the validation fails, the new configuration will not be applied and Sterling Connect:Direct Integrated File Agent keeps using the existing configuration.

How to Run Sterling Connect:Direct Integrated File Agent

On UNIX and Windows, Sterling Connect:Direct Integrated File Agent is fully controlled by the Sterling Connect:Direct server. The server starts and stops the Integrated File Agent automatically as configured by fileagent.enable initialization parameter. To enable Integrated File Agent, set fileagent.enable=Y. On z/OS, you must run the appropriate job to start or stop Sterling Connect:Direct Integrated File Agent.

Before you can run Sterling Connect:Direct Integrated File Agent, you must create a valid configuration. Use the Sterling Connect:Direct Web Services to configure Sterling Connect:Direct Integrated File Agent.

Sterling Connect:Direct Integrated File Agent Monitoring

Sterling Connect:Direct Integrated File Agent logs information to separate log files in its log subdirectory. The level of information that is written to the logs is configurable. In addition, Integrated File Agent writes entries in Connect:Direct's Statistics. Under normal circumstances, Connect:Direct Statistics will be sufficient to track File Agent operations; the log files will be needed only for troubleshooting.

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 basic configuration.

Sterling Connect:Direct Integrated File Agent Configuration Planning

Before you begin configuring Sterling Connect:Direct Integrated File Agent, you must choose or create the Sterling Connect:Direct Integrated File Agent Processes that perform the actions you want to automate. You configure Sterling Connect:Direct Integrated File Agent to connect to the Sterling Connect:Direct Integrated File Agent server and to monitor and detect conditions (such as a file addition to a directory). At detection, Sterling Connect:Direct Integrated File Agent submits the Process for executing actions that need to be performed in response to those conditions.

- Run a test and use the Sterling Connect:Direct Statistics and File Agent logs to verify that the basic File Agent configuration is working correctly.
- After you verify the default Rule, you can create and validate Sterling Connect:Direct File Agent rules, one by one.

Tips for Using Sterling Connect:Direct Integrated File Agent

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

- You must monitor your standard output log files to detect problems or failures in Sterling Connect:Direct Integrated File Agent or configure Sterling Connect:Direct Integrated File Agent to send SNMP traps to Sterling Control Center or another SNMP monitoring application.
- You cannot configure e-mail alerts to notify you when errors occur unless you are using Sterling Control Center with Sterling Connect:Direct Integrated File Agent.
- Sterling Connect:Direct Integrated File Agent uses a checkpoint file *Default_Config.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 Integrated 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:
  - Alter the timestamp of the files in the watch directories, for example by using the touch command.

  - Remove the files from the watch directories and put them back with a new timestamp.
- Sterling Connect:Direct Integrated File Agent detects a file only once unless the file is accessed and saved with a new timestamp.

Chapter 2. Converting a Standalone File Agent configuration file to an Integrated File Agent configuration file

You can use the `cdfaconvertcfg` utility to convert a Standalone File Agent configuration file so that it can be used by Integrated File Agent. The conversion utility is in the Connect:Direct installation directory tree of Integrated File Agent directory. It is invoked as follows:

Help

```
cdfaconvertcfg -h | --help
```

Conversion

```
cdfaconvertcfg -i | -input <infilename> -o | -output <outfilename>
```

where infilename is the filename of a Standalone File Agent .ser file, and outfilename is the filename of the Integrated File Agent JSON generated from the input configuration.

Note:

- In a file name condition, an EQUALS operator is changed to a MATCH operator. This is a cosmetic, terminology update. The Rule continues to function in the same way.
- A file **name** condition containing a LT or GT operator is not converted, and a Warning that the condition has been omitted is reported.

Validate the new configuration file with the Configuration Validation Utility, `cdfacfg`:

```
cdfacfg -f | --file <jsonFilename> -m | max <maxErrors>
```

where jsonFilename is the filename of the configuration file to be validated, and maxErrors is the maximum number of errors to report.

To make the new configuration file the active one, follow these steps:

1. Back up the current active configuration file, Default_Config.json.
2. Delete it.
3. Rename the new configuration file to Default_config.json.

Related concepts
“Rules” on page 13

© Copyright IBM Corp. 1993, 2021

Chapter 3. Basic Configuration

Configure General Settings

The following table describes general configuration parameters. Specify any other parameters required to configure Sterling Connect:Direct File Agent to operate on your site.

Parameters	Description
Comments	Type comments to describe the configuration. Comments are not used during the execution of Sterling Connect:Direct Integrated File Agent.
Connect:Direct Userid	Required. Type the userid to use when connecting to the Sterling Connect:Direct server. This field is case-sensitive. The userid must have permission to submit Sterling Connect:Direct Process and perform external statistics logging on the Sterling Connect:Direct server. Additional permissions may be required to perform steps defined in the Sterling Connect:Direct Processes.
Connect:Direct Password	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. Leave this field empty when using certificate-based authentication. Additional configuration of the userid and Secure+ is required on the Sterling Connect:Direct server.
Continuous signon	Select Yes (default) to stay connected to the API port whenever Integrated File Agent is active, or select No to disconnect Integrated File Agent and reconnect each time Processes are submitted after a directory scan. If Continuous signon is Yes, Integrated 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 Integrated File Agent is stopped. Use this option if files are placed in the watched directories more or less continuously. If Continuous signon is No, Integrated 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, Integrated 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.

© Copyright IBM Corp. 1993, 2021

Parameters	Description
Watch file interval	Type the number of minutes that you want Integrated File Agent to wait before checking the watch directories for files. By default, Integrated File Agent checks the watch directories for files once each minute. This field specifies how long Integrated 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 Integrated File Agent is not scanning the watched directories as often. There is a trade-off between the processing time that Integrated 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 Integrated File Agent to wait before considering a detected file being complete and ready for processing. The default time is 1 minute. This field applies when different tasks can access the same file simultaneously. This may cause problems if Integrated File Agent detects that a file is present in the watched directory and processes it before another application has closed it. Set this delay to allow an application to finish with the file before Integrated File Agent accesses the file.

Configure Monitoring through Sterling Control Center

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. The following table describes the monitoring parameters. You can obtain this information from your Sterling Control Center system administrator.

Parameters	Description
File Agent unique name	Required. Provide a unique name for each Sterling Connect:Direct Integrated 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 Integrated File Agent instance by Sterling Control Center. Failing to do so results in Sterling Control Center treating multiple instances of Sterling Connect:Direct Integrated File Agent as one.
SNMP listener address	Type one or more addresses for the SNMP trap receiver, such as Sterling Control Center. Integrated File Agent uses these addresses to send SNMP traps for statistics. This field is optional. Type a comma separated list of entries in the format address[;port], for example icchost1;1163,icchost2i,172.0.0.1;1163. The port value is optional and will default to the SNMP listener port value, or to port 1163 when 0.

Parameters	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 Integrated 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.
SNMP status trap interval	Type the number of seconds that you want Integrated File Agent to wait before sending status traps to SNMP trap receivers, such as Sterling Control Center. The value can be in the range of 30 .. 3600 seconds. The default is 30 seconds.

SNMP Trap Information

When the Sterling Connect:Direct Integrated 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 4. Watch Directories

Sterling Connect:Direct File Agent can monitor one or more watch directories. This includes local and network directories or S3 object stores that are accessible from the computer and userid running Sterling Connect:Direct File Agent. Sterling Connect:Direct File Agent scans the watched directories and optionally sub directories in regular intervals for newly added or changed files. If a new or changed file has been detected during a director scan, Sterling Connect:Direct File Agent will process the detected file.

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, on Linux, you can also watch Amazon S3 or S3-compatible objects stores.

The following table describes the watch directory parameters.

Parameters	Description
Watch Directory	Required. Provide a valid and fully qualified path to a local or network directory or to an S3 object store. The path must be valid and accessible from the computer running Sterling Connect:Direct File Agent. The userid running Sterling Connect:Direct File Agent must have read permission on the directory and files to scan them.
Directory Description	Type a comment to describe the watch directory. Comments are not used during the execution of Sterling Connect:Direct Integrated File Agent.
Monitor sub directories	Enable this option to let Sterling Connect:Direct File Agent monitor files in the watch directory and in any sub directory. The default is to only monitor files located in the watch directory itself.

Examples

Microsoft Windows

Local directory:

```
C:\Data\Customer\Benefits
```

Network directory using UNC:

```
\\winserver\\datashare\Customer\Benefits
```

UNIX

Directory:

```
/data/cust/benefits
```

z/OS

Datasets starting with CUST.BENEFITS:

```
CUST.BENEFITS.**
```

© Copyright IBM Corp. 1993, 2021

Library with members:

```
CUST.CNTL
```

S3 Cloud Storage Example

S3 bucket “abucket” with a key “akey”:

```
S3://abucket/ akey
```

Chapter 5. Rules

Rules

When Sterling Connect:Direct Integrated File Agent has detected a new or updated file, it uses Rules to determine if and how the file should be processed. Configure the Default Rule to submit a predefined Sterling Connect:Direct Process with arguments for any detected file. Add one or more Rules to submit other Processes with arguments based on one or more match criteria, like

- Watch directory where the file was detected
- Full or partial name of the file detected in a watched directory
- Size of the file detected in a watched directory

Rules can be enabled, disabled or marked as draft for later refinement.

Evaluating Rules

A Rule will evaluate true and be applied for a detected file under the following conditions.

Note: The exception is the Default Rule, which does not have any match criteria. The Default Rule will evaluate true and be applied for a detected file under the following conditions.

- The Rule is enabled.
- At least one match criterion has been added.
- If one or more Watch Directories criteria have been added, the detected file must be in one of these directories.
- If one or more match criteria on File Name or File Size have been added, they all must match.
- The Default Rule is enabled.

Prioritizing Rules

Although you can create multiple Rules, Sterling Connect:Direct File Agent Rules processing ends once criteria for a rule are met. Subsequent rules are not considered anymore. Therefore, you should specify rules in the right order so that those with more specific match criteria are listed first in the configuration. Use Sterling Connect:Direct Web Services User Interface to re-prioritize Rules.

Sterling Connect:Direct File Agent begins Rules processing by evaluating Rule with priority 1, then priority 2 and so on until the first matching Rule is found. If no matching Rule was found, then the Default Rule is evaluated last.

General Parameters

The following table describes the general parameters of a Rule.

Parameters	Description
Rule Name	Required. Provide a unique name for the Rule.
Description	Type a comment to describe the Rule. Comments are not used during the execution of Sterling Connect:Direct Integrated File Agent.
Rule Enabled	Select if the Rule Status should be enabled or disabled. Only enabled Rules will be evaluated and applied.

© Copyright IBM Corp. 1993, 2021

Match Criteria

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

Operators define how Sterling Connect:Direct Integrated File Agent tests for the match criteria using the compare value to evaluate properties of a detected file. Operators like Matches or Does not match do support the wildcard characters asterisk (*) and question mark (*?) in the compare string. The following table describes the different types of Match Criteria that can be added to a Rule.

Parameters	Description
Watch Directory	Select one or more entries from the list of Watch Directories defined in the configuration. The detected file must be in one of these directories.
File Name	Select a compare operator (Matches, Does not match or Contains) and specify a string value. Wildcards (*) are supported. The fully qualified path of the detected file will be compared against the specified value.
File Size	Select a compare operator (Greater than, Less than or Equals) and specify a numeric value. The size of the detected file will be compared against the specified value.

Match Operators

Operators define how Sterling Connect:Direct Integrated File Agent tests for the match criteria using the compare value to evaluate properties of a detected file.

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 Integrated File Agent to search only the directory specified by the path for the file name that match the specified compare string exactly.

The compare string can include the wildcard characters asterisk (*) and question mark (*?). For example, typing "C:\Data\ABC*" as the string to match causes Sterling Connect:Direct Integrated File Agent to process the rule after detecting any file name beginning with ABC in the "C:\Data" 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 watch directories ending in ".txt". However, "09*.txt" will not match on a file name "09March.txt". Instead, use "<path>/09*.txt" or "*/09*.txt" where <path> is the full path to the watch directory, such as "C:\Data".

Not matches

To define a rule based on characters to exclude. The path and file name are checked against the compare string and Sterling Connect:Direct Integrated 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 Integrated File Agent filters for a fully qualified path or file name 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 or size of the detected file, 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.

Less than

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

Greater than

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

Process Information

Specify an existing Sterling Connect:Direct Process that will be submitted when a Rule is applied. Set additional parameters when you need to overwrite defaults in the Process or the Sterling Connect:Direct server. See the Sterling Connect:Direct Process Language for more details.

Parameters	Description
Process Name	Specify the Sterling Connect:Direct Process to be submitted when the Rule applies. Browse for an existing Process from the Process Library or enter a fully qualified path to an existing Process file on the computer running Sterling Connect:Direct Integrated File Agent. If this field is blank, the detected file is ignored without submitting a Process and marked as being processed.
Process Class	Type the numeric class (CLASS) that the Process submitted to the Sterling Connect:Direct server should use for execution. This can be a value between 1-255. If this field is blank, the default class set in the Process or the Sterling Connect:Direct server is used.
Process Priority	Type the numeric priority (PRTY) that the Process submitted to the Sterling Connect:Direct server should use for execution. This can be a value between 0-15. If this field is blank, the default priority set in the Process or the Sterling Connect:Direct server is used. This parameter is different from Rule Priority.
Notification Userid	Type the userid to notify when the Process completes if notification is supported by the Sterling Connect:Direct server. If this field is blank, no user is notified.

Sterling Connect:Direct Integrated File Agent Variables

Sterling Connect:Direct File Agent Variables provide a flexible way to pass arguments to the Process that Sterling Connect:Direct Integrated File Agent submits. A variety of variables are available for file properties, date/time and other values.

When Sterling Connect:Direct Integrated File Agent submits the Process for a detected file, it first resolves any File Agent variable specified in the Build Value and assigns the result to the specified CD Substitution Variable. The CD Substitution Variable is then passed into Process submission, allowing the Process to perform its tasks, for example sending the detected file to a remote Sterling Connect:Direct node.

Observe the following rules when you specify File Agent 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 Integrated File Agent Process.

The following table describes the Sterling Connect:Direct File Agent Variables.

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 Integrated File Agent detected, including any member name. This variable supports PDSE long member names. For example, when you specify this variable, Sterling Connect:Direct Integrated 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 8, “Object Stores support,” on page 27.
	%FA_FSTYPE.	The file or object file system type. Windows, Unix, OS390, AWSS3

Usage	**Variable**	**Description**
Current date and time	%FA_DATE.	The current date. This value has 8 characters that represent the year, month, and day, for example, (yyyymmdd), 20210805.
	%FA_DATE2.	The current date . This value has 6 characters that represent the year, month, and day (yymmdd), for example, 210805.
	%FA_DATE_DAY.	The current day, for example, 05.
	%FA_DATE_MONTH.	The current month, for example, 08.
	%FA_DATE_YEAR.	The current year, for example, 2021.
	%FA_NUM.	The millisecond timestamp. If multiple files are sent within the same second, they will likely 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 ((hhmmss) using a 24-hour clock.
	%FA_TIME_HOUR.	The current hour, for example, 13.
	%FA_TIME_MINUTES.	The current minute, for example, 14.
	%FA_TIME_SECONDS.	The current second, for example, 35.
	%FA_TIME_MS.	The current millisecond, for example, 067.

Usage	Variable	Description
Modification date and time	%FA_FDATE.	Date a detected file was last modified. This value has 8 characters to represent year, month, and day (yyymmdd), for example, 20210805.
	%FA_FDATE2.	Date a detected file was last modified. This value has 6 characters to represent year, month, and day (yymmdd), for example, 210805.
	%FA_FDATE_DAY.	The day a file was last modified, for example, 05.
	%FA_FDATE_MONTH.	The month in which a file was last modified, for example, 08.
	%FA_FDATE_YEAR.	Year in which a file was last modified (yyyy), for example, 2021.
	%FA_FDATE_YEAR2.	Year in which a file was last modified (yy), for example, 21.
	%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.
	%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_NUM2.	A 5-digit number in the range of 00000..99999, for example 00345. The counter is always reset to 0 at File Agent startup and is increased by 1 on every process submission. The counter preserves its current value through a config refresh.
	%FA_NUM3.	A 9-digit number in the range of 000000000..999999999, for example 000012345. The counter is always reset to 0 at File Agent startup and is increased by 1 on every process submission. The counter preserves its current value through a config refresh.
	%FA_FTIME_SECONDS.	The second a file was last modified, for example, 35.
	%FA_FTIME_MS.	The millisecond file was last modified, for example, 067.
UNIX and Microsoft Windows only		
File name and path	%FA_EXT_FOUND.	The file extension of the file that was added, for example, .txt.
	%FA_EXT_FOUND_NP.	The file extension of the file that was added, but without the period before the file extension.
	%FA_NAME_FOUND.	The name of the file that was added, for example, myfile.
	%FA_NOT_PATH.	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.	The path of the file that was added, for example, on Microsoft Windows, C:\watch\, and on UNIX, /home/user/watch..
Microsoft Windows only		

Usage	Variable	Description
	%FA_DRIVE_FOUND.	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		
	%FA_SCHEME.	This is the object scheme when Sterling 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 the value is the object name before substitution occurred, the object name Sterling Connect:Direct File Agent detected. For more details, refer Chapter 8, “Object Stores support,” on page 27.

Microsoft Windows/UNIX Example

If you configure Process arguments as:

```
&SRCFILE=%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. &SRCFILE=/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=.
```

Chapter 6. Logging

Logging

Sterling Connect:Direct Integrated File Agent logs information to separate log files in its log subdirectory. The level of information that is written to the logs is configurable. In addition, Integrated File Agent writes entries in Connect:Direct's Statistics. Under normal circumstances, Connect:Direct Statistics will be sufficient to track File Agent operations; the log files will be needed only for troubleshooting.

The following logs are available:

CDFA.log

Contains information, warnings and error messages generated by Sterling Connect:Direct File Agent. It provides information about the files found, the rule evaluation and what action was taken. This log file is enabled by default.

CDFA_verbose.log

Contains all the above information plus debug messages. This file can grow very rapidly and is not enabled by default. To enable verbose logging, edit the log4j2.properties file and follow the instructions inside.

CDFA_stats.log

Contains only one line per file with Process submission information, including Process name and number, the detected file and the name of the Rule applied. This log file is enabled by default. Example:

```
2021-08-04 09:46:43,529 INFO  - Process Name: CDFA,  Process Number: 8,  File Name:
C:\WatchDir\test_default.txt,  Rule Name: default
2021-08-04 09:57:03,211 INFO  - Process Name: CDFADEL,  Process Number: 23,  File Name: C:\
WatchDir\test_delete.txt,  Rule Name: Delete files
```

First Failing Snapshot (snap*.txt)

Contains additional diagnostics information when Sterling Connect:Direct File Agent detects a sever error, like a Java exception. Snapshot files are generated in a snaps sub directory, which is created when needed.

cdfastart.log, cdfastop.log, cdfamonitor.log, cdfapoll.log

Contain information about the Sterling Connect:Direct server starting, stopping and monitoring Sterling Connect:Direct Integrated File Agent.

© Copyright IBM Corp. 1993, 2021

Chapter 7. Best Practices and Troubleshooting

Best Practices

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 Integrated 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 a rolling file appender in the log4j2.properties file to control logging. The log4j2.properties file configures the maximum size a log file can grow to, and how many backup log files to keep. 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 Integrated File Agent logging.

Modifying the Maximum Size of a Single Log File

1. Open the log4j2.properties file in the Sterling Connect:Direct Integrated File Agent directory.
2. Modify one or more of the following setting:

Log File	Modify This Value
CDFA.log	appender.rolling.policies.size.size=10MB
CDFA_verbose.log	appender.verbose.policies.size.size=10MB
CDFA_stats.log	appender.stats.policies.size.size=10MB

Modifying the number of Log files

1. Open the log4j2.properties file in the Sterling Connect:Direct Integrated File Agent directory.
2. Modify one or more of the following setting:

Log File	Modify This Value
CDFA.log	appender.rolling.strategy.max = 10
CDFA_verbose.log	appender.verbose.strategy.max = 10
CDFA_stats.log	appender.stats.strategy.max = 10

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.

© Copyright IBM Corp. 1993, 2021

Considerations for Watch Directory Scans

The behavior of the watched directory scans is mainly determined by the Watch file interval and File completion delay parameters in the basic configuration. See the Basic Configuration chapter for more details.

The Watch file interval specifies how often watched directories will be scanned. With a shorter interval, new or changes files can be detected more quickly. However, frequently scanning large watch directories may increase the system load.

The File completion delay specifies how long Sterling Connect:Direct File Agent will delay a new or changed file before considering it ready for processing. With a shorter delay, new or updated files will be processed more quickly. However, ensure that the delay is long enough for your applications to finish writing the files to prevent Sterling Connect:Direct File Agent from processing incomplete files.

Scanning large watch directories with thousands of files may take time and can increase the system load and resource usage. It is good practice to let the Sterling Connect:Direct Process remove or archive the file from the watch directory once it has been transferred. For example, the Sterling Connect:Direct Process could do a RUN TASK/JOB to delete the file or archive it in another directory.

Troubleshooting

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

- Set appropriate permissions for watched directories
- For z/OS, specify valid Sterling Connect:Direct server parameters in the Sterling Connect:Direct Integrated File Agent configuration
- Check that required Sterling Connect:Direct Integrated File Agent rules are enabled
- Confirm that the most specific rule is in first position
- Confirm that Processes specified in the Sterling Connect:Direct Integrated File Agent rules exist in the file system or process library.
- Correct syntax errors in Processes
- For Sterling Connect:Direct UNIX and Windows, the apiPort in the Default_Config.json is not taken into consideration. The apiPort in the default configuration is only used by Sterling Connect:Direct z/OS.

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

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

The configuration file (Default_Config.json) is missing or invalid. Review the CDFA.log files for details and run the validation tool manually.

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

- Verify that the Sterling Connect:Direct server is active.
- Check that no other application is accessing a file that Sterling Connect:Direct Integrated File Agent should detect. Sterling Connect:Direct Integrated File Agent cannot process files that are in use by other applications.

Sterling Connect:Direct Integrated 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 Integrated 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 Integrated 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.

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

Edit the Watch Directory definition and disable Monitor sub directories.

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

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

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

Sterling Connect:Direct Integrated 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 Language guide.

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

Sterling Connect:Direct Integrated 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 Integrated File Agent will detect the files.

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

Wait for Sterling Connect:Direct Integrated File Agent to restart with the new configuration before it can recognize that the rule has been disabled.

Chapter 8. Object Stores support

File Agent supports Amazon S3 or S3 compatible object stores, Azure Blob, Google Storage and IBM Cloud Object Storage. A default configuration is provided to access S3 objects using the default Amazon S3 credential mechanisms. For more details on credentials mechanisms for each of these object stores, see Credentials.

Amazon S3 default configuration

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

```
# AWS S3 provider - default
cdfa.provider.1=scheme=S3://
cdfa.provider.1=store.providerName=S3
```

S3 configuration

A set of provider properties is declared by using the following syntax: *cdfa.provider.setName=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.
cdfa.provider.2=scheme= OS3://	OS3://otherbucketname/ otherfolder	This watched directory will be linked to provider 2.
No entries for scheme X4://	X4://container/folder	This watched directory will be rejected

Additional object stores configuration

More properties can be used to fine configure a provider entry. See Stores Properties. Use the `cdfa.provider.setName=property=value` model to declare them.

Out scheme property

When Connect Direct is configured to work with a scheme 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.

When Connect Direct is configured to work with a scheme 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

© Copyright IBM Corp. 1993, 2021

Scheme	Outscheme	Discovered File	%FA_FILE_FOUND.	%FA_WATCHED_FILE_FOUND.
S3://	OS3://	S3://bucket/folder/name	OS3://bucket/folder/name	S3://bucket/folder/name

Configuration example

```
# AMZ:// scheme will use provider S3 and will generate %FA_FILE_FOUND. With scheme S3://
cdfa.provider.AMS3=store.providerName=S3
cdfa.provider.AMS3=scheme=AMZ://
cdfa.provider.AMS3=outscheme=S3://
cdfa.provider.AMS3=s3.accessKey=xxxxxxxxxxxxxxxxxxx
cdfa.provider.AMS3=s3.secretKey=xxxxxxxxxxxxxxxxxxxxxxxx

# QA:// scheme will request properties from Connect Direct initparms
# file.ioexit name=QA must exist in initparms
# Provider type and other properties are retrieved from initparms.cfg file
# This example is only valid for X86_64 Linux
cdfa.provider.QA=scheme=QA://
cdfa.provider.QA=store.configFromCD=YES

# SEC:// scheme will use provider S3
# CAs certificates will be retrieved from Secure Plus keystore only
# This example is only valid for X86_64 Linux and Windows
cdfa.provider.SECURE=store.providerName=S3
cdfa.provider.SECURE=scheme=SEC://
cdfa.provider.SECURE=store.keyStore=SP_ONLY

# BOTH:// scheme will use provider S3 (default)
# CAs certificates will be retrieved from Secure Plus keystore and next from JRE cacerts file
# S3 credentials are retrieved from the default S3 credentials chain
# This example is only valid for X86_64 Linux and Windows
cdfa.provider.MIXEDCAS=scheme=BOTH://
cdfa.provider.MIXEDCAS=store.keyStore=SP_JRE


# MICROSOFT:// scheme will use provider Azure Blob
cdfa.provider.AZURE=store.providerName=AZ
cdfa.provider.AZURE=scheme=MICROSOFT://
cdfa.provider.AZURE=az.connectionString=xxxxxxxxxxxxxxxxxx

# IBM:// scheme will use provider IBM COS
cdfa.provider.IBMCOS=store.providerName=COS
cdfa.provider.IBMCOS=scheme=IBM://
cdfa.provider.IBMCOS=cos.location=ams03

# GOOGLE:// scheme will use provider Google Storage
cdfa.provider.GOOGLE=store.providerName=GS
cdfa.provider.GOOGLE=scheme=GOOGLE://
cdfa.provider.GOOGLE=gs.credentialsPath=xxxxxxxxxxxxxxx
```

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

© Copyright IBM Corp. 1993, 2021

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: